

19-010

2003  
108th Congress 1st Session  
SENATE  
Report

108-102

Calendar No. 209

CAN-SPAM ACT OF 2003  
REPORT  
OF THE  
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

on

S. 877

congress.#13

JULY 16, 2003- Ordered to be printed

	?
	<b>SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION</b>
	<b>one hundred eighth congress</b>
	<b>first session</b>
JOHN MCCAIN, Arizona, <i>Chairman</i>	
TED STEVENS, Alaska CONRAD BURNS, Montana TRENT LOTT, Mississippi KAY BAILEY HUTCHISON, Texas OLYMPIA J. SNOWE, Maine SAM BROWNBAC, Kansas GORDON SMITH, Oregon PETER G. FITZGERALD, Illinois JOHN ENSIGN, Nevada GEORGE ALLEN, Virginia JOHN E. SUNUNU, New Hampshire	ERNEST F. HOLLINGS, South Carolina 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 BARBARA BOXER, California BILL NELSON, Florida MARIA CANTWELL, Washington FRANK LAUTENBERG, New Jersey
JEANNE BUMPUS, <i>STAFF DIRECTOR AND GENERAL COUNSEL</i>	
ANN BEGEMAN, <i>DEPUTY STAFF DIRECTOR</i>	

ROBERT W. CHAMBERLIN, <i>CHIEF COUNSEL</i>
KEVIN D. KAYES, <i>DEMOCRATIC STAFF DIRECTOR</i>
GREGG ELIAS, <i>DEMOCRATIC GENERAL COUNSEL</i>

(ii)

**Calendar No. 209**

**108TH CONGRESS**

*Report*

**SENATE**

1st Session

108-102

--CAN-SPAM ACT OF 2003

JULY 16, 2003- Ordered to be printed

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

**R E P O R T**

[To accompany S. 877]

The Committee on Commerce, Science, and Transportation, to which was referred the bill (S. 877) to regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet, 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 purposes of this legislation are to: (i) prohibit senders of electronic mail (e-mail) for primarily commercial advertisement or promotional purposes from deceiving intended recipients or Internet service providers as to the source or subject matter of their e-mail messages; (ii) require such e-mail senders to give recipients an opportunity to decline to receive future commercial e-mail from them and to honor such requests; (iii) require senders of unsolicited commercial e-mail (UCE) to also include a valid physical address in the e-mail message and a clear notice that the message is an advertisement or solicitation; and (iv) prohibit businesses from knowingly promoting, or permitting the promotion of, their trade or business through e-mail transmitted with false or misleading sender or routing information.

**BACKGROUND AND NEEDS**

Unsolicited commercial e-mail, commonly known as `spam', has quickly become one of the most pervasive intrusions in the lives of Americans. 1

[Footnote]

[Footnote 1: The history of how the word `spam' became synonymous with UCE was printed in Computerworld on April 5, 1999, as follows: `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.']

Approximately 140 million Americans, or nearly half of all United States citizens, regularly use e-mail, including 63 percent of full-time or part-time workers, according to the Pew Internet & American Life Project. The ease of obtaining large lists of these e-mail addresses has made e-mail a popular means for individuals, organizations, and businesses to market goods and services to consumers. Unlike direct mail delivered through the post office to consumers, however, UCE can reach millions of individuals at little to no cost and almost instantaneously. Noting its effectiveness, the Direct Marketing Association has reported that 37 percent of consumers it surveyed have bought something as a result of receiving unsolicited e-mail from marketers. However, in addition to legitimate businesses that wish to use commercial e-mail as another channel for marketing products or services, spam has become a favored mechanism of those who seek to defraud consumers and make a living by preying on unsuspecting e-mail users and those new to the Internet. As a result, Americans using e-mail, whether new users or those who have used it for decades, are finding their e-mail in-boxes deluged with unsolicited, and in most instances unwanted, promotions and advertisements that increasingly contain fraudulent and other objectionable content.

In an April 2003 report entitled, *False Claims in Spam*, the Federal Trade Commission (FTC) found that 66 percent of all spam contains some kind of false, fraudulent, or misleading information, either in the e-mail's routing information, its subject line, or the body of its message. The FTC also determined that most spam messages can generally be grouped into one of several major categories, such as those promoting: investment or get-rich-quick 'opportunities' (20 percent); pornographic websites or adult-oriented material (18 percent); credit card or financial offers (17 percent); and health products and services (10 percent).

### *Rapidly Increasing Volume Of Spam*

The volume of spam has been rapidly increasing year after year and today accounts for over 46 percent of all global e-mail traffic. Many Internet analysts expect the volume of spam to exceed 50 percent of all e-mail by the end of 2003, and possibly sooner. By contrast, in September 2001, spam only accounted for 8 percent of all e-mail sent worldwide, and just 18 percent of all e-mail as late as April 2002. However, over the past year, the rate at which spam is increasing has surpassed most observers' previous expectations and is reaching critically high levels.

