Contemporary Legal Notes

Washington Legal Foundation
Advocate for freedom and justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302

UNDERSTANDING & COMPLYING WITH THE "CAN-SPAM" ACT

by
Kristen J. Mathews
Brown Raysman Millstein
Felder & Steiner LLP

Washington Legal Foundation
CONTEMPORARY LEGAL NOTE Series
Number 47
September 2004

TABLE OF CONTENTS

ABOUT WLF'S LEGAL STUDIES DIVISION

The Washington Legal Foundation (WLF) established its Legal Studies Division to address cutting-edge legal issues by producing and distributing substantive, credible publications targeted at educating policy makers, the media, and other key legal policy outlets.

Washington is full of policy centers of one stripe or another. But WLF's Legal Studies Division has deliberately adopted a unique approach that sets it apart from other organizations.

First, the Division deals almost exclusively with legal policy questions as they relate to the principles of free enterprise, legal and judicial restraint, and America's economic and national security.

Second, its publications focus on a highly select legal policy-making audience. Legal Studies aggressively markets its publications to federal and state judges and their clerks; members of the United States Congress and their legal staffs; government attorneys; business leaders and corporate general counsel; law school professors and students; influential legal journalists; and major print and media commentators.

Third, Legal Studies possesses the flexibility and credibility to involve talented individuals from all walks of life — from law students and professors to sitting federal judges and senior partners in established law firms — in its work.

The key to WLF's Legal Studies publications is the timely production of a variety of readable and challenging commentaries with a distinctly common-sense viewpoint rarely reflected in academic law reviews or specialized legal trade journals. The publication formats include the provocative COUNSEL'S ADVISORY, topical LEGAL OPINION LETTERS, concise LEGAL BACKGROUNDERS on emerging issues, in-depth WORKING PAPERS, useful and practical CONTEMPORARY LEGAL NOTES, law review-length MONOGRAPHS, and occasional books.

WLF's LEGAL OPINION LETTERS and LEGAL BACKGROUNDERS appear on the LEXIS/NEXIS® online information service under the filename "WLF." All WLF publications are also available to Members of Congress and their staffs through the Library of Congress' SCORPIO system.

To receive information about previous WLF publications, contact Glenn Lammi, Chief Counsel, Legal Studies Division, Washington Legal Foundation, 2009 Massachusetts Avenue, NW, Washington, D.C. 20036, (202) 588-0302. Material concerning WLF's other legal activities may be obtained by contacting DanielJ.Popeo,Chairman.

ABOUT THE AUTHOR

Kristen J. Mathews is an associate in the New York office of Brown Raysman Millstein Felder & Steiner LLP.

UNDERSTANDING & COMPLYING WITH THE "CAN-SPAM" ACT

by

Kristen J. Mathews
Brown Raysman Millstein Felder & Steiner LLP

On January 1, 2004, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003[1] (hereinafter, the "CAN-SPAM Act" or the "Act") took effect. The Act governs activities relating to commercial e-mail communications, and expressly supercedes all state laws to the extent that they addressed the permissibility of unsolicited commercial e-mail.[2] In the absence of extensive federal rulemaking and significant judicial decisions that further interpret the Act, companies need to carefully evaluate the Act's provisions, inherent ambiguities and various potential interpretations.[3]

This CONTEMPORARY LEGAL NOTE focuses on the implications of the Act, providing an overview of it and its requirements, and exploring the issues that it raises from both a legal and practical perspective.

I. THE ACT IN GENERAL

The Act's requirements affect essentially all of the types of activities that are commonly conducted in connection with a commercial e-mail campaign. For example, the Act provides requirements associated with:

- sending marketing e-mails to individuals, whether or not they have opted-in to receive such e-mails from the company;
- retaining the services of a third party to send marketing e-mails on the company's behalf;
- providing consideration or other inducements to a third party to send e-mails promoting the company's products or services (e.g., affiliate marketing);
- obtaining e-mail addresses or lists from third parties for e-mail marketing purposes;

- sending marketing e-mails on behalf of another company or advertiser;
- sending joint marketing e-mails, regardless of which company actually transmits the e-mails and regardless of which company's mailing list is used;
- sending commercial e-mails containing third party ads or promotions (including banner ads);
- placing advertisements or promotions in another company's commercial e-mails;
- obtaining e-mail addresses from an unauthorized source, or by automatically deriving them;
- operating a "refer-a-friend" feature or promotion; and
- sending commercial e-mail messages to wireless devices.

