CAN-SPAM and You

Emailing Within the Law

Anne P. Mitchell, Esq.
President

Institute for Spam and
Internet Public Policy

10 Things You Should Know About CAN-SPAM

1. CAN-SPAM applies only to commercial email.

2. CAN-SPAM applies to email for which a primary purpose is to feature your goods, services, or content even if you do not send the email yourself; however

3. CAN-SPAM does not apply to third-party advertisers who advertise in your mailings.

4. CAN-SPAM can apply to email sent out by your affiliates on your behalf; however

5. CAN-SPAM will not apply to email sent out by your affiliates on your behalf unless you know, or should know, that the email is being sent in violation of CAN-SPAM and you stand to gain from it financially, and you don't try to stop it.

6. CAN-SPAM requires that all information in your email headers and body be true, accurate, and not misleading.

7. CAN-SPAM requires you to provide a fully-functioning means of return Internet-based communication for the purpose of the recipient opting-out of your mailings.

8. CAN-SPAM requires you to honor those opt-out requests, and to immediately cease sharing the user's address even with previously agreed-to partners.

9. CAN-SPAM does not require that you use confirmed opt-in for your mailings, however it is one of the best defenses against an accusation of CAN-SPAM violation.

10. CAN-SPAM does not require ISPs to accept email which is CAN-SPAM compliant. In fact, ISPs are specifically exempted from claims that they must accept email if it complies with CAN-SPAM.

1. INTRODUCTION

Federal Senate Bill 877, affectionately known as the "CAN-SPAM Act of 2003" ("Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003"), or just "CAN-SPAM" for short, was passed by the United States Senate in November of 2003, and agreed to by the House of Representatives and signed into law by President George W. Bush in December of 2003.

It is important to keep in mind that this is a brand new law. This means that it has not yet been reviewed by the Court, and the advice you get from anyone regarding the requirements and prohibitions of this law are only as good as their skill at legal construction coupled with their expertise in the industry.

The full text of the parts of CAN-SPAM which are relevant to this book appear in Appendix A.

A note about ISIPP Standards: Throughout this book you will see notes prefaced with "ISIPP Standard". These are notes describing relevant industry standards which were developed and adopted by bulk mailers, online marketers, and ISPs throughout the industry in conjunction with the Institute for Spam and Internet Public Policy ("ISIPP") and the Email Processing Industry Alliance. These are provided as a point of interest and are advisory only, and are not part of the CAN-SPAM Act. They are, however, considered by many to be best practices and will help to ensure delivery of your legitimate commercial email. The full set of ISIPP Standards appears in Appendix B.

2. THE BASICS

I. Cast of Characters

The portions of CAN-SPAM with which we are concerned regulate email which has the potential to benefit, impact, or otherwise touch four separate and distinct parties:

Party #1. The sender of the email ("sender").

Party #2. The vendor whose goods, services or content are primarily featured in the email ("vendor").

Party #3. Third-party advertisers who take advertising space in the email ("third-party advertiser").

Party #4. The recipient of the email ("recipient").

Some interesting notes about the parties:

a. The sender and the vendor can be, and often are, the same entity.

b. The sender may be an affiliate of the vendor.

c. Sender may be a mailer-for-hire retained by vendor to send out their email campaign.

d. The sender may, in some cases, be unknown to the vendor.

e. CAN-SPAM is overwhelmingly concerned with the behaviour of whomever has obtained and is using the recipient's email address as a target for commercial email. This will always be either the sender, the vendor, or both the sender and the vendor.

f. CAN-SPAM is also concerned with the relationships between the sender, the vendor, and the recipient. CAN-SPAM generally takes little notice of third-party advertisers unless there is a relationship other than "publisher/advertiser" between the third-party advertiser and the sender or the vendor.

g. CAN-SPAM does not care about whether or not there is a relationship between a third-party advertiser and the recipient.

II. Anatomy of an Email

In order to really understand the prohibitions contained in CAN-SPAM, one must have a level of familiarity with the construction of an email message beyond "it came, I read, I deleted".

Email consists of two primary parts: the "header", and the "body".

The header is the part of the email which contains information about from where the email originated, the path it took to get to its final destination, the email account which initiated the email, the destination email account, and the subject of the email. Most email programs separate the header information into two parts: that which is typically revealed to the average user when they view the email with their email program (such as the "From:" address, the "To:" address, and the "Subject" line, and that which is hidden from sight unless you really go looking for it (such as the routing information).

The body is the actual email message itself.

There can be other parts to email, such as file attachments, but we need not concern ourselves with those for our purposes.

Now that you understand who the parties are, and the parts of an email message with which we are concerned, it's time to discuss what CAN-SPAM requires of you relative to each.

