

# ABA TECHSHOW 2004

March 25-27

## Canning Spam



**Sharon D. Nelson, Esq.**



President  
Sensei Enterprises, Inc.  
3975 University Drive, Suite 225  
Fairfax, VA 22030  
703.359.0700 (phone)  
703.359.8434 (fax)  
snelson@senseient.com (e-mail)

# Canning Spam: Unclogging Law Firm Mailboxes

By Sharon D. Nelson, Esq. and John W. Simek

© 2004 Sensei Enterprises, Inc.

So how much do you hate spam? Spam-haters have become the world largest club. People talk more about the bane of spam than the latest absurdly unreal “reality” shows. Where we all once had a trickle of unsolicited e-mail that turned into a river, most lawyers now see spam in terms of a tsunami that grows in height on a daily basis and threatens to crush legitimate e-mail correspondence. Only the larger firms have tended to manage filter spam well. And now we have a new federal anti-spam law, whose effectiveness remains a matter of great speculation.

As a practical matter, can we “can the spam?”

## **The Grim Facts**

First, let’s examine the unnerving statistics, as reported by Massachusetts Institute of Technology’s *Technology Review* and *Consumer Reports*, some of which may seem startling. It will not surprise anyone that spam now comprises more than 50 percent of the average inbox, up from 8 percent in 2000. More than 13 billion unsolicited e-mail messages swamp inboxes worldwide every day. America Online reports it routinely blocks more than 1.5 million spam messages per day and yet it also averages 7 million complaints daily about the spam that gets through. According to the Radicati Group Inc., a market research firm specializing in e-mail, the number of spam messages is doubling every 18 months. Ferris Research now estimates spam causes a \$10 billion a year drag on the economy.

## **How the Spammers Find You**

How do spammers get your address in the first place? There is the classic “dictionary attack” in which spammers target guessed names such as johndoe, johndoe1, johndoe2, etc. Spammers all have software to facilitate these attacks — if they don’t receive a “bounceback” indicating that the address is invalid, they add it to their “confirmed valid” database.

If you shop or register for something online, be wary. L.L. Bean will not sell your e-mail address, but “Joe Chen’s Bargain Computers” might do just that. Make sure you look at privacy policies and be skeptical about companies you don’t know to be reputable.

If a lawyer places an e-mail address on his or her law firm site at 8 a.m., he or she is likely to receive the first spam message by 8:10 a.m. Ditto for talking in chat rooms. Spammers use special harvesting software to scan the Net for visible e-mail addresses. As an experiment, The Center for Democracy & Technology, a Washington, D.C., advocacy group, posted 250 new e-mail addresses on its Web site. Within six months, the addresses received more than 10,000 unsolicited e-mails.

Spammers also harvest e-mail addresses from free chat services. That was at least part of the reason that Microsoft closed its chat rooms in 28 countries on October 14<sup>th</sup>, although it allowed them to remain open on a subscription basis in the U.S., Canada and Japan, where visitors are more accountable because their billing details are on record with Microsoft.

How do the rest of them find your address? Often through reselling. Sometimes lawyers are their own worst enemy as they reply angrily “Remove” or “Unsubscribe,” only to have their address now added to spammers “confirmed valid” lists, which they will of course then sell to other spammers. Unsurprisingly, “confirmed valid” lists are generally resold many times over.

The statistic that takes most people aback is the experts’ consensus that roughly 90 percent of all spam is sent by less than 200 people, a view affirmed by the Coalition Against Unsolicited Commercial E-mail, an anti-spam coalition. Jon Praed, an attorney with the Internet Law Group in Arlington, Virginia told *Technology Review* these major league spammers are “hackers gone bad or they are crooks gone geek.”

Whoever they are, they are making law firms miserable. Managing e-mail is a daily task and as we all hit the delete key scores of times, it’s easy to accidentally delete a legitimate e-mail from a client without noticing. Not to mention the frustration of having to wade through the mess we find in our inbox every morning. The authors of this article currently receive several hundred spam messages each day. Spam has become a daily chore and e-mail management a daunting task.

### **State Legislative Solutions: Spammers in the Slammer?**

As the federal government struggled with competing lobbies and got nowhere quickly, 35 states managed to pass anti-spam laws, none of which seemed to accomplish a great deal. Spammers in the slammer, a common state penalty, sounds great to many of us, but many commentators have expressed the concern that prosecutors would not enforce such laws aggressively, both because they lack funding and because they don’t perceive spam as a serious crime. Typically, one would think murder, arson, rape, armed robbery and other significant charges would receive attention far ahead of unsolicited bulk e-mail. Another factor is it’s extremely difficult to trace the source of spam in most cases. Spammers are wily creatures who change their network addresses regularly and relay their e-mail off unsecured servers, primarily in Asia, to hide the true source of the e-mail.

The most stringent of the state spam laws was California, whose law was signed on September 23, 2003, and scheduled to take effect on January 1, 2004. It was called vulnerable to legal challenges, including First Amendment grounds or arguments based on the law’s interference with interstate commerce. The new federal CAN-SPAM Act preempts California’s “opt in” requirement. The California law outlawed sending most commercial e-mail messages to anyone in the state who has not explicitly requested them. That made it the most wide-reaching law of any of the 35 other state laws meant to regulate spam or any of the anti-spam bills that Congress considered. The law, which also

prohibited companies inside the state from sending unsolicited e-mail to anyone outside the state, imposed fines of \$1,000 for each message, up to \$1 million for each campaign. Proponents of the law said it would be more effective than many anti-spam laws because it gave people the right to file private lawsuits rather than depending on state prosecutors. Unfortunately, the California law never got a fair shot as the federal law largely preempted it.

### **Can the federal CAN-SPAM Act Can Spam?**

Congress remained, for a shamefully long time, a lumbering ineffectual giant that listened to the lobbyists for marketing groups, particularly the powerful Direct Marketing Association. Competing anti-spam bills vied against one another, as did their passionate proponents and opponents. Finally, prodded by their constituents, every member of Congress got one clear message: the voters wanted them to do something about spam and were going to be distinctly fed up with a Congress that didn't produce a law quickly. Hence, the CAN-SPAM Act of 2003. The lobbyists did not lose entirely – the Act that emerged from Congress has been greeted with a great deal of skepticism.

The Act has an unwieldy name CONTROLLING THE ASSAULT OF NON-SOLICITED PORNOGRAPHY AND MARKETING ACT OF 2003. Even the Act itself contains the subtitle “CAN-SPAM Act of 2003.” It was signed by President Bush on December 16, 2003 and went into effect January 1, 2004. It pre-empts state anti-spam laws except to the extent that they prohibit falsity or deception in any portion of a commercial electronic mail message or information attached to it. Unlike the California Act, which required that users “opt-in,” the federal law is an “opt-out” law. It does not ban spam outright, and it is questionable whether “opting-out” is ever a methodology that will truly work. The Act does not apply to political or charitable spam. For other unsolicited bulk e-mail, the Act:

- prohibits senders from falsifying or disguising their true identity;
- prohibits the use of misleading subject lines;
- prohibits the harvesting of e-mail addresses by either (1) automatic means from an Internet Web site or proprietary online service maintained by a third party; or (2) an automated system that generates possible electronic addresses by combining names, letters and numbers in numerous permutations;
- prohibits businesses from knowingly promoting themselves through false or misleading e-mails;
- requires the inclusion of a legitimate return e-mail and physical postal address for the sender;
- requires the inclusion of a functioning opt-out mechanism, clear and conspicuous notice of the opportunity to opt-out and require senders to honor any such opt-out

- request;
- requires clear and conspicuous notice that the message is an advertisement or solicitation; and
  - require messages with sexually oriented material to be clearly identified.