In general, the Act provides certain requirements associated with the sending of commercial electronic mail messages, and imposes both criminal and civil liability for the violation of such requirements. For example, the Act:

- requires inclusion of an opt-out notice and mechanism in commercial e-mails;[4]
- requires the honoring of opt-out requests from recipients;[5]
- requires, in some cases, identification of commercial e-mails as advertisements or solicitations;[6]
- requires inclusion in commercial e-mails of the valid physical postal address of the sender(s);[7]
- prohibits sending of e-mail messages with false or misleading header information or subject headings, or using an originating e-mail address, domain name or IP address that was accessed by means of false of fraudulent pretences or representations;[8]
- prohibits e-mail address harvesting and dictionary attacks;[9]
- prohibits unauthorized use of computers to send multiple commercial e-mail messages;[10]
- prohibits unauthorized access to computers or networks to relay or transmit unlawful commercial e-mail;[11]

- prohibits the transmission of multiple commercial e-mail messages with the intent to conceal the origin of the messages;[12]

- prohibits the registration of e-mail or user accounts or domain names using a false identity to send multiple commercial e-mails;[13]

- prohibits the automatic generation of multiple e-mail accounts from which to send unlawful commercial e-mail;[14]

- prohibits the false representation as the registrant of, or successor to, IP addresses to send multiple commercial e-mails;[15] and

- regulates the labeling of sexually oriented e-mail.[16]

The Act may be enforced by certain governmental entities, such as: (i) the Federal Trade Commission ("FTC"), (ii) with respect to certain types of entities, other federal agencies that have authority over those particular types of entities (for example, the Securities and Exchange Commission has authority to enforce the Act against securities brokers and dealers), and (iii) with some limitations, state attorneys general and other state officials and agencies.[17] In addition, Internet access service providers who are adversely affected by a violation of the Act may, in some cases, bring a civil action under the Act.[18]

A company's e-mail marketing practices should not only comply with the Act, but also with any operative privacy policies, contractual obligations, and with other applicable state and federal laws (including without limitation the Children's Online Privacy Protection Act, the Gramm-Leach-Bliley Act and the Heath Insurance Portability and Accountability Act) and, if applicable, foreign laws.[19]

II. SCOPE AND APPLICABILITY OF THE ACT[20]

A. Commercial E-mails

In general, the provisions of the Act apply to commercial electronic mail messages (defined by the Act as "Commercial Electronic Mail Messages" and referred to herein as "Commercial E-Mail").[21] Commercial E-Mail includes any e-mail message, the "primary purpose" of which is the "commercial advertisement or promotion of a commercial product or service."[22] This includes the advertisement or promotion of content on an Internet web site operated for a commercial purpose, provided, however, that the inclusion in an e-mail message of a reference to a commercial entity or a link to the web site of a commercial entity does not, by itself, cause such message to be treated as a Commercial E-Mail if the contents or circumstances of the message indicate a primary purpose other than the commercial

advertisement or promotion of a commercial product or service.[23]

The Act does not provide a definition of "primary purpose," and thus the application of the "primary purpose" test is difficult. Apparently, Congress recognized the difficultly, and directed the FTC to issue regulations by the end of 2004 defining the relevant criteria to facilitate the determination of the primary purpose of an e-mail message.[24]

In August 2004, the FTC issued a Notice of Proposed Rulemaking and Request for Public Comment (NPR) on this topic.[25] The NPR proposes a tri-category framework (discussed further in Section II.A.2 below) for determining the primary purpose of an electronic message, using the Act's definition of a "transactional or relationship message" to define the key term used in the NPR: "transactional or relationship *content*."[26] That key term is then used in the proposed regulation to determine the "primary purpose" of an electronic message.[27]

1. Transactional or Relationship Messages

Transactional or Relationship Messages (as defined by the Act) are specifically excluded from the Act's definition of Commercial E-Mail,[28] and most of the Act's requirements do not apply to such messages. Transactional or Relationship Messages are e-mail messages, the primary purpose of which is to do any one or more of the following:

- facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender;
- 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;
- provide notification concerning a change in the terms or features of; notification of a change in the recipient's standing or status with respect to; or 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;
- provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; and
- deliver goods or services,[29] 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.[30]