As of May 2003, the largest Internet service provider (ISP), America Online, was blocking up to 2.4 billion spam messages each day, or approximately 80 percent of its 3 billion daily inbound e-mails. This number of blocked messages was up from 1 billion per day only 2 months beforehand, and 500 million per day in December 2002. Microsoft, the country's second-largest e-mail provider, also reported this past May that its MSN mail and Hotmail services combined block up to 2.4 billion spam messages each day. Earthlink, the third largest ISP in the United States, reported a 500 percent increase in inbound spam over the past 18 months. With many more similar reports in recent months, the sheer volume of spam is threatening to overwhelm not only the average consumer's in-box, but also the network systems of ISPs, businesses, universities, and other organizations. Putting this volume of spam in perspective, *USA Today* recently reported that more than 2 trillion spam messages are expected to be sent over the Internet this year, or 100 times the amount of direct mail advertising pieces delivered by United States mail last year.

IDC, a leading technology industry analysis firm, recently reported that Americans bear the brunt of this increased growth in spam. According to IDC, North America was receiving approximately 3.9 billion spam messages per day out of the 7.3 billion spam messages sent daily around the globe.

### *Deceptive Sender Information and Subject Lines*

The inconvenience and intrusiveness to consumers of large volumes of spam are exacerbated by the fact that, in many instances, the senders of spam purposefully disguise the source or content of the e-mail by falsifying or including misleading information in the e-mail's 'from', 'reply-to', or 'subject' lines. Thus, the recipient is left with no effective ability to manage the constant inflow of spam into an e-mail in-box because he or she cannot often tell without opening the individual messages who is sending the messages or what they contain. Even after opening a message, a consumer often will not be able to ascertain the true identity of the sender. Furthermore, once receiving unwanted messages, most consumers do not have any way to dependably contact the senders to instruct them to take the recipient off their mailing lists.

The FTC found in its recent report that one-third of all spam contains a fraudulent return e-mail address that is included in the routing information (known as the 'header') of the e-mail message. Early on, spam experts believed that fake return addresses were used to entice recipients to reply to spam and ask that their names be removed from the spammers' e-mail lists. Replying like this was thought to confirm to the spammer that the e-mail account was active, but the FTC did not find enough evidence in a previous study to confirm this risk. Regardless, as discussed further below, spammers have much quicker and more automated ways to confirm valid e-mail addresses even before sending out spam. Furthermore, headers continue to be falsified not only to trick ISPs' increasingly sophisticated spam filters, but also to lure consumers into mistakenly opening messages from what appears to be people they know.

One common method of collecting consumers' addresses, known as a 'dictionary attack', involves rapid, short-burst communications with the target ISP's server (known as 'pinging' the server) with automatically-generated, recipient e-mail addresses in alphabetical (or dictionary) order. In this attack, the spammer's software will record which

addresses cause the server to respond positively that it is ready to accept e-mail for a tested recipient e-mail address. Each positive response from the server confirms a valid address at the target ISP, and the addresses are collected into a list that is used to send a block of spam to that server at a later time. Another common method of obtaining consumers' e-mail addresses is to capture them from websites where users post their addresses in order to communicate with other users of the website. This practice, known as e-mail address `harvesting', is often done by automated software robots that scour the Internet looking for and recording posted e-mail addresses.

Additionally, many spam messages contain `web bugs' or other hidden technological mechanisms to immediately notify a spammer via the Internet when an unsolicited message has been opened. Far short of replying to a spam message, a consumer's mere act of opening a spam message containing a web bug may eventually cause that consumer to receive more spam as a result of confirming to the spammer his or her willingness or susceptibility to open unsolicited e-mail.

In addition to false sender information, spammers often lure consumers to open their e-mail by adding appealing or misleading e-mail subject lines. The FTC reported that 42 percent of spam contains misleading subject lines that trick the recipient into thinking that the e-mail sender has a personal or business relationship with the recipient. Typical examples are subject lines such as `Hi, it's me' and `Your order has been filled'. Moreover, e-mail messages with deceptive subject lines may still lead unsuspecting consumers to websites promoting completely unrelated products or even scams, such as pornography or get-rich-quick pyramid schemes.

Pornographic spam is more likely than other spam to contain fraudulent or misleading subject lines. In its recent report, the FTC found that more than 40 percent of all pornographic spam either did not alert recipients to images contained in the message or contained false subject lines, thus `making it more likely that recipients would open the messages without knowing that pornographic images will appear.' Unsuspecting children who simply open e-mails with seemingly benign subject lines may be either affronted with pornographic images in the e-mail message itself, or automatically and instantly taken--without requiring any further action on their part (like clicking on a link)--to an adult web page exhibiting sexually explicit images.

