Order Code RL31953

CRS Report for Congress
Received through the CRS Web

"Junk E-Mail": An Overview of Issues and Legislation Concerning Unsolicited Commercial Electronic Mail ("Spam")

Updated January 30, 2004

Marcia S. Smith
Specialist in Aerospace and Telecommunications Policy
Resources, Science, and Industry Division

"Junk E-Mail": An Overview of Issues and Legislation Concerning Unsolicited Commercial Electronic Mail ("Spam")

Summary

Unsolicited commercial e-mail (UCE), also called "spam" or "junk e-mail," aggravates many computer users. Not only can spam be a nuisance, but its cost may be passed on to consumers through higher charges from Internet service providers who must upgrade their systems to handle the traffic. Also, some spam involves fraud, or includes adult-oriented material that offends recipients or that parents want to protect their children from seeing. Proponents of UCE insist it is a legitimate marketing technique that is protected by the First Amendment.

On December 16, President Bush signed into law S. 877, the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act. The law, P.L. 108-187, went into effect on January 1, 2004.

The CAN-SPAM Act preempts state laws that specifically address spam, but not state laws that are not specific to e-mail, such as trespass, contract, or tort law, or other state laws to the extent they relate to fraud or computer crime. It does not ban unsolicited commercial e-mail. Rather, it allows marketers to send commercial e-mail as long as it conforms with the law, such as including a legitimate opportunity for consumers to "opt-out" of receiving future commercial e-mails from that sender. It does not require a centralized "do not e-mail" registry to be created by the Federal Trade Commission (FTC), similar to the National Do Not Call registry for telemarketing. The bill requires only that the FTC develop a plan and timetable for establishing a "do not e-mail" registry, and to inform Congress of any concerns it has with regard to establishing it. FTC Chairman Timothy Muris has specifically warned that he does not believe a "do not e-mail" registry would be enforceable or noticeably reduce spam. Mr. Muris and others caution that consumers should not expect any legislation to be a "silver bullet" for solving the spam problem; a combination of consumer education, technological advancements, and legislation is required.

The extent to which P.L. 108-187 reduces "spam" may be debated if for no other reason than there are various definitions of that term. Proponents of the legislation argue that consumers are most irritated by fraudulent e-mail, and that the bill should reduce the volume of such e-mail because of the civil and criminal penalties included therein. Opponents counter that consumers object to unsolicited commercial e-mail, and since the bill legitimizes commercial e-mail (as long as it conforms with the law's provisions), consumers actually may receive more, not fewer, unsolicited commercial e-mail messages. Thus, whether or not "spam" is reduced depends in part on whether it is defined as only fraudulent commercial e-mail, or all unsolicited commercial e-mail.

Spam on wireless devices such as cell phones is a growing concern, and is also addressed in P.L. 108-187. See CRS Report RL31636, *Wireless Privacy: Availability of Location Information for Telemarketing* for more on that topic. This report will be updated as events warrant.

Contents

List of Tables

"Junk E-Mail": An Overview of Issues and Legislation Concerning Unsolicited Commercial Electronic Mail ("Spam")

Overview

One aspect of increased use of the Internet for electronic mail (e-mail) has been the advent of unsolicited advertising, also called "unsolicited commercial e-mail" (UCE), "unsolicited bulk e-mail," "junk e-mail, "or "spam."[1] Complaints focus on the fact that some spam contains, or has links to, pornography, that much of it is fraudulent, and the volume of spam is steadily increasing. In April 2003, the Federal Trade Commission (FTC) reported that of a random survey of 1,000 pieces of spam, 18% concerned "adult" offers (pornography, dating services, etc.) and 66% contained indications of falsity in "from" lines, "subject" lines, or message text.[2] According to Brightmail [http://www.brightmail.com], a company that sells anti-spam software, the volume of spam as a percentage of all e-mail rose from 8% in January 2001 to 56% in November 2003.

Opponents of junk e-mail argue that not only is it annoying and an invasion of privacy (see CRS Report RL31408 for more on Internet privacy), but that its cost is borne by recipients and Internet Service Providers (ISPs), not the marketers. Consumers reportedly are charged higher fees by ISPs that must invest resources to upgrade equipment to manage the high volume of e-mail, deal with customer complaints, and mount legal challenges to junk e-mailers. Businesses may incur costs due to lost productivity, or investing in upgraded equipment or anti-spam software. The Ferris Research Group [http://www.ferris.com], which offers consulting services on managing spam, estimated that spam cost U.S. organizations over $10 billion in 2003.

Proponents of UCE argue that it is a valid method of advertising, and is protected by the First Amendment. The Direct Marketing Association (DMA) released figures in May 2003 showing that commercial e-mail generates more than $7.1 billion in annual sales and $1.5 billion in potential savings to American

---

[1] The origin of the term spam for unsolicited commercial e-mail was recounted in *Computerworld*, April 5, 1999, p. 70: "It all started in early Internet chat rooms and interactive fantasy games where someone repeating the same sentence or comment was said to be making a 'spam.' The term referred to a Monty Python's Flying Circus scene in which actors keep saying 'Spam, Spam, Spam and Spam' when reading options from a menu."

