Order Code RL31953

CRS Report for Congress

"Spam": An Overview of Issues Concerning Commercial Electronic Mail

Updated May 14, 2008

Patricia Moloney Figliola
Specialist in Telecommunications and Internet Policy
Resources, Science, and Industry Division

Congressional Research Service

Prepared for Members and Committees of Congress

"Spam": An Overview of Issues Concerning Commercial Electronic Mail

Summary

Spam, also called unsolicited commercial email (UCE) or "junk email," 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, and that some consumers want to receive such solicitations.

On December 16, 2003, President Bush signed into law the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, P.L. 108-187. It went into effect on January 1, 2004. The CAN-SPAM Act does not ban UCE. Rather, it allows marketers to send commercial email as long as it conforms with the law, such as including a legitimate opportunity for consumers to "opt-out" of receiving future commercial emails from that sender. It preempts state laws that specifically address spam, but not state laws that are not specific to email, such as trespass, contract, or tort law, or other state laws to the extent they relate to fraud or computer crime. It does not require a centralized "Do Not Email" registry to be created by the Federal Trade Commission (FTC), similar to the National Do Not Call registry for telemarketing. The law 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. The FTC submitted a report to Congress on June 15, 2004, concluding that a Do Not Email registry could actually increase spam.

Proponents of CAN-SPAM have argued that consumers are most irritated by *fraudulent* email, and that the law should reduce the volume of such email because of the civil and criminal penalties included therein. Opponents counter that consumers object to *unsolicited* commercial email, and since the law legitimizes commercial email (as long as it conforms with the law's provisions), consumers actually may receive more, not fewer, UCE messages. Thus, whether or not "spam" is reduced depends in part on whether it is defined as only fraudulent commercial email, or all unsolicited commercial email. Many observers caution that consumers should not expect any law to solve the spam problem — that consumer education and technological advancements also are needed.

Note: This report was originally written by Marcia S. Smith; the author acknowledges her contribution to CRS coverage of this issue area.

Contents

Introduction 1

Defining Spam 2

Avoiding and Reporting Spam 3
- Foreign Spam 3

The Federal CAN-SPAM Act: Summary of Major Provisions 4
- Opt-In, Opt-Out, and a "Do Not Email" Registry 7
  - CAN-SPAM Act Provision 8
  - FTC Implementation 8
- Labels 9
  - CAN-SPAM Act Provision 9
  - FTC Implementation 10
- Other Implementation Actions 11
  - Wireless Spam 11
  - "Bounty Hunter" Provision 11
  - Definition of "Primary Purpose" 11
- Related Legislation 12
- Legal Actions Based on the CAN-SPAM Act 13

Federal Trade Commission Activity 14
- May 2008 Rules on CAN-SPAM Compliance 15
- December 2007 Staff Report on Malicious Spam and Phishing 15
- December 2005 Assessment of the CAN-SPAM Act 16

State Laws Regulating Spam 17

Penny Hill Press
http://www.crsdocuments.com

"Spam": An Overview of Issues Concerning Commercial Electronic Mail

Introduction

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 often 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.[2] However, recent research shows that Internet users' concerns about spam are actually decreasing, even while the volume of spam continues to increase. For example, in a survey conducted by the Pew Internet & American Life Project during February and March 2007, respondents stated that they were "less bothered by [spam]" now than they reported being in the previous survey, conducted in June 2003. Specifically, in the 2003 survey, 25% of respondents stated that spam was a "big problem"; in the 2007 survey, that figure had dropped to 18%. Even more striking is that the percentage of participants who responded that spam was "not a problem at all" rose from 16% to 28% between 2003 and 2007. The percentage of respondents stating that spam is "an annoyance, but not a big problem" has stayed roughly the same at 57% and 51% in 2003 and 2007, respectively.[3]

One reason for this change in attitude towards spam is attributed to Internet users' growing savvy with identifying spam on their own as well as their increased use of spam filters (whether provided by their Internet service provider (ISP) or purchased on their own). In 2007, 71% of Internet users use filters, up from 65% in 2005.[4]

---

[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] This report does not address junk mail or junk fax. See CRS Report RL32177, *Federal Advertising Law: An Overview*, by Henry Cohen, or CRS Report RS21647, *Facsimile Advertising Rules Under the Junk Fax Prevention Act of 2005*, by Patricia Moloney Figliola, respectively, for information on those topics.

[3] Pew Internet & American Life Project. Pew Internet Project Data Memo. May 2007. Available at [http://www.pewinternet.org/pdfs/PIP_Spam_May_2007.pdf].

