Order Code RL31953

CRS Report for Congress

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

Updated January 3, 2007

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.

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.

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

Contents

Defining Spam 3

Avoiding and Reporting Spam 4

Restraining Spam: The Federal CAN-SPAM Act 4
- Summary of Major Provisions 5
- Opt-In, Opt-Out, and a "Do Not Email" Registry 7
  - CAN-SPAM Act Provision 9
  - FTC Implementation 9
- Labels 10
  - CAN-SPAM Act Provision 10
  - FTC Implementation 11
- Other Implementation Actions 11
  - Wireless Spam 12
  - "Bounty Hunter" Provision 12
  - Definition of "Primary Purpose" 12
- Legal Actions Based on the CAN-SPAM Act 13
- Reaction to and Effectiveness of the CAN-SPAM Act 15
  - Immediate Reaction to the Law 15
  - Assessments of Act's Effectiveness During Its First Year 16
  - FTC's 2005 Assessment 17
  - Additional Legislation 18

Restraining Spam: State Laws 18

Restraining Spam: Non-Legislative Approaches 20
- Securing Internet Connections 21
- Authentication 22
  - FTC's Four-Step Plan for Creating an Authentication Standard 23
  - Microsoft's "Caller ID," Certificates, and "Postage" 23
  - "Sender ID" and Other Industry-Proposed Standards 24
  - Challenge-Response 25

List of Tables

Table 1. Major Provisions of the CAN-SPAM Act 26

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

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] (**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 Telephone Consumer Protection Act of 1991 and the Junk Fax Prevention Act of 2005*, by Patricia Moloney Figliola, respectively, for information on those topics.)

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] Brightmail, a company that sold anti-spam software, tracked the volume of spam as a percentage of all Internet e-mail for several years. According to the Brightmail statistics, spam rose from 8% in January 2001 to 65% in July 2004. That company was purchased by Symantec in June 2004 and comparable current statistics on spam do not appear to be available on Symantec's website. Other companies report spam statistics, but may not use the same criteria or methodologies for identifying spam. Thus, comparisons between companies are not possible. However, MXLogic (which provides e-mail defense solutions) and Postini (which provides e-mail security and management) statistics show that between 68-81% of e-mail traffic through their systems currently is spam.[3]

---

[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] U.S. 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 website: [http://www.ftc.gov/bcp/conline/edcams/spam/index.html]. Click on "Reports."

[3] Postini's figure was 81% on January 30, 2006 [http://www.postini.com/stats/]. MXLogic's figure of 68% is an average for 2005 presented in a December 13, 2005 press release [http://www.mxlogic.com/news_events/press_releases/12_13_05_CAN_SPAM.html]. MXLogic's press release stated that the 68% for 2005 compares with 77% in 2004.

Opponents of junk e-mail argue that not only is it annoying and an invasion of privacy,[4] 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,[5] which offers consulting services on managing spam, estimated in 2003 that spam cost U.S. organizations over $10 billion.

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 consumers.[6] 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." A March 2004 study by the Pew Internet & American Life Project found that 5% of e-mail users said they had ordered a product or service based on an unsolicited e-mail, which "translates into more than six million people."[7]

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 website.[8] 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.

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

---

[4] See CRS Report RL31408, *Internet Privacy: Overview and Pending Legislation*, by Marcia S. Smith, for more on Internet privacy.

[5] See [http://www.ferris.com].

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

[7] Pew Internet & American Life Project. Pew Internet Project Data Memo. March 2004. Available at [http://www.pewinternet.org/pdfs/PIP_Data_Memo_on_Spam.pdf].

[8] See [http://www.dmaconsumers.org/emps.html].

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.

Defining Spam

One challenge in debating the issue of spam is defining it.[12] 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

---

[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 5, 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/pressrel/us/20050407dirtydozen.html].

[12] "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."

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" (see **Other Implementation Actions** below).

Avoiding and Reporting Spam

Tips on avoiding spam are available on the FTC website[13] and from Consumers Union.[14] 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. 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. [15] The offending spam also may be forwarded to the FTC, at spam@uce.gov, to assist the FTC in monitoring spam trends and developments. Many ISPs use spam filters (though the filters may not catch all spam) and mechanisms for subscribers to report spam.