Compounding these problems is the fact that nearly all spam being sent today is considered untraceable back to its original source without extensive and costly investigation. Although many ISPs try to locate spammers in order to shut down their operations, spammers can rather easily disguise their whereabouts, quickly move to other ISPs, or set up websites at new domains in order to avoid being caught. In addition, FTC Chairman Muris and Commissioners Swindle and Thompson each testified in hearings before the Committee this past spring to the FTC's tremendous difficulty in tracking and finding spammers who send out spam with fraudulent transmission information. In response to members who questioned the FTC's effectiveness in reducing the volume of spam, Chairman Muris testified that their investigations are more effective when `following the money' through the business promoted in the e-mail message to the spammer.

Testimony provided to the Committee by Brightmail Inc., a leading company in anti-spam technology and services for ISPs and corporations, supported the FTC's findings by concluding that nearly 90 percent of all of the spam sent worldwide is `untraceable' to its actual source. Of the spam that does `claim' (in its header information) to come from a certain region of the world, the overwhelming majority of it is sent through computer e-mail servers in countries outside of North America. 2

[Footnote] According to the routing information of the spam Brightmail has analyzed, approximately 60 percent comes from Internet protocol (IP) addresses assigned to Europe (including 10-12 percent alone from Russia), and 16 percent originates in Asia (with China leading that region). Although North America receives over half of all spam sent each day, only 11 percent of spam claims to emanate from North America.

[Footnote 2: Brightmail analyzes data it collects from its `probe network', more than a million continually monitored e-mail addresses seeded in ISPs around the world. These e-mail addresses never send out e-mail and have never been used in e-commerce, but still attract 300-350 million e-mail messages per month, 100 percent of which can be classified as `unsolicited'.]

Some observers suspect that spammers located in North America account for more of the global spam traffic. These observers argue that data showing a small percentage of spam emanating from North America is merely indicative of sophisticated North American spammers' known practice of sending their messages overseas first to `bounce' them off of misconfigured e-mail servers known as `open relays'--a process that masks the true origin of the message. When successfully used, open relays pass on the e-mail message to intended destinations in the United States while deleting or over-writing the original source information that would give away the spammer's true location. However, because 90 percent of all spam is not easily traceable back to its originating address, consumers, ISPs, government investigators, and spam experts alike are left with only theories about the countries truly responsible as the greatest sources of spam.

#### *Fraudulent Schemes, Privacy Risks, and Objectionable Content*

The FTC has consistently reported that many unsolicited e-mail messages contain fraudulent, misleading, or objectionable content. Common types of fraudulent spam promote

chain letters, pyramid schemes, stock and investment scams, and solicitations for bogus charitable causes, all of which may place consumers' privacy and financial assets at significant risk. Also common is spam with pornographic content or links to websites with pornographic content, which many recipients find offensive and which places additional burdens on parents to constantly monitor their children's e-mail (even when they are already using an ISP's 'parental controls').

Consumers who buy products offered through spam face numerous risks, including the exposure and sharing of sensitive personal information over the Internet, and credit card or identity theft. In a recent example, the FTC filed a complaint against 30 Minute Mortgage Inc., which it claimed used an array of deceptions to lure consumers into sharing their personal financial data. According to the FTC, the company advertised itself as a national mortgage lender and used spam to urge potential customers to complete detailed online loan applications. The applications required consumers to supply sensitive personal information, such as their names, addresses, phone numbers, Social Security numbers, employment information, income, first and second mortgage payments, and asset account types and balances. The company assured consumers that when they submitted the loan applications, their sensitive information would be protected. Instead, the FTC alleges the company and its principals sold or offered to sell thousands of completed applications to nonaffiliated third parties.

Spam also is used to lure unwary users to websites that contain viruses, spyware, or other malicious computer code. Late last year, for instance, an Internet adult entertainment company created a 'Trojan horse' program that was downloaded to unsuspecting users' computers. Users were tricked into accepting the program through a spam message that promised to deliver an electronic greeting card. The downloaded program, however, instead routed users to the company's pornography websites.

Pornographers, long on the cutting edge of technology, have taken to employing increasingly brazen techniques to sell their products and services. As mentioned above, the FTC estimates that 18 percent of all spam is pornographic or 'adult-oriented' material. While not all of such spam contains images, spammers often do send graphic sexual images embedded in the body of spam so that simply upon opening the e-mail message, a user is assaulted with explicit photographs or video images. More frequently, though, spam contains HTML code and a JavaScript applet that together automatically load a pornographic web page as soon as the spam message is either opened or, in some cases, simply 'previewed' in certain e-mail programs' preview panes.

#### *Costs to ISPs, Consumers, and Businesses*

Spam imposes significant economic burdens on ISPs, consumers, and businesses. Left unchecked at its present rate of increase, spam may soon undermine the usefulness and efficiency of e-mail as a communications tool. Massive volumes of spam can clog a computer network, slowing Internet service for those who share that network. ISPs must respond to rising volumes of spam by investing in new equipment to increase capacity and customer service personnel to deal with increased subscriber complaints. ISPs also face high costs maintaining e-mail filtering systems and other anti-spam technology on their networks to reduce the deluge of spam. Increasingly, ISPs are also undertaking extensive investigative and legal efforts to track down and prosecute those who send the most spam, in some cases spending over a million dollars to find and sue a single, heavy-volume spammer.

