Order Code RL31488

Regulation of Unsolicited Commercial E-Mail

Updated May 6, 2003

Angie A. Welborn
Legislative Attorney
American Law Division

Regulation of Unsolicited Commercial E-Mail

Summary

Unsolicited commercial e-mail, also known as spam, has received increased legislative attention as consumer complaints about its intrusiveness and potential for perpetrating fraud have grown. While there are no federal laws specifically aimed at restricting or preventing the transmission of spam, there are statutes at both the federal and state level that may be used to recover damages associated with the transmission of unsolicited e-mail and combat the consumer fraud sometimes associated with such messages. This report provides an overview of federal and state statutes, and relevant case law, applicable to the transmission of unsolicited commercial e-mail. A brief summary of pending federal legislation, including S. 563, S. 877, H.R. 122, and H.R. 1933, is also provided. The report will be updated as events warrant.

Contents

Regulation of Unsolicited Commercial E-Mail

Current Federal Law

There are currently no federal laws that specifically address the act of transmitting unsolicited commercial e-mail or the use of certain technologies associated with the transmission of unsolicited commercial e-mail. However, there are other federal laws that may apply to the transmission of unsolicited e-mail under certain circumstances.

Federal Computer Fraud and Abuse Statute. The federal computer fraud and abuse statute protects computers in which there is a federal interest, but it does not specifically address the transmission of unsolicited commercial e-mail.[1] The statute generally shields protected computers from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud. These provisions have been applied to the overloading of computer servers with large amounts of unsolicited e-mail, server damage resulting from the transmission of large amounts of unsolicited e-mail, and may apply to alleged interference with protected computers through the installation of "cookies"[2] and "web bugs" or invisible GIF's.[3]

Internet service providers (ISP's) have used the federal computer fraud and abuse statute to bring charges against persons who send large amounts of unsolicited e-mail to their customers. In general, the ISP's argue that large amounts of unsolicited e-mail damage their computer servers and cause them to expend resources to attempt to stop unsolicited e-mail from reaching their customers. America Online (AOL) has brought a number cases against persons who have transmitted large amounts of unsolicited e-mail through its servers and to its subscribers alleging, *inter alia,* that the processing of large amounts of unsolicited e-mail imposes significant

---

[1] 18 U.S.C. 1030. *See* CRS Report RS20830, *Computer Fraud and Abuse: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws* and CRS Report 97-1025, *Computer Fraud and Abuse: An Overview of 18 U.S.C. 1030 and Related Federal Criminal Laws.*

[2] A "cookie" is a small file stored on the computer of a person who accesses certain websites. When a person returns to that site, the cookie enables the site to identify the person accessing the site and may permit personalization of the site's content.

[3] A "web bug" or invisible GIF is a small computer program that may be installed when an e-mail message is opened. These programs call for downloading a small picture or transparent box from an outside server. Sending the requested file allows the server to acquire the IP address of the requesting computer. Once the file has been requested and the IP address obtained, the requesting computer can be counted and tracked.

costs on the company.[4] AOL has been successful on a number of these claims and has been awarded monetary damages as well as injunctive relief.

Federal Trade Commission Actions. While it does not have the authority to prohibit the transmission of all unsolicited commercial e-mail, the Federal Trade Commission (FTC) does have the authority, under the FTC Act,[5] to address deceptive sales and marketing practices on the Internet, including the use of fraudulent unsolicited commercial e-mail. The FTC monitors unsolicited commercial e-mail and compiles a database of fraudulent messages that have been forwarded by consumers.[6] On April 30, 2003, the FTC released a report by the Commission's Division of Marketing Practices review false claims appearing in unsolicited commercial e-mail. The Commission found that approximately 66% of the unsolicited commercial e-mail analyzed contained false information in either the "From" line, "Subject" line, or in the text of the message.[7]