Restraining Spam: The Federal CAN-SPAM Act

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

---

[13] See [http://www.ftc.gov/bcp/menu-internet.htm], [http://onguardonline.gov/index.html], and [http://www.ftc.gov/spam/].

[14] See [http://www.consumersunion.org/pub/core_product_safety/000210.html].

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

[16] 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.

The Senate originally passed S. 877 on October 22, 2003, by a vote of 97-0. As passed at that time, the bill[17] 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.

Summary of Major Provisions

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 "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).

- 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 (see **Other Implementation Actions** below).

- 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 types of notifications, such as periodic notifications of account balance or other information regarding a subscription, membership,

---

[17] 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 was not included in the amended version of S. 877 passed by the Senate November 25.

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 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 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; see **Other Implementation Actions** below).

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[18] 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."[19] 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.[20] 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.[21]

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 for it.[22] One worry is that the database containing the e-mail addresses of all those

---

[18] 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.

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

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

[21] 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.

[22] 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

(continued...)

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.[23] "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.[24] 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.[25]

CAN-SPAM Act Provision. The CAN-SPAM Act did not require the FTC to create a Do Not Email registry.[26] 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.[27] 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. (See below, **Restraining Spam — Non-Legislative Approaches**, for more on authentication.)

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 serious security, privacy, and enforcement difficulties." (p. I) The report added that

---

[22] (...continued)
PM PT.

[23] 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].

[24] 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).

[25] 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]

[26] 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].

[27] 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].

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.[28]

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 identification that a commercial e-mail is an advertisement, and the warning label for

---

[28] 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].

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.[29] 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.[30]

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.[31] (Italics in original.)

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.

---

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

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

[31] 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]

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.[32]

"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.[33] 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, [34] the final rule clarifies that the Commission does not intend to regulate non-commercial speech. It differentiates between commercial content and "transactional or relationship" content in defining the primary purpose of an e-mail message.

---

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

[33] 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].

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

- 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.[35]

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."[36]

Legal Actions Based on the CAN-SPAM Act

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

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.[37] The FTC charged

---

[35] 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.

[36] 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].

[37] (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

(continued...)

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 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.[38] 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.[39] 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.[40] That case was settled by DC Enterprises and Mr. Carson, who

---

[37] (...continued)
on Violations of the 'Can-Spam' Act. [http://www.usdoj.gov/opa/pr/2004/April/04_crm_281.htm].

[38] 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].

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

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

agreed to pay $25,000, halt further violations of the CAN-SPAM Act, and comply with state regulations regarding mortgage brokers.[41]

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.[42]

Reaction to and Effectiveness of the CAN-SPAM Act

There is considerable interest in the effectiveness of the CAN-SPAM Act, but it should be noted that many observers continue to point out that legislation alone cannot solve the problem. Technological advances, in particular, are needed. Non-legislative approaches to restraining spam are discussed later in this report.

Immediate Reaction to the Law. Both praise and criticism greeted enactment of the CAN-SPAM Act. Among those praising the law are marketing groups such as the DMA,[43] ISPs such as America Online,[44] and Microsoft chairman Bill Gates.[45] 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. The DMA did express reservations, however, about the provision authorizing the FTC to create a "Do Not Email" registry, even though the law does not, in fact, require the FTC to do so.

Some commercial e-mailers also appeared pleased. For example, Scott Richter, the president of an e-mail marketing firm in Colorado, expressed relief that the federal law preempted a stricter California law that was slated to become effective January 1, 2004 (discussed below).[46]

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

---

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

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

[43] Direct Marketing Association press release. The DMA Supports National Anti-Spam Law. December 8, 2003. [http://www.the-dma.org/cgi/disppressrelease?article=531].

[44] 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[http://media.aoltimewarner.com/media/newmedia/cb_press_view.cfm?release_num=55253625]

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

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

loopholes. It's difficult to enforce. It's weaker than many state laws."[47] The Coalition Against Unsolicited Commercial E-Mail (CAUCE) expressed disappointment with the final version of the law, 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."[48] Another criticism is that the law does not allow individuals to sue spammers, only the FTC, ISPs, and state attorneys general can sue.