[4] Pew Internet & American Life Project. Pew Internet Project Data Memo. May 2007. Available at [http://www.pewinternet.org/pdfs/PIP_Spam_May_2007.pdf].

Defining Spam

One challenge in debating the issue of spam is defining it.[5] 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. The final law, the CAN-SPAM Act (see below), took the former approach, defining and allowing 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 law argue that consumers will benefit because they should see a reduction in fraudulent e-mails. Opponents of the law counter that it 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.

On December 16, 2004, the FTC issued its final rule defining the term "commercial electronic mail message," but explicitly declined to define "spam."

---

[5] "Spam" generally refers to e-mail, rather than other forms of electronic communication. The term "spim," for example, is used for unsolicited advertising via Instant Messaging. "Spit" refers to unsolicited advertising via Voice Over Internet Protocol (VOIP). Unsolicited advertising on wireless devices such as cell phones is called "wireless spam."

Avoiding and Reporting Spam

Tips on avoiding spam are available on the FTC website[6] and from Consumers Union.[7] Consumers may file a complaint about spam with the FTC by visiting the FTC website and choosing "File a Complaint" at the bottom of the page.[8] The offending spam also may be forwarded to the FTC, at **spam@uce.gov**, to assist the FTC in monitoring spam trends and developments. The September 2004 issue of *Consumer Reports* has a cover story about spam, including ratings of commercially available spam filters consumers can load onto their computers. Also, individual ISPs use spam filters (though the filters may not catch all spam) and have mechanisms available for subscribers to report spam.

Foreign Spam

Controlling spam is complicated by the fact 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 a 2001 study by the European Commission concluded that Internet subscribers globally pay 10 billion Euros a year in connection costs to download spam.[9] Some European officials complain that the United States is the source of most spam, and the U.S. decision to adopt an opt-out approach in the CAN-SPAM Act (discussed below) was not helpful.[10] In April 2005, a British anti-spam and anti-virus software developing company, Sophos, listed the United States as the largest spam producing country, exporting 35.7% of spam (down from 42.1% in December 2004); South Korea was second, at 25% (up from 13.4% in December 2004).[11] Tracing the origin of any particular piece of spam can be difficult because some spammers route their messages through other computers (discussed below) that may be located anywhere on the globe.

---

[6] See [http://www.ftc.gov/bcp], [http://onguardonline.gov/index.html], and [http://www.ftc.gov/spam/].

[7] See [http://www.consumersunion.org/pub/core_product_safety/000210.html]. Additional spam information is available from CU online at [http://www.consumerreports.org/cro/electronics-computers/computers/internet-and-other-services/net-threats-9-07/spam/0709_net_spam.htm?resultPageIndex=1&resultIndex=1&searchTerm=spam].

[8] The webpage to file a complaint is [https://rn.ftc.gov/pls/dod/wsolcq$.startup?Z_ORG_CODE=PU01].

[9] See [http://ec.europa.eu/justice_home/fsj/privacy/studies/spam_en.htm].

[10] For example, see Mitchener, Brandon. "Europe Blames Weaker U.S. Law for Spam Surge." *Wall Street Journal*, February 3, 2004, p. B1 (via Factiva).

[11] Sophos Reveals Latest "Dirty Dozen" Spam Producing Countries. Press release, April 7, 2005. The other countries on the list are: China (9.7%), France (3.2%), Spain (2.7%), Canada (2.7%), Japan (2.1%), Brazil (2%), United Kingdom (1.6%), Germany (1.2%), Australia (1.2%), and Poland (1.2). [http://www.sophos.com/pressoffice/news/articles/2005/04/sa_dirtydozen05.html].

The Federal CAN-SPAM Act: Summary of Major Provisions

The 108th Congress passed the CAN-SPAM Act, S. 877, which merged provisions from several House and Senate bills.[12] Signed into law by President Bush on December 16, 2003 (P.L. 108-187), it went into effect on January 1, 2004.[13] P.L. 108-187 includes the following major provisions.

- 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 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).

- Commercial e-mail is defined as e-mail, the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose). It does not include transactional or relationship messages (see next bullet). The act directs the FTC to issue regulations within 12 months of enactment to define the criteria to facilitate determination of an e-mail's primary purpose. The FTC did so on December 16, 2004.