E-mail messages that are likely to fall into the definition of Transactional or Relationship Message include, for example, order confirmation e-mails, notifications of delayed delivery of ordered goods, periodic account statements and e-mails including product or software updates or upgrades to which the recipient is entitled under a previous transaction. Most of the provisions of the Act[31] do not apply to Transactional or Relationship Messages even if the messages also contain an advertisement or solicitation that is not the primary purpose of the e-mail.[32] The Act invites but does not obligate the FTC to modify the definition of a Transactional or Relationship Message 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." The FTC requested public comment on these issues.[33] In particular, the FTC requested comment on whether a Transactional or Relationship Message that contains a promotion or advertisement for a commercial product or service should be considered a Commercial E-Mail on the basis that its primary purpose is for the promotion, as opposed to the "Transactional or Relationship" purpose.[34]

2. "Primary Purpose" of an Electronic Mail Message

For the purpose of determining the "primary purpose" of an electronic message, the proposed rule set forth in the NPR categorizes electronic messages according to their content, i.e., whether the messages contain: (i) "content that advertises or promotes a product or service," (ii) content that "pertains to" a "transactional or relationship" function, and/or (iii) "other content."[35]

The first of the three categories defined in the proposed rule is electronic messages that contain only advertising and promotional content. The "primary purpose" of such an electronic message would be deemed to be commercial under the proposed rule. [36]

The second category is electronic messages that contain both advertising or promotional content as well as content pertaining to a transactional or relationship function. These electronic messages would be deemed commercial under the proposed rule if either: (i) the recipient, "reasonably interpreting" the message's subject line, "would likely conclude" that it contains advertising or promotional content, or (ii) the transactional or relationship-related content does not appear at or near the beginning of the message.[37]

The third category defined in the proposed rule is electronic messages that contain advertising or promotional content, *do not* contain content pertaining to a "transactional or relationship function," and *do* contain "other content." Such messages would be deemed commercial under the proposed rule if either: (i) the

recipient, "reasonably interpreting" the message's subject line, "would likely conclude" that the message contains advertising or promotional content, or (ii) the recipient, "reasonably interpreting" the body of the message, "would likely conclude" that its primary purpose is to advertise or promote a product or service.[38] The NPR offers several factors as illustrative of those that are relevant to this interpretation: placement of advertising or promotional content at or near the beginning of the message body, the proportion of the message dedicated to such content, and the use of color, graphics, type size and style to highlight commercial content.[39]

3. E-mail Newsletters

E-mail newsletters may or may not be considered Commercial E-Mails under the Act, depending on whether their "primary purpose" is the "commercial advertisement or promotion of a commercial product or service."[40] The definition of "primary purpose" in the proposed rule set forth in the NPR provides some guidance in determining whether, and to what extent, an e-mail newsletter would be considered a Commercial E-Mail under the Act (even if the recipient has opted in to receive it),[41] although questions remain.

An e-mail newsletter that contains no more than that which would be considered advertising or promotional content would clearly be deemed a Commercial E-Mail under the proposed rule.[42] However, where an e-mail newsletter contains additional content on top of the advertising or promotional content, the determination would depend on the nature of such additional content.[43] If it is solely "transactional or relationship content," then the e-mail would appear to fall into the second category described in Section II.A.2 above.[44] Under that category, the e-mail newsletter would be deemed a Commercial E-Mail if either: (i) a recipient's reasonable interpretation of the subject line of the e-mail would likely be that the message advertises or promotes a product or service, or (ii) the e-mail's "transactional or relationship content" does not appear at or near the beginning of the message.[45]

Alternatively, if the nature of the additional content is not that of "transactional or relationship content," then the e-mail would appear to fall into the third category described in Section II.A.2 above.[46] Under that category, the e-mail newsletter would be deemed a Commercial E-Mail if either: (i) a recipient's reasonable interpretation of the subject line of the e-mail would likely be that the message advertises or promotes a product or service, or (ii) a recipient's reasonable interpretation of the body of the e-mail would be that the primary purpose of the message is to advertise or promote a product or service, based on the placement, proportion and visual emphasis of the advertising or promotional content.[47]

B. "Recipient" of E-mail Defined

As defined by the Act, the "Recipient" means "an authorized user of the electronic mail address to which the message was sent or delivered."[48] Where the Act requires that the Recipient has given affirmative consent, the consent must be given by an authorized user of the e-mail address to which the e-mail is sent. Similarly, where the Act's definition of "Transactional or Relationship Message" requires a prior transaction or relationship between the sender and the Recipient of an e-mail, the relationship or transaction must be, in particular, with an authorized user of the e-mail address to which the e-mail is sent. The affirmative consent of, or a prior transaction or relationship with, another individual who is not an authorized user of the e-mail address would not suffice under the Act to satisfy the definitions of "affirmative consent" or "Transactional or Relationship Message."