Assessments of Act's Effectiveness During Its First Year. 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 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.

A survey of 2,000 e-mail users released by Consumers Union (CU) in August 2004 found that spam comprised more than half of the e-mail of 69% of the respondents, and, three months after the law went into effect, 47% said that they were receiving more spam, not less.[49] CU President Jim Guest was quoted by the *Wall Street Journal* as saying that the law was inadequate, and opt-in should have been required. He reportedly criticized attempts to distinguish between fraudulent spam and unsolicited advertising from legitimate marketers: "'Spam is spam and consumers don't want any of it,' he said."[50]

A company that describes itself as a provider of e-mail defense solutions, MX Logic, tracks compliance with the CAN-SPAM Act. In January 2005, the company announced that, on average, 97% of unsolicited commercial e-mail in all of 2004 failed to comply with the act.[51] An MX Logic official stated that although the intent of act was to be applauded, "clearly it has had no meaningful impact on the unrelenting flow of spam...."[52] The company also reported that spam accounted for 77% of all e-mail traffic through its "Threat Center" in 2004. In February 2005, the company reported that, for January 2005, an average of 5% of e-mail traffic through its Threat Center complied with the CAN-SPAM Act, "down from an all-time high

---

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

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

[49] Consumers Union. Consumer Reports Investigates How to Protect Against Spam, Spyware and Phishing. Press Release, August 9, 20004. [http://www.consumersunion.org/pub/core_product_safety/001305.html#more]

[50] Nasaw, Daniel. "Federal Law Fails to Lessen Flow of Junk E-Mail." *Wall Street Journal*, August 10, 2004, p. D2 (via Factiva).

[51] "On One-Year Anniversary of CAN-SPAM Act, MX Logic Reports 97 Percent of 2004 Spam Failed to Comply with the Law." MX Logic press release, January 3, 2005. Available at [http://www.mxlogic.com/news_events/01_03_05.html].

[52] Ibid.

of 7% in December."[53] According to its website (visited on March 23, 2005), the figure for compliance with the CAN-SPAM Act for February 2005 also is 5%.

Another company, Postini, maintains spam statistics showing that spam accounted for about 50% of all e-mail in early 2003, which grew to 75% by the time the CAN-SPAM Act passed at the end of that year, and by the end of 2004 75-80% of all e-mail.[54] Statistics on the Postini website [http://www.postini.com/stats/] on March 23, 2005 showed spam as 67.8% of all e-mail, however.

The *New York Times*, in a February 1, 2005 article, reported that "according to most measures" the amount of spam has risen from 50%-60% of all e-mail to "perhaps 80 percent or more" since the law was enacted.[55] The article points to the practice of U.S. companies or individuals hosting websites for the merchants whose products are advertised in spam on servers in other countries as a contributor to the amount of spam, since those servers are not subject to the CAN-SPAM Act.

In late December 2004, however, AOL reported a marked decrease in spam for its subscribers.[56] Hailing a "banner year" in the fight against spam, the company stated that it experienced a 75% reduction in spam in 2004, as defined by reports of spam from its members. In addition, AOL stated that the average daily amount of spam it blocks at its gateway using antispam filters dropped 50%, and there was a 22% drop in attempts made to send e-mail from the Internet to AOL members, which AOL believes to be "almost entirely spam." The company attributed the reduction in spam to improved technical antispam countermeasures, and enforcement actions undertaken by government authorities and AOL under the CAN-SPAM Act.

Senator Burns, who sponsored the CAN-SPAM Act, was quoted by the *Washington Post* as saying that great progress has been made, and the act has been a "great first step, and as we look ahead it's important that the [government] utilizes the tools in place to ... effectively stem the tide of this unwanted burden."[57] He and other supporters of the law argue that it is still too early to assess the act's effectiveness.

