Updated April 18, 2001

RS20037

CRS Report for Congress

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

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

## Summary

Unsolicited commercial e-mail (UCE), also called "spam" or "junk e-mail," aggravates many computer users. Not only can it 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. Proponents of UCE insist it is a legitimate marketing technique and protected by the First Amendment. Legislation to place limits on UCE was considered by the last two Congresses, but no bill cleared Congress.. Four bills have been introduced in the 107th Congress: H.R. 95, H.R. 718, H.R. 1017, and S. 630. H.R. 718 has been reported from the House Energy and Commerce Committee (H. Rept. 107-41, Part 1). This report will be updated.

## 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] Issues involved in the debate are reviewed in *Report to the Federal Trade Commission of the Ad-Hoc Working Group on Unsolicited Commercial Email* [http://www.cdt.org/spam].

In 1991, Congress passed the Telephone Consumer Protection Act (P.L. 102-243) that prohibits, *inter alia*, unsolicited advertising via facsimile machines, or "junk fax" (see CRS Report RL30763, *Telemarketing: Dealing with Unwanted Telephone Calls*). Many

[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."

think there should be an analogous law for computers, or some method for letting a consumer know before opening an e-mail message whether or not it is UCE and how to direct the sender to cease transmission of such messages. At a November 3, 1999 hearing of the House Commerce telecommunications subcommittee, a representative of SBC Internet Services stated that 35% of all the e-mail transmitted over SBC's Internet systems in its Pacific Bell and Southwestern Bell regions is UCE.

Opponents of junk e-mail argue that not only is junk e-mail annoying and an invasion of privacy,[2] but that its cost is borne by consumers, not marketers. Consumers reportedly are charged higher fees by Internet service providers 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. Consumers also may incur costs for the time spent reading and/or deleting such e-mail. Some want to prevent bulk e-mailers from sending messages to anyone with whom they do not have an established business relationship, treating junk e-mail the same way as junk fax. The Coalition Against Unsolicited Commercial Email (CAUCE) [http://www.cause.org] is one group opposing spam. Its founder, Ray Everett-Church, is cited in the January 31, 2001 edition of *Newsday* as saying that some Internet Service Providers (ISPs) estimate that spam costs consumers about $2-3 per month.

Proponents of UCE argue that it is a valid method of advertising. The Direct Marketing Association (DMA), for example, argues that instead of banning unsolicited commercial e-mail, individuals should be given the opportunity to notify the sender of the message that they want to be removed from its mailing list — or "opt-out." Hoping to demonstrate that self regulation can work, in January 2000, the DMA launched a new service, the E-mail Preference Service, where consumers who wish to opt out of receiving UCE can register themselves at a DMA Web site [http://www.e-mps.org]. DMA members sending UCE must check their lists of intended recipients and delete those who have opted out via that Web site. Critics argue that most spam does not come from DMA members, so the plan is insufficient.

To date, the issue of restraining junk e-mail has been fought primarily over the Internet or in the courts. Some Internet service providers (ISPs) will return junk e-mail to its origin, and groups opposed to junk e-mail will send blasts of e-mail to a mass e-mail company, disrupting the company's computer systems. Filtering software also is available to screen out e-mail based on keywords or return addresses. Knowing this, mass e-mailers may avoid certain keywords or continually change addresses to foil the software, however. In the courts, ISPs with unhappy customers and businesses that believe their reputations have been tarnished by misrepresentations in junk e-mail have brought suit against mass e-mailers.

Consumers may file a complaint about spam with the Federal Trade Commission (FTC) by visiting the FTC Web site [http://www.ftc.gov] and scrolling down to "complaint form" 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

---

[2] For more on Internet privacy issues, see CRS Report RL30784, *Internet Privacy: An Analysis of Technology and Policy Issues*, and CRS Report RS20035, *Internet Privacy–Protecting Personal Information: Overview and Legislation.*

developments. Three consumer publications are available on the FTC Web site [http://www.ftc.gov/opa/1999/9911/spam.htm]. Separately, CNET.com, a non-government site, has tips for consumers on how to protect themselves from spam at [http://home.cnet.com/internet/0-3793-8-5181225-1.html].

Some UCE either contains indecent material or links to Web sites where indecent material is available. Thus, controls over junk e-mail have also arisen in the context of protecting children from unsuitable material. For example, in 1997, AOL filed suit to prevent a company that sends unsolicited e-mails offering "cyberstrippers" from sending e-mail to AOL subscribers. The company, Over the Air Equipment, agreed on December 18, 1997 to drop its challenge to a preliminary injunction barring it from sending such advertisements to AOL subscribers (Reuters, December 18, 1997, 11:57 AET).

Other spam involves fraud, some of which also may involve links to adult entertainment services. An example cited by the FTC was a scheme in which consumers would receive a spam message that an order had been received and processed and their credit cards would be billed, and to call a specified telephone number with any questions. Unknown to the consumers, the telephone number was in Dominica, West Indies. When the consumers, they were connected to an adult entertainment audiotext service and then were billed for international long-distance calls.

