Order Code RL31488

Regulation of Unsolicited Commercial E-Mail

Updated July 2, 2004

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. On December 16, 2003, the President signed the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 (P.L. 108-187). This is the first federal law specifically aimed at regulating unsolicited commercial e-mail. This report provides an overview of the new federal law, as well as other applicable federal and state statutes, and relevant case law applicable to the transmission of unsolicited commercial e-mail. A brief summary of additional pending federal legislation, including S. 563, S. 1052, S. 1231, S. 1293, S. 1327, H.R. 122, H.R. 1933, H.R. 2214, and H.R. 2515, is also provided. The report will be updated as events warrant.

Contents

Regulation of Unsolicited Commercial E-Mail

CAN-SPAM Act of 2003

On December 16, 2003, the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 was signed by the President.[1] This is the first federal law specifically aimed at regulating unsolicited commercial e-mail. It became effective January 1, 2004. Each major provision of the act is discussed below.

Prohibition on Predatory and Abusive Commercial E-Mail. The CAN-SPAM Act amends Title 18 of the United States Code to add a new section entitled "Fraud and related activity in connection with electronic mail."[2] Under this new section it is unlawful for a person to knowingly (1) access a protected computer without authorization, and intentionally initiate the transmission of multiple commercial electronic mail messages from or through such computer; (2) use a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages; (3) materially falsify header information in multiple commercial electronic mail messages and intentionally initiate the transmission of such messages; (4) register, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiate the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names; or (5) falsely represent oneself to be the registrant or the legitimate successor in interest to the registrant of five or more Internet Protocol addresses, and intentionally initiate the transmission of multiple commercial electronic mail messages from such addresses.

Criminal penalties for violations range from one to five years imprisonment, a fine, or both. A term of imprisonment of up to five years may be imposed if "(A) the offense is committed in furtherance of any felony under the laws of the United States or of any State; or (B) the defendant has previously been convicted under this section or section 1030 [of Title 18], or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system."[3] A three year term may be imposed if the offense is an offense under subsection (1) as noted above; an offense under subsection (4) as noted above and involved 20 or more falsified electronic mail or online user account

---

[1] P.L. 108-187.

[2] P.L. 108-187, Sec. 4(a).

[3] *Id*.

registrations, or 10 or more falsified domain name registrations; the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, or 250,000 during any one-year period; the offense caused loss to one or more persons aggregating $5,000 or more in value during any one-year period; as a result of the offense any individual committing the offense obtained anything of value aggregating $5,000 or more during any one-year period; or the offense was undertaken by the defendant in concert with three or more other persons with respect to whom the defendant occupied a position of organizer or leader. A term of imprisonment of up to one year may be imposed in any other case. Persons convicted of an offense under the new section will also be ordered to forfeit to the United States any property, real or personal, constituting or traceable to gross proceeds obtained from the offense; and any equipment, software, or other technology used or intended to be used to commit or to facilitate the commission of the offense.

Other Protections for Users of Commercial E-Mail. In addition to the new criminal provisions discussed above, the CAN-SPAM Act includes a number of provisions aimed at protecting users of commercial e-mail.[4] The act prohibits false or misleading transmission information in commercial e-mail, and prohibits the use of deceptive subject headings.[5] Commercial electronic mail must also include a clear and conspicuous identification that the message is an advertisement or solicitation; clear and conspicuous notice of the opportunity to decline to receive further commercial e-mail from the sender; and a valid physical postal address of the sender.[6]

The act prohibits the transmission of commercial electronic mail that does not contain a functioning return e-mail address or other Internet-based mechanism that a recipient may use to submit a request not to receive future commercial e-mail from the sender.[7] The e-mail address or mechanism provided must be capable of receiving messages for no less than 30 days after the transmission of the original message. After a recipient transmits to the sender a request not to receive future commercial electronic mail messages, it is unlawful for the sender to further transmit commercial e-mail to the recipient more than 10 business days after receiving such request.[8]

For any violation of the provisions discussed above, an aggravated violation is committed if the transmission involved electronic mail addresses that were "harvested" using an automated means from an Internet website or proprietary online service, or if the address of the recipient was obtained using an automated means that

---

[4] P.L. 108-187, Sec. 5(a).