Though major service providers tend to disagree about the overall monetary impact spam has had on their respective networks, anti-spam initiatives cost providers time and money, and those expenses typically have been passed on as increased charges to consumers. A 2001 European Union study found that spam cost Internet subscribers worldwide \$9.4 billion each year, and *USA Today* reported in April that research organizations estimate that fighting spam adds an average of \$2 per month to an individual's Internet bill. Additionally, some observers expect that free e-mail services (often used by students and employees who obtain free Internet access) will be downsized as the costs of spam increase, which may result in consumers facing significant 'switching costs' as they are forced to migrate to subscription-based services. As reported by the *Boston Globe*, industry analysts are concerned that this trend could influence millions of consumers to abandon the use of e-mail messaging as a viable means of communication.

Spam presents other real costs to consumers who live in remote areas or travel on business when they are forced to spend time sorting through crowded e-mail in-boxes and deleting unwanted messages. Although Internet access through broadband connections is steadily growing, a dial-up modem continues to be the method by which a vast majority of Americans access the Internet and their e-mail accounts. In rural areas, however, dial-up customers may pay per-minute access charges while online or, in some cases, long distance charges for their Internet connection. In addition, business travelers who sign onto e-mail services from remote locations must either pay long-distance fees or elevated per-minute surcharges in hotel rooms. In these cases, deleting spam is more than just a loss of time or productivity; it is actually an additional charge to the consumer or business traveler.

In addition to the costs to ISPs and consumers, recent industry research has focused on the impact of spam's growth on businesses and e-commerce. Ferris Research currently estimates that costs to United States businesses from spam in lost productivity, network system upgrades, unrecoverable data, and increased personnel costs, combined, will top \$10 billion in 2003. Of that total, Ferris estimates that employee productivity losses from sifting through and deleting spam accounts for nearly \$4 billion alone. Recent press reports also indicate that large companies with corporate networks typically spend between \$1 to \$2 per user each month to prevent spam, which is currently estimated to make up

24 percent of such corporations' inbound e-mail. At current growth rates, however, spam could account for nearly 50 percent of all inbound e-mail to large corporations by 2004. Ferris reports that corporate costs of fighting spam today represent a 300 percent increase from 2 years ago, and the Yankee Group estimates that costs to corporations could reach \$12 billion globally within the next 18 months. Based on current spam growth rates, the Radicati Group estimates that, on a worldwide basis, spam could cost corporations over \$113 billion by 2007.

## **SUMMARY OF PROVISIONS**

The CAN-SPAM Act, S. 877, 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.

If enacted, S. 877 would require senders of all commercial e-mail to include a valid return e-mail address and other header information with the message that accurately identifies the sender and Internet location from which the message has been sent. Except for transactional or relationship e-mail messages (as defined therein), the legislation would also require senders of commercial e-mail to provide an Internet-based system for consumers to opt out of receiving further messages from that sender. Moreover, a sender of UCE would be required additionally to include in the e-mail message itself a valid physical address of the sender as well as clear and conspicuous notice that both the message is an advertisement or solicitation and that the recipient may opt out of further UCE from the sender.

S. 877 would also require businesses to ensure that they are not promoted in e-mail sent with false or misleading transmission information. The bill would hold the promoted businesses responsible if they: (i) know or should know about such deceptive promotion; (ii) are receiving or expect to receive an economic benefit from it; and (iii) are taking no reasonable precautions to prevent such promotion or to detect and report it to the FTC.

S. 877 would permit criminal sanctions to be imposed on senders of e-mail who intentionally disguise the source of their messages by falsifying header information. Civil sanctions would also be available for this violation as well as all other violations of the bill. Additionally, aggravated violations would apply to those who violate the provisions of the bill while employing certain problematic techniques used to either generate recipient e-mail addresses, or remove or mask the true identity of the sender.

## **LEGISLATIVE HISTORY**

Senator Burns, the chairman of the Communications Subcommittee, introduced S. 877 on April 10, 2003, with Senator Wyden as an original cosponsor. The bill is also cosponsored by Senators Breaux, Carper, Chambliss, Dodd, Edwards, Gregg, Johnson, Landrieu, Lautenberg, Lieberman, Murkowski, Nelson of Florida, Schumer, Snowe, Stevens, Talent, and Thomas.

S. 877 is based on legislation (S. 630) that was approved and reported out of the Committee during the 107th Congress. In addition to S. 877, 4 other bills relating to spam have been introduced and referred to the Committee during the 108th Congress. The bills are: S. 563, introduced by Senator Dayton; S. 1052, introduced by Senator Nelson of Florida and cosponsored by Senator Pryor; S. 1231, introduced by Senator Schumer and cosponsored by Senator Graham of South Carolina; and S. 1237, introduced by Senator Corzine.