Liability under the act is broad, including not only the spammers themselves, but those who hire them. If a company knowingly hires a spammer who does not comply with the Act, the company may be prosecuted in the same manner as the spammer. Criminal penalties for violation of the Act include stiff fines and up to five years in prison. Civil penalties can be as much as \$250 per e-mail. Repeated misconduct or aggravated violations can result in treble damages.

In a move that has generated a lot of contemptuous criticism, the Act charges the Federal Trade Commission with administering a “Do Not Spam” registry, presumably much like the “Do Not Call” registry. The FTC has six months in which to submit a comprehensive plan for the “Do Not Spam” list to Congress, but critics scoff that there is no way to enforce the list against all of the foreign generated spam. In any event, after Congressional review, the FTC will have three months to implement the plan. The FTC is also charged under the act with developing rules within 270 days to curtail spam messages on cell phones.

The FTC and state attorney generals are charged with the enforcement of the law. Most commentators are relieved that there is any federal law at all, but it remains to be seen how well it will be enforced. Even with the law’s considerable teeth, will states and the FTC commit real resources to anti-spam enforcement?

In the end, finding spammers is an expensive, time-consuming process that often leads to a dead end. Even when they are found, few spammers have significant assets. Earthlink, MSN and AOL have all filed numerous suits against spammers, but for the most part, in spite of 35 state laws on the books and a barrage of suits, spam continues to grow as a percentage of the mail in everyone’s in-box. How can this scourge be stifled effectively? There are some methods today, and the promise of much better methods in the future, especially if Congress finds the courage to employ them nationally and to back them with stiff penalties.

### **Today’s Best Hope: Filters**

In an astonishingly short period of time, most of corporate America has adopted some sort of filter system to screen unwanted e-mail. Though wildly imperfect, filters have become the nation’s No.1 weapon in the fight against spam. One way to measure the effectiveness of a spam filter is to weigh the percentage of junk e-mail blocked versus the false positive rate (the percentage of legitimate mail inadvertently blocked). A 95 percent filtration rate is considered excellent, and some companies claim a higher rate. But be

wary of claims, since corporate users generally report something more like a 70 percent filtration rate. The higher the filtration rate, the higher the false positives, unfortunately. It's generally considered to be unacceptable to have a rate of .1 percent or higher, which translates into losing 1 of 1,000 legitimate e-mails.

One filter used by some of America's corporate giants comes from San Francisco-based Brightmail Inc., which says its filter processes about 10 percent of the world's e-mail. Brightmail has an extremely low false positive rate, about one out of every 1 million spam messages. Though Brightmail claims a filtration rate of more than 90 percent, once again, consumers report the rate is significantly less. A great help, certainly, but not a complete solution. Brightmail is a server-based solution and not available for a small or solo office that doesn't have its own e-mail server.

Though there are many kinds of filtering software, law firms with Exchange servers rely more and more on Symantec's filtering product. The old version was called Symantec AntiVirus/Filtering for Microsoft Exchange and provided very basic methods for identifying spam addresses and unwanted content. The software was time-consuming to manage and had a long list of flaws. The new version is called Symantec Mail Security for Microsoft Exchange and promises to do a much better job of managing unsolicited e-mail. Some of the new features include separate scanning of inbound and outbound mail, comparison of attachment type to the file extension, support for external "black list" databases (known spammers) and support for "white lists" to allow all e-mail from a known good address regardless of content. Unlike the old version, it also can be configured to give or not to give users notification of blocked e-mail, though only if the action selected is to delete the message. If the messages are to be quarantined, it will still give the users notification. As many lawyers have complained, having the long list of notifications in their inbox is almost as irritating as the spam itself, especially if they are retrieving their e-mail via a PDA. It's akin to spam about spam.

*Consumer Reports* Picks the Best Spam Filters:

1. Stata Labs SProxy: According to *Consumer Reports*, this free program outperformed all other spam filters, but be forewarned that it requires some degree of computer skill and comes with complicated installation instructions.
2. Mailshell SpamCatcher Universal: \$20
3. Blue Squirrel Spam Sleuth: \$30
4. Symantec Norton Internet Security 2003 (Spam Alert): \$70

Our own experience is greatest with Symantec's products, which we have no problem recommending, especially with all the enhancements of the current version. At an enterprise level, this is an excellent approach to reducing spam. Not that it works all alone. We combine the Symantec product (Symantec Mail Filter, which comes bundled with Symantec Antivirus, Enterprise Edition) with the application of certain blacklists. For a list of all currently known blacklists, see <http://www.declude.com/junkmail/support/ip4r.htm>.

Although experts disagree on which blacklists are best, the Super Computer Center at the University of California uses these, which seems a pretty decent recommendation:

- [dsn.rfc-ignorant.org](http://dsn.rfc-ignorant.org)
- [sbl.spamhaus.org](http://sbl.spamhaus.org)
- [list.dsbl.org](http://list.dsbl.org)
- [bl.spamcop.net](http://bl.spamcop.net)

Anecdotally, some of our solo and small-law firm clients speak well of Sunbelt's iHateSpam (\$19.95).

Don't expect the problem to go away. Our combination of Symantec, blacklists and our own fine-tuning of the filters has resulted in 92% of incoming mail being blocked as spam. Two percent is spam that gets through (more fine-tuning always in progress) and the remainder is our legitimate e-mail. We have created a daily spam folder for each individual – the only spam that goes there is the spam we catch with our own fine-tuning. We review it once in a while and find that we have to whitelist someone (perhaps our realty or financial counselor, whose words may trip our content filters). In terms of the spam we never see because it is caught by the blacklists, only once have we had legitimate mail blocked by a blacklist and that was because a client had their server configured as an open relay and was therefore blacklisted. Clients who are blacklisted have a much bigger problem, since they need to get off the blacklist to conduct business with anyone who uses blacklists – and that's a steadily growing number! By the way, figure at least 72 hours of business impact to get yourself totally removed from the blacklists if you somehow find yourself on them, even if you jump on the problem assiduously from the beginning.

An ongoing problem for law firms has been legal newsletters, which are often blocked as spam (because of length or content) even though lawyers have subscribed to them. As whitelists become more prevalent in filters, this problem may erode, though it will require the lawyer to take the additional step of placing the sender on the whitelist. The new Symantec product allows for this. Additionally, publishers of electronic newsletters (we publish "Bytes in Brief," a free law and technology newsletter available at [www.senseient.com](http://www.senseient.com)) have learned to let opt-in subscribers receive "notification only" of each issue's publication so the content won't trip filters, as ours often would because of cases involving sexual terms, Internet pornography laws, etc.

Though woefully inadequate, filters are seen by many technologists as a formidable weapon that can be made more potent with modifications. Have you ever heard of Bayesian filters? Named after the 18th century English mathematician Thomas Bayes, his theories of probability have been successfully incorporated in filters that learn from the users themselves. If you typically open penile enlargement e-mails (to pick a common subject), it will regard those as normal e-mails. If you routinely delete them, it will learn to block them. Because individuals train Bayesian filters, they increase their effectiveness over time and foil spammers because the probability of messages getting through is skewed and uncertain.