Under the Act's definition of "Recipient", opt-out requests made by Recipients of Commercial E-Mails apply to the particular e-mail address to which such e-mail was sent, not to other e-mail addresses that the Recipient may also control. The definition states, "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."[49] (Of course, if an individual specifies multiple e-mail addresses in his or her opt-out request, such request should be honored for each of the addresses provided.)

The Act's definition of Recipient may also have an implication for e-mail address updating services, in which a service provider furnishes updated e-mail addresses for individuals whose former e-mail addresses are already on a company's opt-in list. Under the Act's definition of affirmative consent, a company must obtain affirmative consent to send Commercial E-Mail to a particular *e-mail address*, as opposed to a particular *individual*, even if such individual has provided affirmative consent with respect to his or her former (or other) e-mail address. Therefore, a Commercial E-Mail must be clearly and conspicuously identified as an advertisement or solicitation (as discussed in Section IV.A below) if it is sent to the updated e-mail address (unless affirmative consent was given, in particular, with respect to such updated e-mail address).[50]

C. Business-to-Business E-mail

The Act applies to e-mail sent between businesses just as it applies to e-mails that are sent from a business to a consumer. In both cases, the individual authorized user of the receiving e-mail account is considered the "Recipient" of the e-mail.

III. CULPABLE ACTORS UNDER THE ACT

The use of Commercial E-Mails for marketing purposes often involves a number of different parties. The following describes those who may be involved in activities that may have compliance obligations under the Act:

Initiator of the E-mail

A person "initiates" a Commercial E-Mail (hereinafter, the "Initiator") if that person originates or transmits a Commercial E-Mail (not including the routine conveyance of such message, such as that of an ISP),[92] or intentionally pays or provides other consideration to, or induces, another entity to originate or transmit a Commercial E-Mail on the inducer's behalf.[93] More than one person may be considered to have initiated an e-mail message.[94]

The definition of "initiate" is intended to extend the scope of the Act beyond those whose products or services are being promoted, to include service providers or others who dispatch Commercial E-Mail on behalf of such advertisers.

Sender of the E-mail

A "Sender" (as defined in the Act) is a person who initiates a Commercial E-Mail (as discussed above) and whose product, service, or Internet web site is advertised or promoted by the message.[95] Congress intended to make advertisers culpable under the Act even if they themselves do not directly originate or transmit the e-mails. This has the effect of closing a loophole that existed under some state anti-spam laws that only applied to the transmitter of the e-mail and not to the underlying advertiser.[96]

The Act specifically accommodates companies who wish to conduct marketing campaigns under separate divisions or lines of business, without binding the entire company as the "Sender" of Commercial E-Mail. The Act's definition of "Sender" provides that if an e-mail is composed to be coming from a particular business line or division of a company, such as a brand name, rather than from the larger company as a whole, that particular business line or division would be considered the Sender of the e-mail.[97] As a result, the opt-out mechanism that is required to be included in the e-mail, and the opt-out requests that are received from Recipients in response to the e-mail,[98] need only apply to the particular business line or division sending the e-mail. In order to benefit from this provision in the Act, the physical postal address required to be included in the e-mail (as further described in Section IV.D below) should identify the particular business line or division that is sending the e-mail, as opposed to the larger company as a whole, and the e-mail, as a general premise, should be composed as being from the particular business line or division.

Although the Act specifically states that there may be more than one *Initiator* of a Commercial E-Mail,[99] the Act is silent with respect to multiple *Senders* of a Commercial E-Mail. Although multiple entities could satisfy the Act's definition of Sender with respect to the same e-mail message (particularly in the case of joint marketing campaigns or e-mails containing third party advertisements), Congress may not have anticipated the implications of having more than one Sender of the same e-mail. The requirements that an opt-out mechanism and physical postal address be included in the e-mail for each Sender may not have been fully thought through by Congress. The FTC may lend guidance to compliance in these types of situations through its enactment of regulations under the Act. The FTC requested public comment on this issue in its advance notice of proposed rulemaking.[100]

Providers of E-mail Addresses

Any person who acts on behalf of a Sender to assist in initiating a Commercial E-Mail by providing or selecting e-mail addresses to which the e-mail will be sent may be liable under the Act if such person has actual or implied knowledge that any of the potential Recipients have opted out of receiving e-mail from the Sender,[101] or if such person has actual or implied knowledge that the e-mail addresses were obtained via address harvesting or dictionary derivation.[102]