On May 21, 2003, the Committee held a full committee hearing chaired by Senator McCain on the proliferation of spam and options for addressing the threat it poses to consumers, business, ISPs, and the very medium of e-mail. Witnesses at the hearing included two FTC commissioners and a diverse group of companies, associations, and private parties interested in spam. Additionally, several other individuals and organizations provided written testimony for the record.

On June 19, 2003, the Committee held an executive session chaired by Senator McCain at which S. 877 was considered. The bill was approved unanimously by voice vote and was ordered reported with an amendment in the nature of a substitute. Amendments were offered by Senator Burns, to make substantive modifications to the bill as introduced, and also by Senator McCain to make businesses knowingly promoted through e-mail with false or misleading transmission information subject to FTC Act penalties and enforcement.

## **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, July 14, 2003.**

Hon. JOHN MCCAIN,  
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. 877, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Melissa E. Zimmerman (for federal spending), Annabelle Bartsch (for revenues), Victoria Heid Hall (for the state and local impact), and Paige Piper/Bach (for the impact on the private sector).

Sincerely,

Douglas Holtz-Eakin,

*Director.*

Enclosure.

*S. 877--Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003*

Summary: S. 877 would impose new restrictions on the transmission of unsolicited commercial electronic mail (UCE), often referred to as 'spam.' 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 on the email's header line.

The provisions of S. 877 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 Insurance 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. Those agencies would punish violations of the bill's provisions with civil and criminal penalties.

CBO estimates that implementing S. 877 would cost about \$1 million in 2004 and about \$2 million a year in 2005 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 when fully implemented (by 2005). The bill also would have additional effects on revenues and direct spending by imposing costs on banking regulators and by creating new penalties. However, CBO estimates that those additional effects would be negligible.

S. 877 would preempt certain state or local laws that regulate the use of electronic mail to send commercial messages. Such a preemption is a mandate as defined in the Unfunded Mandates Reform Act (UMRA), but CBO estimates that the budgetary impact of the mandate would be minimal and would not exceed the threshold established in UMRA (\$59 million in 2003, adjusted for inflation).

S. 877 would impose private-sector mandates as defined in 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 those mandates would fall below the annual threshold established by UMRA (\$117 million in 2003, adjusted annually for inflation).

Estimated Cost to the Federal Government: The estimated budgetary impact of S. 877 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--

2004 2005 2006 2007 2008  
 -----

CHANGES IN FTC SPENDING SUBJECT TO APPROPRIATION 1

Estimated Authorization Level 2	1	2	2	2	2
---------------------------------	---	---	---	---	---

Estimated Outlays	1	2	2	2	2
-------------------	---	---	---	---	---

CHANGES IN REVENUE

Estimated Revenues	1	3	3	3	3
--------------------	---	---	---	---	---

-----

Basis of estimate: S. 877 would require the FTC to enforce the provisions of the bill under the Federal Trade Commission Act. Based on information from the FTC, CBO expects 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 those activities would cost \$1 million in 2004 and \$2 million a year in subsequent years, assuming appropriation of the necessary amounts.

S. 877 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 those 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. 877 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. 877 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. 877 would reduce such revenues by less than \$500,000 a year.

Estimated impact on state, local, and tribal governments: S. 877 would establish new federal prohibitions on certain types of commercial electronic mail. While the Federal Trade Commission and other federal agencies would generally enforce these prohibitions, in the case of any person engaged in providing insurance, the prohibitions would be enforced under state insurance laws. However, any such state enforcement would be voluntary.

S. 877 would preempt certain state or local laws that regulate the use of electronic mail to send commercial messages. Such a preemption is a mandate under UMRA. CBO estimates that the mandate would have little budgetary impact on state and local governments and would not, therefore, exceed the threshold established in UMRA (\$59 million in 2003, adjusted for inflation).

Estimated impact on the private sector: S. 877 would impose private-sector mandates as defined in the 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 unsolicited commercial electronic mail would further be required to include a valid physical postal address and to identify their messages as UCE within their messages. The bill would require that the electronic-mail address of the UCE sender must remain functioning for at least 30 days after transmission of UCE.

In addition, S. 877 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 the sender's behalf, would be prohibited from initiating the transmission to the recipient starting 10 business days after the receipt of such 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 below the annual threshold established by UMRA for private-sector mandates (\$117 million in 2003, adjusted annually for inflation).

Estimate prepared by: Federal Spending: Melissa E. Zimmerman; Federal Revenues: Annabelle Bartsch; Impact on State, Local, and Tribal Governments: Victoria Heid Hall; and Impact on the Private Sector: Paige Piper/Bach.

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. 877 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. 877 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. 877 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. 877 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. 877 also would 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. S. 877 would furthermore prohibit the unauthorized use of a consumer's e-mail account (also known as 'hijacking') for the purposes of sending out spam. S. 877 also would increase the privacy protection of consumers' e-mail addresses and accounts by outlawing the use of e-mail address collection methods, such as e-mail harvesting and dictionary attacks, when used in connection with the sending of commercial e-mail in violation of S. 877.