Microsoft Research has taken this concept one step further, by creating a “naïve Bayesian filter,” which learns probabilities for words, phrases and other characteristics that distinguish spam. For example, many filters have no trouble blocking “Viagra” but cannot block V\*I\*A\*G\*R\*A. Undoubtedly, you have seen many variations on this theme, and the more modern filters are learning to recognize this trick.

Unfortunately, spammers are wily creatures and their seeming ability to get around each new defense is maddening. More and more, they are getting all of us to open their e-mail because it says something innocuous, such as “Confirming your order,” “Requesting Information” or the like. Lawyers are finding it’s dangerous to delete too quickly, lest they delete a client or potential client’s e-mail.

### **Battlefields of the Future**

Can we change the economics of spam as a countermeasure? Right now, experts estimate it costs spammers between \$200 to \$500 to send a million e-mails, with roughly 100 “paying” responses expected from each transmission. One suggestion from technologists is to create an “e-stamp,” perhaps in a nominal amount such as one-tenth of a cent per e-mail. The amount would be negligible for most users, but would impose a \$1,000 tax on anyone sending a million e-mails. Mail without the stamps would be blocked automatically.

Another technical suggestion is to impose a time cost, by forcing a transmitting computer to perform a quick mathematical problem before the transmission goes through — not enough to disturb a normal user, but enough to confound the computers of spammers. Microsoft Research is currently working on this approach.

Microsoft now blocks more than 2.4 billion spam messages daily and has assembled a crack team of experts to come up with innovative and more effective ways to fight spam. Bill Gates himself has lamented the number of “Get Rich Quick” e-mails he receives every day, though such messages certainly seem to exemplify “carrying coals to Newcastle.” The sad truth is no one is immune and half of us will continue to receive messages promising to add three inches in length to a body part we don’t possess. Perhaps the ladies among us should buy the product and seek to exercise the warranty? In the meantime, hang on to that trusty old delete key, and press, press, press so you too can be a part of the annual \$10 billion loss of productivity caused by spam.

**CONTROLLING THE ASSAULT OF NON-SOLICITED  
PORNOGRAPHY AND MARKETING ACT OF 2003  
(also known as the “CAN-SPAM Act of 2003)**

*Be it enacted by the Senate and House of Representatives of the United States of  
America in Congress assembled,*

**SECTION 1. SHORT TITLE.**

This Act may be cited as the ‘Controlling the Assault of Non-Solicited  
Pornography and Marketing Act of 2003’, or the ‘CAN-SPAM Act of 2003’.

**SEC. 2. CONGRESSIONAL FINDINGS AND POLICY.**

(a) FINDINGS- The Congress finds the following:

(1) Electronic mail has become an extremely important and popular means of communication, relied on by millions of Americans on a daily basis for personal and commercial purposes. Its low cost and global reach make it extremely convenient and efficient, and offer unique opportunities for the development and growth of frictionless commerce.

(2) The convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail. Unsolicited commercial electronic mail is currently estimated to account for over half of all electronic mail traffic, up from an estimated 7 percent in 2001, and the volume continues to rise. Most of these messages are fraudulent or deceptive in one or more respects.

(3) The receipt of unsolicited commercial electronic mail may result in costs to recipients who cannot refuse to accept such mail and who incur costs for the storage of such mail, or for the time spent accessing, reviewing, and discarding such mail, or for both.

(4) The receipt of a large number of unwanted messages also decreases the convenience of electronic mail and creates a risk that wanted electronic mail messages, both commercial and noncommercial, will be lost, overlooked, or discarded amidst the larger volume of unwanted messages, thus reducing the reliability and usefulness of electronic mail to the recipient.

(5) Some commercial electronic mail contains material that many recipients may consider vulgar or pornographic in nature.

(6) The growth in unsolicited commercial electronic mail imposes significant monetary costs on providers of Internet access services, businesses, and educational and nonprofit institutions that carry and receive such mail, as there is a finite volume of mail that such providers, businesses, and institutions can handle without further investment in infrastructure.

(7) Many senders of unsolicited commercial electronic mail purposefully disguise the source of such mail.

(8) Many senders of unsolicited commercial electronic mail purposefully include misleading information in the messages' subject lines in order to induce the recipients to view the messages.

(9) While some senders of commercial electronic mail messages provide simple and reliable ways for recipients to reject (or 'opt-out' of) receipt of commercial electronic mail from such senders in the future, other senders provide no such 'opt-out' mechanism, or refuse to honor the requests of recipients not to receive electronic mail from such senders in the future, or both.

(10) Many senders of bulk unsolicited commercial electronic mail use computer programs to gather large numbers of electronic mail addresses on an automated basis from Internet websites or online services where users must post their addresses in order to make full use of the website or service.

(11) Many States have enacted legislation intended to regulate or reduce unsolicited commercial electronic mail, but these statutes impose different standards and requirements. As a result, they do not appear to have been successful in addressing the problems associated with unsolicited commercial electronic mail, in part because, since an electronic mail address does not specify a geographic location, it can be extremely difficult for law-abiding businesses to know with which of these disparate statutes they are required to comply.

(12) The problems associated with the rapid growth and abuse of unsolicited commercial electronic mail cannot be solved by Federal legislation alone. The development and adoption of technological approaches and the pursuit of cooperative efforts with other countries will be necessary as well.

(b) CONGRESSIONAL DETERMINATION OF PUBLIC POLICY- On the basis of the findings in subsection (a), the Congress determines that--

(1) there is a substantial government interest in regulation of commercial electronic mail on a nationwide basis;

(2) senders of commercial electronic mail should not mislead recipients as to the source or content of such mail; and

(3) recipients of commercial electronic mail have a right to decline to receive additional commercial electronic mail from the same source.

### **SEC. 3. DEFINITIONS.**

In this Act:

(1) AFFIRMATIVE CONSENT- The term 'affirmative consent', when used with respect to a commercial electronic mail message, means that--

(A) the recipient expressly consented to receive the message, either in response to a clear and conspicuous request for such consent or at the recipient's own initiative; and

(B) if the message is from a party other than the party to which the recipient communicated such consent, the recipient was given clear and conspicuous notice at the time the consent was communicated that the recipient's electronic mail address could be transferred to such other party for the purpose of initiating commercial electronic mail messages.

(2) Commercial electronic mail message-

(A) IN GENERAL- The term 'commercial electronic mail message' means any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose).

(B) TRANSACTIONAL OR RELATIONSHIP MESSAGES- The term 'commercial electronic mail message' does not include a transactional or relationship message.

(C) REGULATIONS REGARDING PRIMARY PURPOSE- Not later than 12 months after the date of the enactment of this Act, the Commission shall issue regulations pursuant to section 13 defining the relevant criteria to facilitate the determination of the primary purpose of an electronic mail message.

(D) REFERENCE TO COMPANY OR WEBSITE- The inclusion of a reference to a commercial entity or a link to the website of a commercial entity in an electronic mail message does not, by itself, cause such message to be treated as a commercial electronic mail message for purposes of this Act if the contents or circumstances of the message indicate a primary purpose other than commercial advertisement or promotion of a commercial product or service.

(3) COMMISSION- The term 'Commission' means the Federal Trade Commission.

(4) DOMAIN NAME- The term 'domain name' means any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet.