- Some 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

---

[12] Nine bills were introduced in the 108th Congress prior to passage of the CAN-SPAM Act: 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) were "opt-out" bills. S. 563 (Dayton) was a "do not e-mail" bill. S. 1231 (Schumer) combined elements of both approaches. S. 1293 (Hatch) created criminal penalties for fraudulent e-mail.

[13] The Senate originally passed S. 877 on October 22, 2003, by a vote of 97-0. As passed at that time, the bill 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.

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 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. The act allows, but does not require, the FTC to modify that definition.

- 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.

- 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 five 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 five or more e-mail accounts or online user accounts, or two 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 five 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 one-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. (The rules were issued in August 2004. See CRS Report RL31636, *Wireless Privacy and Spam: Issues for Congress*, by Marcia S. Smith, for more on this topic.)

Conversely, the act does not —

- Create a "Do Not Email registry" where consumers can place their e-mail addresses in a centralized database to indicate they do not want commercial e-mail. The law required 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. (The FTC released that report in June 2004; see next section.)

- 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 law 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 nine months of enactment setting forth a system for doing so. (The study was released in September 2004.)

Opt-In, Opt-Out, and a "Do Not Email" Registry

Much of the debate on how to stop spam focuses on whether consumers should be given the opportunity to "opt-in" (where 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. The CAN-SPAM Act is an "opt out" law, requiring senders of all commercial e-mail to provide a legitimate[14] opt-out opportunity to recipients.

During debate on the CAN-SPAM Act, several anti-spam groups argued that the legislation should go further, and prohibit commercial e-mail from being sent to recipients unless they opt-in, similar to a policy adopted by the European Union (see below). 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."[15] Some of the state laws (see below) adopted the opt-in approach, including California's anti-spam law.

The European Union adopted an opt-in requirement for e-mail, which became effective October 31, 2003.[16] Under the EU policy, prior affirmative consent of the recipient must be obtained before sending commercial e-mail unless there is an existing customer relationship. In that case, the sender must provide an opt-out opportunity. The EU directive sets the broad policy, but each member nation must pass its own law as to how to implement it.[17]

As noted, Congress chose opt-out instead of opt-in, however. One method of implementing opt-out is to create a "Do Not Email" 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. During consideration of the CAN-SPAM Act, then-FTC Chairman Timothy Muris and other FTC officials repeatedly expressed skepticism about the advisability of a Do Not Email registry despite widespread public support

---

[14] 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.

[15] See [http://www.cauce.org/node/57].

[16] See [http://www.europa.eu.int/scadplus/leg/en/lvb/l24120.htm].

[17] Not all EU nations have yet passed such legislation. According to the Associated Press (December 7, 2003, 12:30), the EU 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. Sweden reportedly adopted spam legislation in March 2004.

for it.[18] One worry is that the database containing the e-mail addresses of all those who do not want spam would be vulnerable to hacking, or spammers otherwise might be able to use it to obtain the e-mail addresses of individuals who explicitly do not want to receive spam. In an August 19, 2003, speech to the Aspen Institute, Mr. Muris commented that the concept of a Do Not Email registry was interesting, "but it is unclear how we can make it work" because it would not be enforceable.[19] "If it were established, my advice to consumers would be: Don't waste the time and effort to sign up."

Following initial Senate passage of S. 877, an unnamed FTC official was quoted by the *Washington Post* as saying that the FTC's position on the registry is unchanged, and "Congress would have to change the law" to require the FTC to create it.[20] After the House passed S. 877, Mr. Muris released a statement complimenting Congress on taking a positive step in the fight against spam, but cautioned again that legislation alone will not solve the problem.[21]

CAN-SPAM Act Provision. The CAN-SPAM Act did not require the FTC to create a Do Not Email registry.[22] Instead, it required the FTC to submit a plan and timetable for establishing a registry, authorized the FTC to create it, and instructed the FTC to explain to Congress any concerns about establishing it.

FTC Implementation. The FTC issued its report to Congress on June 15, 2004.[23] The report concluded that without a technical system to authenticate the origin of e-mail messages, a Do Not Email registry would not reduce the amount of spam, and, in fact, might increase it.

The FTC report stated that "spammers would most likely use a Registry as a mechanism for verifying the validity of e-mail addresses and, without authentication, the Commission would be largely powerless to identify those responsible for misusing the Registry. Moreover, a Registry-type solution to spam would raise

---

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

[19] Muris, Timothy. The Federal Trade Commission and the Future Development of U.S. Consumer Protection Policy. Remarks to the Aspen Summit, Aspen, CP, August 19, 2003. [http://www.ftc.gov/speeches/muris/030819aspen.htm].

