AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Calendar No. 735

107TH CONGRESS, 2d Session | SENATE | REPORT 107–318

CONTROLLING THE ASSAULT OF NON-SOLICITED PORNOGRAPHY AND MARKETING ACT OF 2002, OR THE "CAN-SPAM ACT OF 2002"

R E P O R T

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ON

S. 630

OCTOBER 16, 2002.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE

19–010 WASHINGTON : 2002

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

ERNEST F. HOLLINGS, South Carolina, *Chairman*

DANIEL K. INOUYE, Hawaii
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
JOHN B. BREAUX, Louisiana
BYRON L. DORGAN, North Dakota
RON WYDEN, Oregon
MAX CLELAND, Georgia
BARBARA BOXER, California
JOHN EDWARDS, North Carolina
JEAN CARNAHAN, Missouri
BILL NELSON, Florida

JOHN MCCAIN, Arizona
TED STEVENS, Alaska
CONRAD BURNS, Montana
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
SAM BROWNBACK, Kansas
GORDON SMITH, Oregon
PETER G. FITZGERALD, Illinois
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia

KEVIN D. KAYES, *Staff Director*
MOSES BOYD, *Chief Counsel*
GREGG ELIAS, *General Counsel*
JEANNE BUMPUS, *Republican Staff Director and General Counsel*
ANN BEGEMAN, *Republican Deputy Staff Director*
ROBERT W. CHAMBERLIN, *Republican Chief Counsel*

Calendar No. 735

107TH CONGRESS, 2d Session | SENATE | REPORT 107–318

CONTROLLING THE ASSAULT OF NON-SOLICITED PORNOGRAPHY AND MARKETING ACT OF 2002, OR THE "CAN-SPAM ACT OF 2002"

OCTOBER 16, 2002.—Ordered to be printed

Mr. HOLLINGS, from the Committee on Commerce, Science, and Transportation, submitted the following

REPORT

[To accompany S. 630]

The Committee on Commerce, Science, and Transportation, to which was referred the bill (S. 630) to prohibit senders of unsolicited commercial electronic mail from disguising the source of their messages, to give consumers the choice to cease receiving a sender's unsolicited commercial electronic mail messages, and for other purposes, having considered the same, reports favorably thereon with an amendment in the nature of a substitute and recommends that the bill (as amended) do pass.

PURPOSE OF THE BILL

The purpose of this legislation is to allow consumers the option to decline to receive unsolicited electronic mail (e-mail) from commercial sources. The bill would require senders of unsolicited commercial e-mail (UCE) to include accurate return address or "header" information to identify the sender. The legislation would mandate that senders of UCE provide an Internet-based system for consumers to opt-out of receiving further unsolicited messages from that sender. It would also require the sender to include a physical address in the e-mail itself for identification and opt-out purposes. Criminal sanctions could be imposed on parties who intentionally disguise the source of their UCE messages by falsifying header information. Civil sanctions would be available for other violations of the bill.

BACKGROUND AND NEEDS

UCE, commonly known as "spam," has quickly become one of the most pervasive intrusions in the lives of Americans who use e-mail. Software industry analysts report that approximately 15 percent of all e-mail traffic is spam. Unlike unsolicited postal mail, spam can be sent in massive volumes for very little additional cost, so the volume of spam has been rising exponentially—by some estimates, more than doubling every 6 months. As a result, e-mail users are forced to deal with a deluge of unsolicited, and in most instances unwanted, advertisements in their computer e-mail in-boxes.

The inconvenience and intrusiveness of spam is exacerbated by the fact that, in many instances, the senders of UCE purposefully disguise the source of the e-mail or include misleading information in the e-mail's subject line. Thus, the recipient is left with no effective ability to manage the inflow of spam—he or she cannot easily tell who is sending the messages, what they contain, or how to contact the sender to instruct him or her to take the recipient off the mailing list.

Moreover, the Federal Trade Commission (FTC) has noted that many unsolicited e-mail messages contain indecent, misleading, or fraudulent content. Common types of fraudulent spam promote chain letters, pyramid schemes, stock and investment scams, and so forth. Also common is spam with pornographic content or links to websites with pornographic content, which some recipients may find offensive and may place additional burdens on parents to more closely monitor their children's e-mail.