[5] *Id* at Sec. 5(a)(1) and (2).

[6] *Id* at Sec. 5(a)(5).

[7] *Id* at Sec. 5(a)(3).

[8] *Id* at Sec. 5(a)(4).

generates possible e-mail addresses by combining names, letters, or numbers into numerous permutations.[9]

Additionally, the act requires that messages containing sexually oriented material include warning labels as to the content of the message.[10]

Enforcement. Generally, violations of the CAN-SPAM Act will be enforced by the Federal Trade Commission as unfair or deceptive acts or practices under the Federal Trade Commission Act.[11] Other agencies with jurisdiction over specific entities will have similar enforcement authority.

State attorneys general also have authority to bring civil actions for violations of certain provisions in the act.[12] Actions may be brought to recover actual monetary damages suffered by the residents of the state or statutory damages. The state must serve prior written notice of any action upon the Federal Trade Commission or other appropriate agency. The FTC (or other agency with jurisdiction over the entities in question) may intervene in the action, and upon intervention, be heard on all matters involving the action, remove the action to the appropriate United States District Court, and file petitions for appeal. State attorneys general may not bring a civil action against a particular defendant if the FTC (or another agency) has instituted a civil or administrative action against the same defendant.

Internet service providers are also allowed to bring civil actions for certain violations to enjoin further violation, or to recover damages.[13] The act does not provide for actions by private individuals.

Preemption of State Law. Generally, the act preempts any state law that "expressly regulates the use of electronic mail to send commercial messages."[14] State laws that prohibit falsity or deception in any portion of a commercial e-mail messages are not preempted. Also excluded from preemption are state laws that are not specific to e-mail, including trespass, contract, or tort law; or other state laws that relate to acts of fraud or computer crime.[15]

---

[9] *Id* at Sec. 5(b)(1).

[10] *Id* at Sec. 5(d). The Federal Trade Commission issued a Final Rule implementing this provision on April 19, 2004. The rule requires the sender of sexually oriented e-mail messages to include the phrase "SEXUALLY-EXPLICIT" at the beginning of the message's subject line. Under the new rule, the sender must also exclude any sexually oriented material from the subject line. The new rule will be codified at 16 CFR 361.1. 69 FR 21024 (April 19, 2004).

[11] *Id* at Sec. 7(a). *See* 15 U.S.C. 57a.

[12] *Id* at Sec. 7(f).

[13] *Id* at Sec. 7(g).

[14] *Id* at Sec. 8(b)(1). See *infra* for a discussion of state laws.

[15] *Id* at Sec. 8(b)(2).

Do-Not-E-Mail Registry. The CAN-SPAM Act did not create a do-not-e-mail registry similar to the Federal Trade Commission's do-not-call registry.[16] However, the act does direct the FTC to transmit to the Senate Commerce and House Energy and Commerce Committees a report that (1) sets forth a plan and a timetable for establishing a nationwide marketing Do-Not-E-Mail registry; (2) includes an explanation of any practical, technical, security, privacy, enforceability, or other concerns that the Commission has regarding such a registry; and (3) includes an explanation of how the registry would be applied with respect to children with e-mail accounts.[17] The report must be transmitted within six months of the date of enactment of the act. The act also gives the Commission the authority to establish and implement the plan set forth in the report.[18] Such implementation could take place no earlier than nine months after the date of enactment of the act.

Acting upon Congress' directive in the CAN-SPAM Act, the FTC released a report entitled *National Do Not Email Registry: A Report to Congress* on June 15, 2004.[19] In the report, the Commission concluded that "without a system in place to authenticate the origin of e-mail messages, [a National Do Not Email Registry] would fail to reduce the burden of spam and may even increase the amount of spam received by consumers."[20] The Commission found, based upon input from various sources, that "spammers would most likely use a Registry as a mechanism for verifying the validity of email addresses and, without authentication, the Commission would be largely powerless to identify those responsible for misusing the Registry."[21] Rather than proposing a plan to implement a National Do Not Email Registry, the Commission proposed "a program to encourage the widespread adoption of email authentication standards that would help law enforcement and ISPs better identify spammers."[22] If, after the development of an authentication system, spam continued to be a problem, and if technological developments eliminated the security and privacy risks associated with a Registry, the Commission stated that it would consider proposing the creation of a National Do Not Email Registry.[23]

Other Provisions. The act directs the FTC to submit three additional reports. The first, to be submitted to the Senate Commerce and House Energy and Commerce Committees within nine months after the date of enactment, must set forth a system for rewarding those who supply information about violations of the act, including procedures for the Commission to grant rewards to the first person that identifies a

---

[16] For more information on the national do-not-call registry, see CRS Report RL31642, *Regulation of the Telemarketing Industry: State and National Do-Not-Call Registries*.