## State Action

Although the U.S. Congress has not passed a law addressing junk e-mail, several states have passed or considered such legislation. According to the National Conference of State Legislatures, as of March 2000, 15 states (California, Connecticut, Delaware, Illinois, Iowa, Louisiana, Nevada, North Carolina, Oklahoma, Rhode Island, Tennessee, Vermont, Virginia, Washington, and West Virginia) have enacted such laws and 16 introduced spam legislation in their 2000 sessions.[3]

## Congressional Action

The House and Senate each passed legislation during the 105th Congress addressing UCE, but no bill ultimately cleared Congress. The Senate-passed version of S. 1618 (concerning "slamming") would have required senders of UCE to clearly identify in the subject line of the message that it was an advertisement, required Internet service providers to make software available to their subscribers to block such e-mail, and prohibited sending e-mail to anyone who had asked not to receive such mail ("opt-out") The House-passed version of the bill ( H.R. 3888) included a sense of Congress statement that industry should self-regulate. Conference agreement was not reached. Several UCE bills were introduced in the 106th Congress. One, H.R. 3113, passed the House.

In the 107th Congress, four bills have been introduced: H.R. 95 (Green), H.R. 718 (Wilson), H.R. 1017 (Goodlatte), and S. 630 (Burns). Note that these bills refer to "providers of Internet access service" which is abbreviated "ISP," for Internet Service Provider, in the text below.

---

[3] National Conference of State Legislatures (Denver, CO office). States Enact Anti-Spam Legislation. March 1, 2000.

**H.R. 95 (Green)**, the Unsolicited Commercial Electronic Mail Act, has been referred to the House Energy and Commerce Committee and the House Judiciary Committee. The bill would make it unlawful to intentionally initiate transmission of UCE containing certain false identifying information; initiate the transmission of UCE to any person in the United States unless it contains a valid e-mail address, conspicuously displayed, to which the recipient may opt-out; initiate UCE to a recipient who has requested to be removed from all distribution lists under the control of the initiator after the expiration of a reasonable period of time for removal from such lists, and such a request shall be deemed to terminate a pre-existing business relationship as defined in the Act; initiate the transmission of UCE to any person in the United States unless the message provides in a clear and conspicuous manner an identification that the message is UCE and notice of the opportunity to opt-out; and initiate the transmission of UCE to any person in the United States to violation of a policy governing the use of an ISP's equipment (the bill sets requirements for those ISP policies).

Under the bill, ISPs would not be liable for actions taken in good faith to block the transmission or receipt of UCE, or for harm resulting from innocent retransmission of it. The FTC would be required to send a notification of alleged violation to UCE initiators so identified by a recipient or an ISP, or if the FTC has other reason to believe a violation has taken place. The bill sets requirements for the FTC notification and subsequent FTC, court, and private actions. State and local governments are not permitted to impose civil liabilities inconsistent with the Act, but the Act does not preempt civil remedies under state trespass or contract law or other provisions of federal, state, or local criminal law, or civil remedies available under such law that relate to acts of computer fraud or abuse.

**H.R. 718 (Wilson)** was referred to the House Energy and Commerce Committee and the House Judiciary Committee. As introduced, it was the same as H.R. 3113 from the 106th Congress, but has changed during markup in the House Energy and Commerce Committee, which reported it with an amendment in the nature of a substitute on April 4, 2001 (H. Rept. 107-41, Part 1). As reported, the bill would:

- define unsolicited commercial electronic mail (UCE), *inter alia*, as commercial e-mail sent to a recipient without the recipient's prior consent and with whom the initiator does not have a pre-existing business relationship.
- amend 18 U.S.C. 1030[4] to prohibit the intentional initiation of transmission of any UCE to a protected computer in the United States with knowledge that certain identifying information is false.
- make it unlawful to initiate the transmission of a commercial e-mail message to any person within the United States unless such message contains a valid return e-mail address, conspicuously displayed, to which a recipient may opt-out.
- make it unlawful to initiate transmission of UCE to a recipient within the United States—
  - → if the recipient has opted-out and a reasonable period of time has expired for removal from distribution lists. The bill also requires that the recipient's e-mail

---

[4] 18 U.S.C. 1030 is the federal computer fraud and abuse statute; it defines a protected computer as a computer exclusively for the use of a financial institution or the U.S. government, used by or for a financial institution or the U.S. government, or used in interstate or foreign commerce or communication.

address be deleted or suppressed from all mailing lists owned by the initiator (and its agents or assigns), and makes it unlawful for the initiator (and such agents or assigns) to sell, lease, exchange, license, or engage in any other transaction involving mailing lists bearing the recipient's e-mail address.

→ unless it provides in a manner that is clear and conspicuous: identification that the message is UCE, notice of the opportunity to opt-out, and the physical mailing address of the initiator.