FTC's 2005 Assessment. Under the law, the FTC was required to provide Congress with an assessment of the act's effectiveness, and recommend any

---

[53] "MX Logic Reports 13 Percent of Spam Messages Use Email Authentication Schemes." MX Logic press release, February 10, 2005 [http://www.mxlogic.com/news_events/02_10_05.html].

[54] Quoted in: McGuire, David. "A Year After Legislation, Spam Still Widespread; Technology Seen as Best Deterrent." *Washington Post*, January 4, 2005, p. E5 (via Factiva).

[55] Zeller, Tom Jr. "Law Barring Junk E-Mail Allows a Flood Instead." *New York Times*, February 1, 2005, p. 1 (via Factiva)

[56] America Online Announces Breakthroughs in Fight Against Spam. [http://media.timewarner.com/media/newmedia/cb_press_view.cfm?release_num=55254331]. AOL Press Service, December 27, 2004.

[57] Quoted in: McGuire, *Washington Post*, January 4, 2005, op cit.

necessary changes. The FTC submitted its report in December 2005.[58] 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.[59] 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).

Additional 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.

Restraining Spam: State Laws

According to the SpamLaws website [http://www.spamlaws.com], 38 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. The specifics of each law varies. Summaries of and links to each law are provided on that website.[60]

---

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

[59] 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].

[60] See CRS Report RL31488, *Regulation of Unsolicited Commercial E-Mail*, by Angie A. Welborn, for 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 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.[61]

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.[62] 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, who was sentenced to nine years in prison, appealed his conviction;[63] his conviction was upheld by a 3-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.[64]

---

[61] 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).

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

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

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

Restraining Spam: Non-Legislative Approaches

As discussed above, the extent to which the law will restrain spam is not clear. Even before the CAN-SPAM Act was passed, many cautioned that legislation alone would be insufficient. Senator McCain, for example, was quoted as saying that he supported the passage of legislation, but was 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."[65]

During 2003, in congressional testimony and other speeches, then-FTC Chairman Muris repeatedly argued that a combination of legislation, technological advancements, and consumer education is needed. 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."[66] During congressional debate on the CAN-SPAM Act, the White House, and the Departments of Justice and Commerce also warned that federal legislation alone cannot solve the spam problem — that development and adoption of new technologies also is needed.[67]

Mr. Muris 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 e-mailer testified at an FTC forum on spam that he could profit even if his response rate was less than 0.0001%.[68]

ISPs are motivated to reduce spam because they want to retain subscribers who might weary of spam and abandon e-mail entirely, reduce the need to upgrade server capacity to cope with the traffic, and avoid the costs associated with litigation. Though lawsuits may be costly, for the past several years, ISPs have, in fact, taken spammers to court using laws that existed prior to the CAN-SPAM Act. As noted above, America Online, Earthlink, Microsoft, and Yahoo! filed lawsuits under the provisions of the CAN-SPAM Act in March 2004. But the ISPs continue to look for new approaches to reducing spam. Those four ISPs are also working together through the Anti-Spam Technical Alliance to devise technological measures to address spam, as discussed below.

---

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

[66] Muris, Aspen Summit speech, op. cit.

[67] Statement of Administration Policy. S. 877. Available at [http://www.whitehouse.gov/omb/legislative/sap/index-date.html]. Scroll down to S. 877. See also, 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].

[68] Muris, Aspen Summit speech, op. cit.

Spam filters are widely used today by ISPs, corporations, universities, and other organizations. Spammers are aware of that, however, and routinely find methods for defeating the filters by misspelling words, using symbols instead of letters, or "spoofing" the return address (spoofing is discussed below). Coupled with the fact that the filters may inadvertently block wanted e-mails, they are not considered an ideal solution. Some of the other non-legislative approaches to reducing spam are described below.