[17] *Id* at Sec. 9(a).

[18] *Id* at Sec. 9(b).

[19] A copy of the report can be found at [http://www.ftc.gov/reports/dneregistry/report.pdf].

[20] Federal Trade Commission, *National Do Not Email Registry: A Report to Congress*, p. i (June 15, 2004).

[21] *Id*.

[22] *Id* at ii.

[23] *Id*.

violator and supplies information that leads to the successful collection of a civil penalty by the Commission.[24] The report must also include procedures to minimize the burden of submitting a complaint to the Commission concerning violations of the act, including procedures to allow for electronic submission. A second report, to be submitted within 18 months after the date of enactment of the act, must set forth a plan for requiring commercial e-mail to be "identifiable from its subject line, by means of compliance with Internet Engineering Task Force Standards, the use of the characters 'ADV' in the subject line, or other comparable identifier, or an explanation of any concerns the Commission has that cause the Commission to recommend against the plan."[25] The final report, to be submitted no later than 24 months after the date of enactment, shall provide "a detailed analysis of the effectiveness and enforcement of the provisions of the act and the need (if any) for the Congress to modify such provisions."[26]

The act also directs the Federal Communications Commission to promulgate regulations, within 270 days of the enactment of the act, to protect consumers from unwanted mobile service commercial messages.[27]

Other Federal Laws

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.[28] 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"[29] and "web bugs" or invisible GIF's.[30]

---

[24] *Id* at Sec. 11(1).

[25] *Id* at Sec. 11(2).

[26] *Id* at Sec. 10(a).

[27] *Id* at Sec. 14(b). For more information, see CRS Report RL31636, *Wireless Privacy: Availability of Location Information for Telemarketing*.

[28] 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*.

[29] 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.

[30] 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.

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 costs on the company.[31] 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. Prior to the enactment of the CAN-SPAM Act, the Federal Trade Commission did not have any specific authority with respect to commercial e-mail. However, under the FTC Act, it did have the authority to address deceptive sales and marketing practices on the Internet, including the use of fraudulent commercial e-mail.

Over the past several years, the FTC has monitored unsolicited commercial e-mail and compiled a database of fraudulent messages that were forwarded by consumers.[32] 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.[33]

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."[34] The Commission alleges that Brian Westby used the deceptive spam to direct consumers to an adult

---

[31] *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/].

[32] 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].

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

[34] *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 Commission 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].

website. The FTC asked the court to issue a temporary injunction, pending trial. The court granted a preliminary injunction on April 22, 2003.[35]

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*[36], the FTC targeted a company soliciting recruits for a work at home opportunity that would allegedly earn 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.[37]

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.[38] Other scams perpetrated through the use of unsolicited e-mail include fraudulent credit repair offers, deceptive health and diet offers, and fraudulent vacation offers.[39]

---

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

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

[37] *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).

[38] 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].

[39] The FTC has compiled a list of the twelve most common e-mail scams. For information see [http://www.ftc.gov/bcp/conline/pubs/alerts/doznalrt.pdf].

State Laws Regarding Unsolicited Commercial E-Mail

As noted above, the CAN-SPAM Act preempts state laws that expressly regulate the use of electronic mail to send commercial messages.[40] The act became effective on January 1, 2004, and as such, many of the state laws discussed below are likely preempted.

State Statutes. To date, at least thirty-six states have enacted legislation placing certain restrictions on the transmission of unsolicited commercial e-mail.[41] Nevada became the first state to enact such legislation in 1997.[42] 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 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.[43] 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.[44] In addition, some state statutes include specific provisions relating to the transmission of adult oriented advertisements via

---

[40] P.L. 108-187, Sec. 8(b)(1).