[20] 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).

[21] U.S. Federal Trade Commission. 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]

[22] The FTC issued a warning to consumers in February 2004 that a website (unsub.us) promoting a National Do Not Email Registry is a sham and might be collecting e-mail addresses to sell to spammers. See [http://www.ftc.gov/opa/2004/02/spamcam.htm].

[23] U.S. Federal Trade Commission. National Do Not Email Registry: A Report to Congress. Washington, FTC, June 2004. A press release, and a link to the report, is available at [http://www.ftc.gov/opa/2004/06/canspam2.htm].

serious security, privacy, and enforcement difficulties." (p. I) The report added that protecting children from "the Internet's most dangerous users, including pedophiles," would be difficult if the Registry identified accounts used by children in order to assist legitimate marketers from sending inappropriate messages to them. (p. I) The FTC described several registry models that had been suggested, and computer security techniques that some claimed would eliminate or alleviate security and privacy risks. The FTC stated that it carefully examined those techniques — a centralized scrubbing of marketers' distribution lists, converting addresses to one-way hashes (a cryptographic approach), and seeding the Registry with "canary" e-mail addresses — to determine if they could effectively control the risks "and has concluded that none of them would be effective." (p. 16)

The FTC concluded that a necessary prerequisite for a Do Not Email registry is an authentication system that prevents the origin of e-mail messages from being falsified, and proposed a program to encourage the adoption by industry of an authentication standard. If a single standard does not emerge from the private sector after a sufficient period of time, the FTC report said the Commission would initiate a process to determine if a federally mandated standard is required. If the government mandates a standard, the FTC would then consider studying whether an authentication system, coupled with enforcement or other mechanisms, had substantially reduced the amount of spam. If not, the Commission would then reconsider whether or not a Do Not Email registry is needed.

On August 1, 2005, the FTC issued a press release summarizing the results of testing it had conducted to determine if online retailers were honoring opt-out requests. The FTC found that 89% of the merchants it tested did, in fact, stop sending e-mails when requested to do so.[24]

Labels

Another approach to restraining spam is requiring that senders of commercial e-mail 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 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.

CAN-SPAM Act Provision. The CAN-SPAM Act: (1) requires clear and conspicuous identification that a commercial e-mail is an advertisement, but is not specific about how or where that identification must be made; (2) requires the FTC to prescribe warning labels for sexually-oriented e-mails within 120 days of enactment; and (3) 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

---

[24] FTC Survey Tests Top E-Tailers' Compliance with Can-spam's Opt-Out Provisions. August 1, 2005. See [http://www.ftc.gov/opa/2005/08/optout.htm].

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.

FTC Implementation. On May 19, 2004, an FTC rule regarding labeling of sexually oriented commercial e-mail went into effect. The rule was adopted by the FTC (5-0) on April 13, 2004. A press release and the text of the ruling are available on the FTC's website.[25] The rule requires that the mark "SEXUALLY-EXPLICIT" be included both in the subject line of any commercial e-mail containing sexually oriented material, and in the body of the message in what the FTC called the "electronic equivalent of a 'brown paper wrapper.'" The FTC explained that the "brown paper wrapper" is what a recipient initially sees when opening the e-mail, and it may not contain any other information or images except what the FTC prescribes. The rule also clarifies that the FTC interprets the CAN-SPAM Act provisions to include both visual images and written descriptions of sexually explicit conduct.

On July 20, 2005, the FTC announced that it had charged seven companies with violating federal laws requiring these labels. Four of the companies settled with the FTC, which imposed a total of $1.159 million in civil penalties. U.S. District Court suits were filed against the other three companies.[26]

The act also required the FTC to submit a report to Congress on a plan for making commercial e-mail identifiable from its subject line, or to explain what concerns would lead the FTC to recommend against such a plan. That report was submitted in June 2005. It concluded that requiring UCE senders to use a prefix such as ADV probably would not result in less spam.

> Experience with subject line labeling requirements in the states and in other countries does not support the notion that such requirements are an effective means of reducing spam.... Indeed, spam filters widely available at little or no cost ... more effectively empower consumers to set individualized email preferences to reduce unwanted UCE from both spammers and legitimate marketers. Mandatory subject line labeling, by comparison, would be an imprecise tool ... that, at best, might make it easier to segregate *labeled* UCE from *unlabeled* UCE. ... [I]t is extremely unlikely that outlaw spammers would comply with a requirement to label the email messages they send. By contrast, legitimate marketers likely *would* comply.... As a result ... labeled UCE messages sent by law-abiding senders would be filtered out. Meanwhile, unlabeled UCE messages sent by outlaw spammers would still reach consumers' in-boxes.[27] (Italics in original.)