### **PAPERWORK**

S. 877 would require the FTC to make recommendations to Congress for a workable plan to create a nationwide marketing Do-Not-E-mail list within 6 months of completing implementation of its national telemarketing Do-Not-Call list. S. 877 would also 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 is expected to generate similar amounts of administrative paperwork as other legislation requiring multiple agency enforcement, recommendations for implementing a program, 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 2003' or as the 'CAN-SPAM Act of 2003'.

### *Section 2. Congressional findings and policy*

This section describes the rising volume of UCE, the threat it poses to e-mail's popularity and utility, the costs it imposes, and a number of practices that spammers commonly use to frustrate recipients' ability to identify and control the flow of UCE. This section also notes that State statutes have not been effective in managing the problem to date, and that Federal legislation will need to be coupled with technological approaches and international cooperation. Based on these findings, this section would, if enacted, express the policy determination that there is a substantial government interest in regulating commercial e-mail on a Federal basis to prevent commercial e-mail that misleads recipients as to the source or content of the message and to ensure that recipients have a way to tell a sender of commercial e-mail to stop.

### *Section 3. Definitions*

This section would define 19 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. 877 are of particular importance:

*Affirmative Consent*- The term 'affirmative consent' means that the message is being sent with the express consent 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. If the recipient's consent was prompted by a request for such consent, as opposed to consent expressed at the recipient's own initiation (as in the case where a consumer wants a product catalogue and e-mails the company to ask for it), then such request must be clear and conspicuous or affirmative consent will not be deemed present. 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. The only limitation on such third-party affirmative consent is that the person granting such consent must have been provided clear and conspicuous notice, at the time such consent is granted, that the person's e-mail address may be transferred to such third parties. The purpose of this limitation is to ensure that consumers are fully informed of the scope of any third-party consent they may grant.

*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.

*Electronic Mail Message*- The term 'electronic mail message' means a message sent to a unique electronic mail address. The definition is intended to apply to the message in the form that it is sent, regardless of whether or in what form it is received. For example, an electronic mail message may be blocked by filtering software, or truncated or altered by some other type of software installed by the recipient or the recipient's Internet service provider. Such downstream effects have no impact on what constitutes the underlying electronic mail message for purposes of this Act.

*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, and any other information that appears in the line purporting to identify the person initiating the message (commonly referred to as the 'from' line).

*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, 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 been given the ability via conspicuous notice to decline receiving additional messages from the sender. The definition also clarifies that a recipient's implied consent may apply only to a particular division or line of business within a particular corporation, rather than the entire corporation, if the corporation represented itself as a particular division or line of business in its dealings with the recipient. The rationale for this is that it would be unfair to read the recipient's implied consent more broadly, when the recipient may not have been aware of the identity of the broader corporation.

*Initiate-* The term `initiate', in reference to a commercial e-mail message, means to originate or transmit, or procure the origination or transmission of, such an e-mail message. More than one person may be considered to have initiated a 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.

*Procure-* The term `procure', when used with respect to the initiation of a commercial electronic mail message, means intentionally to pay or induce another person to initiate the message on one's behalf, while knowingly or consciously avoiding knowing the extent to which that person intends to comply with this Act. The intent of this definition is to make a company responsible for e-mail messages that it hires a third party to send, unless that third party engages in renegade behavior that the hiring company did not know about. However, the hiring company cannot avoid responsibility by purposefully remaining ignorant of the third party's practices. The `consciously avoids knowing' portion of this definition is meant to impose a responsibility on a company hiring an e-mail marketer to inquire and confirm that the marketer intends to comply with the requirements of this Act.

*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. If the second company in this example, however, originates or transmits e-mail on behalf of the first company, then, under the definitions in section 3 of the bill, both companies would be considered to have `initiated' the e-mail, even though only the first company is considered to be the `sender'.

*Transactional or Relationship Message-* The term `transactional or relationship message' means an electronic mail message the primary purpose of which is to: facilitate, complete, or confirm a transaction; provide specified types of information with respect to a product or service used or purchased by the recipient; provide information directly related to a current employment relationship or benefit plan; or deliver goods or services that are included under the terms of a previous transaction. This definition is intended to cover messages directly related to a commercial transaction or relationship that the recipient has already agreed to enter into, such as receipts, monthly account statements, or product recall notices. Such messages could also include some promotional information about other products or services, but only if the promotional material is truly ancillary to a primary purpose listed in this definition.

*Unsolicited Commercial Electronic Mail Message-* The term `unsolicited commercial electronic mail message' means any commercial electronic message that is not a transactional or relationship message and is sent to a recipient without the recipient's prior affirmative or implied consent.

