Order Code RL31953

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

Updated June 25, 2003

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

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

Summary

Unsolicited commercial e-mail (UCE), also called "spam" or "junk e-mail," aggravates many computer users. Not only can spam be a nuisance, but its cost may be passed on to consumers through higher charges from Internet service providers who must upgrade their systems to handle the traffic. Also, some spam involves fraud, or includes adult-oriented material that offends recipients or that parents want to protect their children from seeing. Proponents of UCE insist it is a legitimate marketing technique that is protected by the First Amendment. While 34 states have anti-spam laws, there is no federal law specifically concerning spam. Nine "anti-spam" bills are pending in the 108th Congress: H.R. 1933 (Lofgren), H.R. 2214 (Burr-Tauzin-Sensenbrenner), H.R. 2515 (Wilson), S. 563 (Dayton), S. 877 (Burns-Wyden), S. 1052 (Nelson-FL), S. 1231 (Schumer), S. 1293 (Hatch), and S. 1327 (Corzine). Tables providing brief "side-by-side" comparisons of the bills are included in this report.

Spam on wireless devices such as cell phones is discussed in CRS Report RL31636, *Wireless Privacy: Availability of Location Information for Telemarketing*. State spam laws, and an existing federal law (the Computer Fraud and Abuse statute) that is being used by some Internet Service Providers to bring suit against spammers, are discussed in CRS Report RL31488, *Regulation of Unsolicited Commercial E-Mail*.

This report will be updated as events warrant.

Contents

Overview 1
Avoiding and Restraining Spam 2
State Action 4
Congressional Action: 105th-107th Congresses 4
Congressional Action: 108th Congress 5

List of Tables

Table 1: Brief Comparison of Pending Spam Legislation in the House 6
Table 2: Brief Comparison of Pending Spam Legislation in the Senate 10

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

Overview

One aspect of increased use of the Internet for electronic mail (e-mail) has been the advent of unsolicited advertising, also called "unsolicited commercial e-mail (UCE)," "unsolicited bulk e-mail," "junk e-mail, "or "spam."[1] Complaints focus on the fact that some spam contains or has links to pornography, that much of it is fraudulent, and the volume of spam is steadily increasing. In April 2003, the Federal Trade Commission (FTC) reported that of a random survey of 1,000 pieces of spam, 18% concerned "adult" offers (pornography, dating services, etc.) and 66% contained indications of falsity in "from" lines, "subject" lines, or message text.[2] According to Brightmail [http://www.brightmail.com], a company that sells anti-spam software, the volume of spam rose from 8% of all e-mail in January 2001 to 45% in January 2003. Some project that spam will reach or exceed 50% of all e-mail by 2004.

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

Proponents of UCE argue that it is a valid method of advertising, and is protected by the First Amendment. The Direct Marketing Association (DMA) 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

---

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

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

from the mailing list. Hoping to demonstrate that self regulation could work, in January 2000, the DMA launched the E-mail Preference Service where consumers who wish to opt-out can register themselves at a DMA Web site [http://www.e-mps.org]. DMA members sending UCE must check their lists of recipients and delete those who have opted out. Critics argued that most spam does not come from DMA members, so the plan is insufficient, and on October 20, 2002, the DMA agreed. Concerned that the volume of unwanted spam was undermining the use of e-mail as a marketing tool, the DMA announced that it now would pursue legislation to battle the rising volume of spam.

One challenge of controlling spam is that some of it originates outside the United States and thus is not subject to U.S. laws or regulations. Spam is a global problem, and the European Commission estimates that Internet subscribers globally pay 10 billion Euros a year in connection costs to download spam [http://europa.eu.int/comm/internal_market/privacy/studies/spam_en.htm]. Several European countries have anti-spam laws. The FTC and other U.S. and foreign agencies have called on organizations in 59 countries to close "open relays" that allow spam to be routed through third-party computers, permitting spammers to avoid detection [http://www.ftc.gov/opa/2003/05/swnetforce.htm].

Avoiding and Restraining Spam

Tips on avoiding spam are available on the FTC Web site [http://www.ftc.gov/bcp/menu-internet.htm], and from [http://home.cnet.com/internet/0-3793-8-5181225-1.html], a non-government site. Consumers may file a complaint about spam with the FTC by visiting the FTC Web site [http://www.ftc.gov] and choosing "File a Complaint" at the bottom of the page. The offending spam also may be forwarded to the FTC (UCE@ftc.gov) to assist the FTC in monitoring UCE trends and developments.