Transferors of Opted-out E-mail Addresses

Any person who sells, leases, exchanges or otherwise transfers or releases the e-mail address of a Recipient who has opted-out (other than to comply with the Act or the law, for example, to update an opt-out list) with knowledge that the Recipient has opted-out, may be liable under the Act.[103]

Promoters

Any person who promotes, or allows the promotion of, such person's trade or business in a Commercial E-Mail that contains false or misleading header information, or any third party who provides goods, products, property or services to such a person, under certain limited circumstances, may be liable under the Act.[104] In particular, this liability applies in the event the company knew or should have known that its products or services were being promoted in such a message, received or expected to receive an economic benefit from such promotions, and took no reasonable action to prevent the transmission or detect it and report it to the FTC. This provision of the Act enables enforcement against an advertiser in an e-mail even if the entity that originated or transmitted the e-mail cannot be identified, and it therefore cannot be proven that the advertiser retained the entity to transmit the e-mail and was therefore an "Initiator" of the e-mail.[105]

To mitigate culpability under this provision of the Act, it is recommended that a company that retains a third party to send e-mails promoting its products or services (for example, a marketing affiliate agreement), or who has knowledge of a

third party doing so, include in its agreement with such third party and/or in its published policies, a provision that expressly prohibits any such third parties from including false or misleading header information in such e-mails. In addition, if a company obtains knowledge of this occurring, it should have contractual rights (not in limitation of any other rights or remedies) to take action to prevent it in the future.

Other

Any person is liable under the Act if they automatically register multiple e-mail or user accounts for the transmission of certain unlawful Commercial E-Mails,[106] or if they knowingly relay or retransmit certain unlawful Commercial E-Mails from a computer or network that such person has accessed without authorization.[107]

IV. SUMMARY OF REQUIREMENTS OF THE ACT

A. Inclusion of Identification of E-mail as Advertisement or Solicitation

The Act requires that Commercial E-Mails must provide "clear and conspicuous identification that the message is an advertisement or solicitation."[108] This requirement does not apply, however, if the Recipient has given prior affirmative consent (as defined by the Act) to receipt of the Commercial E-Mail.[109] As defined by the Act, a Recipient has given "affirmative consent" to receive a Commercial E-Mail if he or she has 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.[110] Affirmative consent requires some kind of active choice or selection by the individual; merely remaining passive, as in the case where an individual does not modify a default setting such as a pre-checked consent box, would not satisfy this definition.[111]

Affirmative consent need not be on a Sender-by-Sender basis. A Recipient could affirmatively consent to messages from one particular company, but could also consent to receive messages on a particular subject matter without regard to the identity of the Sender, or even to messages from the unnamed marketing partners of a particular company.[112] However, if the message is from a party other than the party to which the Recipient communicated such consent *(i.e.*, if party A solicits an individual's consent to receive Commercial E-Mails from party B), the Act requires that the Recipient must have been 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 (*i.e.*, Party B, even if Party B is unnamed) for the purpose of initiating commercial electronic mail messages.[113]

The Act's definition of affirmative consent may have implications for e-mail address matching services,[114] in which a service provider matches a company's off-line

marketing list (which contains only physical addresses) with the e-mail addresses for the individuals on the list. Under the Act's definition of affirmative consent, if the individual did not Affirmatively Consent to the service provider's transfer of his or her e-mail address to the company (or, for example, to unnamed companies in the relevant market niche), then Commercial E-Mails that are sent by the company to the e-mail addresses provided must be clearly and conspicuously identified as advertisements or promotions.

The Act does not define "clear and conspicuous" with regard to the required identification of an e-mail as an advertisement or solicitation. Although the FTC may provide further guidance on what constitutes a clear and conspicuous notice, except with respect to sexually oriented Commercial E-Mail,[115] the FTC is precluded by the Act from requiring any specific words, characters, marks or labels in a Commercial E-Mail, or from requiring that the identification must be included in any particular part of such e-mail, such as the subject line or body of the e-mail.[116] For example, in contrast to many state anti-spam statutes that preceded the Act, the FTC may not require that a Commercial E-Mail include the characters "ADV:" (which stands for "advertisement") in the subject line.