Prior to the issuance of the report, the FTC brought its first case involving spam with deceptive subject lines. On April 15, 2003, the Commission asked a federal judge to halt "an allegedly illegal spam operation that uses deceptively bland subject lines, false return addresses, and empty 'reply-to' links to expose unsuspecting consumers, including children, to sexually explicit material."[8] The Commission alleges that Brian Westby used the deceptive spam to direct consumers to an adult web site. The FTC asked the court to issue a temporary injunction, pending trial. The court granted a preliminary injunction on April 22, 2003.[9]

The FTC has brought a number of other actions against consumer fraud schemes that involve unsolicited commercial e-mail. Many cases involve alleged pyramid schemes, often disguised as work at home opportunities, that are perpetrated through the use of unsolicited e-mail. In *FTC v. Martinelli*[10], the FTC targeted a company soliciting recruits for a work at home opportunity that would allegedly earn

---

[4] *See e.g.,* America Online v. National Healthcare Discount, 174 F. Supp.2d 890 (ND Iowa, 2001); America Online v. IMS, 1998 U.S. Dist. LEXIS 20645 (ED Va., 1998); America Online v. LCGM, 46 F. Supp.2d 444 (ED Va., 1998). For more information on American Online's efforts to prevent the transmission of unsolicited e-mail, see [http://legal.web.aol.com/decisions/dljunk/].

[5] 15 U.S.C. 45.

[6] The FTC's actions with regard to unsolicited commercial e-mail were outlined in congressional testimony given by the Bureau of Consumer Protection on April 26, 2001. This testimony can be found at [http://www.ftc.gov/os/2001/04/unsolicommemail.htm].

[7] A copy of the report can be found at [http://www.ftc.gov/reports/spam/030429spamreport.pdf].

[8] *See* FTC Press Release, *FTC Asks Court to Block Deceptive Spam Operation*, April 17, 2003. [http://www.ftc.gov/opa/2003/04/westby.htm]. A copy of the complaint, *Federal Trade Commissio v. Brian D. Westby*, Case No. 03C-2540, United States District Court for the Northern District of Illinois, Eastern Division, can be found at [http://www.ftc.gov/os/2003/04/brianwestbycmp.pdf].

[9] *See* [http://www.ftc.gov/os/2003/04/brianwestbyord.pdf].

[10] FTC v. Martinelli, No. 399 CV 1272 (D. Conn. filed July 7, 1999).

participants $13.50 per hour. The e-mail messages sent claimed that if the recipient sent a registration fee of over $28 they would receive everything they needed for the job. In fact, what participants received was a kit that instructed them to place ads or send messages similar to the ones to which they responded in an attempt to recruit new participants. Their earnings would be based on the number of people they were able to recruit. In its complaint, the FTC alleged that the defendants misrepresented to consumers the salary that could be earned; failed to disclose that this was a pyramid scheme; and provided others the means to commit the deceptive acts. A court entered a stipulated final order banning the defendants from engaging in similar schemes and requiring them to pay $72,000 in consumer redress.

The Commission has also brought a number of cases against alleged credit repair scams that use unsolicited e-mail to advertise their services. These e-mail messages generally encourage consumers to purchase information instructing them how to acquire a new credit identity by applying for federally-issued identification numbers and using these numbers in place of social security numbers to build a new credit file. The messages fail to mention that using a false identification number to apply for credit is a felony. Both the FTC and the Department of Justice have pursued actions against these types of deceptive solicitations.[11]

Other recent cases pursued under the FTC Act address chain letters sent via e-mail that encourage recipients to send cash to names posted on a list in order to have their names added to the list and offer "reports" that instruct others on how to send unsolicited e-mail for a profit.[12] Other scams perpetrated through the use of unsolicited e-mail include fraudulent credit repair offers, deceptive health and diet offers, and fraudulent vacation offers.[13]

State Laws Regarding Unsolicited Commercial E-Mail

State Statutes. Approximately twenty-nine states have enacted legislation placing certain restrictions on the transmission of unsolicited commercial e-mail, though none completely prohibits the act of transmitting such messages.[14] Nevada became the first state to enact such legislation in 1997.[15] Under Nevada law, it is unlawful to send an unsolicited commercial e-mail message unless it is labeled or otherwise identifiable as an advertisement. The message must include the sender's