Securing Internet Connections

Spammers increasingly are taking advantage of "always on" Internet connections, such as cable modems or Digital Subscriber Lines (DSL), belonging to consumers who are unaware that spam is being routed through their computers. In a January 2004 consumer alert entitled "Who's Spamming Who? Could it Be You?," the FTC called on consumers to be vigilant about securing their computers by using firewalls and anti-virus software, being cautious in opening e-mail attachments from unknown senders, and taking other steps.[69] The FTC estimated that 30% of all spam is sent by compromised computers — called "zombies" — in home offices and living rooms. Comcast reportedly has begun blocking access to "port 25," through which home and small business customers can send e-mail directly to the Internet instead of through Comcast servers, because some of those accounts are being used for spam. It is not blocking all access to Port 25; only for those customers whose computers are sending suspicious amounts of e-mail. Some critics have called for Port 25 to be completely blocked by all ISPs. Richard Wong, of Openwave Systems and the Messaging Anti-Abuse Working Group, estimates that one-third of ISPs block port 25, and another third are considering it.[70] The Anti-Spam Technical Alliance, which includes Microsoft, AOL, Yahoo!, and Earthlink, called for ISPs and E-mail Service Providers (ESPs) to block or limit use of Port 25.[71]

In addition, the FTC and regulatory agencies in more than two dozen countries announced "Operation Secure Your Server" in January 2004,[72] an effort to close "open relays" or "open proxies" in businesses that similarly can be used by spammers to reroute their messages and thereby disguise their origin. The agencies sent letters to "tens of thousands" of owners or operators of servers that might be used in this manner urging them to take steps to protect their computers from misuse.

---

[69] See [http://www.ftc.gov/bcp/conline/pubs/alerts/whospamalrt.htm].

[70] Krim, Jonathan. "Comcast Slows Flow of Spam; ISP Limits Access to Abused Gateway." *Washington Post*, June 12, 2004, p. D12 (via Factiva).

[71] Microsoft Corp. Anti-Spam Technical Alliance Publishes Industry Recommendations to Help Stop Spam. Press Release, June 22, 2004. [http://www.microsoft.com/presspass/press/2004/jun04/06-22ASTAPR.asp].

[72] See [http://www.ftc.gov/secureyourserver/]. According to that website, the other countries participating in this effort are: Albania, Argentina, Australia, Brazil, Bulgaria, Canada, Chile, Colombia, Denmark, Ecuador, Finland, Hungary, Jamaica, Japan, Lithuania, Netherlands, Norway, Panama, Peru, Romania, Serbia, Singapore, South Korea, Spain, Switzerland, Taiwan, and the United Kingdom. (Website last visited August 8, 2005.)

Authentication

Another alternative is to require senders to "authenticate" who they are so that recipients may determine whether or not it is spam. As the FTC report on the National Do Not Email Registry explained, when an e-mail message is transmitted from a sender's computer to a recipient's computer, the Simple Mail Transfer Protocol (SMTP) requires only that the receiving computer verify that a valid transmission is being received, not whether the "servername" is the actual name of the sending computer. That is, the receiving computer does not require authentication of the sending computer. The only piece of information which must be accurate is the recipient's address. Others steps in the e-mail process similarly do not require authentication.[73] In October 2005, the DMA announced that it will require its member companies to adopt e-mail authentication systems.[74] The DMA did not specify which authentication system must be used, noting that several are available on the market. There are a variety of approaches to authentication. The FTC and the National Institute of Standards and Technology (NIST, part of the Department of Commerce) held a two-day summit on authentication on November 9-10, 2004.[75]

Authentication is not a sure solution, however. MX Logic reported, for example, that spammers themselves are adopting two of the existing authentication protocols (Sender ID and SPF, see below) to make their messages appear more legitimate.[76] The Message Anti-Abuse Working Group [http://www.maawg.org]), which includes many software companies and ISPs, issued a white paper on July 8, 2005 after evaluating SPF and SenderID. Overall, MAAWG concluded that —

> No sender verification/authentication scheme can guarantee that your message will go straight to the intended recipient's inbox; nor can they guarantee that a message you receive really does come from who you think it came from....
>
> At best, SPF and Sender ID are comparable to a license plate issued by a foreign country: they show that the vehicle is permitted to drive in that country, but make no indication as to whether that country's regulations are similar to yours — and we can only assume that the driver inside is permitted to use that vehicle.[77]

---

[73] FTC National Do Not Email Registry report, op. cit., pp. 4-8 describe how the e-mail system works.