The FTC publishes general guidelines for companies to consider as they develop online ads to ensure that they comply with applicable laws. These guidelines may be instructive in anticipating the FTC's approach to enforcement under the Act. In its "Dot Com Disclosures: Information About Online Advertising" publication, the FTC lends guidance to what, in general, constitutes "clear and conspicuous" under the several laws within the FTC's purview. The FTC's guidelines emphasize: (i) the placement of the disclosure (in this case, the notice that the e-mail is an advertisement or solicitation) in an ad (or, in this case, in an e-mail), (ii) the prominence of the disclosure (*i.e.*, its size, color and graphic treatment in relation to other parts of the ad), (iii) whether items in other parts of the ad distract attention from the disclosure, (iv) whether the ad is so lengthy that the disclosure needs to be repeated, (v) whether the language of the disclosure is understandable to the intended audience, and (vi) whether the ad uses text or visual cues to encourage consumers to scroll down to view the disclosure.[117] In general, the FTC uses the "overall net impression" test, that is, whether the reasonable reader will know that the e-mail is an advertisement or solicitation (without assuming that the reader will read the entire e-mail).

B. Requirement to Include Opt-Out Notice and Mechanism in Commercial E-Mails

The Act requires that a Commercial E-Mail include a functioning return e-mail address or other Internet-based mechanism, clearly and conspicuously displayed, that the Recipient may use to opt out of receiving future Commercial E-Mail from the Sender.[118] The Recipient must be able "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 electronic mail messages from that Sender at the electronic mail address where the message was received."[119] Note that if there is more than one Sender of the e-mail, a literal reading of the Act may require that an opt-out mechanism for each Sender be included.[120] A clear and conspicuous notice of this opt-out opportunity must also be provided in the e-mail.[121]

Although the Act requires that a Commercial E-Mail message include a mechanism by which the Recipient can opt-out of receiving all future messages from the Sender, the Act also expressly provides that the e-mail may, in addition, provide opt-out mechanisms that enable the Recipient to opt-out of receiving only certain types of Commercial E-Mails from the Sender.[122] For example, the e-mail may provide an additional opt-out mechanism to enable the Recipient to opt out of a particular newsletter, while continuing to receive other types of Commercial E-Mail communications from the Sender. That is, the e-mail may provide "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" as long as "the list or menu includes an option under which the Recipient may choose not to receive any commercial electronic mail messages from the sender."[123]

C. Requirement to Honor Opt-Out Requests

The Act requires that the opt-out mechanism provided in an e-mail must remain capable of receiving and processing Recipients' opt-out requests for no less than thirty days after the transmission of the original message.[124] However, if an opt-out mechanism is "unexpectedly and temporarily unable to receive messages or process requests due to a technical problem beyond the control of the sender" and "the problem is corrected within a reasonable time period," the failure would not, in itself, be considered a violation of the Act.[125]

The Act requires that opt-out requests submitted by Recipients via the means provided by the Sender must be honored within ten business days following the Sender's receipt of the opt-out request.[126] Note that if there is more than one Sender of the e-mail, strictly construed, the Act requires that each Sender honor opt-out requests directed at such Sender.[127] It should also be noted that the FTC is expected to consider reducing or extending the number of days the Sender has to comply with a Recipient's opt-out request,[128] and in fact requested public comment on this issue.[129]

Once a Recipient has opted-out of receiving Commercial E-Mail from a Sender, the Act prohibits the subsequent sale, lease, exchange or other transfer or release of the e-mail address of such Recipient (for purposes other than compliance with the Act or the law) with knowledge that the Recipient has opted-out.[130] This requirement of the Act is intended to prevent a Sender or other person from treating an opt-out request as a confirmation of a "live" e-mail address, and selling that information to other would-be e-mail marketers.[131]

If a Recipient opts out from receiving Commercial E-Mail messages from a Sender and then subsequently provides affirmative consent (as defined by the Act) to receive such messages, the Sender may resume sending messages to that Recipient, within the scope of the Recipient's affirmative consent.[132]

An ambiguity arises under the Act's opt-out requirements when a Recipient opts out of receiving e-mails from one company (company A) and subsequently opts in to receive e-mails from another company (company B) as well as company B's unnamed "affiliate partners," one of which, unbeknownst to the Recipient, is company A. Here, if company B, on the basis of such opt-in, sends a Commercial E-Mail containing a company A advertisement to the Recipient, it is unclear under the Act whether either company A or company B would be construed to have violated the obligation to honor the Recipient's opt-out request, given that the Recipient was not given the name of company B's affiliate (that is, company A) when he opted-in to receive e-mails from company B. In any event, since the Recipient is not, in this situation, expecting to receive company A promotions, best practices would dictate that affiliate marketing programs should not rely on affirmative consent to receive marketing e-mails from un-named companies.