Spam imposes economic burdens as well. Massive volumes of spam can clog a computer network, slowing Internet service for those who share that network. Internet service providers (ISPs) must respond to rising spam volumes by investing in equipment to increase capacity, and the costs of such investments ultimately get passed on to the consumers that ISPs serve. Meanwhile, individual consumers and businesses are forced to spend time sorting through crowded e-mail in-boxes and deleting unwanted messages. Additionally, some consumers may be assessed fees based on the amount of time they spend online, which would include time they spend deleting junk e-mail. Left unchecked, spam may significantly undermine the usefulness and efficiency of e-mail as a communications tool.

The CAN-SPAM Act, S. 630, aims to address the problem of spam by creating a Federal statutory regime that would give consumers the right to demand that a spammer cease sending them messages, while creating civil and criminal sanctions for the sending of spam meant to deceive recipients as to its source or content. Under the legislation, enforcement would be undertaken by the FTC and, in some cases, industry-specific regulatory authorities. In addition, the bill would enable State attorneys general and ISPs to bring actions against violators.

LEGISLATIVE HISTORY

Senators Burns and Wyden introduced S. 630 on March 27, 2001. The bill is cosponsored by Senators Lieberman, Landrieu, Torricelli, Breaux, Murkowski, Allen, Snowe, Thomas, Hutchinson, and Stevens. On April 26, 2001, the Subcommittee on Communica-

tions held a hearing chaired by Senator Burns on the proliferation of UCE and methods to provide consumers meaningful solutions to opt out of receiving it. A diverse group of associations and private parties interested in this issue provided testimony. The FTC testified in support of S. 630. On May 17, 2002, the Senate Commerce, Science, and Transportation Committee held an executive session at which S. 630 was considered. The bill was approved unanimously by voice vote and was ordered reported with an amendment in the nature of a substitute offered by Senators Burns and Wyden, and an amendment thereto offered by Senator Boxer regarding the large scale third-party collection or "harvesting" of consumer e-mail addresses from websites.

ESTIMATED COSTS

In accordance with paragraph 11(a) of rule XXVI of the Standing Rules of the Senate and section 403 of the Congressional Budget Act of 1974, the Committee provides the following cost estimate, prepared by the Congressional Budget Office:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, June 24, 2002.

Hon. ERNEST F. HOLLINGS,
Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 630, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2002.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Ken Johnson (for federal costs), Erin Whitaker (for the revenue impact), Angela Seitz (for the state and local impact), and Lauren Marks (for the impact on the private sector).

Sincerely,

BARRY B. ANDERSON
(For Dan L. Crippen, Director).

Enclosure.

S. 630—Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2002

Summary: S. 630 would impose new restrictions on the transmission of unsolicited commercial electronic mail (UCE). The bill would require all senders of UCE to identify the messages as UCE, provide accurate header information, include a functioning return email address, and stop sending messages to recipients who opt not to receive them. In addition, the bill would create criminal penalties for knowingly sending UCE that contains false information in the email's header line.

The provisions of S. 630 would be enforced primarily by the Federal Trade Commission (FTC) under the authorities provided in the Federal Trade Commission Act, which includes assessments of civil penalties for violations of the act. However, agencies such as the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System, the Federal Deposit Insur-

ance Corporation (FDIC), the Office of Thrift Supervision (OTS), the National Credit Union Administration (NCUA), the Securities and Exchange Commission (SEC), and the Secretary of Transportation would enforce the bill as it applies to businesses within the agencies' respective jurisdictions. These agencies would punish violations of the bill's provisions with civil and criminal penalties.

CBO estimates that implementing S. 630 would cost about $2 million in 2003 and about $1 million a year in 2004 and thereafter, assuming appropriation of the necessary amounts. CBO estimates that civil penalties collected as a result of enacting this bill would increase governmental receipts (revenues) by about $3 million a year over the 2003–2012 period. The bill also would have additional effects on revenues and direct spending by imposing costs on banking regulators and by creating new criminal penalties. However, CBO estimates that these additional effects would be negligible. Because the bill would affect both receipts and direct spending, pay-as-you-go procedures would apply.