[2] Federal Trade Commission. False Claims in Spam: A Report by the FTC's Division of Marketing Practices. April 30, 2003. P. 10. Available at the FTC's spam Web site: [http://www.ftc.gov/bcp/conline/edcams/spam/index.html]

consumers.[3] In a joint open letter to Congress published in *Roll Call* on November 13, 2003, three marketing groups — DMA, the American Association of Advertising Agencies, and the Association of National Advertisers — asserted that "12% of the $138 billion Internet commerce marketplace is driven by legitimate commercial e-mail. This translates into a minimum of $17.5 billion spent in response to commercial e-mails in 2003 for bedrock goods and services such as travel, hotels, entertainment, books, and clothing."[4]

DMA argued for several years that instead of banning UCE, individuals should be given the opportunity to "opt-out" by notifying the sender that they want to be removed from the mailing list. (The concepts of opt-out and opt-in are discussed below.) Hoping to demonstrate that self regulation could work, in January 2000, the DMA launched the E-mail Preference Service where consumers who wish to opt-out can register themselves at a DMA Web site [http://www.e-mps.org]. DMA members sending UCE must check their lists of recipients and delete those who have opted out. Critics argued that most spam does not come from DMA members, so the plan was insufficient, and on October 20, 2002, the DMA agreed. Concerned that the volume of unwanted and fraudulent spam is undermining the use of e-mail as a marketing tool, the DMA announced that it would pursue legislation to battle the rising volume of spam.

One challenge of controlling spam is that some of it originates outside the United States and thus is not subject to U.S. laws or regulations. Spam is a global problem, and the European Commission estimates that Internet subscribers globally pay 10 billion Euros a year in connection costs to download spam [http://europa.eu.int/comm/internal_market/privacy/studies/spam_en.htm]. The European Union has adopted an "opt-in" requirement for e-mail, which became effective October 31, 2003, whereby prior affirmative consent of the recipient must be obtained before sending commercial e-mail. Opt-in is not required where there is an existing customer relationship, but in that case, the sender must provide an opt-out opportunity. (See [http://www.europa.eu.int/scadplus/leg/en/lvb/l24120.htm]. The EU directive sets the broad policy, but each member nation must pass its own law as to how to implement it.[5]) The FTC and other U.S. and foreign agencies have called on organizations in 59 countries to close "open relays" that allow spam to be routed through third-party computers, permitting spammers to avoid detection [http://www.ftc.gov/opa/2003/05/swnetforce.htm].

---

[3] Quoted in: Digits. Wall Street Journal, May 22, 2003, p. B3.

[4] Available at: [http://www.the-dma.org/cgi/dispnewsstand?article=1638].

[5] Not all EU nations have yet passed such legislation. According to the Associated Press (December 7, 2003, 12:30), the EU has asked nine countries (Belgium, Germany, Greece, Finland, France, Luxembourg, the Netherlands, Portugal, and Sweden) to provide within two months an explanation of when they will pass such legislation. AP identified six countries that have taken steps to implement the EU law: Austria, Britain, Denmark, Ireland, Italy, and Spain.

What Is Spam?

Another challenge in debating the issue of spam is defining it. To some, it is any commercial e-mail to which the recipient did not "opt-in" by giving prior *affirmative consent* to receiving it. To others, it is commercial e-mail to which *affirmative* or *implied consent* was not given, where implied consent can be defined in various ways (such as whether there is a pre-existing business relationship). Still others view spam as "unwanted" commercial e-mail. Whether or not a particular e-mail is unwanted, of course, varies per recipient. Since senders of UCE do find buyers for some of their products, it can be argued that at least some UCE is reaching interested consumers, and therefore is wanted, and thus is not spam. Consequently, some argue that marketers should be able to send commercial e-mail messages as long as they allow each recipient an opportunity to indicate that future such e-mails are not desired (called "opt-out"). Another group considers spam to be only fraudulent commercial e-mail, and believe that commercial e-mail messages from "legitimate" senders should be permitted. The DMA, for example, considers spam to be only fraudulent UCE.

The differences in defining spam add to the complexity of devising legislative or regulatory remedies for it. Some of the bills introduced in the 108th Congress took the approach of defining commercial e-mail, and permitting such e-mail to be sent to recipients as long as it conformed with certain requirements. Other bills defined *unsolicited* commercial e-mail and prohibited it from being sent unless it met certain requirements.

P.L. 108-187 (S. 877) defines commercial e-mail and allows marketers to send such e-mail as long as they abide by the terms of the law, such as ensuring that the e-mail does not have fraudulent header information or deceptive subject headings, and includes an opt-out opportunity and other features that proponents argue will allow recipients to take control of their in-boxes. Proponents of the legislation argue that consumers will benefit because they should see a reduction in fraudulent e-mails. Opponents of the legislation counter that the bill legitimizes sending commercial e-mail, and to the extent that consumers do not want to receive such e-mails, the amount of unwanted e-mail actually may increase. If the legislation reduces the amount of fraudulent e-mail, but not the amount of unwanted e-mail, the extent to which it reduces "spam" would depend on what definition of that word is used. (Debate over the potential effectiveness of the legislation is discussed below under **Congressional Action: 108th Congress**).