(5) ELECTRONIC MAIL ADDRESS- The term 'electronic mail address' means a destination, commonly expressed as a string of characters, consisting of a unique user name or mailbox (commonly referred to as the 'local part') and a reference to an Internet domain (commonly referred to as the 'domain part'), whether or not displayed, to which an electronic mail message can be sent or delivered.

(6) ELECTRONIC MAIL MESSAGE- The term 'electronic mail message' means a message sent to a unique electronic mail address.

(7) FTC ACT- The term 'FTC Act' means the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(8) HEADER INFORMATION- The term 'header information' means the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic

mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message.

(9) INITIATE- The term `initiate', when used with respect to a commercial electronic mail message, means to originate or transmit such message or to procure the origination or transmission of such message, but shall not include actions that constitute routine conveyance of such message. For purposes of this paragraph, more than one person may be considered to have initiated a message.

(10) INTERNET- The term `Internet' has the meaning given that term in the Internet Tax Freedom Act (47 U.S.C. 151 nt).

(11) INTERNET ACCESS SERVICE- The term `Internet access service' has the meaning given that term in section 231(e)(4) of the Communications Act of 1934 (47 U.S.C. 231(e)(4)).

(12) PROCURE- The term `procure', when used with respect to the initiation of a commercial electronic mail message, means intentionally to pay or provide other consideration to, or induce, another person to initiate such a message on one's behalf.

(13) PROTECTED COMPUTER- The term `protected computer' has the meaning given that term in section 1030(e)(2)(B) of title 18, United States Code.

(14) RECIPIENT- The term `recipient', when used with respect to a commercial electronic mail message, means an authorized user of the electronic mail address to which the message was sent or delivered. If a recipient of a commercial electronic mail message has one or more electronic mail addresses in addition to the address to which the message was sent or delivered, the recipient shall be treated as a separate recipient with respect to each such address. If an electronic mail address is reassigned to a new user, the new user shall not be treated as a recipient of any commercial electronic mail message sent or delivered to that address before it was reassigned.

(15) ROUTINE CONVEYANCE- The term `routine conveyance' means the transmission, routing, relaying, handling, or storing, through an automatic technical process, of an electronic mail message for which another person has identified the recipients or provided the recipient addresses.

(16) SENDER-

(A) IN GENERAL- Except as provided in subparagraph (B), the term `sender', when used with respect to a commercial electronic mail message, means a person who initiates such a message and whose product, service, or Internet web site is advertised or promoted by the message.

(B) SEPARATE LINES OF BUSINESS OR DIVISIONS- If an entity operates through separate lines of business or divisions and holds itself out to the recipient throughout the message as that particular line of business or division rather than as the entity of which such line of business or division is a part, then the line of

business or the division shall be treated as the sender of such message for purposes of this Act.

(17) Transactional or relationship message-

(A) IN GENERAL- The term `transactional or relationship message' means an electronic mail message the primary purpose of which is--

(i) to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender;

(ii) to provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient;

(iii) to provide--

(I) notification concerning a change in the terms or features of;

(II) notification of a change in the recipient's standing or status with respect to; or

(III) at regular periodic intervals, account balance information or other type of account statement with respect to,

a subscription, membership, account, loan, or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender;

(iv) to provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or

(v) to deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender.

(B) MODIFICATION OF DEFINITION- The Commission by regulation pursuant to section 13 may modify the definition in subparagraph (A) to expand or contract the categories of messages that are treated as transactional or relationship messages for purposes of this Act to the extent that such modification is necessary to accommodate changes in electronic mail technology or practices and accomplish the purposes of this Act.

**SEC. 4. PROHIBITION AGAINST PREDATORY AND ABUSIVE COMMERCIAL E-MAIL.**

(a) OFFENSE-

(1) IN GENERAL- Chapter 47 of title 18, United States Code, is amended by adding at the end the following new section:

`Sec. 1037. Fraud and related activity in connection with electronic mail

`(a) IN GENERAL- Whoever, in or affecting interstate or foreign commerce, knowingly--

`(1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer,

`(2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages,

`(3) materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages,

`(4) registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names, or

`(5) falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses,

or conspires to do so, shall be punished as provided in subsection (b).

`(b) PENALTIES- The punishment for an offense under subsection (a) is--

`(1) a fine under this title, imprisonment for not more than 5 years, or both, if--

`(A) the offense is committed in furtherance of any felony under the laws of the United States or of any State; or

`(B) the defendant has previously been convicted under this section or section 1030, or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system;

`(2) a fine under this title, imprisonment for not more than 3 years, or both, if--

`(A) the offense is an offense under subsection (a)(1);

`(B) the offense is an offense under subsection (a)(4) and involved 20 or more falsified electronic mail or online user account registrations, or 10 or more falsified domain name registrations;

`(C) the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, or 250,000 during any 1-year period;

`(D) the offense caused loss to one or more persons aggregating \$5,000 or more in value during any 1-year period;

`(E) as a result of the offense any individual committing the offense obtained anything of value aggregating \$5,000 or more during any 1-year period; or

`(F) the offense was undertaken by the defendant in concert with three or more other persons with respect to whom the defendant occupied a position of organizer or leader; and

`(3) a fine under this title or imprisonment for not more than 1 year, or both, in any other case.

`(c) FORFEITURE-

`(1) IN GENERAL- The court, in imposing sentence on a person who is convicted of an offense under this section, shall order that the defendant forfeit to the United States--

`(A) any property, real or personal, constituting or traceable to gross proceeds obtained from such offense; and

`(B) any equipment, software, or other technology used or intended to be used to commit or to facilitate the commission of such offense.

`(2) PROCEDURES- The procedures set forth in section 413 of the Controlled Substances Act (21 U.S.C. 853), other than subsection (d) of that section, and in Rule 32.2 of the Federal Rules of Criminal Procedure, shall apply to all stages of a criminal forfeiture proceeding under this section.

`(d) DEFINITIONS- In this section:

`(1) LOSS- The term 'loss' has the meaning given that term in section 1030(e) of this title.

`(2) MATERIALLY- For purposes of paragraphs (3) and (4) of subsection (a), header information or registration information is materially falsified if it is altered or concealed in a manner that would impair the ability of a recipient of the message, an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation.

`(3) MULTIPLE- The term 'multiple' means more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period.

`(4) OTHER TERMS- Any other term has the meaning given that term by section 3 of the CAN-SPAM Act of 2003.'.

(2) CONFORMING AMENDMENT- The chapter analysis for chapter 47 of title 18, United States Code, is amended by adding at the end the following:

`Sec. `1037. Fraud and related activity in connection with electronic mail.'

(b) UNITED STATES SENTENCING COMMISSION-

(1) DIRECTIVE- Pursuant to its authority under section 994(p) of title 28, United States Code, and in accordance with this section, the United States Sentencing Commission shall review and, as appropriate, amend the sentencing guidelines and policy statements to provide appropriate penalties for violations of section 1037 of title 18, United States Code, as added by this section, and other offenses that may be facilitated by the sending of large quantities of unsolicited electronic mail.

(2) REQUIREMENTS- In carrying out this subsection, the Sentencing Commission shall consider providing sentencing enhancements for--

(A) those convicted under section 1037 of title 18, United States Code, who--

(i) obtained electronic mail addresses through improper means, including--

(I) harvesting electronic mail addresses of the users of a website, proprietary service, or other online public forum operated by another person, without the authorization of such person; and

(II) randomly generating electronic mail addresses by computer; or

(ii) knew that the commercial electronic mail messages involved in the offense contained or advertised an Internet domain for which the registrant of the domain had provided false registration information; and

(B) those convicted of other offenses, including offenses involving fraud, identity theft, obscenity, child pornography, and the sexual exploitation of children, if such offenses involved the sending of large quantities of electronic mail.