[74] "DMA Requires Members to Adopt E-Mail Authentication Systems." PR Newswire, October 17, 2005, 10:53 (via Factiva).

[75] The transcript is available at [http://www.ftc.gov/bcp/workshops/e-authentication/index.htm]. A one-day industry-sponsored summit was held on July 12, 2005. Copies of the presentations are available at [http://emailauthentication.org/summit2005/].

[76] Keizer, Gregg. "Spammers Most Likely Users of E-Mail Authentication." TechWeb, July 11, 2005, 3:40 pm, via Yahoo!.

[77] MAAWG. Important Considerations for Implementers of SPF and/or Sender ID. [http://www.maawg.org/about/whitepapers/spf_sendID/]. July 8, 2005, p. 2.

FTC's Four-Step Plan for Creating an Authentication Standard. The FTC report on a National Do Not Email Registry (cited earlier) discussed ongoing industry efforts at developing authentication standards. The Commission reported on Microsoft's Caller ID for Email initiative, a standard developed by Meng Weng Wong called Sender Policy Framework (SPF),[78] Yahoo!'s proposal for "domain keys," and efforts by an Internet Engineering Task Force (IETF) working group. The FTC noted that estimates vary widely as to when e-mail authentication will be reality: "Some believe that all e-mail will be authenticated within a year. Others are less sanguine."[79]

The Commission expressed its view that the marketplace should be given an opportunity to test and phase-in an authentication standard, but added that the pace might be accelerated by Commission support. The report identified several areas where its support might be beneficial, such as focusing efforts so that smaller ISPs and businesses, and individuals with their own domains, can ultimately use the standard, and in evaluating the international implications of the standard. It proposed a four-step plan: conducting a two-day "Authentication Summit"in the fall of 2004 (discussed earlier); convening a Federal Advisory Committee to help the FTC develop an authentication system if industry fails to produce a standard after a "sufficient" time; mandating the use of an authentication standard if industry does not adopt one itself; and subsequently evaluating whether the mandatory standard, combined with enforcement actions, is effective in reducing spam. If the answer to the last question is no, the Commission would reconsider the need to create a Do Not Email registry.

Microsoft's "Caller ID," Certificates, and "Postage". In a February 24, 2004 speech,[80] Microsoft Corp. Chairman Bill Gates detailed three initiatives for dealing with the spam problem.

One of the initiatives deals with "spoofing," where spammers use false addresses — often legitimate e-mail addresses that the spammer obtained through legitimate or illegitimate means — in the "from" line to avoid spam filters and deceive recipients into opening the message. Mr. Gates announced that his company would pilot test a **"Caller ID for E-Mail"** system to enable ISPs to determine if a "from" line is spoofed. He said that Microsoft would make available a list of all the numeric Internet addresses assigned to Microsoft computers that send out mail. Other ISPs would then be able to check an incoming message purporting to be from a Microsoft computer to determine if that actually was its origin. If not, then the message would be blocked. Mr. Gates envisioned other e-mail senders similarly making their numeric addresses known in order to implement the system broadly. He noted that Brightmail, Amazon.com, and Sendmail Inc. were working with Microsoft on this initiative. Microsoft subsequently reached agreement to merge its

---

[78] For more on SPF, see [http://www.openspf.org/].

[79] FTC National Do Not Email Registry report, op. cit., p. 13.

[80] Gates, Bill. Remarks to RSA Conference 2004. The speech itself is at [http://www.microsoft.com/billgates/speeches/2004/02-24rsa.asp]. A Microsoft Corp. press release summarizing it is available at [http://www.microsoft.com/presspass/press/2004/feb04/02-24RSAAntiSpamTechVisionPR.asp].

Caller ID with another authentication method, Sender Policy Framework (SPF), yielding "Sender ID," which is discussed below.