Avoiding and Reporting Spam

Tips on avoiding spam are available on the FTC Web site [http://www.ftc.gov/bcp/menu-internet.htm] and from Consumers Union [http://www.consumersunion.org/pub/core_product_safety/000210.html#more]. Consumers may file a complaint about spam with the FTC by visiting the FTC Web site [http://www.ftc.gov] and choosing "File a Complaint" at the bottom of the page. The offending spam also may be forwarded to the FTC (UCE@ftc.gov) to assist the FTC in monitoring UCE trends and developments.

Restraining Spam

To date, the objective of restraining junk e-mail has been fought primarily over the Internet or in the courts. Some groups opposed to junk e-mail will send blasts of e-mail to a mass e-mail company, disrupting the company's computer systems. The FTC has taken action against spam involving fraud under its existing authority, and is requesting expanded legislative authority to track, investigate, and sue spammers.[6] In addition, three major ISPs — America OnLine (AOL), Earthlink, and Microsoft Network — all have brought lawsuits under existing laws to stop spammers.[7]

Another approach is to pass laws placing restrictions on UCE or on commercial e-mail generally. As discussed below, many states have passed anti-spam laws, and now a federal law has been enacted (P.L. 108-187). The federal law supersedes state spam laws, but not other state laws that may relate to spam (see below).

Opt-In, Opt-Out, and a "Do Not E-Mail" Registry. As discussed earlier, much of the spam debate focuses on whether consumers should be given the opportunity to opt-in (where affirmative prior consent is required) or opt-out (where consent is assumed unless the consumer notifies the sender that such e-mails are not desired) of receiving UCE or all commercial e-mail. P.L. 108-187 requires senders of all commercial e-mail to provide a legitimate[8] opt-out opportunity to recipients.

One method of implementing opt-out is to create a "do not e-mail" registry where consumers could place their names on a centralized list to opt-out of all commercial e-mail instead of being required to respond to individual e-mails. The concept is similar to the National Do Not Call registry where consumers can indicate they do not want to receive telemarketing calls. The CAN-SPAM Act does not take the step of actually requiring the FTC to create a do not e-mail registry. It does, however, require the FTC to submit a plan and timetable for establishing a registry, authorize the FTC to create it, and instruct the FTC to explain to Congress any concerns about establishing it.

FTC Chairman Timothy Muris expressed concerns in testimony to Congress and elsewhere. On June 11, 2003, he commented that there is no single solution to the spam problem, saying that "a balanced blend of technological fixes, business and

---

[6] The FTC proposal for increased authority was detailed at hearings on reauthorization of the FTC on June 11, 2003 before the Senate Commerce Committee and the House Energy and Commerce Committee. A copy of the FTC statement is available at [http://commerce.senate.gov] and [http://energycommerce.house.gov] under hearings for that day.

[7] CRS Report RL31488, Regulation of Unsolicited Commercial E-Mail, summarizes existing laws and FTC actions.

[8] Some spam already contains instructions, usually to send a message to an e-mail address, for how a recipient can opt-out. However, in many cases this is a ruse by the sender to trick a recipient into confirming that the e-mail has reached a valid e-mail address. The sender then sends more spam to that address and/or includes the e-mail address on lists of e-mail addresses that are sold to bulk e-mailers. It is virtually impossible for a recipient to discern whether the proffered opt-out instructions are genuine or duplicitous.

consumer education, legislation, and enforcement will be required."[9] Although there appears to be widespread public support for a "do not e-mail" (or "do not spam") list,[10] some worry that the database containing the e-mail addresses of all those who do not want spam would be vulnerable to hackers, potentially exacerbating rather than solving the problem. Others, including Mr. Muris, argue that such a registry would not be enforceable (for more on the FTC's position, see that section below).

Several anti-spam groups argue, however, that legislation should go further, prohibiting commercial e-mail from being sent to recipients unless they have opted-in. As noted earlier, the European Union has adopted an opt-in approach (unless there is an existing customer relationship). Eight U.S. groups, including Junkbusters, the Coalition Against Unsolicited Commercial Email (CAUCE), and the Consumer Federation of America, wrote a letter to several Members of Congress expressing their view that the opt-out approach (as in P.L. 108-187) would "undercut those businesses who respect consumer preferences and give legal protection to those who do not."[11] The founder of the Spamhaus Project [http://www.spamhaus.org/], Steve Linford, asserts that "Spammers are cheering the [U.S.] opt-out legislation. It legalizes the status quo."[12] He also states that 90% of the world's spam originates in the United States. (See **Congressional Action: 108th Congress** below for more on reaction to the new federal law.)

Prior Business Relationship. One variation that was included in some of the bills introduced in the 108th Congress is to allow UCE to be sent to recipients with whom the sender has a prior business relationship, an approach similar to that for junk fax (see CRS Report RL30763 for information on the law pertaining to junk fax). This is not included in P.L. 108-187, since marketers may send commercial e-mail to anyone as long as they conform with the requirements in the law, such as offering opt-out. The legislation does, however, specifically permit "transactional and relationship messages" to be sent to recipients without being subject to other provisions of the Act by excluding such messages from the definition of commercial e-mail. "Transactional or relationship messages" are defined as including various types of notifications, including periodic notifications of account balance or other information regarding a subscription, membership, account, loan or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender; providing information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or delivering goods or services,

---

[9] Timothy Muris, Chairman, Federal Trade Commission. Prepared statement to Senate Commerce Committee, June 11, 2003, p. 13; [http://www.commerce.senate.gov]. Mr. Muris gave the same statement to the House Energy and Commerce Committee the same day. See [http://energycommerce.house.gov].