---

[11] *See e.g.,* FTC v. Cliff Cross and d/b/a Build-It-Fast, Civ. No. M099CA018 (W.D. Tex. filed Feb. 1, 1999); FTC v. Ralph Lewis Mitchell, Jr., No. CV 99-984 TJH (C.D. Cal. filed Jan. 29, 1999); U.S. v. David Story, d/b/a Network Publications, 3-99CV0968-L (N.D. Tex. filed April 29, 1999).

[12] A summary of these cases, as well as copies of the complaints and settlement documents can be found at [http://www.ftc.gov/opa/2002/02/eileenspam1.htm].

[13] The FTC has compiled a list of the twelve most common e-mail scams. For information see [http://www.ftc.gov/opa/1998/9807/dozen.htm].

[14] For a complete list of state statutes see [http://www.spamlaws.com/state/summary.html].

[15] N.R.S. §§ 41.705 - 41.735, added by Nevada Acts 1997 ch. 341, Senate Bill 13. The statute was subsequently amended to criminalize certain acts related to the transmission of electronic mail in 2001. *See* Nevada Acts 2001 ch. 274, Senate Bill 48.

name, physical address, and e-mail address, as well as instructions for opting out of the sender's distribution list. The law also prohibits the use of false routing information and the distribution of software designed to create false routing information. A later amendment to the original statute made it unlawful to send unsolicited commercial e-mail with the intent to disrupt the normal operation or use of a computer, Internet site, or e-mail address.

Much of the legislation enacted subsequent to the Nevada statute prohibits the transmission of unsolicited e-mail containing false or misleading header or routing information.[16] States have also enacted legislation requiring that unsolicited e-mail contain opt-out information or provide information about the sender, including a physical address or telephone number.[17] In addition, some state statutes include specific provisions relating to the transmission of adult oriented advertisements via unsolicited e-mail, requiring these messages to be labeled as such.[18] While not a direct regulation of unsolicited e-mail, other states have enacted statutes that criminalize the misuse of e-mail with the intent to harass, or the transmission of "lewd, lascivious, or obscene material."[19]

Legal Challenges to State Statutes. Legal challenges have been brought against at least two state statutes - California and Washington. The challenges alleged that the state statutes placed an undue burden on interstate commerce in violation of the dormant commerce clause of the United States Constitution. In each case, the court upheld the statute, finding that the local benefits of the Act outweighed the burden placed on those sending the unsolicited messages via e-mail.[20]

---

[16] Arkansas, Ark. Code § 5-41-205; Colorado, CRS § 6-2.5-103(1), (2), and (3); Connecticut, Conn. Stat. § 53-451(b); Delaware, Del. Code § 937; Idaho, Idaho Code § 48-603E(3); Illinois, 815 ILCS 511/10(a); Iowa, Iowa Code § 714E.1; Kansas, not yet codified, *see* Senate Bill 467 (2002); Louisiana, La. R. S. § 73.6(B); Maryland, not yet codified, *see* Senate Bill 538 and House Bill 915 (2002), effective October 1, 2002; Minnesota, not yet codified, *see* Minnesota Laws 2002, ch. 395, effective March 2003; North Carolina, NC Stat. § 14-458(a)(6); Oklahoma, Ok. Stat. Title 15 § 776.1; Rhode Island, RI Stat. § 11-52-4.1(7); South Dakota, not yet codified, *see* Senate Bill 183 (2002); Utah, Utah Code § 13-36-103; Virginia, Va. Code § 18.2-152.4(7); Washington, RCW § 19.190.020; and West Virginia, W. Va. Code § 46A-6G-2.