---

[25] See [http://www.ftc.gov/opa/2004/04/adultlabel.htm].

[26] FTC Cracks Down on Illegal "X-Rated" Spam. July 20, 2005. [http://www.ftc.gov/opa/2005/07/alrsweep.htm]

[27] FTC. Subject Line Labeling As A Weapon Against Spam: A Report to Congress. June 17, 2005. p. i-ii. [http://www.ftc.gov/reports/canspam05/050616canspamrpt.pdf]

Other Implementation Actions

The act required the FTC or the Federal Communications Commission (FCC) to take a number of other actions with regard to implementing the CAN-SPAM Act. The FTC routinely issues Notices of Proposed Rulemaking or the results thereof regarding this act, which are too numerous to include in this report. Selected issues are addressed below. See the FTC's spam website [http://www.ftc.gov/spam] for more information.

Wireless Spam. The act required the FCC to issue regulations concerning spam on wireless devices such as cell phones. The FCC issued those regulations in August 2004.[28]

"Bounty Hunter" Provision. The act required the FTC to conduct a study on whether rewarding persons who identify a spammer and supply information leading to the collection of a civil penalty could be an effective technique for controlling spam (the "bounty hunter" provision). The study was released on September 15, 2004.[29] The FTC concluded that the benefits of such a system are unclear because, for example, without large rewards (in the $100,000 to $250,000 range) and a certain level of assurance that they would receive the reward, whistleblowers might not be willing to assume the risks of providing such information. The FTC offered five recommendations if Congress wants to pursue such an approach:

- tie eligibility for a reward to imposition of a final court order, instead of to collecting a civil penalty;
- fund the rewards through congressional appropriations, instead of through collected civil penalties;
- restrict reward eligibility to insiders with high-value information;
- exempt FTC decisions on eligibility for rewards from judicial or administrative review; and
- establish reward amounts high enough to attract insiders with high-value information.

Definition of "Primary Purpose". The act required the FTC to issue regulations, within one year of enactment, defining the relevant criteria to facilitate determination of an e-mail's "primary purpose." The FTC issued its final rule on December 16, 2004, exactly one year after the law was enacted. According to the FTC's press release, [30] the final rule clarifies that the Commission does not intend to regulate non-commercial speech. It differentiates between commercial content and

---

[28] See CRS Report RL31636, *Wireless Privacy and Spam: Issues for Congress*, for more information.

[29] A press release is available at [http://www.ftc.gov/opa/2004/09/bounty.htm], and the report, A CAN-Spam Informant Reward System, is available at [http://www.ftc.gov/reports/rewardsys/040916rewardsysrpt.pdf].

[30] FTC press release, FTC Issues Final Rule Defining What Constitutes a "Commercial Electronic Mail Message," December 16, 2004.

"transactional or relationship" content in defining the primary purpose of an e-mail message.

- If an e-mail contains only a commercial advertisement or promotion of a commercial product or service, its primary purpose is deemed to be commercial.

- If an e-mail contains both commercial content and transactional or relationship content, the primary purpose is deemed to be commercial if the recipient would likely conclude that it was commercial through reasonable interpretation of the subject line, or if the transactional and relationship content does not appear in whole or in substantial part at the beginning of the body of the message.

- If an e-mail contains both commercial content, and content that is neither commercial content nor transactional or relationship content, the primary purpose is deemed to be commercial if the recipient would likely conclude that it was commercial through reasonable interpretation of the subject line, or if the recipient would likely conclude the primary purpose was commercial through reasonable interpretation of the body of the message.

- If an e-mail contains only transactional or relationship content, it is not deemed to be a commercial e-mail message.

"Commercial" content is defined in the final rule as "the commercial advertisement or promotion of a commercial product or service," which includes "content on an Internet website operated for a commercial purpose." That is the same as the definition in the CAN-SPAM Act.[31]

The FTC specifically declined to define the term "spam" because the act sets forth a regulatory scheme built around the terms "commercial electronic mail message" and "transactional or relationship message."[32]

Related Legislation

On December 22, 2006, President Bush signed the Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2005 (U.S. SAFE WEB Act, (P.L. 109-455). The law allows the FTC and parallel foreign law enforcement agencies to share information while investigating allegations of "unfair and deceptive practices" that involve foreign commerce, but raised some privacy concerns because the FTC would not be required to make public any of the information it obtained through foreign sources.