[10] A survey by the ePrivacy Group found that 74% of consumers want such a list. Lisa Bowman, Study: Do-Not-Spam Plan Winning Support, c|net news.com, July 23, 2003, 12:28 PM PT.

[11] [http://www.cauce.org/pressreleases/20030522.shtml].

[12] Declaring a World War on Spam. Wired News, July 1, 2003, 09:31 AM. [http://www.wired.com/news/politics/0,1283,59459,00.html]

including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender. The CAN-SPAM Act permits the FTC to expand or contract that definition as necessary to accommodate changes in e-mail technology or practices.

Labels. Another possibility that has been considered is requiring that senders of UCE or all commercial e-mail to use a label, such as "ADV," in the subject line of the message, so the recipient will know before opening an e-mail message that it is an advertisement. That would also make it easier for spam filtering software to identify UCE or all commercial e-mail and eliminate it. Some propose that adult-oriented spam have a special label, such as ADV-ADLT, to highlight that the e-mail may contain material or links that are inappropriate for children, such as pornography.

The CAN-SPAM Act requires clear and conspicuous identification that a commercial e-mail is an advertisement (but they do not state how or where that identification must be made); requires FTC-prescribed warning labels for sexually-oriented e-mails within 120 days of enactment (see the "Implementation" section at the end of this report for the status of that action); and requires the FTC to submit a report within 18 months of enactment setting forth a plan for requiring commercial e-mail to be identifiable from its subject line using ADV or a comparable identifier, or by means of compliance with Internet Engineering Task Force standards. However, the clear and conspicuous identification that a commercial e-mail is an advertisement, and the warning label for sexually-oriented material, are not required if the recipient has given prior affirmative consent to receipt of such messages.

Non-Legislative Approaches. The fact that the amount of spam is rising despite the number of state laws restraining it suggests that legislation is not a sure solution to the spam problem. Some spam originates outside the United States or is routed through non-U.S. computers, or legislation may include so many "loopholes" that it is ineffective. Senator McCain was quoted as saying that he supports legislation, but is not optimistic about its effect: "I'll support it, report it, vote for it, take credit for it, but will it make much difference? I don't think so."[13]

One proposed non-legislative alternative is trying to make spam less attractive economically by increasing the cost of sending spam, perhaps by establishing systems whereby recipients could charge spammers "postage" for UCE or all commercial e-mail.

Another alternative is using "challenge-response" software that requires the sender to respond to an action requested in an automatically generated return e-mail before the original e-mail reaches the intended recipient. Earthlink offers this option to its subscribers. Challenge-response is based on the concept that spammers are sending e-mail with automated systems that cannot read a return e-mail and respond to a question (such as "how many kittens are in this picture"), but a person can, so if the e-mail was sent by an individual rather than a bulk e-mail system, the person will answer the question or perform a requested action and the e-mail will be delivered.

---

[13] Chris Taylor. Spam's Big Bang. Time, June 16, 2003, p. 52.

It is not clear to what extent such software may become popular. *Business Week* outlined some of the potential unintended consequences, including recipients not receiving confirmation of orders placed over the Internet (which often are generated by automated systems), and difficulty if the sender is using an Internet-access device that does not display graphics (e.g., a Blackberry) or is visually impaired.[14]

Still another non-legislative option is leaving the issue of controlling spam to the ISPs, since they have the economic incentive to do so in terms of retaining subscribers who might weary of spam and abandon e-mail entirely, avoiding the costs associated with litigation, and reducing the need to upgrade server capacity to cope with the traffic. Many ISPs (and consumers) already use spam filtering software, but with the increase in the amount of spam, a large number of such messages still get through. On June 5, 2003, the Associated Press reported that Earthlink's spam filter blocks up to 80% of spam, and AOL blocks 80% of incoming e-mail traffic.[15] In June 2003, Microsoft announced the creation of a special team of researchers and programmers to develop new technological tools to fight spam.

Bush Administration Position

The White House issued a Statement of Administration Policy[16] on S. 877 on October 22, 2003. While supporting Senate passage of the bill, it cautioned that federal legislation alone cannot solve the spam problem — that development and adoption of new technologies also is needed. The Administration called for the bill to be strengthened in accordance with a September 11 letter sent to the Chairman of the Senate Commerce Committee by the Departments of Commerce and Justice, to better serve consumers and avoid creating obstacles to law enforcement.

At the time the House was considering S. 877, the Departments of Justice and Commerce issued a joint statement calling the bill "a useful step in helping consumers and businesses" deal with spam. They cautioned again, however, that legislation development and adoption of new technologies also is needed.[17]

Federal Trade Commission Position

As noted earlier, FTC Chairman Muris told both the Senate Commerce Committee and the House Energy and Commerce Committee on June 11, 2003, that there is no single solution to the spam problem. He argues that a combination of legislation, technological advancements, and consumer education is needed.