[17] California, Cal. Bus. & Prof. Code § 17538.4; Colorado, CRS § 6-2.5-103(5); Iowa, Iowa Code § 714E.1(2)(d); Kansas, not yet codified, *see* Senate Bill 467 (2002); Minnesota, not yet codified, *see* Minnesota Laws 2002, ch. 395, effective March 2003; Missouri, R.S. Mo. § 407.1310.1.; Rhode Island, RI Stat. § 6-47-2; Tennessee, Tenn. Code § 47-18-2501(b); and Utah, Utah Code § 13-36-103.

[18] California, Cal. Bus. & Prof. Code § 17538.4(g); Kansas, not yet codified, *see* Senate Bill 467 (2002); Minnesota, not yet codified, *see* Minnesota Laws 2002, ch. 395, effective March 2003; New Mexico, not yet codified, *see* Senate Bill 699, approved April 3, 2003; Pennsylvania, Penn. Stat. Title 18 § 5903; Tennessee, Tenn. Code § 47-18-2501(e); Utah, Utah Code § 13-36-103; and Wisconsin, Wis. Stat. § 944.25.

[19] *See e.g.*, 27 Md. Code Ann. §§ 555C(1)(B) and (C).

[20] State v. Heckel, 24 P.3d 404 (S. Ct. Wash. 2001); Ferguson v. Friendfinders, Inc., 115 Cal. Rptr.2d 258 (2002).

In *State of Washington v. Heckel*, the defendant, a resident of another state, challenged Washington's restriction on unsolicited commercial e-mail alleging that the statute placed an unconstitutional burden on interstate commerce.[21] The defendant was an Oregon resident who was charged with violating a state law that prohibits the use of false or misleading routing information and false or misleading subject lines in unsolicited commercial e-mail.[22] The Washington law applies if a message is sent from within Washington, if the sender knows that the recipient is a Washington resident, or if the sender is able to confirm the residency of the recipient by contacting the registrant of the internet domain name contained in the recipient's e-mail address.[23]

The defendant argued that the Washington statute violated the dormant commerce clause of the Constitution[24] by discriminating against persons doing business outside the state. The court rejected this argument finding that the statute "applies evenhandedly to in-state and out-of-state spammers" and would be equally enforceable against a Washington resident engaging in the same practices.[25] The court then articulated the balancing test that must be applied when considering state statutes that may burden interstate commerce by stating that "where the statute regulates evenhandedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive relative to the putative local benefits."[26] The court determined that the statute's "local benefits surpass any alleged burden on interstate commerce," thus rejecting the defendant's challenge and upholding the statute.[27]

In *Ferguson v. Friendfinders, Inc.*, a California resident filed suit against advertisers who were sending unsolicited commercial e-mail in violation of the California Business and Professional Code § 17538.4.[28] The statute applies to e-mail that is sent to "a California resident via an electronic mail service provider's service or equipment located in this state."[29] A lower court dismissed the suit, finding that the provisions in question violated the dormant commerce clause of the

---

[21] 24 P.3d 404 (S. Ct. Wash. 2001).

[22] RCW § 19.190.020.

[23] *Id.*

[24] The dormant commerce clause is "the principle that the states impermissibly intrude on this federal power [to regulate interstate commerce] when they enact laws that unduly burden interstate commerce." 24 P.3d at 409.

[25] 24 P.3d at 409.

[26] *Id* (citations omitted).

[27] *Id.*

[28] 115 Cal. Rptr.2d 258 (2002). Section 17538.4 requires unsolicited commercial e-mail messages to include opt-out instructions and contact information. The statute also requires that certain messages be labeled with the letters "ADV" or "ADV:ADLT" at the beginning of the subject line.

[29] *Cal. Bus. & Prof. Code* § 17538.4(d).

Constitution.[30] The appellate court reversed the lower court's opinion and upheld the statute.