---

[31] The FTC's notice of proposed rulemaking had a slightly different definition. The final rule emphasizes that, in the final rule, the definition is the same as in the act.

[32] This explanation is offered on p. 11 of the text of the *Federal Register* notice as it appears on the FTC website at [http://www.ftc.gov/opa/2005/01/primarypurp.htm].

Legal Actions Based on the CAN-SPAM Act

Many lawsuits have been brought against spammers. The following discussion is illustrative, not comprehensive.

On October 10, 2007, the FTC announced that it had filed a civil lawsuit against an international enterprise, with defendants in the United States, Canada, and Australia, that used spam to drive traffic to websites selling pills that the FTC alleges do not work.[33] The FTC's spam database received over 175,000 spam messages sent on behalf of the operation. The action, announced at an international meeting of government authorities and private industry about spam, spyware, and other online threats, is the first brought by the agency using the U.S. SAFE WEB Act to share information with foreign partners. In addition, the FTC alleges that the operation violated the CAN-SPAM Act by initiating commercial e-mails that contained false "from" addresses and deceptive subject lines, and failed to provide an opt-out link or physical postal address.

On April 29, 2004, the FTC announced that it had filed a civil lawsuit against a Detroit-based spam operation, Phoenix Avatar, and the Department of Justice (DOJ) announced that it had arrested two (and were seeking two more) Detroit-area men associated with the company who are charged with sending hundreds of thousands of spam messages using false and fraudulent headers.[34] The FTC charged Phoenix Avatar with making deceptive claims about a diet patch sold via the spam in violation of the FTC Act, and with violations of the CAN-SPAM Act because the spam did not contain a valid opt-out opportunity and the "reply to" and "from" addresses were fraudulent. The DOJ filed criminal charges against the men under the CAN-SPAM Act for sending multiple commercial e-mails with materially false or fraudulent return addresses. According to the FTC, from January 1, 2004 until the lawsuit was filed, about 490,000 of the spam messages forwarded by consumers to the FTC were linked to Avatar Phoenix.

The FTC simultaneously announced that it had filed a legal action against an Australian spam enterprise operating out of Australia and New Zealand called Global Web Promotions. The FTC stated that it was assisted by the Australian Competition and Consumer Commission and the New Zealand Commerce Committee in bringing the case. According to the FTC, since January 1, 2004, among the spam forwarded by consumers to the FTC, about 399,000 are linked to Global Web Promotions. The FTC charges that a diet patch, and human growth hormone products, sold by Global Web Promotions are deceptive and in violation of the FTC Act. The products are

---

[33] "HoodiaLife" and "HoodiaPlus," was supposed to contain hoodia gordonii and cause significant weight loss; the other, called "HGHLife" and "HGHPlus," was supposed to be a "natural human growth hormone enhancer" that would dramatically reverse the aging process.

[34] (1) FTC Announces First Can-Spam Act Cases. [http://www.ftc.gov/opa/2004/04/040429canspam.htm]; (2) Department of Justice Announces Arrests of Detroit-Area Men on Violations of the 'Can-Spam' Act. [http://www.usdoj.gov/opa/pr/2004/April/04_crm_281.htm].

shipped from within the United States. The FTC further charges that the spam violates the CAN-SPAM Act because of fraudulent headers.

The FTC also filed a complaint against six companies and five individuals who, the FTC alleges, acting as a single business enterprise, sent e-mails containing sexually-explicit content without the required warning label and violated other provisions of the Adult Labeling Rule, the CAN-SPAM Act, and the FTC Act.[35] A federal district court issued a Temporary Restraining Order against the defendants.

Separately, four of the largest ISPs — AOL, Earthlink, Microsoft, and Yahoo! — working together as part of the Anti-Spam Alliance, filed civil suits under the CAN-SPAM Act against hundreds of alleged spammers in March 2004.[36] The suits were filed in federal courts in California, Georgia, Virginia and Washington. A number of other suits since have been filed.

The Massachusetts Attorney General filed the first state CAN-SPAM case against a Florida business called DC Enterprises, and its proprietor William T. Carson in July 2004, which also was filed under the Massachusetts Consumer Protection Act.[37] That case was settled by DC Enterprises and Mr. Carson, who agreed to pay $25,000, halt further violations of the CAN-SPAM Act, and comply with state regulations regarding mortgage brokers.[38]

It should be noted, however, that some ISPs are having difficulty recovering monetary judgments from spam cases (though not necessarily cases brought under the CAN-SPAM Act). Microsoft, for example, reportedly has won $620 million in judgments, but has collected only $500,000.[39]

Federal Trade Commission Activity

The FTC enforces the CAN-SPAM Act and conducts other consumer-education initiatives related to combating spam.