To date, the objective of restraining junk e-mail has been fought primarily over the Internet or in the courts. Some groups opposed to junk e-mail will send blasts of e-mail to a mass e-mail company, disrupting the company's computer systems. The FTC has taken action against spam involving fraud under its existing authority, and is requesting expanded legislative authority to track, investigate, and sue spammers.[3] In addition, three major ISPs — America OnLine (AOL), Earthlink, and Microsoft Network — all have brought lawsuits under existing laws to stop spammers.[4]

Another approach is to enact specific anti-spam legislation. As discussed below, more than half the states already have enacted spam laws, though no federal legislation has passed. An oft-discussed approach is requiring senders of UCE to

---

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

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

provide a legitimate opportunity for recipients to "opt-out" of receiving additional messages.[5] Others want to prevent bulk e-mailers from sending messages to anyone with whom they do not have an established business relationship, treating junk e-mail the same way as junk fax (see CRS Report RL30763 for information on the law pertaining to junk fax).

Another approach is creating a "do not e-mail" list similar to the "do not call" list for telemarketers, where individuals can place their names on a list to opt-out of receiving UCE. Another possibility is requiring that senders of UCE use a label such as "ADV" in the subject line of the message so the recipient will know before opening an e-mail message that it is an advertisement. That would also make it easier for spam filtering software to identify UCE and eliminate it. Some propose that adult-oriented spam have a special label to highlight that the material may be inappropriate for children, in particular.

Several anti-spam groups argue that legislation should go further, prohibiting commercial e-mail from being sent to recipients who have not specifically requested such messages or otherwise given their affirmative prior consent — called "opt-in." Eight 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 advanced in several of the pending bills would "undercut those businesses who respect consumer preferences and give legal protection to those who do not." [http://www.cauce.org/pressreleases/20030522.shtml].

Others argue that legislation cannot stop spam because much spam originates outside the United States or is routed through non-U.S. computers, or because legislation includes so many "loopholes" that it is ineffective. Senator McCain was quoted in Time magazine as saying that he supports legislation but is not optimistic about its effect: "I'll support it, report it, vote for it, take credit for it, but will it make much difference? I don't think so."[6] The fact that spam is rising despite the growing number of state laws suggests that legislation is not a sure solution.

One proposed alternative is trying to make spam less attractive economically by increasing the cost of sending spam, perhaps by establishing systems whereby recipients could charge spammers "postage" for UCE. A technological alternative is using "challenge-response" software that requires the sender to respond to an action requested in an automatically generated return e-mail before the original e-mail reaches the intended recipient. Earthlink offers this option to its subscribers. Challenge-response is based on the concept that spammers are sending e-mail with

---

[5] Some spam already contains instructions, usually to send a message to an e-mail address, for how a recipient can indicate that future such messages are not desired. 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.

[6] Quoted in: Chris Taylor. Spam's Big Bang! Time, June 16, 2003, p. 52.

automated systems that cannot read a return e-mail and respond to a requested action (such as "click here"), but a person can, so if the e-mail was sent by an individual rather than a bulk e-mail system, the person will perform the requested action and the e-mail will be delivered. It is not clear to what extent such software may become popular, since it places an additional burden on the sender and could delay an e-mail's arrival.

Some argue that the issue of controlling spam should be left to the ISPs, since they have the economic incentive to do so in terms of retaining subscribers who might weary of spam and abandon e-mail entirely, avoiding the costs associated with litigation, and reducing the need to upgrade server capacity to cope with the traffic. Many ISPs already use spam filtering software,[7] but with the increase in the amount of spam, a large number of such messages still get through. In June 2003, Microsoft announced the creation of a special team of researchers and programmers to develop new technological tools to fight spam. However, Microsoft also is supporting the need for federal legislation, as is AOL.

State Action

According to the SpamLaws Web site [http://www.spamlaws.com], 34 states have passed laws regulating spam: Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Idaho, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wisconsin, and Wyoming. The specifics of each law varies. Summaries of and links to each law are provided on that Web site. CRS Report RL31488, Regulation of Unsolicited Commercial E-Mail, provides a brief review of the state laws and challenges to them.