3. DOING IT RIGHT: DO THESE!

The list of things which CAN-SPAM requires for commercial email is nearly as long as the list of things which are prohibited. Fortunately, despite the doomsayers, neither list is terribly onerous, and if you are an emailer or online marketer who is concerned about your own good image and doing the right thing, you are probably already doing most of the things required by CAN-SPAM.

I. Make Sure That Every Single Bit of Information in Your Headers is Accurate, True, and in No Way Misleading.

If your email already meets this requirement, you are so very well on your way to CAN-SPAM compliance that you almost don't need to read the rest of this book. Almost.

In fact, this first requirement is so important, that it bears repeating:

"Make sure that every single bit of information in your headers is accurate, true, and in no way misleading."

a. "From:" Lines

Your "From:" line must accurately identify the entity which actually sent the email. In this context "entity which actually sent the email" can mean either the entity which is featured in or provided the content of the email (the vendor) or the entity which actually sent the email out on the vendor's behalf (the sender). Remember that the sender and the vendor are often the same entity.

Note that if your email is sent from or through a computer which does not belong to you, and your use of or access to that computer was obtained through false or fraudulent means, or it is used simply as a means of disguising the actual point of origin of your email, then even if all of your header information is technically accurate, you will be in violation of CAN-SPAM. Don't do it.

b. "Subject:" Lines

Your subject lines must contain accurate, truthful information. Stupidity, on the part of either the sender or vendor, or the recipient, is no defense. If you didn't realize that your subject line could be misconstrued, but you should have realized that your subject line could be misconstrued, CAN-SPAM will still get you.

Similarly, if you think that any idiot should be able to figure out what your subject line means, but in fact many idiots receiving your email think that it means something else, CAN-SPAM may side with the idiots. In short, make sure that your subject lines are very clear in conveying the reason for and content of your email.

c. Origin, Routing, and Destination Information

It should go without saying that not including accurate information about the origin of the email, the destination of the email, and the route it took to get from here to there, is asking for trouble. It should go without saying, but just in case, there, it's been said. Fortunately, for the most part this is a case where you have to really want to do the wrong thing in order to end up doing the wrong thing. Generally speaking, properly set up outbound mail processes will do the right thing all on their own, and correct and accurate origin, routing, and destination information will be provided.

ISIPP Standard: The ISIPP Standard regarding multiple recipient addresses in a single piece of mailing list email suggests that all mailing list mail should be sent "one address per piece", meaning that each piece should be addressed only to the primary recipient, and should not be cc:ed or bcc:ed to additional addresses. If there are 100 users on the list, 100 individual pieces of email should be sent.

II. Immediately and Zealously Honour Opt-Out and Unsubscribe Requests

a. Every commercial email must contain some sort of Internet-based opt-out mechanism. This can be something as simple as an email address to which the recipient can respond requesting to be removed from the mailing list, to a sophisticated coded URL which, when clicked, automatically identifies and unsubscribes the recipient from a particular mailing.

ISIPP Standard: The ISIPP Standards for the handling and processing of unsubscribe (opt-out) requests include that the process should be as simple as possible (one step as compared to two or more steps), and should result in the subscriber being immediately removed from the mailing list.

b. Once a recipient has opted-out of a mailing, or otherwise requested to be removed from your mailing list, you must:

i. Remove them from the mailing list.
ii. Not send email to them again.
iii. Not add them to any other mailing list.
iv. Not share their email address with anybody else, including partners with whom the opting-out recipient had previously agreed to have their email address shared.

Note that CAN-SPAM does not require you to forward or otherwise share the opt-out request with your partners, and, indeed, it is not recommended that you do so, as to do so would violate CAN-SPAM's prohibition against sharing the opting-out recipient's email address with anybody following the opt-out event. This makes perfect sense when you think about it: if the recipient has been added to your partners' mailing list, it is that partner's responsibility to mail that recipient in accordance with CAN-SPAM's requirements.

CAN-SPAM gives you ten days from the date that you receive the opt-out request to purge the email address from your mailings, but it is recommended that you do it as soon as possible after receiving the request.

III. Include Your Business Address

CAN-SPAM requires that you include in your email "a valid physical postal address". It is open to debate as to whether a post office box satisfies this requirement. It is safer to assume that the answer is "no", and to include a real street address. That said, however, practically speaking if you are doing everything right, and comply with all other provisions of CAN-SPAM, you are extremely unlikely to be hauled into court just for using a post office box instead of a street address in your email.

IV. Provide Indication if the Email is an Advertisement

If the email you are sending is an advertisement or solicitation, and you do not have the prior affirmative consent of the recipient to send them such email, then you must provide in the message "a clear and conspicuous identification that the message is an advertisement or solicitation".