---

[35] FTC press release, Court Stops Spammers From Circulating Unwanted Sexually-Explicit E-mails, January 11, 2005. [http://www.ftc.gov/opa/2005/01/globalnetsolutions.htm].

[36] Mangalindan, Mylene. "Web Firms File Spam Suit Under New Law." *Wall Street Journal*, March 11, 2004, p. B4 (via Factiva).

[37] Hines, Matt. "Massachusetts Files Suit Under Can-Spam." C|NET News.com, July 2, 2004, 11:54 am PDT.

[38] Bray, Hiawatha. "Spammer to Pay $25,000 Settlement." *Boston Globe*, October 8, 2004, p. D3 (via Factiva).

[39] "ISPs Push to Collect Money from Spammers." *Communications Daily*, February 18, 2005, p. 9.

May 2008 Rules on CAN-SPAM Compliance

On May 12, 2008, the FTC approved new four new provisions clarifying the requirements of the CAN-SPAM Act. The provisions are intended to clarify the Act's requirements.

The new rule provisions address four topics: (1) an e-mail recipient cannot be required to pay a fee, provide information other than his or her e-mail address and opt-out preferences, or take any steps other than sending a reply e-mail message or visiting a single Internet Web page to opt out of receiving future e-mail from a sender; (2) the definition of "sender" was modified to make it easier to determine which of multiple parties advertising in a single e-mail message is responsible for complying with the Act's opt-out requirements; (3) a "sender" of commercial e-mail can include an accurately-registered post office box or private mailbox established under United States Postal Service regulations to satisfy the Act's requirement that a commercial e-mail display a "valid physical postal address"; and (4) a definition of the term "person" was added to clarify that CAN-SPAM's obligations are not limited to natural persons.

In addition, the Commission's Statement of Basis and Purpose (SBP) accompanying the final rule addresses a number of topics that are not the subject of any new rule provisions. These include: CAN-SPAM's definition of "transactional or relationship message"; the Commission's decision not to alter the length of time a "sender" of commercial e-mail has to honor an opt-out request; the Commission's determination not to designate additional "aggravated violations" under the Act; and the Commission's views on how CAN-SPAM applies to forward-to-a-"friend" e-mail marketing campaigns, in which someone either receives a commercial e-mail message and forwards the e-mail to another person, or uses a Web-based mechanism to forward a link to or copy of a Web page to another person. The SBP explains that, as a general matter, if the seller offers something of value in exchange for forwarding a commercial message, the seller must comply with the Act's requirements, such as honoring opt-out requests.

December 2007 Staff Report on Malicious Spam and Phishing

In this staff report, the FTC describes findings from its July 2007 workshop, "Spam Summit: The Next Generation of Threats and Solutions" and proposes follow-up action steps that stakeholders can adopt to mitigate the harmful effects of malicious spam and phishing. In addition to proposing action steps for stakeholders, the report provides an overview of the agency's role in protecting consumers from the threats of fraudulent spam and phishing. The report also announces results from the FTC's 2007 Harvesting and Filtering Study, which suggest that Internet service providers' spam filters continue to serve an integral role in reducing the amount of spam that reaches consumers' in-boxes.

July 2007 Spam Summit

In July 2007, the FTC hosted "Spam Summit: The Next Generation of Threats and Solutions."[40] This event was a follow-on effort of the FTC's 2003 Spam Forum. Issues included defining the problem; new methods for sending spam; the "covert economy" (e.g., to what extent does stolen information, such as government-issued identity numbers, credit cards, bank cards and personal identification numbers, user accounts, and e-mail addresses, play a role in spam?); deterring malicious spammers and cybercriminals; emerging threats (e.g., what emerging threats are occurring in media other than e-mail including spam over instant messaging, etc.?); putting consumers back in control (how can we empower consumers and businesses in the fight against spam and malware?); and stakeholder best practices.