Congressional Action: 105th-107th Congresses

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

---

[7] On June 5, 2003, the Associated Press reported that Earthlink's spam filter blocks up to 80% of spam, and AOL blocks 80% of incoming e-mail traffic. Anick Jesdanun, Technology for Challenging Spam is Challenged, AP, June 5, 2003, 23:59.

Congressional Action: 108th Congress

Nine bills are currently pending. H.R. 1933, H.R. 2214, H.R. 2515, S. 877, S. 1052, and S. 1327 are "opt-out" bills. (H.R. 1933 and S. 1327 have the same title and are similar, but not identical.) S. 563 is a "do not e-mail" bill. S. 1231 combines elements of both approaches. S. 1293 creates criminal penalties for fraudulent e-mail.

The provisions of these bills are summarized in the following two tables — one for House bills and one for Senate bills. Some of the provisions affect all commercial e-mail, while others affect only *unsolicited* commercial e-mail (spam). S. 877 was ordered reported, amended, by the Senate Commerce Committee on June 19, 2003. Table 2 shows the provisions in the bill as it was ordered reported.

Table 1: Brief Comparison of Pending Spam Legislation in the House

Provision	H.R. 1933 (Lofgren)/S. 1326 (Corzine)	H.R. 2214 (Burr-Tauzin-Sensenbrenner)	H.R. 2515 (Wilson)
Title	REDUCE Spam Act	Reduction in Distribution of Spam Act	Anti-Spam Act
Definition of Commercial E-Mail	E-mail whose primary purpose is commercial advertisement or promotion of commercial product or service, unless the sender has a personal relationship with the recipient.	E-mail whose primary purpose is commercial advertisement or promotion of commercial product or service, with exceptions.	E-mail that contains a commercial advertisement or promotion of a product or service, but is not a commercial transactional e-mail message (as defined in the Act).
Definition of Unsolicited Commercial E-mail (UCE)	Commercial e-mail sent to a recipient with whom the sender does not have a pre-existing business relationship, and is not sent at the request of, or with the express consent of, the recipient. Pre-existing business relationship means that there has been a business transaction between the sender and recipient within the past 5 years and the recipient was provided at that time with an opt-out opportunity and did not exercise it, or the recipient opted-in and has not revoked that permission.	Commercial e-mail transmitted without prior consent. Consent means the recipient has expressly consented to receive the message, and it includes consent to receipt of a message from a third party pursuant to transfer of the recipient's e-mail address if the recipient was notified that such transfer could occur. If commercial e-mail is delivered to a recipient at an e-mail address that was reassigned from a previous user, the recipient is considered to have consented to the same extent as the previous address user unless the sender knows that the address has been reassigned or the new user has opted-out.	Not defined.
Prohibits false or misleading header information	Yes, in UCE.	Yes, in all commercial e-mail.	Yes, in all commercial e-mail.
Prohibits deceptive subject headings	Yes, in UCE.	No	Yes, in all commercial e-mail.
Prohibits false, misleading, or deceptive information in body of message	No	No	No

Provision	H.R. 1933 (Lofgren)/S. 1326 (Corzine)	H.R. 2214 (Burr-Tauzin-Sensenbrenner)	H.R. 2515 (Wilson)
Prohibits transmission of e-mail from improperly or illegally harvested e-mail addresses	No	Yes, for all commercial e-mail.	Yes, in commercial e-mail prohibited under other sections of the Act. Also prohibits dictionary attacks.
Prohibits sending e-mails through computers accessed without authorization	NA	NA	NA
Creates "do not e-mail" registry at FTC	No	No	No
Penalties for falsifying sender's identity	No	Yes	Yes
Requires FTC-prescribed "warning labels" on sexually oriented material	No, but see requirements for subject line labels (next).	Yes	Yes
Requires specific characters in subject line of UCE to indicate the message is an advertisement	Yes, "ADV:" for advertisement; "ADV-ADLT:" for adult-oriented advertisements. Or identification may comply with standards set by Internet Engineering Task Force.	No, but message must provide clear and conspicuous identification that it is an advertisement.	No, but message must contain clear and conspicuous identification that it is a commercial e-mail message.
Requires opt-out mechanism	UCE must contain valid sender-operated return e-mail address to which recipient may opt-out.	Commercial e-mail must contain functioning return e-mail address or other Internet-based mechanism to which the recipient may opt-out.	Commercial e-mail must contain functioning return e-mail address or other Internet-based mechanism to which the recipient may opt-out.
Damages or Penalties	Civil penalties to be set by FTC, except that under private right of action, court may impose penalties up to $10 per violation.	Varies per section of Act.	Varies per section of Act. Also creates criminal penalties for falsifying sender's identity, failing to placing warning lables on sexually oriented material, illicit e-mail address harvesting, and other sections of the act.