---

[14] Stephen H. Wildstrom. A Spam-Fighter More Noxious Than Spam. *Business Week*, July 7, 2003, p. 21.

[15] Anick Jesdanun, Technology for Challenging Spam is Challenged, AP, June 5, 2003, 23:59.

[16] Available at [http://www.whitehouse.gov/omb/legislative/sap/index-date.html]. Scroll down to S. 877.

[17] U.S. Department of Justice. Joint Statement of the Departments of Justice and Commerce on E-Mail Spam Legislation. Press Release 03-643. November 21, 2003. Available at: [http://www.usdoj.gov/opa/pr/2003/November/03_opa_643.htm]

Mr. Muris expanded on those comments in an August 19, 2003 speech to the Aspen Institute [http://www.ftc.gov/speeches/muris/030819aspen.htm]. Drawing attention to the significant differences between telemarketing and spam, he specifically cautioned against expectations that a "do not spam" registry would be enforceable or noticeably reduce spam. Calling spam "one of the most daunting consumer protection problems that the Commission has ever faced ," he noted that "Despite the concerted efforts of government regulators, Internet service providers, and other interested parties, the problem continues to worsen."

He cited two significant differences between spam and other types of marketing. First, spammers can easily hide their identities and cross international borders. Second, sending additional spam "is essentially costless" to the spammer; the cost is borne by ISPs and recipients instead. This "cost shifting" means there is no incentive to the spammer to reduce the volume of messages being sent, and a bulk emailer testified at an FTC forum on spam that he could profit even if his response rate was less than 0.0001%.

Concluding that spam is a problem that market forces will not solve, Mr. Muris agreed that it appeared to be a "prime candidate for governmental intervention." He added, however, that the very technology that makes e-mail such a powerful tool also makes spam a problem that cannot be solved through the FTC's law enforcement and regulatory efforts. "Rather, solutions must be pursued from many directions — technological, legal, and consumer action."

Regarding the current debate in Congress, Mr. Muris commented that "Unfortunately, the legislative debate seems to be veering off on the wrong track, exploring largely ineffective solutions." Specifically, he called the "do not spam" list concept interesting, "but it is unclear how we can make it work" because it would not be enforceable. "If it were established, my advice to consumers would be: Don't waste the time and effort to sign up." He cautioned that legislation can only make a limited contribution to solving the fundamental issues of anonymity and cost shifting, and warned that some of the pending legislative proposals "could be harmful or, at best, useless."

He noted three areas in which legislation would be helpful. He reiterated the need for five procedural changes that he said would assist in tracking down spammers (which he had raised in previous congressional testimony); for additional penalties for spammers; and for standards for non-deceptive UCE. He called the latter the "least important issue" even though it is the subject of most of the pending legislation.

Following initial Senate passage of S. 877 in October 2003, an unnamed FTC official was quoted by the *Washington Post* as saying that the FTC's position on the registry is unchanged, and if the Commission remains unconvinced that it would work, "Congress would have to change the law" to require the FTC to create it.[18]

---

[18] Krim, Jonathan. Senate Votes 97-0 to Restrict E-Mail Ads; Bill Could Lead to No-Spam Registry. Washington Post, October 23, 2003, p. A1 (via Factiva).

On November 21, after the House passed S. 877, Mr. Muris released a statement complimenting Congress on taking a positive step in the fight against spam, but cautioning again that legislation alone will not solve the problem.[19]

State Action

According to the SpamLaws Web site [http://www.spamlaws.com], 36 states have passed laws regulating spam: Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Idaho, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Minnesota, Missouri, Nevada, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wisconsin, and Wyoming. The specifics of each law varies. Summaries of and links to each law are provided on that Web site. CRS Report RL31488, *Regulation of Unsolicited Commercial E-Mail*, provides a brief review of the state laws and challenges to them.

The CAN-SPAM Act preempts state spam laws, but not other state laws that are not specific to electronic mail, such as trespass, contract, or tort law, or other state laws to the extent they relate to fraud or computer crime.. California's anti-spam law is considered relatively strict, requiring opt-in for unsolicited commercial e-mail, unless there is a prior business relationship (in which case, opt-out is required), and would have become effective January 1, 2004. The impending implementation of the California law is often cited as one of the factors stimulating Congress to complete action on a less restrictive, preemptive federal law before the end of 2003.[20]

Congressional Action: 105th-107th Congresses

In the 105th Congress, the House and Senate each passed legislation (H.R. 3888, and S. 1618), but no bill ultimately cleared Congress. In the 106th Congress, several UCE bills were introduced. One, H.R. 3113 (Wilson-Green), passed the House. There was no further action. Several spam bills were introduced in the 107th Congress, but none passed. One, H.R. 718 (Wilson-Green), was reported from the House Energy and Commerce Committee (H.Rept. 107-41, Part I), and the House Judiciary Committee (H.Rept. 107-41, Part II). The two versions were substantially different. A Senate bill, S. 630 (Burns), was reported (S.Rept. 107-318) from the Senate Commerce Committee. There was no further action.