December 2005 Assessment of the CAN-SPAM Act

Under the law, the FTC was required to provide Congress with an assessment of the act's effectiveness, and recommend any necessary changes. The FTC submitted its report in December 2005.[41] The FTC concluded that the act has been effective in terms of adoption of commercial e-mail "best practices" that are followed by "legitimate" online marketers, and in terms of providing law enforcement agencies and ISPs with an additional tool to use against spammers. Additionally, the FTC concluded that the volume of spam has begun to stabilize, and the amount reaching individuals' inboxes has decreased because of improved anti-spam technologies.[42] However, it also found that the international dimension of spam has not changed significantly, and that there has been a shift toward the inclusion of "increasingly malicious" content in spam messages, such as "malware," which is intended to harm the recipient. Other negative changes noted by the FTC are that spammers are using increasingly complex multi-layered business arrangements to frustrate law enforcement, and are hiding their identities by providing false information to domain registrars (the "Whois" database).

The FTC did not recommend any changes to the CAN-SPAM Act, but encouraged Congress to pass the US SAFE WEB Act (S. 1608, see next paragraph), noted that continued consumer education efforts are needed, and called for improved anti-spam technologies, particularly domain-level authentication (discussed later in this report).

---

[40] The Spam Summit webpage is online at [http://www.ftc.gov/bcp/workshops/spamsummit/]. The page includes links to both days' transcripts.

[41] FTC. Effectiveness and Enforcement of the CAN-SPAM Act: A Report to Congress. December 2005 [http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf].

[42] A November 2005 FTC report concluded that anti-spam technologies used by ISPs are very effective in preventing spam from reaching recipients. A press release summarizing the report is available at [http://www.ftc.gov/opa/2005/11/spam3.htm].

State Laws Regulating Spam

Thirty-eight states have passed laws regulating spam: Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, 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.[43]

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 passed an anti-spam law that would have become effective January 1, 2004 and was considered relatively strict. It required opt-in for UCE unless there was a prior business relationship, in which case, opt-out is required. The anticipated implementation of that California law is often cited as one of the factors that stimulated Congress to complete action on a less restrictive, preemptive federal law before the end of 2003.[44]

A number of lawsuits have been filed under the state laws. Two notable cases involve the Maryland and Virginia laws. In December 2004, a Maryland judge ruled that Maryland's anti-spam law is unconstitutional, because it seeks to regulate commerce outside of the state.[45] An individual, Eric Menhart, who was a resident of the District of Columbia, but had a business in Maryland whose domain name was "maryland-state-resident.com," filed suit against a New York-based spammer. According to the spamlaws.com website, the Maryland law prohibits sending commercial e-mail that uses a third party's domain name without permission, or that contains false or missing routing information, or with a false or misleading subject line. The law applies, *inter alia*, to e-mail sent from within Maryland, or if the sender knows that the recipient is a Maryland resident. Mr. Menhart reportedly is appealing the ruling.

A lawsuit brought under Virginia's anti-spam law, however, led to a conviction of two North Carolina residents: Jeremy Jaynes, and his sister, Jessica DeGroot. According to the spamlaws.com website, the Virginia law makes it illegal, *inter alia*, to send unsolicited bulk e-mails containing falsified routing information, and allows the court to exercise personal jurisdiction over a nonresident who uses a computer or computer network located in Virginia. The case reportedly is the first felony spam case in the country. According to press accounts, Mr. Jaynes and Ms. DeGroot were convicted of misrepresenting the origin of e-mails that sold software and other products (a third defendant was acquitted). The e-mails went through AOL servers located in Virginia. Ms. DeGroot's conviction was later overturned, and Mr. Jaynes,

---

[43] National Council for State Legislatures website, [http://www.ncsl.org/programs/lis/legislation/spamlaws02.htm].

[44] 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).

[45] Baker, Chris. "Maryland Spam Law Ruled Illegal." *Washington Times*, December 15, 2004, p. C6 (via Factiva).

who was sentenced to nine years in prison, appealed his conviction;[46] his conviction was upheld by a three-judge panel for the Virginia Court of Appeals on September 5, 2006. Jaynes plans to appeal this decision, as well, but Virginia Attorney General Robert McDonnell said in a statement that his office plans to ask the court to revoke bond and order Jaynes to begin serving his sentence.[47]

GalleryWatch.com
http://www.crsdocuments.com
Penny Hill Press

[46] Bruilliard, Karin. "Woman's Spam Conviction Thrown Out." *Washington Post*, March 2, 2005, p. E01 (via Factiva).

[47] Rondeaux, Candace. "Anti-Spam Conviction Is Upheld." *Washington Post*, September 6, 2006, p. B03. Online at [http://www.washingtonpost.com/wp-dyn/content/article/2006/09/05/AR2006090501166_pf.html].