(c) SENSE OF CONGRESS- It is the sense of Congress that--

(1) Spam has become the method of choice for those who distribute pornography, perpetrate fraudulent schemes, and introduce viruses, worms, and Trojan horses into personal and business computer systems; and

(2) the Department of Justice should use all existing law enforcement tools to investigate and prosecute those who send bulk commercial e-mail to facilitate the commission of Federal crimes, including the tools contained in chapters 47 and 63 of title 18, United States Code (relating to fraud and false statements); chapter 71 of title 18, United States Code (relating to obscenity); chapter 110 of title 18, United States Code (relating to the sexual exploitation of children); and chapter 95 of title 18, United States Code (relating to racketeering), as appropriate.

## **SEC. 5. OTHER PROTECTIONS FOR USERS OF COMMERCIAL ELECTRONIC MAIL.**

(a) REQUIREMENTS FOR TRANSMISSION OF MESSAGES-

(1) PROHIBITION OF FALSE OR MISLEADING TRANSMISSION INFORMATION- It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading. For purposes of this paragraph--

(A) header information that is technically accurate but includes an originating electronic mail address, domain name, or Internet Protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations shall be considered materially misleading;

(B) a 'from' line (the line identifying or purporting to identify a person initiating the message) that accurately identifies any person who initiated the message shall not be considered materially false or materially misleading; and

(C) header information shall be considered materially misleading if it fails to identify accurately a protected computer used to initiate the message because the person initiating the message knowingly uses another protected computer to relay or retransmit the message for purposes of disguising its origin.

(2) PROHIBITION OF DECEPTIVE SUBJECT HEADINGS- It is unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message if such person has actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that a subject heading of the message would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message (consistent with the criteria used in enforcement of section 5 of the Federal Trade Commission Act (15 U.S.C. 45)).

(3) Inclusion of return address or comparable mechanism in commercial electronic mail-

(A) IN GENERAL- It is unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message that does not contain a functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that--

(i) a recipient may use to submit, in a manner specified in the message, a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from that sender at the electronic mail address where the message was received; and

(ii) remains capable of receiving such messages or communications for no less than 30 days after the transmission of the original message.

(B) MORE DETAILED OPTIONS POSSIBLE- The person initiating a commercial electronic mail message may comply with subparagraph (A)(i) by providing the recipient a list or menu from which the recipient may choose the specific types of commercial electronic mail messages the recipient wants to receive or does not want to receive from the sender, if the list or menu includes an option under which the recipient may choose not to receive any commercial electronic mail messages from the sender.

(C) TEMPORARY INABILITY TO RECEIVE MESSAGES OR PROCESS REQUESTS- A return electronic mail address or other mechanism does not fail to satisfy the requirements of subparagraph (A) if it is unexpectedly and temporarily unable to receive messages or process requests due to a technical problem beyond the control of the sender if the problem is corrected within a reasonable time period.

(4) PROHIBITION OF TRANSMISSION OF COMMERCIAL ELECTRONIC MAIL AFTER OBJECTION-

(A) IN GENERAL- If a recipient makes a request using a mechanism provided pursuant to paragraph (3) not to receive some or any commercial electronic mail messages from such sender, then it is unlawful--

(i) for the sender to initiate the transmission to the recipient, more than 10 business days after the receipt of such request, of a commercial electronic mail message that falls within the scope of the request;

(ii) for any person acting on behalf of the sender to initiate the transmission to the recipient, more than 10 business days after the receipt of such request, of a commercial electronic mail message with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that such message falls within the scope of the request;

(iii) for any person acting on behalf of the sender to assist in initiating the transmission to the recipient, through the provision or selection of addresses to which the message will be sent, of a commercial electronic mail message with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that such message would violate clause (i) or (ii); or

(iv) for the sender, or any other person who knows that the recipient has made such a request, to sell, lease, exchange, or otherwise transfer or release the electronic mail address of the recipient (including through any transaction or other transfer involving mailing lists bearing the electronic mail address of the recipient) for any purpose other than compliance with this Act or other provision of law.

(B) SUBSEQUENT AFFIRMATIVE CONSENT- A prohibition in subparagraph (A) does not apply if there is affirmative consent by the recipient subsequent to the request under subparagraph (A).

(5) INCLUSION OF IDENTIFIER, OPT-OUT, AND PHYSICAL ADDRESS IN COMMERCIAL ELECTRONIC MAIL- (A) It is unlawful for any person to initiate the transmission of any commercial electronic mail message to a protected computer unless the message provides--

- (i) clear and conspicuous identification that the message is an advertisement or solicitation;
- (ii) clear and conspicuous notice of the opportunity under paragraph (3) to decline to receive further commercial electronic mail messages from the sender; and
- (iii) a valid physical postal address of the sender.

(B) Subparagraph (A)(i) does not apply to the transmission of a commercial electronic mail message if the recipient has given prior affirmative consent to receipt of the message.

(6) MATERIALLY- For purposes of paragraph (1), the term 'materially', when used with respect to false or misleading header information, includes the alteration or concealment of header information in a manner that would impair the ability of an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation, or the ability of a recipient of the message to respond to a person who initiated the electronic message.

(b) Aggravated Violations Relating to Commercial Electronic Mail-

(1) Address harvesting and dictionary attacks-

(A) IN GENERAL- It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message that is unlawful under subsection (a), or to assist in the origination of such message through the provision or selection of addresses to which the message will be transmitted, if such person had actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that--

- (i) the electronic mail address of the recipient was obtained using an automated means from an Internet website or proprietary online service operated by another person, and such website or online service included, at the time the address was obtained, a notice stating that the operator of such website or online service will not give, sell, or otherwise transfer addresses maintained by such website or online service to any other party for the purposes of initiating, or enabling others to initiate, electronic mail messages; or
- (ii) the electronic mail address of the recipient was obtained using an automated means that generates possible

electronic mail addresses by combining names, letters, or numbers into numerous permutations.

(B) DISCLAIMER- Nothing in this paragraph creates an ownership or proprietary interest in such electronic mail addresses.

(2) AUTOMATED CREATION OF MULTIPLE ELECTRONIC MAIL ACCOUNTS- It is unlawful for any person to use scripts or other automated means to register for multiple electronic mail accounts or online user accounts from which to transmit to a protected computer, or enable another person to transmit to a protected computer, a commercial electronic mail message that is unlawful under subsection (a).

(3) RELAY OR RETRANSMISSION THROUGH UNAUTHORIZED ACCESS- It is unlawful for any person knowingly to relay or retransmit a commercial electronic mail message that is unlawful under subsection (a) from a protected computer or computer network that such person has accessed without authorization.

(c) SUPPLEMENTARY RULEMAKING AUTHORITY- The Commission shall by regulation, pursuant to section 13--

(1) modify the 10-business-day period under subsection (a)(4)(A) or subsection (a)(4)(B), or both, if the Commission determines that a different period would be more reasonable after taking into account--

(A) the purposes of subsection (a);

(B) the interests of recipients of commercial electronic mail; and

(C) the burdens imposed on senders of lawful commercial electronic mail; and

(2) specify additional activities or practices to which subsection (b) applies if the Commission determines that those activities or practices are contributing substantially to the proliferation of commercial electronic mail messages that are unlawful under subsection (a).