S. 630 would impose an intergovernmental mandate as defined in the Unfunded Mandates Reform Act (UMRA) because it would preempt certain state and local laws that regulate the use of electronic mail to send commercial messages. CBO estimates that complying with that mandate would result in no direct costs to state and local governments and thus would not exceed the threshold established by that act ($58 million in 2002, adjusted annually for inflation).

S. 630 would impose private-sector mandates as defined by UMRA by requiring that senders of commercial electronic mail include certain information within their messages. Based on information provided by government and industry sources, CBO expects that the direct costs of complying with the mandates would fall well below the annual threshold established by UMRA ($115 million in 2002, adjusted annually for inflation).

Estiamted cost to the Federal Government; The estimated budgetary impact of S. 630 is shown in the following table. The costs of this legislation fall within budget function 370 (commerce and housing credit).

	By fiscal year, in millions of dollars—				
	2003	2004	2005	2006	2007
CHANGES IN FTC SPENDING SUBJECT TO APPROPRIATION [1]					
Estimated Authorization Level [2]	2	1	1	1	1
Estimated Outlays	2	1	1	1	1
CHANGES IN REVENUES					
Estimated Revenues	1	3	3	3	3

[1] S. 630 also would increase direct spending by less than $500,000 a year.

[2] The FTC received a gross 2002 appropriation of $156 million. This amount will be offset by an estimated $108 million in fees the FTC collects for merger reviews.

Basis of estimate: S. 630 would require that the FTC enforce the provisions of the bill under the Federal Trade Commission Act. Based on information from the FTC, CBO excepts that the agency would need to upgrade its database of UCE complaints, hire additional staff to investigate possible violations, and assist companies attempting to comply with the bill's provisions. CBO estimates that these activities would cost $2 million in 2003 and $1 million a year

in subsequent years, assuming appropriation of the necessary amounts.

S. 630 would create a variety of new civil and criminal penalties, which are classified in the budget as governmental receipts (revenues). The FTC would enforce the bill with civil penalties using its authority under the Federal Trade Commission Act. Based on information from the FTC, CBO estimates that these enforcement efforts would cause revenues to rise by $3 million a year under the bill. The bill also would create new criminal penalties and authorize other agencies, including the SEC and the Department of Transportation, to enforce the bill's provisions on industries within their jurisdictions using both civil and criminal penalties. However, CBO estimates that the effect of those additional provisions on revenues would not be significant in any year.

Collections of criminal fines are deposited in the Crime Victims Fund and spent in subsequent years. Because any increase in direct spending would equal the amount of fines collected (with a lag of one year or more), the additional direct spending also would be negligible.

The OCC, NCUA, OTS, FDIC, and the Board of Governors of the Federal Reserve System would enforce the provisions of S. 630 as they apply to financial institutions. The OCC, NCUA, and OTS charge fees to the institutions they regulate to cover all of their administrative costs; therefore, any additional spending by these agencies to implement the bill would have no net budgetary effect. That is not the case with the FDIC, however, which uses insurance premiums paid by all banks to cover the expenses it incurs to supervise state-chartered banks. The bill's requirement that the FDIC enforce the bill's restrictions on UCE sent by these banks would cause a small increase in FDIC spending but would not affect its premium income. In total, CBO estimates that S. 630 would increase net direct spending of the OCC, NCUA, OTS, and FDIC by less than $500,000 a year.

Budgetary effects on the Federal Reserve are recorded as changes in revenues (governmental receipts). Based on information from the Federal Reserve, CBO estimates that enacting S. 630 would reduce such revenues by less than $500,000 a year.

Pay-as-you-go considerations: The Balanced Budget and Emergency Deficit Control Act sets up pay-as-you-go procedures for legislation effecting direct spending or receipts. The net changes inoutlays and governmental receipts that are subject to pay-as-you-go procedures are shown in the following table. (The estimated impact on outlays is less than $500,000 a year.) For the purposes of enforcing pay-as-you-go procedures, only the effects through 2006 are counted.

	By fiscal year, in millions of dollars—										
	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Changes in Outlays	0	0	0	0	0	0	0	0	0	0	0
Changes in Receipts	0	1	3	3	3	3	3	3	3	3	3

Estimated impact on state, local, and tribal governments: S. 630 would impose an intergovernmental mandate as defined in UMRA because it would preempt certain state and local laws that regulate the use of electronic mail to send commercial messages. CBO esti-

mates that complying with that mandate would result in no direct costs to state and local governments and thus would not exceed the threshold established by that Act ($58 million in 2002, adjusted annually for inflation).