Provision	H.R. 1933 (Lofgren)/S. 1326 (Corzine)	H.R. 2214 (Burr-Tauzin-Sensenbrenner)	H.R. 2515 (Wilson)
Penalties for persons who promote their trade, business, goods, products, etc. in e-mail that violates Act, under specific circumstances	NA	NA	NA
Reward for first person identifying a violator and supplying information leading to the collection of a civil penalty	Yes, not less than 20% of the penalty.	No	No
Private Right of Action	Yes. Recipient of UCE or ISP may bring civil action in a U.S. district court to enjoin further violations and recover damages.	Yes, but for ISPs only.	Yes, but for ISPs only.
Affirmative Defense/Safe Harbor	Person is not liable if the person has established and implemented, with due care, reasonable practices and procedures to prevent violations, and violation occurred despite good faith efforts to comply, or if, within 2-days ending upon the initiation of the transmission that is in violation, such person initiated the transmission of such message, or one substantially similar to it, to less than 1,000 e-mail addresses.	It is an affirmative defense against charges that a commercial e-mail message falsifies the sender's identity if the defendant sent fewer than 100 such messages during any 30-day period.	NA
Enforcement	By FTC	By FTC and U.S. Attorney General.	By FTC and U.S. Attorney General.
State action allowed	NA	Yes, but not if FTC or Attorney General already has commenced an action. FTC must be notified in all cases, and may intervene.	Yes, but U.S. district courts, the U.S. courts of any territory, and the D.C. court have exclusive jurisdiction over all civil actions brought by states. State must notify FTC, and FTC may intervene.

Provision	H.R. 1933 (Lofgren)/S. 1326 (Corzine)	H.R. 2214 (Burr-Tauzin-Sensenbrenner)	H.R. 2515 (Wilson)
Class action suits allowed	NA	No	NA
Effect on ISPs	ISPs may bring civil action in U.S. district court. Does not change law regarding when ISP may disclose customer communications or records; does not require ISP to block, transmit, route, relay, handle or store certain types of e-mail; does not prevent or limit ISP from adopting a policy regarding commercial e-mail including declining to transmit certain commercial e-mail; and does not render lawful any such policy that is unlawful under any other provision of law.	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.	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, receive or store certain types of e-mail.
Supersedes state and local laws and regulations	State and local governments may not impose civil liabilities inconsistent with Act. The Act does not preempt certain remedies available under certain other federal, state, or local laws.	Yes, with exceptions.	Yes, with exceptions.

NA = Not Addressed

Table 2: Brief Comparison of Pending Spam Legislation in the Senate

Provision	S. 563 (Dayton)	S. 877 (Burns-Wyden) (As ordered reported)	S. 1052 (Nelson-FL)	S. 1231 (Schumer)	S. 1293 (Hatch)	S. 1327 (Corzine)
Title	Computer Owners Bill of Rights Act	CAN SPAM Act	Ban on Deceptive Unsolicited Bulk Electronic Mail Act	SPAM Act	Criminal Spam Act	REDUCE Spam Act
Definition of Commercial E-Mail	None	E-mail whose primary purpose is commercial advertisement or promotion of commercial product or service, with exceptions.	None	E-mail whose primary purpose is to advertise or promote, for a commercial purpose, a commercial product or service.	E-mail whose primary purpose is commercial advertisement or promotion of a commercial product or service.	E-mail whose primary purpose is commercial advertisement or promotion of commercial product or service