(d) REQUIREMENT TO PLACE WARNING LABELS ON COMMERCIAL ELECTRONIC MAIL CONTAINING SEXUALLY ORIENTED MATERIAL-

(1) IN GENERAL- No person may initiate in or affecting interstate commerce the transmission, to a protected computer, of any commercial electronic mail message that includes sexually oriented material and--

(A) fail to include in subject heading for the electronic mail message the marks or notices prescribed by the Commission under this subsection; or

(B) fail to provide that the matter in the message that is initially viewable to the recipient, when the message is opened by any recipient and absent any further actions by the recipient, includes only--

(i) to the extent required or authorized pursuant to paragraph (2), any such marks or notices;

(ii) the information required to be included in the message pursuant to subsection (a)(5); and

(iii) instructions on how to access, or a mechanism to access, the sexually oriented material.

(2) PRIOR AFFIRMATIVE CONSENT- Paragraph (1) does not apply to the transmission of an electronic mail message if the recipient has given prior affirmative consent to receipt of the message.

(3) PRESCRIPTION OF MARKS AND NOTICES- Not later than 120 days after the date of the enactment of this Act, the Commission in consultation with the Attorney General shall prescribe clearly identifiable marks or notices to be included in or associated with commercial electronic mail that contains sexually oriented material, in order to inform the recipient of that fact and to facilitate filtering of such electronic mail. The Commission shall publish in the Federal Register and provide notice to the public of the marks or notices prescribed under this paragraph.

(4) DEFINITION- In this subsection, the term `sexually oriented material' means any material that depicts sexually explicit conduct (as that term is defined in section 2256 of title 18, United States Code), unless the depiction constitutes a small and insignificant part of the whole, the remainder of which is not primarily devoted to sexual matters.

(5) PENALTY- Whoever knowingly violates paragraph (1) shall be fined under title 18, United States Code, or imprisoned not more than 5 years, or both.

#### **SEC. 6. BUSINESSES KNOWINGLY PROMOTED BY ELECTRONIC MAIL WITH FALSE OR MISLEADING TRANSMISSION INFORMATION.**

(a) IN GENERAL- It is unlawful for a person to promote, or allow the promotion of, that person's trade or business, or goods, products, property, or services sold, offered for sale, leased or offered for lease, or otherwise made available through that trade or business, in a commercial electronic mail message the transmission of which is in violation of section 5(a)(1) if that person--

(1) knows, or should have known in the ordinary course of that person's trade or business, that the goods, products, property, or services sold, offered for sale, leased or offered for lease, or otherwise made available through that trade or business were being promoted in such a message;

(2) received or expected to receive an economic benefit from such promotion; and

(3) took no reasonable action--

(A) to prevent the transmission; or

(B) to detect the transmission and report it to the Commission.

(b) Limited Enforcement Against Third Parties-

(1) IN GENERAL- Except as provided in paragraph (2), a person (hereinafter referred to as the `third party') that provides goods, products, property, or services to another person that violates subsection (a) shall not be held liable for such violation.

(2) EXCEPTION- Liability for a violation of subsection (a) shall be imputed to a third party that provides goods, products, property, or services to another person that violates subsection (a) if that third party--

(A) owns, or has a greater than 50 percent ownership or economic interest in, the trade or business of the person that violated subsection (a); or

(B)(i) has actual knowledge that goods, products, property, or services are promoted in a commercial electronic mail message the transmission of which is in violation of section 5(a)(1); and  
(ii) receives, or expects to receive, an economic benefit from such promotion.

(c) EXCLUSIVE ENFORCEMENT BY FTC- Subsections (f) and (g) of section 7 do not apply to violations of this section.

(d) SAVINGS PROVISION- Except as provided in section 7(f)(8), nothing in this section may be construed to limit or prevent any action that may be taken under this Act with respect to any violation of any other section of this Act.

## **SEC. 7. ENFORCEMENT GENERALLY.**

(a) VIOLATION IS UNFAIR OR DECEPTIVE ACT OR PRACTICE- Except as provided in subsection (b), this Act shall be enforced by the Commission as if the violation of this Act were an unfair or deceptive act or practice proscribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(b) ENFORCEMENT BY CERTAIN OTHER AGENCIES- Compliance with this Act shall be enforced--

(1) under section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), in the case of--

(A) national banks, and Federal branches and Federal agencies of foreign banks, by the Office of the Comptroller of the Currency;  
(B) member banks of the Federal Reserve System (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, organizations operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601 and 611), and bank holding companies, by the Board;

(C) banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System) and insured State branches of foreign banks, by the Board of Directors of the Federal Deposit Insurance Corporation; and

(D) savings associations the deposits of which are insured by the Federal Deposit Insurance Corporation, by the Director of the Office of Thrift Supervision;

(2) under the Federal Credit Union Act (12 U.S.C. 1751 et seq.) by the Board of the National Credit Union Administration with respect to any Federally insured credit union;

- (3) under the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.) by the Securities and Exchange Commission with respect to any broker or dealer;
- (4) under the Investment Company Act of 1940 (15 U.S.C. 80a-1 et seq.) by the Securities and Exchange Commission with respect to investment companies;
- (5) under the Investment Advisers Act of 1940 (15 U.S.C. 80b-1 et seq.) by the Securities and Exchange Commission with respect to investment advisers registered under that Act;
- (6) under State insurance law in the case of any person engaged in providing insurance, by the applicable State insurance authority of the State in which the person is domiciled, subject to section 104 of the Gramm-Bliley-Leach Act (15 U.S.C. 6701), except that in any State in which the State insurance authority elects not to exercise this power, the enforcement authority pursuant to this Act shall be exercised by the Commission in accordance with subsection (a);
- (7) under part A of subtitle VII of title 49, United States Code, by the Secretary of Transportation with respect to any air carrier or foreign air carrier subject to that part;
- (8) under the Packers and Stockyards Act, 1921 (7 U.S.C. 181 et seq.) (except as provided in section 406 of that Act (7 U.S.C. 226, 227)), by the Secretary of Agriculture with respect to any activities subject to that Act;
- (9) under the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.) by the Farm Credit Administration with respect to any Federal land bank, Federal land bank association, Federal intermediate credit bank, or production credit association; and
- (10) under the Communications Act of 1934 (47 U.S.C. 151 et seq.) by the Federal Communications Commission with respect to any person subject to the provisions of that Act.

(c) EXERCISE OF CERTAIN POWERS- For the purpose of the exercise by any agency referred to in subsection (b) of its powers under any Act referred to in that subsection, a violation of this Act is deemed to be a violation of a Federal Trade Commission trade regulation rule. In addition to its powers under any provision of law specifically referred to in subsection (b), each of the agencies referred to in that subsection may exercise, for the purpose of enforcing compliance with any requirement imposed under this Act, any other authority conferred on it by law.

(d) ACTIONS BY THE COMMISSION- The Commission shall prevent any person from violating this Act 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 Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. Any entity that violates any provision of that subtitle is subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act in the same manner, by the same means, and with the same jurisdiction, power, and duties as though all applicable terms and provisions of the Federal Trade Commission Act were incorporated into and made a part of that subtitle.