Estimated impact on the private sector: S. 630 would impose private-sector mandates as defined by UMRA by requiring that senders of commercial electronic mail include certain information within their messages. The bill would require that all senders of commercial electronic mail include a valid return electronic mail address and an accurate subject heading within their message. Senders of UCE would further be required to identify their messages as UCE and to include a valid physical postal address within their messages. The bill would specify that the electronic mail address of the UCE sender must remain functioning for at least 30 days after transmission of UCE.

In addition, S. 630 would require persons who send UCE to provide the recipients of their messages with an option to discontinue receiving UCE from the sender and to notify recipients of that option to discontinue in each UCE message. If a recipient makes a request to a sender not to receive some or any UCE messages from such sender, then the sender, or anyone acting on their behalf, would be prohibited from initiating a transmission to the recipient 10 days after the receipt of such a request. Based on information from government and industry sources, CBO estimates that the direct costs of complying with the mandates contained in the bill would fall well below the annual threshold established by UMRA for private-sector mandates ($115 million in 2002, adjusted annually for inflation).

Previous CBO estimate: On April 13, 2001, CBO transmitted a cost estimate H.R. 718, the Unsolicited Commercial Electronic Mail Act of 2001, as ordered reported by the House Committee on Energy and Commerce on April 4, 2001. Although the two bills are similar, H.R. 718 does not contain the provisions requiring banking regulators to enforce the bill within their jurisdictions. The estimated costs of the bills are very similar, with the only difference reflecting later enactment. In our earlier cost estimate for H.R. 718, CBO included an estimated impact for 2002, based on the assumption that the bill would be enacted near the start of 2002.

Estimate prepared by: Federal Costs: Ken Johnson; Revenues: Erin Whitaker; Impact on State, Local, and Tribal Governments: Angela Seitz; and Impact on the Private Sector: Lauren Marks.

Estimate approved by: Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

REGULATORY IMPACT STATEMENT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee provides the following evaluation of the regulatory impact of the legislation, as reported:

NUMBER OF PERSONS COVERED

S. 630 would provide all individuals using e-mail certain protections from fraudulent or misleading behavior by senders of commercial e-mail, and an opportunity to elect whether or not to receive UCE. Additionally, the legislation would mandate that all

persons who send commercial e-mail meet certain requirements, including proper identification and providing an Internet-based reply system for recipients so they may opt out of future UCE sent by that sender. Therefore, S. 630 would cover all consumers who receive e-mail, and all senders of commercial e-mail.

ECONOMIC IMPACT

The legislation would result in new or incremental costs for senders of commercial e-mail to comply with the legislation's requirements, to the extent that those senders have not already made provisions to prevent fraudulent or misleading headers or subject headings, ensure proper identification of the sender, and provide Internet-based reply mechanisms that allow recipients to choose whether to receive future messages. Certain reports have noted the fairly low cost borne by senders of commercial e-mail and the increased costs that ISPs and their customers pay to handle increasing commercial e-mail traffic. The Committee notes that many direct marketing groups and companies that use commercial e-mail have already implemented Internet-based response systems for recipients. Therefore, many of the costs that would be expected to be incurred from S. 630 have already been absorbed by the marketing and sales industries that send commercial e-mail. However, certain industries with extensive marketing affiliates claim that the costs of integrating opt-out systems network-wide may be significant.

PRIVACY

S. 630 would increase the personal privacy of all users of e-mail by providing them with the ability to decline to receive future UCE from the same sender. S. 630 would also require senders of UCE to identify themselves to the recipients by truthful header information and a mailing address where a recipient can contact the sender, thereby better informing the recipient of the identity of the sender.

PAPERWORK

S. 630 would require the FTC to perform a study, and submit a report to the Congress, within 24 months after the date of enactment of the legislation. The legislation should generate similar amounts of administrative paperwork as other legislation requiring multiple agency enforcement and a report to Congress.

SECTION-BY-SECTION ANALYSIS

Section 1. Short Title

This section would provide that the legislation may be cited as the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2002" or as the "CAN-SPAM Act of 2002."