Congressional Action: 108th Congress

The 108th Congress passed S. 877, which merges a number of provisions from several House and Senate bills.[21] It was signed into law by President Bush on

---

[19] FTC. Statement of Timothy J. Muris Regarding Passage of the Can-Spam Act of 2003. November 21, 2003. [http://www.ftc.gov/opa/2003/11/spamstmt.htm]

[20] For example, see: Glanz, William. House Oks Measure Aimed at Spammers; Senate Likely to Approve Changes. Washington Times, November 22, 2003, p. A1 (via Factiva).

[21] Nine bills were introduced in the 108th Congress prior to passage of the CAN-SPAM Act: (continued...)

December 16, 2003 (P.L. 108-187) and went into effect on January 1, 2004. The Senate originally passed S. 877 on October 22, 2003, by a vote of 97-0. As passed at that time, the bill[22] combined elements from several of the Senate bills. The House passed (392-5) an amended version of S. 877 on November 21, 2003, melding provisions from the Senate-passed bill and several House bills. The Senate concurred in the House amendment, with an amendment, on November 25, through unanimous consent. The Senate amendment included several revisions, requiring the House to vote again on the bill. The House agreed with the Senate amendment by unanimous consent on December 8, 2003.

Major Provisions of the CAN-SPAM Act. The major provisions of P.L. 108-187 include the following.

- Commercial e-mail may be sent to recipients as long as the message conforms with the following requirements:
  — transmission information in the header is not false or misleading;
  — subject headings are not deceptive;
  — a functioning return e-mail address or comparable mechanism is included to enable recipients to indicate they do not wish to receive future commercial e-mail messages from that sender at the e-mail address where the message was received (**the "opt-out" requirement**);
  — the e-mail is not sent to a recipient by the sender, or anyone acting on behalf of the sender, more than 10 days after the recipient has opted-out, unless the recipient later gives affirmative consent to receive the e-mail (i.e., opts back in); and
  — the e-mail must be clearly and conspicuously identified as an advertisement or solicitation (although the legislation does not state how or where that identification must be made).

- Some of those requirements (including the prohibition on deceptive subject headings, and the opt-out requirement) do not apply if the message is a "transactional or relationship message," which include various types of notifications, such as periodic notifications of account balance or other information regarding a subscription, membership, account, loan or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender; providing information directly related to an employment relationship or related benefit plan

---

[21] (...continued)
H.R. 1933 (Lofgren), H.R. 2214 (Burr-Tauzin-Sensenbrenner), H.R. 2515 (Wilson-Green), S. 877 (Burns-Wyden), S. 1052 (Nelson-FL), and S. 1327 (Corzine) are "opt-out" bills. (H.R. 1933 and S. 1327 have the same title and are similar, but not identical.) S. 563 (Dayton) is a "do not e-mail" bill. S. 1231 (Schumer) combines elements of both approaches. S. 1293 (Hatch) creates criminal penalties for fraudulent e-mail.

[22] The original Senate-passed bill contained a Title not related to spam (Title II — Realtime Writers Act), which is not discussed in this report. It is not included in the amended version of S. 877 passed by the Senate November 25.

in which the recipient is currently involved, participating, or enrolled; or delivering goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender.

- Sexually oriented commercial e-mail must include, in the subject heading, a "warning label" to be prescribed by the FTC (in consultation with the Attorney General), indicating its nature. The warning label does not have to be in the subject line, however, if the message that is initially viewable by the recipient does not contain the sexually oriented material, but only a link to it. In that case, the warning label, and the identifier, opt-out, and physical address required under section 5 (a)(5) of the Act; must be contained in the initially viewable e-mail message as well. Sexually oriented material is defined as any material that depicts sexually explicit conduct, unless the depiction constitutes a small and insignificant part of the whole, the remainder of which is not primarily devoted to sexual matters. These provisions do not apply, however, if the recipient has given prior affirmative consent to receiving such e-mails.

- Businesses may not knowingly promote themselves with e-mail that has false or misleading transmission information.

- All state laws specifically related to spam are preempted, but not other state laws that are not specific to electronic mail, such as trespass, contract, or tort law, or other state laws to the extent they relate to fraud or computer crime.

- Violators may be sued by FTC, state attorneys general, and ISPs (but not by individuals).

- Violators of many of the provisions of the act are subject to statutory damages of up to $250 per e-mail, to a maximum of up to $2 million, which may be tripled by the court (to $6 million) for "aggravated violations."

- Violators may be fined, or sentenced to up to 3 or 5 years in prison (depending on the offense), or both, for accessing someone else's computer without authorization and using it to send multiple commercial e-mail messages; sending multiple commercial e-mail messages with the intent to deceive or mislead recipients or ISPs as to the origin of such messages; materially falsifying header information in multiple commercial e-mail messages; registering for 5 or more e-mail accounts or online user accounts, or 2 or more domain names, using information that materially falsifies the identity of the actual registrant, and sending multiple commercial e-mail messages from any combination of such accounts or domain names; or falsely representing oneself to be the registrant or legitimate

successor in interest to the registrant of 5 of more Internet Protocol addresses, and sending multiple commercial e-mail messages from such addresses. "Multiple" means more than 100 e-mail messages during a 24-hour period, more than 1,000 during a 30-day period, or more than 10,000 during a 1-year period. Sentencing enhancements are provided for certain acts.

