

CRS Report for Congress

Received through the CRS Web

“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 three Congresses (105th-107th), but no federal law was enacted (27 states have anti-spam laws, however). Two bills have been introduced in the 108th Congress: S. 563 (Dayton) and S. 877 (Burns). 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>].

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

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.”

“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 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>].

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 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. According to Brightmail, a company that sells anti-spam software, about 40% of all e-mail traffic is spam (*Washington Post*, March 13, 2003, p. 1.)

Opponents of junk e-mail argue that not only is it 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.cauce.org>] is one group opposing spam. Its founder, Ray Everett-Church, was 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. 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/en/dataprot/studies/spam.htm].

Proponents of UCE argue that it is a valid method of advertising. The Direct Marketing Association (DMA), for example, 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. 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 argue that most spam does not come from DMA members, so the plan is insufficient. On October 20, 2002, the DMA agreed it was insufficient, announcing that it would pursue legislation to battle the rising volume of spam. A DMA official said spam must be curbed “to preserve the promise of e-mail as the next great marketing channel” [<http://www.the-dma.org/cgi/disppressrelease?article=354>].

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

² For more on Internet privacy issues, see CRS Report RL31408.

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.

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. Other spam involves fraud. On February 12, 2002, the FTC announced that seven defendants caught in an FTC sting involving illegal chain letters had agreed to settle charges, and that it was mailing warning letters to more than 2,000 individuals still involved in the chain letter scheme (the FTC press release is available at [<http://www.ftc.gov/opa/2002/02/eileenspam1.htm>]).

State Action

Although the U.S. Congress has not passed a federal law addressing junk e-mail, many states have passed or considered such legislation. According to the SpamLaws Web site [<http://www.spamlaws.com>], 27 states have passed laws regulating spam: Arkansas, California, Colorado, Connecticut, Delaware, Idaho, Illinois, Iowa, Kansas, Louisiana, Maryland, Minnesota, Missouri, Nevada, North Carolina, Oklahoma, Ohio, Pennsylvania, Rhode Island, South Dakota, Tennessee, 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.

Congressional Action: 105th-107th Congresses

Congress has been debating legislation to restrict UCE for several years.³ 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), 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), 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

S. 877 (Burns). Senators Burns introduced S. 877, the CAN SPAM Act, on April 10, 2003. It is very similar to legislation he introduced in the 107th Congress (S. 630). The bill would amend Chapter 63 of Title 18 U.S.C. (concerning mail fraud), and would:

³ Legislation is also pending concerning spam sent to mobile handsets, such as cellular telephones or personal digital assistants (PDAs). See CRS Report RL31636.

- define UCE as commercial e-mail sent without the recipient's prior affirmative or implied consent and that is not a transactional or relationship message.
- prohibit initiating the transmission of UCE to a protected computer in the United States with knowledge and intent that the message contains or is accompanied by header information that is materially false or misleading.
- prohibit false or misleading transmission information in commercial e-mail.
- prohibit deceptive subject headings in commercial e-mail. If a person establishes and implements reasonable practices and procedures to prevent a violation of this provision, and the violation occurs despite good faith efforts to comply with them, that person would not be in violation of this provision.
- require the inclusion of a functioning return address or other Internet-based mechanism in UCE to which the recipient can opt-out. If a recipient opts-out, it would be unlawful for the sender, or a person acting on behalf of the sender, to send additional UCE more than 10 business days after receipt of the opt-out request. UCE messages would have to 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. If a person establishes and implements reasonable practices and procedures to prevent violations, and the violation occurs despite good faith efforts to comply with them, the person would not be in violation of these provisions.
- impose statutory damages of \$10 per violation (as defined in the Act) up to \$500,000, or \$1.5 million if the court finds that the defendant committed the violation willfully and knowingly (except that the limits do not apply to the section prohibiting false or misleading header information).
- be enforced by the FTC under the FTC Act, except for certain entities that are regulated by other agencies (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).
- allow states to 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. State attorneys general would have to notify the FTC or other appropriate federal regulator and that regulator could intervene. If the FTC or another federal agency institutes a civil or administrative action for violation of the Act, no state attorney general could bring an action against that defendant while the action was pending.
- allow an ISP that is adversely affected by a violation of the Act to bring civil action in U.S. district court to enjoin further violations or recover damages.
- supersede state or local government statutes, regulations or rules regulating the use of e-mail to send commercial messages, with exceptions.
- prohibit transmission of unlawful UCE from improperly harvested e-mail addresses.
- not impair the enforcement of sections 223 or 231 of the Communications Act of 1934, chapter 71 of Title 18 U.S.C., or any other federal criminal statute. Nothing in the Act affects the FTC's authority to bring enforcement actions regarding false or deceptive representations in commercial e-mail messages.
- not affect the lawfulness or unlawfulness under any other provision of law of the adoption, implementation, or enforcement by an ISP of a policy declining to transmit, route, relay, handle, or store certain types of e-mail.
- require the FTC to submit a study to Congress within 24 months of enactment analyzing the effectiveness and enforcement of the provisions of the Act and the need, if any, to modify those provisions.

S. 563 (Dayton). S. 563, the Computer Owners' Bill of Rights Act, includes a section that would require the FTC to establish a "do not e-mail" registry for anyone who does not wish to receive UCE, and prohibits UCE from being sent to any computer so registered unless authorized by FTC regulations.