D. Inclusion of Senders' Valid Physical Postal Address

The Act requires that a Commercial E-Mail must include "a valid physical postal address of the sender."[133] The requirement applies regardless of whether the Recipient affirmatively consented to receive the e-mail. Note that if there is more than one Sender of the e-mail, literally read, the Act requires that each Sender's physical postal address be included.[134]

The FTC requested public comment on whether the inclusion of a post office box or commercial mail drop address would satisfy this requirement.[135]

E. "Refer a Friend"

Many companies include on their web sites, or in their marketing e-mails, features by which individuals can send information about the company's products or services to their friends. The solicitation of an individual's referral of a friend raises certain issues under the Act. If the company, through its systems, originates or transmits the e-mail to the friend, then the company may then be considered an Initiator and/or Sender of the e-mail to the friend.[136] Additionally, if the company can be said to have induced the individual to originate or transmit the e-mail to the friend on the company's behalf, then the company may also then be considered an Initiator and/or Sender of the e-mail to the friend.[137] In either case, the requirements of the Act may apply to the company.

If so, in addition to the other requirements of the Act, the friend's e-mail address should be compared against the company's opt-out list, and the e-mail should not be sent if the friend's e-mail address is on the list.[138] Obviously, in situations in which the e-mail is forwarded to the friend directly by the user, not via the company's systems, the company may not have an opportunity to check the friend's e-mail address against its opt-out list. However, the Act, literally read, would nonetheless consider the company in these types of situations to be an Initiator and Sender of the e-mail to the friend.

Where a company provides a feature on its web site that enables users to have e-mail messages sent to their friends at e-mail addresses of the user's selection, one may argue that a company that merely invites and enables an individual to send or forward e-mails to such individual's friend, and does not identify the friend or provide the friend's e-mail address, would have engaged in the mere "routine conveyance" (like that of an ISP) of the e-mail transmitted by the individual to the friend. Therefore, it would follow that the company would not be considered to be a Sender or Initiator of the e-mail.[139] A company that wishes to utilize this approach should implement its "refer a friend" campaigns in a manner that the individual, and not the company, appears as the sender of the e-mail. The company should limit its role to the greatest extent possible to one providing mere automatic transmission, routing, relaying, handling and storing, without any role that could be construed as "coordinating the recipient addresses" of the e-mail.[140] The company also should not retain the friend's e-mail address for its own use.

Additionally, in the event that a company receives an opt-out request from the "friend" who has been forwarded a company e-mail, the company should honor such opt-out request on a going forward basis.

The FTC, in connection with its permissive rulemaking, may provide further guidance as to how a company may operate a "refer a friend" e-mail campaign under the Act, and requested public comment on this issue.[141]

F. Special Issues for Joint Marketing; Third Party Ads and Affiliate Marketing

1. Joint Marketing; Third Party Ads

Additional issues are raised under the Act with regard to joint e-mail marketing campaigns, as there are usually at least two Senders of a joint Commercial E-Mail (even if only one party actually transmits the e-mail, and even if the e-mail is only sent to one of the party's address list). This may be the case with respect to a co-branded campaign in which two or more parties market their products and services in the same e-mail. This may also be the case in an e-mail promotion or newsletter sent by one party, but containing advertisements (including banner ads) for one or more other companies' products and services. As a result, under a strict reading of the Act,

each of the companies may be considered "Senders" under the Act.

Among the Act's other requirements, in the case of a joint Commercial E-Mail, the address list to which the e-mail is sent should exclude all individuals who have opted out of Commercial E-Mail from any of the Senders.[142] In addition, the Commercial E-Mail should also include a working opt-out notice and mechanism for Recipients to opt-out of receiving Commercial E-Mails from each Sender in the future.[143] The e-mail must also contain all Senders' physical postal addresses.

The FTC requested public comment on whether, and if so how, the Act should apply to e-mails for which there are more than one Sender, as defined by the Act.[144]

2. Affiliate Marketing

Issues are also raised under the Act with regard to affiliate marketing relationships, where a company's products and services are promoted in an e-mail that the company did not itself transmit. In the typical affiliate marketing relationship, a company that sells products and services on its web site (a "merchant") enters into an agreement (often an online "click-through" agreement) with another company (an "affiliate") in which the affiliate will direct traffic to the merchant's web site and receive, in exchange, a share of the revenue derived by the merchant from such traffic.