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

[42] 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.

[43] Arkansas, Ark. Code § 5-41-205; Arizona, not yet codified, *see* S.B. 1280, approved May 16, 2003; 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); Indiana, not yet codified, House Bill 1083, approved April 17, 2003; Iowa, Iowa Code § 714E.1; Kansas, not yet codified, *see* Senate Bill 467 (2002); Louisiana, La. R. S. § 73.6(B); Maryland, Md. Commercial Law Code § 14-3001 *et seq.*; Minnesota, Minn. Stat. § 395F.694, sub. 2; 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.

[44] 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, Minn. Stat. § 395F.694, sub. 4; Missouri, R.S. Mo. § 407.1310.1.; North Dakota, N.D. Cent. Code § 51-27-05; Rhode Island, RI Stat. § 6-47-2; Tennessee, Tenn. Code § 47-18-2501(b); and Utah, Utah Code § 13-36-103.

unsolicited e-mail, requiring these messages to be labeled as such.[45] 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."[46]

Virginia recently became the first state to make the transmission of unsolicited bulk e-mail a felony under certain circumstances.[47] A person is guilty of a Class 6 felony under the Virginia law if he or she used a computer or computer network with the intent to falsify or forge electronic mail transmission information or other routing information; and the volume of e-mail transmitted exceeded 10,000 attempted recipients in any 24-hour period, 100,000 attempted recipients in any 30-day time period, or one million attempted recipients in any one-year time period, or the revenue generated from the specific e-mail transmission exceeded $1,000, or the total revenue generated from all such e-mail transmitted to any e-mail service provider exceeded $50,000. In Virginia, a Class 6 felony carries a prison term of up to five years.[48]

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.[49]

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.[50] 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.[51] The Washington law applies if a message is sent from within Washington, if the sender knows that the recipient is a

---

[45] Alaska, not yet codified, *see* H.B. 82, approved May 3, 2003, effective July 30, 2003; Arkansas, not yet codified, *see* Act 1019 of 2003, approved April 2, 2003; California, Cal. Bus. & Prof. Code § 17538.4(g); Kansas, not yet codified, *see* Senate Bill 467 (2002); Maine, not yet codified, *see* H.B. 210, approved May 27, 2003; Minnesota, Minn. Stat. § 325F.694, sub. 3; New Mexico, not yet codified, *see* Senate Bill 699, approved April 3, 2003; North Dakota, N.D. Cent. Code 51-27-04; 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.

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

[47] Va. Code § 18.2-152.3:1.

[48] Va. Code § 18.2-10(f).

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

[50] 24 P.3d 404 (S. Ct. Wash. 2001).

[51] RCW § 19.190.020.

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.[52]

The defendant argued that the Washington statute violated the dormant commerce clause of the Constitution[53] 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.[54] 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."[55] 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.[56]

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.[57] 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."[58] A lower court dismissed the suit, finding that the provisions in question violated the dormant commerce clause of the Constitution.[59] 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.[60] 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

---

[52] *Id.*

[53] 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.

[54] 24 P.3d at 409.

[55] *Id* (citations omitted).

[56] *Id.*

[57] 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.

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

[59] 115 Cal. Rptr.2d at 260.

[60] *Id* at 263.

service provider who has equipment in the state.[61] 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."[62] Thus, the court determined that the burdens imposed on interstate commerce did not outweigh the benefits of the statute.[63]

Additional Federal Legislation

A number of bills related to unsolicited commercial e-mail were introduced in the 108th Congress. Apart from the passage of S. 877 (P.L. 108-187), no action has been taken on the floor of either chamber with respect to any of the bills discussed below.

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."[64] 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. 1052, the **Ban on Deceptive Unsolicited Bulk Electronic Mail Act of 2003**, would make it unlawful for any person to knowingly and intentionally use a computer or computer network to falsify or forge electronic mail transmission information or other source, destination, routing, or subject heading information in connection with the transmission of unsolicited bulk commercial e-mail through, or into, the computer network of an e-mail service provider or its subscribers.[65] It would also be unlawful to transmit an e-mail message to a recipient who requests not to receive unsolicited bulk commercial e-mail; or collect e-mail addresses from public and private spaces for the purpose of transmitting unsolicited bulk commercial e-mail.[66] Violations of the act would be considered a RICO predicate and would constitute an unfair or deceptive act or practice under the Federal Trade Commission Act.[67]

---

[61] *Id* at 264.