For "legitimate" high-volume e-mail senders, Microsoft proposed an approach similar to what was implemented in the Internet privacy arena, where certain organizations offer "seals of approval" to websites that abide by certain privacy principles. These "seals" are offered by organizations such as the Better Business Bureau Online (BBB Online), WebTrust, or TRUSTe.[81] Microsoft proposed a similar regime where trusted entities would establish "reasonable behavior" practices, and issue a **certificate** that would indicate to a recipient or a spam filter that the sender is not a spammer. The marketers reportedly would fund the certificate system and pay for the certificates.[82]

The concept of requiring e-mail senders to pay **postage** for their messages, analogous to traditional mail service, has been broached for several years on the premise that it would increase the costs to spammers of sending out their messages, making spamming less economical. Since the postage would probably apply to all e-mail senders, however, there are concerns that it would restrain the use of e-mail, and the concept has not been widely embraced. However, Microsoft proposed a variation wherein rather than paying money, the sender would be required to devote a certain amount of computer processing time to each message as a demonstration that it is not spam. Mr. Gates views this approach as beneficial to legitimate small volume e-mail senders. The concept is based on the assumption that spammers send millions of messages a day, spending only a fraction of a second on each message, but that legitimate small-volume e-mail senders would have "an abundance of computer processing power available. Although they can't afford to spend cash for a certificate, they can afford to spend a few seconds on each message."[83] Microsoft did not rule out the possibility of requiring a financial payment, however, which it called a "micropayment."[84] Details were not provided.

"Sender ID" and Other Industry-Proposed Standards. On June 22, 2004, Microsoft announced that it had reached agreement with Mr. Meng Weng Wong to merge his SPF standard with Microsoft's Caller ID proposal into a standard called "Sender ID." According to the Microsoft press release, in Sender ID, organizations would publish information about their outgoing e-mail servers (such as IP addresses) in the Domain Name System using XML format. Backward compatibility for the 20,000 domains that already have published information in SPF's TXT format would be provided. Microsoft's announcement stated that the converged standard would enable receiving systems to test for spoofing at both the

---

[81] See CRS Report RL31408, *Internet Privacy: Overview and Pending Legislation*, by Marcia S. Smith, for more on Internet privacy seals.

[82] Krim, Jonathan. "Microsoft to Launch Plan to Control Spam." *Washington Post*, February 25, 2004, p. E1 (via Factiva).

[83] Microsoft Corp. February 24, 2004 press release, op. cit.

[84] Microsoft Corp. Q&A: Microsoft's Anti-Spam Technology Roadmap. Press release, February 24, 2004. Available at [http://www.microsoft.com/presspass/features/2004/Feb04/02-24CallerID.asp].

message transport (SMTP) level used by SPF, and in message body headers, as proposed in Caller ID.

The Sender ID proposal was submitted to the IETF for consideration as an industry-wide standard, but it was rejected, reportedly because of patent and licensing issues.[85] As noted above, the Messaging Anti-Abuse Working Group evaluated SenderID and SPF and found that problems could be encountered when forwarding or re-sending messages.[86]

Yahoo! and Cisco also have merged their efforts to develop an authentication standard. The merged effort is called DomainKeys Identified Mail (DKIM) and uses digital signatures.[87] DKIM combines Yahoo!'s DomainKeys with Cisco's Identified Internet Mail.

Challenge-Response. "Challenge-Response" is another authentication approach. It 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. 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. Earthlink offers this option to its subscribers. It is not clear to what extent such software may become popular, however. *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.[88]

---

[85] Stevenson, Reed. Microsoft Issues Patch — E-mail ID Plan Rejected. Reuters, September 14, 2004, 16:07 (via Factiva).

[86] MAAWG Press Release available at [http://www.maawg.org/news/maawg050711].

[87] For more on DKIM, see a presentation made at the July 2005 industry authentication summit: [http://emailauthentication.org/summit2005/08_DKIM_EAllman.pdf].

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

Table 1. Major Provisions of the CAN-SPAM Act

Provision	P.L. 108-187 (S. 877)
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 Email" registry at FTC	No, but requires FTC to submit to Congress, within six 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.

Provision	P.L. 108-187 (S. 877)
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.
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.

Provision	P.L. 108-187 (S. 877)
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 nine 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.

Provision	P.L. 108-187 (S. 877)
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.
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.

crsphpgw

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