Provision	S. 563 (Dayton)	S. 877 (Burns-Wyden) (As ordered reported)	S. 1052 (Nelson-FL)	S. 1231 (Schumer)	S. 1293 (Hatch)	S. 1327 (Corzine)
Definition of Unsolicited Commercial E-mail (UCE)	None	Commercial e-mail sent without the recipient's prior affirmative or implied consent and that is not a transactional or relationship message (as defined in the Act). A visit to a Web site, if the recipient did not knowingly submit his e-mail address, is not a transaction. Affirmative consent means the recipient has expressly consented to receive the message. Implied consent means there has been a business transaction between the sender and recipient within the past 3 years and the recipient was provided at that time with an opt-out opportunity and did not exercise it.	None	Commercial e-mail sent without prior affirmative consent or implied consent, or sent after the recipient has opted-out, with an exception. Affirmative consent means the message falls within the scope of an express and unambiguous invitation or permission granted by the recipient and not subsequently revoked; the recipient knew permission was being granted; and the recipient did not subsequently opt-out. Implied consent means there has been a business transaction between the sender and recipient within the past 3 years and the recipient was provided at that time with an opt-out opportunity and did not exercise it.	None	Commercial e-mail sent without the recipient's prior affirmative or implied consent and that is not a transactional or relationship message. (Affirmative and implied consent are not defined.)

Provision	S. 563 (Dayton)	S. 877 (Burns-Wyden) (As ordered reported)	S. 1052 (Nelson-FL)	S. 1231 (Schumer)	S. 1293 (Hatch)	S. 1327 (Corzine)
Prohibits false or misleading header information	No	Yes, in all commercial e-mail.	Illegal to falsify or forge certain header information.	Yes, in all commercial e-mail.	Yes	Yes, in UCE.
Prohibits deceptive subject headings	No	Yes, in all commercial e-mail.	No	Yes, in all commercial e-mail.	No	Yes, in UCE.
Prohibits false, misleading, or deceptive information in body of message	No	No, but does not affect FTC's authority to bring enforcement actions for materially false or deceptive representations in commercial e-mail.	No	Yes	No	No
Prohibits transmission of e-mail from improperly or illegally harvested e-mail addresses	No	Yes, for unlawful UCE. Also prohibits dictionary attacks and the automated creation of multiple e-mail or on-line accounts from which to transmit, or enable someone else to transmit, UCE.	Prohibits collecting e-mail addresses from public and private spaces for the purpose of transmitting UCE.	Yes, of all commercial e-mail to addresses obtained through illegal harvesting or automated means.	No	No
Prohibits sending e-mails through computers accessed without authorization	NA	Prohibits accessing a computer without authorization and transmitting UCE from or through it.	NA	NA	Prohibits accessing a computer without authorization and transmitting multiple e-mails from or through it.	NA

Provision	S. 563 (Dayton)	S. 877 (Burns-Wyden) (As ordered reported)	S. 1052 (Nelson-FL)	S. 1231 (Schumer)	S. 1293 (Hatch)	S. 1327 (Corzine)
Creates "do not e-mail" registry at FTC	Yes	No, but requires FTC to submit recommendations concerning creation of such a registry.	No	Yes, but "safe harbor" provided if e-mail address has been or list for less than 30 days or person reasonably relied on registry and takes reasonable measures to comply with the Act. FTC to issue regulations for the list, and may create specific categories to protect minors, e.g. regarding e-mail that contains or advertises adult content or links to such content. Senders shall honor such categories without regard to actual or implied consent given by the minor.	No	No
Penalties for falsifying sender's identity	No	No	No	No	Yes	No
Requires FTC-prescribed "warning labels" on sexually oriented material	No	No	No	No, but see provision regarding "do not e-mail" registry (above).	No	No, but see requirements for subject line labels (next).