Section 2. Congressional Findings and Policy

This section cites the marketing benefits commercial e-mail can provide to businesses advertising on the Internet, but emphasizes that the ability to send virtually unlimited amounts of UCE could force recipients to waste substantial time and resources reviewing and discarding such e-mail. In addition, huge volumes of UCE could impose significant costs to ISPs via system upgrades to han-

dle the volume of spam sent to end users, who ultimately would bear the costs of those upgrades through increased service rates. This section also states that an increasing number of spammers purposefully include misleading information in subject lines, and that some UCE contains material that recipients may consider vulgar or pornographic in nature. In light of the increased amount of UCE, the section finds that unless there is a reliable method by which consumers can refuse to accept such e-mail, the benefits of the Internet may be diminished. Because of the impact on Internet commerce, the section also states that there is a substantial government interest in regulating UCE to ensure such e-mail messages are not misleading as to their source and that recipients have a right to decline UCE from the same source.

Section 3. Definitions

This section would define terms used throughout the bill, some of which have a specific contextual meaning in the statutory regime created by the legislation. The following definitions included in S. 630 are of particular importance:

AFFIRMATIVE CONSENT.—The term "affirmative consent" means that the message is being sent with the express consent, or at the express direction, of the recipient. Pursuant to this definition, affirmative consent is intended to require some kind of active choice or selection by the recipient; merely remaining passive, as in the case where a consumer fails to modify a default setting expressing consent, is not a sufficient basis for affirmative consent. However, this definition does not require consent on an individual, sender-by-sender basis. A recipient could affirmatively consent to messages from one particular company, but could also consent to receive either messages on a particular subject matter (e.g., gardening products) without regard to the identity of the sender, or messages from unnamed marketing partners of a particular company. All of these are examples of ways consumers could provide affirmative consent under the provisions of the legislation.

COMMERCIAL ELECTRONIC MAIL MESSAGE.—The term "commercial electronic mail message" means any electronic mail message where the primary purpose is the commercial advertisement or promotion of a product or service. This definition is intended to cover marketing e-mails. Advertisements for content on an Internet website operated for a commercial purpose are included within the definition because an e-mail urging the recipient to visit a particular commercial website is just as much a marketing message as an e-mail urging the purchase of a specific product or service. However, the definition is not intended to cover an e-mail that has a primary purpose other than marketing, even if it mentions or contains a link to the website of a commercial company or contains an ancillary marketing pitch. Thus, the definition expressly excludes e-mail messages whose primary purpose is to facilitate, complete, confirm, provide, or request information concerning a preexisting transaction or relationship. For example, an e-mail message providing a monthly bank account statement to the recipient, or providing a product recall notice, would not be considered a commercial electronic mail message under the legislation, even

if the message includes at the bottom some promotional information about the sender's other products.

HEADER INFORMATION.—The term "header information" means the source, destination, and routing information attached to the beginning of an e-mail message, including the originating domain name and originating e-mail address.

IMPLIED CONSENT.—The term "implied consent," in reference to a commercial e-mail message, means that two requirements are met. First, a business transaction, between the sender and recipient, must have occurred within a 3-year period ending upon receipt of the message. A business transaction may include a transaction involving the provision, free of charge, of information, goods, or services requested by the recipient. However, it is intended that merely visiting a free website and browsing its content does not constitute a "transaction" for purposes of this definition. Second, the recipient of the message must have been given clear and conspicuous notice of an opportunity not to receive UCE from the sender and has not exercised that opportunity. Unlike affirmative consent, implied consent does not require an active choice or request by the recipient, so long as the recipient has the been given the ability via conspicuous notice to decline receiving additional messages from the sender.

INITIATE.—The term "initiate," in reference to a commercial e-mail message, means to originate or procure the origination of such e-mail message. Thus, if one company hires another to handle the tasks of composing, addressing, and coordinating the sending of a marketing appeal, both companies could be considered to have initiated the message—one for procuring the origination of the message, the other for actually originating it. However, the definition specifies that a company that merely engages in routine conveyance, such as an ISP that simply plays a technical role in transmitting or routing a message and is not involved in coordinating the recipient addresses for the marketing appeal, shall not be considered to have initiated the message.