- The Federal Communications Commission, in consultation with the FTC, must prescribe rules to protect users of wireless devices from unwanted commercial messages. (See CRS Report RL31636 for more on this topic.)

Conversely, the bill does not —

- Create a "do not e-mail registry" where consumers can place their e-mail addresses in a centralized database to indicate they do not want commercial e-mail. The bill requires only that the FTC develop a plan and timetable for establishing such a registry and to inform Congress of any concerns it has with regard to establishing it.

- Require that consumers "opt-in" before receiving commercial e-mail.

- Require commercial e-mail to include an identifier such as "ADV" in the subject line to indicate it is an advertisement. The bill does require the FTC to report to Congress within 18 months of enactment on a plan for requiring commercial e-mail to be identifiable from its subject line through use of "ADV" or a comparable identifier, or compliance with Internet Engineering Task Force standards, or an explanation of any concerns FTC has about such a plan.

- Include a "bounty hunter" provision to financially reward persons who identify a violator and supply information leading to the collection of a civil penalty, although the FTC must submit a report to Congress within 9 months of enactment setting forth a system for doing so.

Reaction to the CAN-SPAM Act. Both praise and criticism greeted enactment of the CAN-SPAM Act. Among those praising the bill are marketing groups such as the DMA,[23] ISPs such as America Online,[24] and Microsoft chairman

---

[23] Direct Marketing Association. Senate Updates Spam Bill; Must Return to House for Final Action. News Release, November 25, 2003 [http://www.the-dma.org/cgi/dispnewsstand?article=1662+++++]

[24] America Online, an Industry Leader in the Fight for Tougher Anti-Spam Laws, Applauds Bipartisan Congressional Agreement and Action on Tough New Spam Laws, America Online, Press Release November 21, 2003

(continued...)

Bill Gates.[25] Generally, they support a single federal law, instead of a "patchwork quilt" of state laws, and legislation that permits "legitimate" commercial e-mail while taking measures against fraudulent e-mail. Scott Richter, the president of an e-mail marketing firm in Colorado, expressed relief that the bill will preempt the stricter California law (discussed above): "We are very excited....All of our clients had been worried about the California law. In the last two hours we have been booking a lot of orders for January."[26] The DMA did express reservations, however, about the provision authorizing the FTC to create a "do not e-mail" registry, even though the bill does not, in fact, require the FTC to do so.

Critics include those who wanted opt-in legislation, including advocates of California's opt-in law. California State Senator Debra Bowen was quoted as saying that the CAN-SPAM Act, "... doesn't can spam. It legalizes it.... It's full of loopholes. It's difficult to enforce. It's weaker than many state laws."[27] The Coalition Against Unsolicited Commercial E-Mail (CAUCE) expressed disappointment with the final version of the bill, saying that it "fails the most fundamental test of any anti-spam law, in that it neglects to actually tell any marketers not to spam."[28] Another criticism is that the law does not allow individuals to sue spammers, only the FTC, ISPs, and state attorneys general can sue.

The effectiveness of this legislation in reducing spam probably cannot be ascertained in the near term. One of the bill's sponsors, Senator Conrad Burns, acknowledged that "I don't think you will see really a cutback in spam until someone is caught and prosecuted and they know for sure that we are serious about the enforcement of the law...."[29]

Another factor in the law's effectiveness is that it does not affect spam sent from other countries. Some observers anticipate that U.S.-based spammers will simply move offshore. Members of Congress and others have called for an international approach to restraining spam, which, as noted earlier, is a world-wide problem.

Finally, the extent to which it reduces "spam" depends in part on how that word is defined. Some consider spam to be only fraudulent commercial e-mail, and anticipate that the civil and criminal penalties in the law may reduce the volume of

---

[24] (...continued)
[http://media.aoltimewarner.com/media/newmedia/cb_press_view.cfm?release_num=55253625]

[25] Gates, Bill. A Spam-Free Future. Washington Post, November 24, 2003, p. A 21 (via Factiva).

[26] Quoted in: Andrews, Edmund L. and Saul Hansell. Congress Set to Pass Bill That Restrins Unsolicited E-Mail. New York Times, November 22, 2003, p. 1 (via Factiva).

[27] Quoted in: Lee, Jennifer B. Antispam Bill Passes Senate by Voice Vote. New York Times, November 26, 2003, p. 3 (via Factiva).

[28] CAUCE Statement on House and Senate Spam Bill Vote. November 25, 2003. Available at: [http://www.cauce.org/news/index.shtml].

[29] Quoted in: Lee, Jennifer B. Antispam Bill Passes Senate by Voice Vote. New York Times, November 26, 2003, p. 3 (via Factiva).

that type of commercial e-mail. Others consider spam to be any unsolicited commercial e-mail, and since the law permits commercial e-mail to be sent as long as it complies with the law's requirements, they argue that consumers may see an increase, not a decrease, in commercial e-mail.