#### *Section 4. Criminal penalty for commercial electronic mail containing fraudulent routing information*

This section would provide misdemeanor criminal liability for intentionally sending commercial electronic mail 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 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 up to 1 year, or both. This section further states that header information that is technically correct but includes an originating e-mail address, the 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 for users of commercial electronic mail*

This section contains the bill's principal requirements for persons initiating commercial e-mail and 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 initiate a commercial e-mail message that contains or is accompanied by header information (source, destination and routing information, 'from' line) that is false or misleading. As in section 4, if the e-mail includes an originating e-mail address in the header the access to which 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 person initiating the message 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 a commercial e-mail 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 recipients 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 was not foreseeable in light of the potential volume of response messages and 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 persons who act in good faith to receive opt-out messages but are unable to do so because of these occasional and accidental system failures. However, the exception is not available to a person who sends out a large volume of commercial e-mail but sets up a reply mechanism with very limited capacity. In such a case, the failure of the system is foreseeable. The exception is also not available to a person who fails to make repairs in a reasonable time. The intent of this exception is to protect against truly accidental outages, not to protect parties who have not made a reasonable and good faith effort to ensure a working opt-out mechanism. 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 business days after receiving the recipient's request. This 10 business-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 will 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. In addition, subparagraph (D) prohibits the sale or other transfer of the e-mail address of a recipient submitting an opt-out request. This is intended to prevent a sender or other person from treating an opt-out request as a confirmation of a 'live' e-mail address, and selling that information to other would-be spammers.

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 UCE, and would require the inclusion of a valid physical postal address for the sender.

Section 5(b) addresses several techniques frequently employed by the most problematic spammers. These techniques would be classified as aggravated violations, and parties that use them would be subject to sharply increased liability.

Paragraph (1)(A)(i) deals with 'address harvesting'. Specifically, it would make it an aggravated violation to send unlawful 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. Paragraph (1)(A)(ii) would do the same thing with respect to unlawful UCE sent to addresses generated through 'dictionary attacks', in which a spammer sends messages to a succession of automatically generated e-mail addresses (such as asmith@isp.com, bsmith@isp.com, csmith@isp.com) in the expectation that some of them will turn out to be the addresses of real people. The paragraph contains a disclaimer to clarify that these provisions should not be read as establishing 'ownership' of e-mail addresses by a person operating a website or proprietary online service from which those addresses are harvested, or by any other person.

Paragraph (2) would make it an aggravated violation for ISP or other e-mail service subscribers to use an automated means to register for multiple e-mail accounts from which to send unlawful UCE. This is a technique spammers use to cycle rapidly through different originating addresses, making the spammers hard to track down and the UCE they send more difficult for ISPs and other e-mail service providers to filter. Finally, paragraph (3) is intended to make it an aggravated violation to hijack computers or open relays for the purpose of sending unlawful spam.

Section 5(c) would provide an opportunity for a defendant in an action alleging a violation of this bill (other than a violation involving falsified header information) to escape liability by showing that it had adopted reasonable practices and procedures to prevent violations and has made good faith efforts to maintain compliance with the provisions of the bill. This defense is intended to protect those persons who have preventive 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. Businesses knowingly promoted by electronic mail with false or misleading transmission information*

Section 6, which was offered as an amendment by Senator McCain at the Committee's executive session, would make businesses knowingly promoted in an e-mail with false or misleading transmission information subject to FTC Act penalties and enforcement remedies. Unlike other violations of the bill, enforcing violations of this section would not be dependent upon finding the person who 'initiated' the e-mail (as defined in section 3). Instead, this section would hold businesses that use deliberately falsified spam as a means to promote themselves liable to FTC enforcement, regardless of whether the FTC is able to identify the spammer who initiated the e-mail.

The purpose of this section would be to give the FTC a tool to more effectively 'follow the money' and enforce the law against businesses that hire spammers to send e-mail to consumers in large volumes with deliberately falsified header information. These businesses might otherwise escape liability under section 5 of the bill because that section would require the FTC to prove that a business 'procured' a spammer to send the e-mail on its behalf. This section would therefore set a different standard for the FTC to meet when enforcing the law against online or offline businesses that promote themselves through spam messages with deliberately falsified sender and routing information. Additionally, this section is limited in important ways that focus FTC enforcement on the deliberately falsified header spam used by high-volume spammers, minimizing the risk to legitimate retailers who do not disguise their identity in e-mail marketing.

Section 6(a) would prohibit any person from promoting, or knowingly permitting the promotion of, that person's trade or business in a commercial e-mail message that is in violation of section 5(a)(1). Section 6(a) would therefore apply only to e-mail that contains false sender or routing information, the key element of the criminal provisions under section 4 as well as a violation of section 5. Testimony from the Committee's hearings indicated that the use of falsified identity information is something that legitimate marketers and retailers will never do; however, it is exactly what volume spammers will continue to do in order to get their e-mails past ISP filters. As such, the use of false headers for commercial e-mail is a bright-line, objective standard that all parties can agree identifies a message as 'spam'.