V. Clearly Mark Sexually Explicit Material

If your business includes the provision of material which is sexually explicit, you must indicate the presence of sexually explicit content in the "subject:" line, using the marks or terms developed and required by the Federal Trade Commission. The Federal Trade Commission has until the end of April, 2004, to develop these marks and terms, and as of the time of this writing, they have not yet done so. In theory, you do not have to comply with this requirement until the FTC announces these marks and terms. However, to be safe, you should consider developing and using your own "subject:" line terms to indicate sexually explicit material until the FTC announces the ones which they have developed.

4. THE 7 DEADLY EMAIL SINS: DON'T DO THESE!

In addition to the requirements outlined above, here are several prohibitions contained in CAN-SPAM. Most of these are obvious, and not anything any legitimate mailer would do anyways. Some of them are restatements of the requirements above. All of them need to be strictly followed.

I. Do Not Send to Harvested Email Addresses

This includes addresses which you yourself have harvested and those which have been harvested by others. CAN-SPAM defines "harvesting" as meaning that the email address of the recipient "was obtained using an automated means from an Internet website or proprietary online service operated by another person". While the law specifically applies to email addresses harvested from a site which, at the time that the email address was added to the site, promised that the email address would not be transferred to another party, unless you are absolutely sure that this was not the case for each and every email address on the harvested list, you are better off just staying completely way from harvested email addresses.

II. Don't Use Automated Means to Try to Guess at Email Addresses

This rule refers specifically to so-called "dictionary attacks", or, as CAN-SPAM describes it, "using an automated means that generates possible electronic mail

addresses by combining names, letters, or numbers into numerous permutations". This means that you cannot do this, you cannot have someone else do this for you, you cannot let your email be sent out via this method, and you can't send email to addresses obtained by this method. Period.

III. Don't Use an Automated Process to Sign Up for Multiple Email or User Accounts.

CAN-SPAM specifically prohibits using an automated process to sign up for, register, or otherwise create multiple email addresses or user accounts for the purpose of sending email which would otherwise violate the law.

IV. Don't Send Email From or Through Any Computer for Which You Do Not Have Access or Use Permission

This includes using open relays, open proxies, and any terminals, computers, or computer networks to which you do not have specific permitted access.

V. Don't Send Email Which Contains Misleading, Deceptive, or Fraudulent Header Information or Content.

Be sure that your header information is complete, truthful and accurate, that the subject of your email clearly identifies the purpose and content of your email, and that the content is neither deceptive or misleading.

VI. Don't Continue to Send Email to Someone Who Has Opted-Out or Unsubscribed from Your Mailing List.

Tempting though it may be, remove them from your list. CAN-SPAM gives you ten days to accomplish this task, however it is recommended that you do it as soon as you possibly can to avoid any problems.

VII. Don't Share or Otherwise Transfer the Email Address of Someone Who Has Opted-Out or Unsubscribed from Your Mailing List to Anyone Else.

This applies even to partners with whom the email address owner had previously agreed to your sharing their email address. Once you get a request to be removed from your mailing list, don't share that email address with anyone else, ever. Also, make sure that you don't keep the email address anywhere that someone could accidentally or intentionally discover it and send mail to it, as that too may be a violation of this provision.

And finally, remember that if you have someone else send your mailing out for you, and the methods they use to send out your mailing violate CAN-SPAM, and you knew or should have known that they were using such unpermitted methods, you are as liable under the law as are they. No longer can vendors avoid liability by hiding behind "it wasn't me who pressed "send"!"

5. CONCLUSION

The purpose of CAN-SPAM is to help define and brighten the line between legitimate and illegitimate email, and to help law enforcement agencies to find and prosecute spammers.

Whether or not you agree with the way in which the line has been drawn, ethical emailers will abide by the requirements and prohibitions of CAN-SPAM, distinguishing themselves from those who aren't, and don't.

Think of CAN-SPAM as the minimum daily requirement for establishing the legitimacy and helping to ensure the delivery of your email. Many emailers already adhere to standards as tight or tighter than those demanded by the new Federal law, and have found that their business has not only not suffered for it, but in fact has improved as their online reputation has gained, and they pay only to send email to those who really want to receive it and who are receptive to their message.

APPENDIX A: Selected Sections of the CAN-SPAM Act of 2003

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. 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.

APPENDIX B: ISIPP Industry Standards

I. Bounce Handling:

1. Bounce Handling Policy: senders should mark an address as "dead", meaning the sender should remove the address from the delivery list and not attempt to deliver to the address until the sender has reason to believe that delivery rejection would not occur, if the following two conditions are both met:

A. Three (3) consecutive delivery rejections have occurred; AND

B. The time between the most recent consecutive delivery rejection and the initial consecutive delivery rejection is greater than fifteen days.