On appeal, the defendants argued that the statute, "when viewed in the context of Internet reality," attempted to regulate beyond California's borders.[31] The court rejected this argument citing the language of the statute and its express application only to e-mail that is sent to a California resident by means of an electronic mail service provider who has equipment in the state.[32] Additionally, the court rejected the argument that the statute discriminated against interstate commerce, and went on to apply the balancing test applied in *Heckel*, discussed above. The court found that the state had "a substantial legitimate interest in protecting its citizens from the harmful effects of deceptive UCE [unsolicited commercial e-mail] and that [the statute] furthered that important interest."[33] Thus, the court determined that the burdens imposed on interstate commerce did not outweigh the benefits of the statute.[34]

Federal Legislation

Several pieces of legislation addressing unsolicited commercial e-mail have been introduced in recent sessions of Congress, but none has passed both houses.[35]

107th Congress

Several bills related to the transmission of unsolicited commercial e-mail were introduced during the 107th Congress. In general, the proposals sought to place restrictions on the transmission of unsolicited commercial e-mail or require unsolicited commercial messages to be labeled, but did not seek to ban on such transmissions outright unless the requirements were not met. Many of the proposals would have also required unsolicited e-mail to include opt-out information. None of the legislation discussed below was enacted.

H.R. 95, the **Unsolicited Commercial Electronic Mail Act of 2001**, would have made it unlawful to send to a protected computer unsolicited electronic mail that includes false or inaccurate header information.[36] The bill would have also

---

[30] 115 Cal. Rptr.2d at 260.

[31] *Id* at 263.

[32] *Id* at 264.

[33] *Id* at 268.

[34] *Id* at 269.

[35] For general information concerning unsolicited e-mail and legislation that has been introduced, see CRS Report RS20037, *"Junk E-mail": An Overview of Issues and Legislation Concerning Unsolicited Commercial Electronic Mail ("Spam").*

[36] H.R. 95, 107th Cong., Sec. 4.

required all unsolicited e-mail to provide the name, physical address and return e-mail address of the sender, as well as opt-out instructions.[37]

H.R. 718, the **Unsolicited Commercial Electronic Mail Act of 2001**, was referred to the House Energy and Commerce Committee and the House Judiciary Committee. Both committees held mark-ups of the bill and reported substantially different versions. The version reported from the House Energy and Commerce Committee would have, *inter alia*, amended the federal computer fraud and abuse statute to prohibit the transmission of unsolicited commercial e-mail containing false identifying information to any protected computer[38] in the United States.[39] Additionally, it would have made it unlawful to initiate the transmission of a commercial e-mail message to any person within the United States unless such message contains a valid return e-mail address, conspicuously displayed, to which a recipient may opt-out.

The version reported out of the House Judiciary Committee, entitled the **Anti-Spamming Act**, would have also amended the federal computer fraud and abuse statute to address the transmission of unsolicited commercial e-mail to protected computers, but only if 10 or more messages were being transmitted in one or more transactions.[40] The bill would have also required the Attorney General, with regard to any e-mail, not just unsolicited commercial e-mail, to prescribe marks or notices to be included in messages that contain a sexually oriented advertisement. Failure to include the prescribed marks could result in a fine or imprisonment.

H.R. 1017, entitled the **Anti-Spamming Act of 2001**, would have amended the federal computer fraud and abuse statute to make it unlawful to intentionally initiate the "transmission of a bulk unsolicited electronic mail message to a protected computer with knowledge that such message falsifies an Internet domain, header information, date or time stamp, originating e-mail address or other identifier."[41] It would have also been unlawful to sell or distribute computer programs that are designed or produced for the purpose of falsifying such information and sending such messages.[42]

---

[37] H.R. 95, 107th Cong., Sec. 5(a).

[38] The phrase "protected computer" is defined in the federal computer fraud and abuse statute as a computer "exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or which is used in interstate or foreign commerce or communication." 18 U.S.C. 1030(e)(2).

[39] For the full text of the Energy and Commerce Committee's amendment, see H.Rept. 107-41, Part I.

[40] For the full text of the House Judiciary Committee's amendment, see H.Rept. 107-41, Part II.

[41] H.R. 1017, 107th Cong., Sec. 2.