RECIPIENT.—The term "recipient" means an authorized user of the e-mail address to which an e-mail message was sent or delivered. If such a user has other e-mail addresses in addition to the address to which the message was sent, each of those addresses will be treated as an independent recipient for purposes of this legislation. For example, a person may have an e-mail address provided by his ISP and also subscribe to a second free e-mail service. Under the legislation, each of these addresses is considered independent, although they are both owned by the same person. Therefore, if an unsolicited commercial message is sent by the same sender to each of the recipient's e-mail addresses and the recipient does not wish to receive future messages, the recipient must opt out for each address. However, if an e-mail address is reassigned to a new user, as may happen after one user gives up an e-mail address in connection with a change in ISP or a change in employer, the new user shall not be treated as a recipient of any commercial e-mail message sent or delivered to that address before it was reassigned.

SENDER.—The term "sender" means a person who initiates a commercial e-mail and whose product, service or Internet web site is advertised or promoted by the message. Thus, if one company hires another to coordinate an e-mail marketing campaign on its behalf, only the first company is the sender, because the second company's product is not advertised by the message.

UNSOLICITED COMMERCIAL ELECTRONIC MAIL MESSAGE.—The term "unsolicited commercial electronic mail message" means any commercial electronic message that is sent to a recipient without the recipient's prior affirmative or implied consent.

Section 4. Criminal Penalty for Unsolicited Commercial Electronic Mail Containing Fraudulent Routing Information

This section would provide misdemeanor criminal liability for intentionally sending UCE with falsified information concerning the transmission or source of the message. The section would amend chapter 63 of title 18, United States Code, to require that a person who sends an unsolicited commercial e-mail, with knowledge and intent that the message contains or is accompanied by header information that is materially false or materially misleading shall be fined or imprisoned for one year, or both. This section further states that header information that includes an originating e-mail address, the use of which was not authorized by the legitimate holder of the address, or access to which was obtained by means of false or fraudulent pretense or representations, would be considered materially misleading. This provision is intended to address the situation where a spammer hacks into, or upon false pretenses obtains access to, an innocent party's e-mail account and uses it to send out spam.

Section 5. Other Protections Against Unsolicited Commercial Electronic Mail

This section contains the bill's principal requirements for senders of UCE, violations of which would not be criminal but would be unfair or deceptive acts or practices enforced by the FTC and other Federal agencies.

Section 5(a)(1) would prohibit falsified transmission information. Specifically, it would be unlawful to send a commercial e-mail message that contains or is accompanied by header information (source, destination and routing information) that is materially or intentionally false or misleading. As in section 4, if the sender includes an e-mail address in the header that was not authorized by the legitimate holder of that address, or if access to an e-mail address was obtained fraudulently, the commercial e-mail would be considered materially misleading. The intent of this subsection is to eliminate the use of inaccurate originating e-mail addresses that disguise the identities of the senders.

Section 5(a)(2) would prohibit the knowing use of deceptive subject headings in commercial e-mail messages. The test is whether the sender knows that the subject heading would be likely to mislead a reasonable recipient about a material fact regarding the content or subject matter of the message. Thus, minor typographical

errors or truly accidental mislabeling should not give rise to liability under this section.

Section 5(a)(3) would require that when a commercial e-mail is unsolicited, the message must have a functioning return e-mail address or other Internet-based reply mechanism (such as a link to a web page at which a user can "click" to select e-mail options) through which a recipient can opt out of future messages. The return address, or other Internet-based reply mechanism, must remain capable of receiving communications from the recipient of the UCE for at least 30 days from the date of the original e-mail. The temporary inability of a return address to accept e-mails due to a technical or capacity problem would not be a violation of the law if the problem is corrected within a reasonable time period. It is recognized that computer systems are fallible on occasion, and this exception is intended to protect senders of UCE who act in good faith to receive opt-out messages but are unable do to so because of these occasional system failures. It is expected that these failures will be corrected in a time that is deemed reasonable to effect the necessary repairs according to industry standards and practice. Senders that do not make repairs in a reasonable time would be considered in violation of the law and subject to penalties. Subparagraph (B) is intended to make clear that the opt-out mechanism required by the subsection would not need to be an "all or nothing" proposition. A recipient must have the option of declining to receive all further messages, but a sender could also give the recipient the option of receiving some types of messages but not others.