(e) AVAILABILITY OF CEASE-AND-DESIST ORDERS AND INJUNCTIVE RELIEF WITHOUT SHOWING OF KNOWLEDGE- Notwithstanding any other provision of this Act, in any proceeding or action pursuant to subsection (a), (b), (c), or (d) of this section to enforce compliance, through an order to cease and desist or an injunction, with section 5(a)(1)(C), section 5(a)(2), clause (ii), (iii), or (iv) of section 5(a)(4)(A), section 5(b)(1)(A), or section 5(b)(3), neither the Commission nor the Federal Communications Commission shall be required to allege or prove the state of mind required by such section or subparagraph.

(f) Enforcement by States-

(1) CIVIL ACTION- In any case in which the attorney general of a State, or an official or agency of a State, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by any person who violates paragraph (1) or (2) of section 5(a), who violates section 5(d), or who engages in a pattern or practice that violates paragraph (3), (4), or (5) of section 5(a), of this Act, the attorney general, official, or agency of the State, as *parens patriae*, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction--

(A) to enjoin further violation of section 5 of this Act by the defendant; or

(B) to obtain damages on behalf of residents of the State, in an amount equal to the greater of--

(i) the actual monetary loss suffered by such residents; or

(ii) the amount determined under paragraph (3).

(2) AVAILABILITY OF INJUNCTIVE RELIEF WITHOUT SHOWING OF KNOWLEDGE- Notwithstanding any other provision of this Act, in a civil action under paragraph (1)(A) of this subsection, the attorney general, official, or agency of the State shall not be required to allege or prove the state of mind required by section 5(a)(1)(C), section 5(a)(2), clause (ii), (iii), or (iv) of section 5(a)(4)(A), section 5(b)(1)(A), or section 5(b)(3).

(3) Statutory damages-

(A) IN GENERAL- For purposes of paragraph (1)(B)(ii), the amount determined under this paragraph is the amount calculated by multiplying the number of violations (with each separately addressed unlawful message received by or addressed to such residents treated as a separate violation) by up to \$250.

(B) LIMITATION- For any violation of section 5 (other than section 5(a)(1)), the amount determined under subparagraph (A) may not exceed \$2,000,000.

(C) AGGRAVATED DAMAGES- The court may increase a damage award to an amount equal to not more than three times the amount otherwise available under this paragraph if--

(i) the court determines that the defendant committed the violation willfully and knowingly; or

(ii) the defendant's unlawful activity included one or more of the aggravating violations set forth in section 5(b).

(D) REDUCTION OF DAMAGES- In assessing damages under subparagraph (A), the court may consider whether--

(i) the defendant has established and implemented, with due care, commercially reasonable practices and procedures designed to effectively prevent such violations; or

(ii) the violation occurred despite commercially reasonable efforts to maintain compliance the practices and procedures to which reference is made in clause (i).

(4) ATTORNEY FEES- In the case of any successful action under paragraph (1), the court, in its discretion, may award the costs of the action and reasonable attorney fees to the State.

(5) RIGHTS OF FEDERAL REGULATORS- The State shall serve prior written notice of any action under paragraph (1) upon the Federal Trade Commission or the appropriate Federal regulator determined under subsection (b) and provide the Commission or appropriate Federal regulator with a copy of its complaint, except in any case in which such prior notice is not feasible, in which case the State shall serve such notice immediately upon instituting such action. The Federal Trade Commission or appropriate Federal regulator shall have the right--

(A) to intervene in the action;

(B) upon so intervening, to be heard on all matters arising therein;

(C) to remove the action to the appropriate United States district court; and

(D) to file petitions for appeal.

(6) CONSTRUCTION- For purposes of bringing any civil action under paragraph (1), nothing in this Act shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to--

(A) conduct investigations;

(B) administer oaths or affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

(7) VENUE; SERVICE OF PROCESS-

(A) VENUE- Any action brought under paragraph (1) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(B) SERVICE OF PROCESS- In an action brought under paragraph (1), process may be served in any district in which the defendant--

(i) is an inhabitant; or

(ii) maintains a physical place of business.

(8) LIMITATION ON STATE ACTION WHILE FEDERAL ACTION IS PENDING- If the Commission, or other appropriate Federal agency under subsection (b), has instituted a civil action or an administrative action for

violation of this Act, no State attorney general, or official or agency of a State, may bring an action under this subsection during the pendency of that action against any defendant named in the complaint of the Commission or the other agency for any violation of this Act alleged in the complaint.

(9) REQUISITE SCIENTER FOR CERTAIN CIVIL ACTIONS- Except as provided in section 5(a)(1)(C), section 5(a)(2), clause (ii), (iii), or (iv) of section 5(a)(4)(A), section 5(b)(1)(A), or section 5(b)(3), in a civil action brought by a State attorney general, or an official or agency of a State, to recover monetary damages for a violation of this Act, the court shall not grant the relief sought unless the attorney general, official, or agency establishes that the defendant acted with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, of the act or omission that constitutes the violation.

(g) Action by Provider of Internet Access Service-

(1) ACTION AUTHORIZED- A provider of Internet access service adversely affected by a violation of section 5(a)(1), 5(b), or 5(d), or a pattern or practice that violates paragraph (2), (3), (4), or (5) of section 5(a), may bring a civil action in any district court of the United States with jurisdiction over the defendant--

(A) to enjoin further violation by the defendant; or

(B) to recover damages in an amount equal to the greater of--

(i) actual monetary loss incurred by the provider of Internet access service as a result of such violation; or

(ii) the amount determined under paragraph (3).

(2) SPECIAL DEFINITION OF 'PROCURE'- In any action brought under paragraph (1), this Act shall be applied as if the definition of the term 'procure' in section 3(12) contained, after 'behalf' the words 'with actual knowledge, or by consciously avoiding knowing, whether such person is engaging, or will engage, in a pattern or practice that violates this Act'.

(3) STATUTORY DAMAGES-

(A) IN GENERAL- For purposes of paragraph (1)(B)(ii), the amount determined under this paragraph is the amount calculated by multiplying the number of violations (with each separately addressed unlawful message that is transmitted or attempted to be transmitted over the facilities of the provider of Internet access service, or that is transmitted or attempted to be transmitted to an electronic mail address obtained from the provider of Internet access service in violation of section 5(b)(1)(A)(i), treated as a separate violation) by--

(i) up to \$100, in the case of a violation of section 5(a)(1);

or

(ii) up to \$25, in the case of any other violation of section

5.

(B) LIMITATION- For any violation of section 5 (other than section 5(a)(1)), the amount determined under subparagraph (A) may not exceed \$1,000,000.

(C) AGGRAVATED DAMAGES- The court may increase a damage award to an amount equal to not more than three times the amount otherwise available under this paragraph if--

(i) the court determines that the defendant committed the violation willfully and knowingly; or

(ii) the defendant's unlawful activity included one or more of the aggravated violations set forth in section 5(b).

(D) REDUCTION OF DAMAGES- In assessing damages under subparagraph (A), the court may consider whether--

(i) the defendant has established and implemented, with due care, commercially reasonable practices and procedures designed to effectively prevent such violations; or

(ii) the violation occurred despite commercially reasonable efforts to maintain compliance with the practices and procedures to which reference is made in clause (i).

(4) ATTORNEY FEES- In any action brought pursuant to paragraph (1), the court may, in its discretion, require an undertaking for the payment of the costs of such action, and assess reasonable costs, including reasonable attorneys' fees, against any party.