A sender should have the capability to manage delivery rejections differently between ISPs, whether based on previous agreements or explicit requests from these ISPs.

2. Reply Coding Standards: receiving systems should comply with RFC and DSN codes. RFC 821, DSN or RFC 1894 are relevant standards. For example, ISPs can use RFC 550 5.7.1 "Go Away" to indicate that the ISP is intentionally rejecting the delivery of an email that is thought to be in violation of the list hygiene policies indicated herein.

Link to white paper regarding bounce handling
Link to PowerPoint presentation regarding bounce handling standards

II. Publication of Email Permissions Policies for Sending and Receiving of Email

Both receivers (ISPs and spam filtering companies) and senders (such as email service providers, email campaign provders, and email service bureaus) should publish clear, publicly accessible requirement as to what they require for receipt and transmission of email, and sending of email, respectively. These requirements should be applied consistently.

Receivers

1. Establish, implement, and post requirements for acceptance and delivery of e-mail (including first line contact information for delivery issue reporting) clearly on website, and apply consistently.

2. Establish, implement and publish uniform processes for complaint feedback loop clearly on website and apply consistently.

Senders

1. Establish, implement, and post a policy prohibiting the sending of unsolicited commercial e-mail (spam) clearly on website and enforce the policy consistently.

2. Implement automated system to process complaints, requests to unsubscribe, and delivery failure notifications. Additionally, honor all requests from recipients to modify permission preferences.

Link to Publication of Email Permissions Policies for Sending and Receiving Email PowerPoint presentation

III. Unsubscribe Request Handling

1. List managers should endeavor to provide an unsubscribe process which requires the fewest number of "clicks" possible. A "1-click" unsubscribe process is the ideal; it is understood that in some minority of instances, a 2-click process may be necessary for security reasons. Subscribers

should not have to go through the process of having to provide a password or to surmount other obstacles to removing themselves from mailings they no longer wish to receive.

2. An unsubscribe request should result in the subscriber being immediately removed from the mailing list, and subscribers should not be required to continue to receive, and should not continue to receive, certain types of mailings from the sending site once they have submitted their unsubscribe request. An exception to the latter is understood for free sites which as part of their terms and conditions require users to receive promotional mailings in exchange for free services.

3. If the ongoing receipt of certain types of email is required in order for a user to participate and continue to participate in a program, this should be made very clear and explicit during the sign-up process, and before the user concludes the sign-up process.

IV. Multiple Addresses in Mailing List Mail

All mailing list mail should be sent "one address per piece", meaning that each piece should be addressed only to the primary recipient, and should not be cc:ed or bcc:ed to additional addresses. If there are 100 users on the list, 100 individual pieces of email should be sent.

V. Communication Between Senders and Receivers (EDDB)

Senders and receivers should participate in an inter-industry communications facilitation program to help ensure that they can communicate effectively and in a timely manner when an email delivery problem occurs. This can be ISIPP's Email Deliverability Database, or another such program.

ISIPP has developed the Email Deliverability Database ("EDDB") in order to support this standard. The objective of EDDB is to facilitate communications between sending and receiving systems regarding email transmission. This helps to ensure that users get the email they want, that legitimate email gets delivered, that spam does not get through, and that delivery issues are resolved quickly.

EDDB allows participants to have immediate access to contact information for organizations in the sending and receiving industries. Access is set up such that one can only access information about one's analog at the other organization. So, for example, someone at a help desk at a sending organization can contact someone at the abuse desk at a receiving site, or vice versa, while a manager at either organization would be able to access contact information for both management and the desk at the other organization, and the CEO of one organization would have access to the contact information for everyone from the CEO on down at the other organization.

Link to flash presentation regarding how EDDB works

Link to sign up for EDDB

APPENDIX C: Resources

A. Subscribe to ISIPP's Spam Law and Policies Updates

B. "Deliver Me: Ensuring that Your Email Gets Delivered" eDeliverability eBook

C. Institute for Spam and Internet Public Policy ("ISIPP")
Experts, Analysts, and Consulting to the Public and Private Sectors regarding the Internet and Spam

D. Full text of CAN-SPAM Act of 2003 at SpamLaws.com

ABOUT THE AUTHOR

Anne P. Mitchell is an attorney, and the President and CEO of the Institute for Spam and Internet Public Policy. A graduate of Stanford Law School, and a Professor of Law at Lincoln Law School of San Jose, Mitchell is considered to be an expert in the email industry in general, and spam and email deliverability issues in particular, and is the Chair of the Email Processing Industry Alliance. Previously a founder of Habeas, Inc., and before that the Director of Legal and Public Affairs for Mail Abuse Prevention System, Mitchell has been involved in all levels and aspects of Internet and Spam law and public policy, and often consults with legislators, attorneys, and other leaders in both the public and private sectors.