[62] *Id* at 268.

[63] *Id* at 269.

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

[65] S. 1052, 108th Cong., Sec. 2(a)(1).

[66] S. 1052, 108th Cong., Sec. 2(a)(2) and (3).

[67] S. 1052, 108th Cong., Sec. 2(b)(1) and (2).

The bill would also require senders of unsolicited bulk commercial e-mail to provide recipients with a clear and conspicuous opportunity to request not to receive future unsolicited e-mail.[68]

S. 1231, the **Stop Pornography and Abusive Marketing Act**, or the **SPAM Act**, would, *inter alia,* require the Federal Trade Commission to establish a nationwide no-spam registry in which any person that does not wish to receive unsolicited commercial e-mail my register e-mail addresses.[69] It would be unlawful for a person to initiate an unsolicited commercial e-mail message to a registered address, and civil penalties of up to $5,000 could be imposed for each violation.[70]

In addition to the creation of the national registry, the bill would also impose a number of other requirements with respect to the transmission of unsolicited commercial e-mail. The act would require such messages to include in the subject line, the characters 'ADV:',[71] and require all commercial and unsolicited commercial e-mail to include a valid return address, a valid postal address, and provide the recipient with the right to decline to receive further messages from the sender.[72] Under the act, it would be unlawful for a person to initiate the transmission of commercial e-mail or unsolicited commercial e-mail in violation of an Internet service provider's policies with respect to e-mail, account registration and use, or other terms of service;[73] or to initiate the transmission of commercial or unsolicited commercial e-mail that contains false, misleading, or deceptive information in the subject line, header or router information, or the body of the message.[74] It would also be unlawful for a person to initiate the transmission of a commercial or unsolicited commercial e-mail messages to addresses obtained through harvesting or by using a automated method of generating e-mail addresses.[75]

Generally, the act would be enforced by the Federal trade Commission, but actions by states, Internet service providers, and individual consumers would also be allowed.[76]

S. 1293, the **Criminal Spam Act of 2003**, would provide criminal penalties for persons who knowingly access a protected computer without authorization, and intentionally initiate the transmission of multiple commercial electronic mail

---

[68] S. 1052, 108th Cong., Sec. 2(c).

[69] S. 1231, 108th Cong., Sec. 101(a).

[70] S. 1231, 108th Cong., Sec. 101(d); Sec. 102(b)(1).

[71] S. 1231, 108th Cong., Sec. 201(a).

[72] S. 1231, 108th Cong., Sec. 204; Sec. 206.

[73] S. 1231, 108th Cong., Sec. 202.

[74] S. 1231, 108th Cong., Sec. 203.

[75] S. 1231, 108th Cong., Sec. 205.

[76] S. 1231, 108th Cong., Title III.

messages from or through such computer.[77] Criminal penalties could also be imposed for knowingly using a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages; falsifying header information in multiple commercial electronic mail messages and intentionally initiating the transmission of such messages; or registering, using information that falsifies the identity of the actual registrant, for 5 or more electronic mail accounts or online user accounts or 2 or more domain names, and intentionally initiating the transmission of multiple electronic mail messages from such accounts.

Penalties for violations include a fine, imprisonment for not more than five years, or both, if the offense is committed in furtherance of any felony; or the defendant has been previously convicted of the same or similar offenses. Lesser terms of imprisonment may be imposed under other circumstances. In addition to fines and imprisonment, the bill requires the forfeiture of any property constituting or traceable to gross profits or other proceeds obtained from the offense; and any equipment, software, or other technology used or intended to be used to commit or to promote the commission of such offense. Civil actions may be brought by the Attorney General or by any person engaged in the business of providing an Internet access service to the public.

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,[78] 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."[79] Violators could be subject to a fine or imprisonment for up to one 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."[80] Senders would also be required to establish a valid sender-operated return address

---

[77] S. 1293, 108th Cong., Sec. 2(a).

[78] S. 1327 appears to be substantially similar to H.R. 1933.