Section 5(a)(4) would require that once a sender receives a request from a recipient to not send any more UCE, the sender must cease the transmission of UCE to that recipient within 10 days of receiving the recipient's request. This 10-day window also applies to any person acting on behalf of the sender to initiate the transmission of the UCE, or any person who provides or selects e-mail addresses for the sender, so long as those persons know that a request to cease the messages was made by the recipient. Those persons cannot avoid liability under this section by consciously avoiding knowing that a recipient requested to opt out of receiving unsolicited commercial messages. The intent of this requirement is to ensure that persons providing e-mail marketing services would be responsible for making a good faith inquiry of their clients (the senders, under the definitions of this bill) to determine whether there are recipients who should not be e-mailed because they have previously requested not to receive e-mails from that sender. E-mail marketers who willfully remain unaware of prior recipient opt-outs would not be excused from liability under this legislation.

Section 5(a)(5) would require UCE to contain clear and conspicuous identification that the e-mail is an advertisement or solicitation. The section would also require clear and conspicuous notice of the opportunity to decline receiving further unsolicited commercial e-mail, and would require the inclusion of a valid physical postal address for the sender.

Section 5(b) would address the activity known as "address harvesting." This section would make it an additional violation of the law to initiate UCE to a recipient whose address was obtained, using an automatic address gathering program or process, from a

website or proprietary online service that has a policy of not sharing its users' e-mails for purposes of sending spam.

Section 5(c) would create an affirmative defense for senders of UCE in certain circumstances. A person would not be considered in violation of sections 5(a) (2), (3), (4), or (5) if that person has adopted reasonable practices and procedures to prevent violations and has made good faith efforts to maintain compliance with the bill's provisions. The affirmative defense is intended to protect those persons who have preventative practices in place but through unforeseen circumstances find themselves in violation. It is expected that persons who regularly fail to comply with the bill's provisions would not meet the requirements of reasonable practices or procedures, nor be able to make a clear showing of good faith efforts to be compliant.

Section 6. Enforcement by the Federal Trade Commission

Sections 6(a) and 6(d) prescribe that section 5 would be enforced by the FTC under section 18 of the FTC Act (15 U.S.C. 41 et seq.) as if the violation were an unfair or deceptive act or practice. The Commission would be required to prevent persons from violating this legislation in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the FTC Act were incorporated and made a part of this legislation. Therefore, all the jurisdictional, remedial, and civil enforcement provisions of the FTC Act would be applicable to commercial e-mail under the provisions of this legislation.

Sections 6(b) and 6(c) provide for enforcement by other agencies for entities subject to their jurisdiction due to the jurisdictional limitations of the FTC. These agencies include the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Department of Transportation, the Department of Agriculture, the Farm Credit Administration, the Securities and Exchange Commission and the Federal Communications Commission, for those entities subject to their jurisdiction. Under section 6(c), these agencies and the others set forth in section 6(b), may exercise authority provided by their own statutory grants to enforce the substantive provisions of this legislation.

Section 6(e) would grant State attorneys general the right to bring a civil action for violations of section 5. A State may bring an action in parens patriae for aggrieved citizens of the State in Federal district court to obtain injunctive relief or recover actual or statutory damages, whichever is greater. Statutory damages under this section are up to $10 per unlawful message, with the precise per message amount set by the court based on the degree of culpability and other equitable factors. For any violation of section 5, the maximum total amount of damages would be capped at $500,000. If the court finds violations of section 5 were committed willfully or knowingly, the legislation would allow the maximum damages to be increased up to $1,500,000. Reasonable attorneys' fees would be awarded to the State for a successful action.

Section 6(f) would allow a provider of Internet access service adversely affected by a violation of section 5 to bring a civil action in Federal district court. This could include a service provider who carried unlawful spam over its facilities, or who operated a website

or online service from which recipient e-mail addresses were harvested in connection with a violation of section 5(b). The provider may obtain injunctive relief or actual or statutory damages calculated in the same manner as section 6(e). The court would be permitted to assess the costs of such an action, including reasonable attorneys' fees, against any party.

Section 7. Effects on Other Laws

Section 7(a) would limit the effect the legislation would have on current Federal statutes. It clarifies that nothing in the legislation should be construed to interfere with the enforcement of the provisions of the Communications Act of 1934 relating to obscenity, or sexual exploitation of children, or the FTC Act for materially false or deceptive representations in commercial e-mail messages.