## **SEC. 8. EFFECT ON OTHER LAWS.**

(a) FEDERAL LAW- (1) Nothing in this Act shall be construed to impair the enforcement of section 223 or 231 of the Communications Act of 1934 (47 U.S.C. 223 or 231, respectively), chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, United States Code, or any other Federal criminal statute.

(2) Nothing in this Act shall be construed to affect in any way the Commission's authority to bring enforcement actions under FTC Act for materially false or deceptive representations or unfair practices in commercial electronic mail messages.

(b) STATE LAW-

(1) IN GENERAL- This Act supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.

(2) STATE LAW NOT SPECIFIC TO ELECTRONIC MAIL- This Act shall not be construed to preempt the applicability of--

(A) State laws that are not specific to electronic mail, including State trespass, contract, or tort law; or

(B) other State laws to the extent that those laws relate to acts of fraud or computer crime.

(c) NO EFFECT ON POLICIES OF PROVIDERS OF INTERNET ACCESS SERVICE- Nothing in this Act shall be construed to have any effect on the lawfulness or unlawfulness, under any other provision of law, of the adoption, implementation, or enforcement by a provider of Internet access service of a policy of declining to transmit, route, relay, handle, or store certain types of electronic mail messages.

## **SEC. 9. DO-NOT-E-MAIL REGISTRY.**

(a) IN GENERAL- Not later than 6 months after the date of enactment of this Act, the Commission shall transmit to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Energy and Commerce a report that--

- (1) sets forth a plan and timetable for establishing a nationwide marketing Do-Not-E-Mail registry;
- (2) includes an explanation of any practical, technical, security, privacy, enforceability, or other concerns that the Commission has regarding such a registry; and
- (3) includes an explanation of how the registry would be applied with respect to children with e-mail accounts.

(b) AUTHORIZATION TO IMPLEMENT- The Commission may establish and implement the plan, but not earlier than 9 months after the date of enactment of this Act.

## **SEC. 10. STUDY OF EFFECTS OF COMMERCIAL ELECTRONIC MAIL.**

(a) IN GENERAL- Not later than 24 months after the date of the enactment of this Act, the Commission, in consultation with the Department of Justice and other appropriate agencies, shall submit a report to the Congress that provides a detailed analysis of the effectiveness and enforcement of the provisions of this Act and the need (if any) for the Congress to modify such provisions.

(b) REQUIRED ANALYSIS- The Commission shall include in the report required by subsection (a)--

- (1) an analysis of the extent to which technological and marketplace developments, including changes in the nature of the devices through which consumers access their electronic mail messages, may affect the practicality and effectiveness of the provisions of this Act;
- (2) analysis and recommendations concerning how to address commercial electronic mail that originates in or is transmitted through or to facilities or computers in other nations, including initiatives or policy positions that the Federal Government could pursue through international negotiations, fora, organizations, or institutions; and

(3) analysis and recommendations concerning options for protecting consumers, including children, from the receipt and viewing of commercial electronic mail that is obscene or pornographic.

**SEC. 11. IMPROVING ENFORCEMENT BY PROVIDING REWARDS FOR INFORMATION ABOUT VIOLATIONS; LABELING.**

The Commission shall transmit to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Energy and Commerce--

(1) a report, within 9 months after the date of enactment of this Act, that sets forth a system for rewarding those who supply information about violations of this Act, including--

(A) procedures for the Commission to grant a reward of not less than 20 percent of the total civil penalty collected for a violation of this Act to the first person that--

(i) identifies the person in violation of this Act; and

(ii) supplies information that leads to the successful collection of a civil penalty by the Commission; and

(B) procedures to minimize the burden of submitting a complaint to the Commission concerning violations of this Act, including procedures to allow the electronic submission of complaints to the Commission; and

(2) a report, within 18 months after the date of enactment of this Act, that sets forth a plan for requiring commercial electronic mail to be identifiable from its subject line, by means of compliance with Internet Engineering Task Force Standards, the use of the characters 'ADV' in the subject line, or other comparable identifier, or an explanation of any concerns the Commission has that cause the Commission to recommend against the plan.

**SEC. 12. RESTRICTIONS ON OTHER TRANSMISSIONS.**

Section 227(b)(1) of the Communications Act of 1934 (47 U.S.C. 227(b)(1)) is amended, in the matter preceding subparagraph (A), by inserting ` , or any person outside the United States if the recipient is within the United States' after `United States'.

**SEC. 13. REGULATIONS.**

(a) IN GENERAL- The Commission may issue regulations to implement the provisions of this Act (not including the amendments made by sections 4 and 12). Any such regulations shall be issued in accordance with section 553 of title 5, United States Code.

(b) LIMITATION- Subsection (a) may not be construed to authorize the Commission to establish a requirement pursuant to section 5(a)(5)(A) to include any specific words, characters, marks, or labels in a commercial electronic mail message, or to include the identification required by section 5(a)(5)(A) in any particular part of such a mail message (such as the subject line or body).

#### **SEC. 14. APPLICATION TO WIRELESS.**

(a) EFFECT ON OTHER LAW- Nothing in this Act shall be interpreted to preclude or override the applicability of section 227 of the Communications Act of 1934 (47 U.S.C. 227) or the rules prescribed under section 3 of the Telemarketing and Consumer Fraud and Abuse Prevention Act (15 U.S.C. 6102).

(b) FCC RULEMAKING- The Federal Communications Commission, in consultation with the Federal Trade Commission, shall promulgate rules within 270 days to protect consumers from unwanted mobile service commercial messages. The Federal Communications Commission, in promulgating the rules, shall, to the extent consistent with subsection (c)--

(1) provide subscribers to commercial mobile services the ability to avoid receiving mobile service commercial messages unless the subscriber has provided express prior authorization to the sender, except as provided in paragraph (3);

(2) allow recipients of mobile service commercial messages to indicate electronically a desire not to receive future mobile service commercial messages from the sender;

(3) take into consideration, in determining whether to subject providers of commercial mobile services to paragraph (1), the relationship that exists between providers of such services and their subscribers, but if the Commission determines that such providers should not be subject to paragraph (1), the rules shall require such providers, in addition to complying with the other provisions of this Act, to allow subscribers to indicate a desire not to receive future mobile service commercial messages from the provider--

(A) at the time of subscribing to such service; and

(B) in any billing mechanism; and

(4) determine how a sender of mobile service commercial messages may comply with the provisions of this Act, considering the unique technical aspects, including the functional and character limitations, of devices that receive such messages.

(c) OTHER FACTORS CONSIDERED- The Federal Communications Commission shall consider the ability of a sender of a commercial electronic mail message to reasonably determine that the message is a mobile service commercial message.

(d) MOBILE SERVICE COMMERCIAL MESSAGE DEFINED- In this section, the term 'mobile service commercial message' means a commercial electronic mail message that is transmitted directly to a wireless device that is utilized by a subscriber of commercial mobile service (as such term is defined in section

332(d) of the Communications Act of 1934 (47 U.S.C. 332(d)) in connection with such service.

**SEC. 15. SEPARABILITY.**

If any provision of this Act or the application thereof to any person or circumstance is held invalid, the remainder of this Act and the application of such provision to other persons or circumstances shall not be affected.

**SEC. 16. EFFECTIVE DATE.**

The provisions of this Act, other than section 9, shall take effect on January 1, 2004.