→ that uses an ISP's equipment if the ISP has a policy that meets certain requirements set forth in the bill, after a reasonable period of time following a request by a recipient to opt-out. The Act does not prevent or limit an ISP from adopting a policy regarding commercial or other e-mail and from enforcing such policy through technical means, through contract, or pursuant to any remedy available under other laws. ISPs are not liable for actions taken in good faith to block UCE.

- make it unlawful for an ISP that has a policy requiring compensation specifically for the transmission of UCE into its system to fail to provide opt-out to a subscriber unless the subscriber has agreed to receive UCE in exchange for discounted or free Internet access services. It shall be an affirmative defense if the violation was not intentional.
- give the FTC enforcement authority through the FTC Act.
- allow UCE recipients and ISPs to bring action to enjoin violations and/or recover actual monetary loss, or $500 per violation up to $50,000, whichever is greater. A court may increase the amount up to three times for willful, repeated violators. Class actions are prohibited. Courts may protect trade secrets.
- allow state attorneys general to bring civil action on behalf of the residents of that state in an appropriate state court or U.S. district court to enjoin violations, enforce compliance, or recover actual monetary loss or receive $500 in damages fo reach violation, and the amount may be tripled for wilful or repeated violations. The state attorney general shall notify the FTC before it files such an action, or at the same time if advance notification is not possible. The FTC may intervene. State and local governments may not impose civil liabilities inconsistent with the Act, but the Act does not preempt civil actions under State trespass or contract law or any laws relating to computer fraud or abuse arising from unauthorized transmission of UCE.

**H.R. 1017 (Goodlatte)**, the Anti-Spamming Act of 2001, was referred to the House Judiciary Committee. It would amend 18 U.S.C. 1030 to prohibit the intentional and unauthorized transmission of bulk unsolicited e-mail to a protected computer (see footnote 4) with knowledge that the message falsifies certain identifying information; prohibit the sale or distribution of computer programs—designed or produced primarily to conceal the source of routing information of bulk unsolicited e-mail prohibited by this Act, that have only limited commercial purpose or use other than concealing such information, or are marketed by the violator or someone working with the violator and with the violator's knowledge for use in concealing such information; to set penalties for violations; and to add definitions.

**S. 630 (Burns)**, the CAN SPAM Act, was referred to the Senate Commerce Committee. It would amend Chapter 63 of Title 18 U.S.C. (concerning mail fraud) to set penalties for intentionally initiating the transmission of UCE to a protected computer in the United States with knowledge that the message contains or is accompanied by header information that is materially or intentionally false or misleading. It would be unlawful to

initiate the transmission to a protected computer of a commercial e-mail message containing or accompanied by header information that is false, misleading, or not legitimately obtained; that has a subject heading that the person knows is likely to mislead the recipient about the contents of the message; and that does not contain a functioning return e-mail address to which the recipient can opt-out. If a recipient opts-out, it shall be unlawful for the sender to send additional UCE more than 10 days after receipt of the opt-out request. UCE messages sent to a protected computer must provide in a clear and conspicuous manner: identification that the message is an advertisement or solicitation; notice of the opportunity to opt-out; and a valid physical postal address for the sender. Nothing in the Act prevents an ISP from having a policy of declining to transmit, route, relay, handle, or store certain types of e-mail.

In general, the Act would be enforced by the FTC under the FTC Act, except for certain industries (e.g, national banks and federal branches and federal agencies of foreign banks would be enforced by the Office of the Comptroller of the Currency under the Federal Deposit Insurance Act). States may bring civil actions on behalf on residents of that state to enjoin practices prohibited by the Act or to obtain damages equal to the greater of actual monetary loss or statutory damages (the smaller of up to $10 per prohibited message or $500,000, with triple those amounts allowed for violations committed wilfully and knowingly). State attorneys general must notify the FTC before filing an action, or at the time of filing if advance notice is not possible, and the FTC may intervene. If the FTC or another federal agency has instituted a civil or administrative action for violation of the Act, no state attorney general may bring an action against that defendant while the action is pending. An ISP adversely affected by a violation of the Act may bring civil action in U.S. district court to enjoin further violations, recover damages equal to the greater of actual monetary loss or statutory damages (the smaller of up to $10 per prohibited message or $500,000, with triple those amounts allowed for violations committed wilfully and knowingly). A showing that a recipient has submitted a complaint to an e-mail address maintained and publicized by the ISP for the purpose of receiving UCE complaints shall create a rebuttable presumption that the message was unsolicited within the meaning of this Act. A person shall not be liable for damages if such person has established and implemented, with due care, reasonable practices and procedures to effectively prevent violations of this Act and any violation occurred despite good faith efforts to maintain compliance with such practices and procedures. State and local governments are not permitted to impose civil liabilities inconsistent with the Act, but the Act does not preempt civil remedies under state trespass or contract law or other provisions of federal, state, or local criminal law, or civil remedies available under such law that relate to acts of computer fraud perpetrated by UCE, provided that the mere sending of UCE in a manner that complies with this Act shall not constitute an act of computer fraud.