Implementation of the Act

On January 28, 2004, the FTC released a notice of proposed rulemaking (NPRM) on the warning labels for sexually-oriented e-mails that it is required to produce within 120 days of the law's enactment.

The Act defines "sexually oriented material" as any material that depicts sexually explicit conduct, unless the depiction constitutes a small and insignificant part of the whole, the remainder of which is not primarily devoted to sexual matters. Inter alia, the FTC is proposing that the phrase "SEXUALLY-EXPLICIT-CONTENT" be required to be displayed as the first 27 characters of the subject line of any such e-mail, substituting the word "content" for "material" because the substance of an e-mail message is more accurately defined by the word content, according to the FTC. The FTC hopes that the wording and punctuation will make it easy for spam filters to identify and block such messages.

The text of the FTC's proposal is available at: [http://www.ftc.gov/opa/2004/01/adult.htm]. The public comment period closes on February 17.

Table 1. Major Provisions of the CAN-SPAM Act

Provision	S. 877 (as passed by the House and Senate)
Title	Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act
Definition of Commercial E-Mail	E-mail whose primary purpose is commercial advertisement or promotion of commercial product or service, with exceptions. Transactional or relationship message (as defined in the Act) is not commercial e-mail. FTC shall issue regulations within 12 months after enactment further defining the relevant criteria to facilitate the determination of the "primary purpose" of a commercial e-mail message.
Definition of Unsolicited Commercial E-mail	Not defined.
Creates "do not e-mail" registry at FTC	No, but requires FTC to submit to Congress, within 6 months of enactment, plan and timetable for creating such a registry; to explain any concerns it has about creating it; and to explain how it would be applied with respect to children. Authorizes (but does not require) FTC to establish and implement the plan.
Prohibits deceptive subject headings	Yes, in all commercial e-mail.
Prohibits false, misleading, or deceptive information in body of message	No, but does not affect FTC's authority to bring enforcement actions for materially false or deceptive representations in commercial e-mail.
Prohibits transmission of e-mail from improperly or illegally harvested e-mail addresses	Yes, in commercial e-mail prohibited under other sections of the Act. Also prohibits dictionary attacks, and using automated means to register for multiple e-mail or on-line user accounts from which to transmit, or enable someone else to transmit unlawful commercial e-mail as defined by the Act.
Prohibits sending e-mails through computers accessed without authorization	Prohibits accessing a computer without authorization and transmitting multiple commercial e-mail messages from or through it.
Prohibits businesses from knowingly promoting themselves with e-mail that has false or misleading transmission information	Yes
Penalties for falsifying sender's identity	Yes
Requires FTC-prescribed "warning labels" on sexually oriented material	Yes, unless recipient has given prior affirmative consent to receipt of the message.

Provision	S. 877 (as passed by the House and Senate)
Requires specific characters in subject line to indicate the message is an advertisement	No, but commercial e-mail must provide clear and conspicuous identification that it is an advertisement, but not if the recipient has given prior affirmative consent to receive the message. Also, FTC must report to Congress within 18 months of enactment on plan for requiring commercial e-mail to be identifiable from its subject line through use of "ADV" or comparable identifier, or compliance with Internet Engineering Task Force standards, or an explanation of any concerns FTC has about such a plan.
Requires opt-out mechanism	Commercial e-mail must provide clear and conspicuous notice of opportunity to opt-out, and functioning e-mail return address or other Internet-based mechanism to which the recipient may opt-out. Sender cannot send commercial e-mail to recipient more than 10 days after recipient has opted out. Sender, or anyone acting on sender's behalf, cannot sell, lease, exchange, or otherwise transfer recipient's e-mail address for any purpose other than compliance with this Act or if the recipient has given express consent. Opt out does not apply if recipient later opts back in by affirmative consent.
Damages or Penalties	Civil and criminal penalties; vary per violation.
Reward for first person identifying a violator and supplying information leading to the collection of a civil penalty	No, but requires FTC to transmit a report to Congress within 9 months of enactment that sets forth a system for rewarding those who supply information about violations, including granting a reward of not less than 20% of civil penalty collected.
Private Right of Action	For ISPs only.
Affirmative Defense/Safe Harbor	No, but in assessing damages, courts may consider whether defendant established and implemented, with due care, reasonable practices and procedures to effectively prevent violations, or the violation occurred despite commercially reasonable efforts to maintain compliance with such practices and procedures.
Enforcement	By FTC, except for certain entities that are regulated by other agencies.
State action allowed	Yes, but must notify FTC or other appropriate regulator, which may intervene.
Effect on ISPs	ISPs may bring civil action in U.S. district court. Does not affect the lawfulness or unlawfulness under other laws of ISP policies declining to transmit, route, relay, handle, or store certain types of e-mail.

Provision	S. 877 (as passed by the House and Senate)
Supersedes state and local laws and regulations	Yes, but does not preempt other state laws that are not specific to electronic mail, such as trespass, contract, or tort law, or other state laws to the extent that they relate to fraud or computer crime.
Provisions regarding spam on wireless devices	Requires Federal Communications Commission, in consultation with FTC, to promulgate rules within 270 days of enactment to protect consumers from unwanted mobile service commercial messages.