[42] *Id.*

The **Netizens Protection Act of 2001, H.R. 3146**, would have required all unsolicited e-mail messages to provide the name, physical address, and e-mail address of the person sending the message and to provide a method by which the recipient of the message may request that no further messages be sent.[43] The bill would have also prohibited false or misleading subject lines in bulk e-mail transmissions.[44]

The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2001, S. 630, would have, *inter alia*, made it unlawful to send to a protected computer unsolicited commercial e-mail containing false or misleading header information.[45] It would have also been unlawful to transmit messages with a subject heading that is likely to mislead the recipient about "a material fact regarding the contents or subject matter of the message."[46] In addition, the bill would have required the inclusion of a return address and opt-out information in commercial e-mail sent to a protected computer.[47]

The Senate Committee on Commerce, Science and Transportation held a full committee consideration and mark up of the legislation on May 17, 2002. The Committee ordered the bill to be reported favorably with an amendment in the nature of a substitute. The Committee's amendment was similar to the original bill, though it would have also prohibited the transmission of unsolicited e-mail to e-mail addresses that were "harvested" from web sites or other internet services using automated means.

Other legislation would have prohibited the use of the text, graphic, or image messaging systems of wireless telephone systems to transmit unsolicited commercial messages;[48] and prohibited the transmission of sexually oriented advertisements to minors if such messages do not contain prescribed markings developed by the National Institute of Standards and Technology.[49] While not specifically aimed at restricting unsolicited commercial e-mail, additional legislation would have required schools and libraries receiving universal service assistance to block access to Internet services that enable users to access the World Wide Web and transfer electronic mail in an anonymous manner.[50]

108th Congress

To date four bills addressing unsolicited commercial e-mail, or spam, have been introduced during the 108th Congress.

---

[43] H.R. 3146, 107th Cong., Sec. 2(a)(1) and (2).

[44] H.R. 3146, 107th Cong., Sec. 2(a)(3).

[45] S. 630, 107th Cong., Sec. 4.

[46] S. 630, 107th Cong., Sec. 5(a)(2).

[47] S. 630, 107th Cong., Sec. 5(a)(3) - (5).

[48] H.R. 113, 107th Cong.

[49] H.R. 2472, 107th Cong.

[50] H.R. 1846, 107th Cong.

S. 563, the **Computer Owners' Bill of Rights**, would, *inter alia*, require the Federal Trade Commission to establish a registry of persons who do not wish to receive "unsolicited marketing e-mail."[51] The registry would be made available to the public, and transmission of unsolicited marketing e-mail to those on the list would be prohibited. Exceptions to the general prohibition could be authorized by the FTC under regulations promulgated pursuant to the legislation if enacted. Violations of the prohibition set forth would be subject to a civil penalty of up to $10,000.

S. 877, the **Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003**, or **CAN-SPAM Act of 2003**, would create criminal penalties for "the transmission, to a protected computer in the United States[52], of an unsolicited commercial electronic mail message, with knowledge and intent that the message contains or is accompanied by header information that is materially false or materially misleading."[53] Violations would be subject to a fine or imprisonment of up to 1 year or both.

The bill would also prohibit the transmission of a commercial electronic mail message with a subject heading that is likely to mislead a recipient about a material fact regarding the contents or subject of the message; require unsolicited commercial electronic mail to contain a functioning return electronic mail address that could be by a recipient to submit a request not to receive future messages; prohibit the transmission of unsolicited commercial electronic mail after the recipient has requested not to receive any additional transmissions; require the inclusion of a clear and conspicuous identification that the message is an advertisement or solicitation, an opportunity to opt-out, and a valid physical address of the sender; and prohibit the transmission of unsolicited e-mail to e-mail addresses that were "harvested" from web sites or other internet services using automated means.[54]

The Act would be enforced by the Federal Trade Commission and other relevant agencies.[55] State attorneys general would be able to bring civil actions on behalf of the residents of their state in an appropriate United States district court.[56] Damages in an amount equal to the greater of the actual monetary loss suffered by such residents or statutory damages of up to $500,000 could be awarded.[57] The bill also

---

[51] S. 563, 108th Cong., Sec. 5.