Section 7(b)(1) sets forth the general rule concerning the preemption of State law by the legislation. The legislation would supersede State and local statutes, regulations, and rules regulating the use of e-mail to send commercial messages. Given the inherently interstate nature of e-mail communications, the Committee believes that the creation of one, national standard would be beneficial to consumers, businesses, and regulators. Section 7(b)(2) of the legislation would create exceptions to the general rule in section 7(b)(1), providing that the legislation would not preempt any civil action under State trespass, contract or tort law, or any Federal or State criminal law or civil remedy that relates to acts of computer fraud perpetrated by means of the unauthorized transmission of unsolicited commercial e-mail.

Section 7(b)(3) would clarify the scope of the exceptions set forth in 7(b)(2). Section 7(b)(3) is included to ensure that the preemptive effect of this bill could not be evaded by State enactment of a law that seeks to regulate UCE but simply uses a different label, such as fraud or trespass. To prevent such an evasion, section 7(b)(3) would limit the section 7(b)(2) exceptions so that State and local statutes would not be exempted from preemption if they treat the mere act of sending UCE as a sufficient basis for liability. Thus, section 7(b)(3) would clarify that this bill would preempt State laws that are simply re-titled efforts to impose a regulatory regime on UCE that differs from the regime imposed by this legislation, such as a law that makes it an unlawful "trespass" to transmit UCE without including the sender's phone number.

Section 7(b)(3), however, is a narrow limitation. It would not require preemption of State trespass, contract, tort, and computer fraud laws under any circumstances that those laws are used to sue senders of unsolicited commercial e-mail. For example, the provision would not apply to State or local contract or trespass laws that allow Internet access providers to sue senders of UCE for violations of the providers' terms of use. Nor does the provision apply to the enforcement of State fraud laws against senders of UCE if the content of the e-mail message is fraudulent or the means of transmission of the e-mail involves fraudulent or deceptive acts, such as using fraudulent pretenses to gain unauthorized access to an e-mail account from which to send UCE. In such cases, the State laws in question do not make the mere sending of an unsolicited commercial e-mail a sufficient basis for liability. Instead, liability rests on the sending of the e-mail plus some other action,

such as violation of contractual terms, acts of fraud or deception in connection with initiating the transmission of the e-mail, or inclusion of fraudulent content in the e-mail message.

Section 7(c) would clarify that this legislation would have no impact on the lawfulness of ISPs' efforts to filter or block e-mails traversing their systems.

Section 8. Study of Effects of Unsolicited Commercial Electronic Mail

This section would require the FTC, in consultation with the Department of Justice and other appropriate agencies, to submit a report to Congress within 24 months after enactment of this legislation, on the effectiveness and enforcement of the provisions of this legislation and any modifications to the legislation which may be considered appropriate. The FTC would also be required to include in the report an analysis of the extent to which technological and marketplace developments may affect the practicality and effectiveness of the legislation.

Section 9. Separability

This section states that if any provision or application of a provision of the legislation is held invalid, the remainder of the legislation and application of its provisions will not be affected.

Section 10. Effective Date

This section provides that the provisions of this legislation would take effect 120 days after the date of enactment.

CHANGES IN EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new material is printed in italic, existing law in which no change is proposed is shown in roman):

TITLE 18, UNITED STATES CODE

CHAPTER. 63. MAIL FRAUD

§ 1351. Unsolicited commercial electronic mail containing fraudulent transmission information

(a) IN GENERAL.—Any person who initiates the transmission, to a protected computer in the United States, of an unsolicited commercial electronic mail message, with knowledge and intent that the message contains or is accompanied by header information that is materially false or materially misleading shall be fined or imprisoned for not more than 1 year, or both, under this title. For purposes of this subsection, header information that includes an originating electronic mail address the use of which in connection with the message was not authorized by the legitimate holder of the address, or access to which was obtained by means of false or fraudulent pretense or representations, shall be considered materially misleading.

(b) DEFINITIONS.—Any term used in subsection (a) that is defined in section 3 of the CAN-SPAM Act of 2002 has the meaning given it in that section.

○