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

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

where the recipient could notify the sender not to send any further messages.[81] 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.[82] 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."[83]

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.[84] The rulemaking would also be required to address procedures for submitting a complaint to the Commission concerning violations; civil 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 Commission.[85]

Private rights of action by recipients of an unsolicited commercial e-mail messages and Internet service providers would also be allowed.[86]

H.R. 2214, the **Reduction in Distribution of Spam Act of 2003**, includes a number of civil and criminal provisions related to the transmission of commercial e-mail. The act would prohibit the transmission of any commercial e-mail messages unless it contains a clear and conspicuous identification that the message is an advertisement or solicitation; clear and conspicuous notice of the opportunity to decline to receive future unsolicited commercial e-mail messages from the sender; a functioning return e-mail address or other Internet-based mechanism that the recipient may use to submit a request not to receive any future messages; and a valid physical address for the sender.[87] The sender or any person acting on behalf of the sender would be prohibited from initiating the transmission of an unsolicited e-mail message to any recipient who has requested not to receive such messages from the sender for a three year period beginning 10 days after the receipt of the original request.[88] The transmission of a commercial e-mail with fraudulent header information, as well as the transmission of commercial e-mail to an address illegally

---

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

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

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

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

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

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

[87] H.R. 2214, 108th Cong., Sec. 101(a).

[88] H.R. 2214, 108th Cong., Sec. 101(b).

harvested, would also be prohibited.[89] These provisions would be enforced by the Federal Trade Commission, through private rights of action brought by Internet service providers, and actions brought by states.[90]

The act would also amend title 18 of the United States Code to create criminal penalties for certain actions related to the transmission of unsolicited commercial e-mail.[91] Generally, criminal penalties could be imposed if the sender falsified his or her identity in a commercial e-mail message or for the failure to place warning labels on unsolicited commercial e-mail containing sexually oriented material.[92]

H.R. 2515, the **Anti-Spam Act of 2003**, would place a number of restrictions on the transmission of unsolicited commercial electronic mail. The bill would require the inclusion of a clear and conspicuous identification that the message is a commercial electronic mail message, a clear and conspicuous notice of the opportunity to decline to receive future messages from the sender or any covered affiliate of the sender, and an e-mail address or other mechanism that the recipient may use to send a request not to receive future messages, and a valid street address of the sender.[93] After receiving notice from a recipient that he or she does not wish to receive future messages, the sender would be prohibited from initiating the transmission of any commercial electronic mail message to the recipient for five years.[94]

H.R. 2515 would also prohibit the transmission of a commercial electronic mail message that contains false or misleading header information or that contains a subject heading that would be likely to mislead a recipient about a material fact regarding the contents or subject matter of the message.[95] The bill also includes prohibitions on the transmission of commercial electronic mail messages to addresses that were illegally harvested or to addresses that were generated by "use of automated means based on permutations of combining names, letters, or numbers for the purpose of sending commercial electronic mail."[96] Messages containing sexually oriented material would be required to include a label indicating that such material is included therein.[97]

If enacted, the act would be enforced by the Federal Trade Commission,[98] with private rights of action available to providers of Internet access service and state

---

[89] H.R. 2214, 108th Cong., Sec. 101(c) and (d).

[90] H.R. 2214, 108th Cong., Sec. 102 - Sec. 105.

[91] H.R. 2214, 108th Cong., Title II.

[92] H.R. 2214, 108th Cong., Sec. 201.

[93] H.R. 2515, 108th Cong., Sec. 101(a).

[94] H.R. 2515, 108th Cong., Sec. 101(b).

[95] H.R. 2515, 108th Cong., Sec. 101(c).

[96] H.R. 2515, 108th Cong., Sec. 101(d) and (e).

[97] H.R. 2515, 108th Cong., Sec. 101(f).

[98] H.R. 2515, 108th Cong., Sec. 105.

attorneys general.[99] The bill also includes criminal penalties for falsifying the sender's identity in commercial electronic mail, failure to place warning labels on commercial electronic mail containing sexually oriented materials, and illicit harvesting of electronic mail addresses.[100]

[99] H.R. 2515, 108th Cong., Sec. 102 and Sec. 103.

[100] H.R. 2515, 108th Cong., Title II.