[52] *See supra* n38.

[53] S. 877, 108th Cong., Sec. 4.

[54] S. 877, 108th Cong., Sec. 5.

[55] S. 877, 108th Cong., Sec. 6.

[56] S. 877, 108th Cong., Sec. 6(e).

[57] S. 877, 108th Cong., Sec. 6(e)(2). The actual amount of statutory damages would be determined by multiplying the number of willful, knowing, or negligent violations by an amount, at the discretion of the court, of up to $10 (with each separately addressed unlawful message received by such residents treated as a separate violation). If the court determines that the defendant committed the violation willfully and knowingly, the court could increase

(continued...)

authorizes actions by any provider of internet access service to be brought in any district court of the United States with jurisdiction over the defendant.[58] An internet service provider could recover damages similar to those available in actions brought by states.

H.R. 122, the **Wireless Telephone Spam Protection Act** would prohibit the use of the text, graphic, or image messaging systems of wireless telephone systems to transmit unsolicited commercial messages.

H.R. 1933, the **Restrict and Eliminate the Delivery of Unsolicited Commercial Electronic Mail or Spam Act of 2003**, or the **REDUCE Spam Act of 2003**, would amend title 18 of the United States Code to create criminal penalties for the "transmission of any unsolicited commercial electronic mail message, with knowledge and intent that the message contains or is accompanied by header information that is false or materially misleading."[59] Violators could be subject to a fine or imprisonment for up to 1 year or both.

The bill would also prohibit the transmission of unsolicited commercial e-mail unless certain requirements are met. The transmission of unsolicited commercial e-mail would be prohibited unless the subject line of such e-mail includes "an identification that complies with the standards adopted by the Internet Engineering Task Force for identification of unsolicited commercial electronic mail messages; or in the case of the absence of such standards, 'ADV:' as the first four characters."[60] Senders would also be required to establish a valid sender-operated return address where the recipient could notify the sender not to send any further messages.[61] It would be unlawful for a person to send any unsolicited electronic mail to a recipient after the recipient has requested not to receive any further messages from that sender.[62] It would also be unlawful for any person to transmit any unsolicited e-mail that contains a subject heading "that such person knows, or reasonably should know, is likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents of subject matter of the message."[63]

The Act would be enforced by the Federal Trade Commission, which would be required to initiate a rulemaking proceeding within 30 days enactment to address the enforcement of the Act.[64] The rulemaking would also be required to address procedures for submitting a complaint to the Commission concerning violations; civil

---

[57] (...continued)
the limit on the total damages awarded from $500,000 to $1,500,000.

[58] S. 877, 108th Cong., Sec. 6(f).

[59] H.R. 1933, 108th Cong., Sec. 3.

[60] H.R. 1933, 108th Cong., Sec. 4(a).

[61] H.R. 1933, 108th Cong., Sec. 4(b)(1).

[62] H.R. 1933, 108th Cong., Sec. 4(b)(3).

[63] H.R. 1933, 108th Cong., Sec. 4(c)(2).

[64] H.R. 1933, 108th Cong., Sec. 5(a) and (b).

penalties for violations; procedures for granting "a reward of not less than 20 percent of the total civil penalty imposed to the first person that identifies the person in violation of [the Act]; and supplies information that leads to the successful collection of a civil penalty by the Commission;" and civil penalties for knowingly submitting a false complaint to the Commssion.[65]

Recipients of an unsolicited commercial e-mail messages, or Internet services providers, adversely affected by violations of the Act would be able to bring private rights of action in any district court of the United States with jurisdiction over the defendant.[66] Actual damages or statutory damages of up to $10 per violation could be awarded.[67]

---

[65] H.R. 1933, 108th Cong., Sec. 5(b)(1) - (4).

[66] H.R. 1933, 108th Cong., Sec. 6(a).

[67] H.R. 1933, 108th Cong., Sec. 6(a)(2) and (b).