Provision	S. 563 (Dayton)	S. 877 (Burns-Wyden) (As ordered reported)	S. 1052 (Nelson-FL)	S. 1231 (Schumer)	S. 1293 (Hatch)	S. 1327 (Corzine)
Requires specific characters in subject line of UCE to indicate the message is an advertisement	No	No, but message must provide clear and conspicuous identification that it is an advertisement.	No	Yes, "ADV" must be in subject line, but "safe harbor" provided if the sender is a member of an FTC-approved self regulatory organization and complies with those requirements.	No	Yes, "ADV:" for advertisement; "ADV-ADLT:" for adult-oriented advertisements. Or identification may comply with standards set by Internet Engineering Task Force.
Requires opt-out mechanism	Creates opt-out mechanism through do not e-mail registry.	Commercial e-mail must contain functioning e-mail return address or other Internet-based mechanism to which the recipient may opt-out.	Person sending UCE must provide recipient clear and conspicuous opportunity to request to opt-out.	All commercial e-mail, including UCE, must have functioning e-mail address or other Internet-based mechanism to which the recipient may opt-out.	No	UCE must contain valid sender-operated return e-mail address to which recipient may opt-out.
Damages or Penalties	Up to $10,000 per violation	Varies per violation.	Civil penalties and fines to be set in accordance with 18 U.S.C.	Varies per section of Act.	Establishes civil and criminal penalties which vary per specifics of the violation.	To be set by FTC, except that under private right of action, statutory damages of up to $10 per violation.
Penalties for persons who promote their trade, business, goods, products, etc. in e-mail that violates Act, under specific circumstances	NA	Yes	NA	NA	NA	NA

Provision	S. 563 (Dayton)	S. 877 (Burns-Wyden) (As ordered reported)	S. 1052 (Nelson-FL)	S. 1231 (Schumer)	S. 1293 (Hatch)	S. 1327 (Corzine)
Reward for first person identifying a violator and supplying information leading to the collection of a civil penalty	No	No	No	No	No	Yes, not less than 20% of the penalty.
Private Right of Action	No	No	No	Recipient adversely affected may, if otherwise permitted by laws or rules of State court, bring, in an appropriate court of the State, an action to enjoin further violation and recover damages.	ISPs may bring civil action in U.S. District Court.	Yes. Recipient of UCE or ISP may bring civil action in a U.S. district court to enjoin further violations and recover damages.

Provision	S. 563 (Dayton)	S. 877 (Burns-Wyden) (As ordered reported)	S. 1052 (Nelson-FL)	S. 1231 (Schumer)	S. 1293 (Hatch)	S. 1327 (Corzine)
Affirmative Defense/Safe Harbor	NA	Person is not liable if the person has established and implemented, with due care, reasonable practices and procedures to prevent violations, and violation occurred despite good faith efforts to comply.	NA	Establishes "safe harbors" as noted above.	No	Person is not liable if the person has established and implemented, with due care, reasonable practices and procedures to prevent violations, and violation occurred despite good faith efforts to comply, or if, within 2-days ending upon the initiation of the transmission that is in violation, such person initiated the transmission of such message, or one substantially similar to it, to less than 1,000 e-mail addresses.

Provision	S. 563 (Dayton)	S. 877 (Burns-Wyden) (As ordered reported)	S. 1052 (Nelson-FL)	S. 1231 (Schumer)	S. 1293 (Hatch)	S. 1327 (Corzine)
Enforcement	By FTC.	By FTC, except for certain entities that are regulated by other agencies.	Violation considered a predicate offense under RICO and an unfair or deceptive practice under FTC Act.	By FTC, except for certain entities that are regulated by other agencies.	By the Attorney General.	By FTC.
State action allowed	NA	Yes, but must notify FTC or other appropriate regulator, which may intervene.	NA	Yes, but must notify FTC, which may intervene.	NA	NA
Class action suits allowed	NA	NA	NA	No	NA	NA

Provision	S. 563 (Dayton)	S. 877 (Burns-Wyden) (As ordered reported)	S. 1052 (Nelson-FL)	S. 1231 (Schumer)	S. 1293 (Hatch)	S. 1327 (Corzine)
Effect on ISPs	NA	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.	NA	ISPs may bring civil action in U.S. district court. Senders of commercial e-mail including UCE must comply with ISP policies with respect to electronic mail, account registration and use, or other terms of service.	ISPs may bring civil action in U.S. district court.	ISPs may bring civil action in U.S. district court. Does not change law regarding when ISP may disclose customer communications or records; does not require ISP to block, transmit, route, relay, handle or store certain types of e-mail; does not prevent or limit ISP from adopting a policy regarding commercial e-mail including declining to transmit certain commercial e-mail; and does not render lawful any such policy that is unlawful under any other provision of law.
Supersedes state and local laws and regulations	NA	Yes, with exceptions.	NA	NA	NA	NA

NA = Not addressed
RICO = Racketeer Influenced and Corrupt Organizations Act