Section 6(a) would hold a promoted business subject to enforcement only when it: (1) knows or should know it is being promoted by falsified spam, (2) is receiving or expects to receive an economic benefit from such promotion, and (3) is taking no reasonable precautions to prevent such spam, or to detect and report it to the FTC. The latter provision is an important safeguard to give legitimate companies an opportunity to proactively avoid mistaken FTC action if they have been victimized by 'spoofed sender' spam--unauthorized messages sent using their corporate name or one of their employee's e-mail addresses as the purported sender. This is increasingly becoming a preferred tactic of spammers who include a legitimate company's information in the e-mail's 'from' line (or other parts of the header information) in order to either bypass ISP filters, trick consumers into opening the message, or sell counterfeit goods of that company.

Section 6(b) would prevent the extension of liability under section 6(a) to website hosts, landlords, equipment lessors and other third parties that may provide goods or services unwittingly to a falsely promoted business. These businesses would be protected against FTC enforcement action unless they own or control the falsely promoted business, or actually know about the falsified spam and financially benefit from it.

Section 6(c) would limit enforcement of this section to the FTC. This section, however, would not in any way revise, remove, or diminish any other FTC, State attorney general, or ISP enforcement provisions set forth elsewhere in S. 877.

#### *Section 7. Enforcement by the Federal Trade Commission*

Sections 7(a) and 7(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 7(b) and 7(c) would 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 7(c), these agencies and the others set forth in section 7(b), may exercise authority provided by their own statutory grants to enforce the substantive provisions of this legislation.

Section 7(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 or other court of competent jurisdiction to obtain injunctive relief or recover actual or statutory damages, whichever is greater. Statutory damages under this section are (i) up to \$100 per message with falsified header information; or (ii) \$25 per message that is otherwise unlawful under this legislation, up to cap of \$1,000,000. If the court finds violations of section 5 were committed willfully or knowingly, or if the defendant's unlawful activity included one or more of the aggravated violations set forth in section 5(b), the statutory damage amount could be tripled. Reasonable attorneys' fees would be awarded to the State for a successful action.

Section 7(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 or other court of competent jurisdiction. 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)(1)(A)(i). The provider may obtain injunctive relief or actual or statutory damages calculated in the same manner as section 7(e). The court would be permitted to assess the costs of such an action, including reasonable attorneys' fees, against any party.

#### *Section 8. Effect on other laws*

Section 8(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 of the FTC Act for materially false or deceptive representations or unfair practices in commercial e-mail messages.

Section 8(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 that expressly regulate the use of e-mail to send commercial messages except for statutes, regulations, or rules that target fraud or deception in such e-mail. Thus, a State law requiring some or all commercial e-mail to carry specific types of labels, or to follow a certain format or contain specified content, would be preempted. By contrast, a State law prohibiting fraudulent or deceptive headers, subject lines, or content in commercial e-mail would not be preempted. Given the inherently interstate nature of e-mail communications, the Committee believes that this bill's creation of one national standard is a proper exercise of the Congress's power to regulate interstate commerce that is essential to resolving the significant harms from spam faced by American consumers, organizations, and businesses throughout the United States. This is particularly true because, in contrast to telephone numbers, e-mail addresses do not reveal the State where the holder is located. As a result, a sender of e-mail has no easy way to determine with which State law to comply. Statutes that prohibit fraud and deception in e-mail do not raise the same concern, because they target behavior that a legitimate business trying to comply with relevant laws would not be engaging in anyway. Section 8(b)(2) of the legislation clarifies that there would be no preemption of State laws that do not expressly regulate e-mail, such as State common law, general anti-fraud law, and computer crime law.

Section 8(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 9. Recommendations concerning Do-Not-E-mail Registry*

This section would require the FTC, within 6 months of implementing its national telemarketing Do-Not-Call list, to come up with a plan for creating a Do-Not-E-mail list or else

explain to Congress why the creation of such a list is not feasible at such time. The FTC is currently in the process of implementing the Do-Not-Call list, and the timing of this provision is intended to permit the FTC to analyze its experience with Do-Not-Call before turning to the question of Do-Not-E-mail. The Committee therefore intends that the 6-month deadline established by this section would be measured from the date that the Do-Not-Call list is fully enforceable against telemarketers, not from the date when consumers may first sign up for the list. The Committee also notes that a Do-Not-E-mail list appears to raise significant technical, security, and privacy questions that would need to be resolved before such a list could be implemented, and this provision gives the FTC time to consider such issues and their impact on the efficacy of creating such a list.

*Section 10. 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; an analysis of ways to address the international aspects of the spam problem; and an analysis of what could be done to protect consumers, especially children, from pornographic UCE.

*Section 11. 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 would not be affected.

*Section 12. 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 *italics*, existing law in which no change is proposed is shown in *roman*):

## **TITLE 18, UNITED STATES CODE**

## **CHAPTER 63. MAIL FRAUD**

### ***Sec. 1351. 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 a 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 is technically accurate but includes an originating electronic mail address the access to which for purposes of initiating the message 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 2003 has the meaning given it in that section.*