Often, the affiliate generates traffic to the merchant's web site using mass e-mail campaigns. In this situation, the merchant may be considered a "Sender" and an "Initiator" of such e-mails (because it has provided consideration or inducement to the affiliate for the sending of the e-mail), and therefore would be held responsible if the affiliate's e-mail campaign was non-complaint with the Act's requirements. In these situations, among the other requirements of the Act, the merchant's list of opted-out e-mail addresses would have to be excluded from the list of e-mail addresses to which the affiliate sends the e-mail messages,[145] and, in addition, the e-mail must also include a working opt-out notice and mechanism for Recipients to opt-out of receiving commercial e-mails from the merchant in the future. Also, the e-mail must contain the merchant's physical postal address. The merchant may also be liable if the merchant's e-mails contain false or misleading header information or subject headers, or if the e-mail addresses used were obtained through harvesting or dictionary derivation.

G. Use of E-Mail Services Providers as Contractors

The Act raises implications when a company uses a third party service provider to either send Commercial E-Mails on its behalf or to provide e-mail addresses to which the company will send Commercial E-Mails. As an advertiser in the e-mail, even if the e-mail is sent, or the address is provided, by a contractor, the company that

advertises in the e-mail and procures or induces the e-mail's transmission is responsible for compliance with the Act's requirements.

Whenever working with an e-mail services provider, a company should therefore select its provider very carefully and obtain adequate contractual provisions to ensure full compliance with the Act. For example, where a service provider is furnishing e-mail addresses, if the nature of the e-mail campaign relies on the prior affirmative consent of the Recipients to receive the e-mails, the prior opt-in mechanism must satisfy the Act's requirements. Among other things, Recipients should have been notified, at the time of opting-in, that their e-mail address could be transferred to a third party for purposes of sending Commercial E-Mail. (Otherwise, the e-mail must be identified clearly and conspicuously as an advertisement or solicitation.) The contract should also provide that the e-mail addresses provided were not obtained through harvesting or dictionary derivation.

Also, a service provider who sends Commercial E-Mails on behalf of a company must be required to honor opt-out requests that may be received either directly from the Recipient or forwarded from the company, within the time frames set forth in the Act.[146] Furthermore, the contract should specifically require that the service provider not transmit e-mails with false or misleading header information. In any case, any e-mail that is sent must satisfy all of the requirements of the Act.

A company commissioning a third party service provider for these types of services is well-advised not to rely on the service provider's standard contractual representation of "compliance with the law." The Act imposes complicated operational requirements on these types of services providers. Since the commissioning party, as a "Sender," could potentially be found liable for the service provider's violation, the commissioning party should reach a clear understanding with the provider as to how the Act will be honored.

On a similar note, a service provider that sends Commercial E-Mails on behalf of its customers is also culpable under the Act as an Initiator of the e-mails. Accordingly, from the service provider's perspective, the contract for services should contain representations by the customer as to the rights that they have to use, and to authorize the service provider to use, any e-mail addresses that are provided by the company. A service provider should also ensure that the e-mails it sends contain all the notices and information, and a functioning opt-out mechanism, as required by the Act, and that they comply with all of the other requirements of the Act.

As the FTC is likely to clarify, and possibly in some cases tighten the Act, in any long-term relationship both parties need to have an understanding as to how new requirements will be addressed. In any case, it is clear that either company should negotiate for a meaningful indemnity to cover failures of compliance by the other party.

H. No Materially False or Misleading Header Information or Misleading Subject Lines

The Act prohibits the Initiation of a Commercial E-Mail or a Transactional or Relationship Message that contains or is accompanied by materially false or materially misleading header information.[147] As defined by the Act, "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."[148] The "from" line in an e-mail address, for example, would be considered header information. The Act further specifies that header information that includes an originating e-mail address, domain name or IP address that was accessed by means of false or fraudulent pretenses or representations shall be considered materially misleading.[149]

The "from" line of an e-mail must identify an Initiator of the e-mail.[150] If there is more than one Initiator of an e-mail, only one of the Initiators is required to be identified in the "from" line.

The Act also prohibits the initiation of a Commercial E-Mail with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that the 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.[151] This provision is intended to prohibit a typical tactic used to entice or trick a Recipient into opening an e-mail message under false pretenses by including a subject line that mischaracterizes the nature of the message.

I. Address Harvesting and Dictionary Attacks; Automatic Creation of Multiple Accounts; Unauthorized Relay or Transmission

The Act contains provisions intended to curb two common methods used by some organizations to obtain e-mail addresses to which they send Commercial E-Mail — e-mail address harvesting and dictionary attacks. E-mail addresses can be harvested (or extracted) from public newsgroup and chat room postings, web sites and other on-line areas using automated "spider" or "robot" programs. Dictionary attacks are mass e-mail dispatches sent to automatically-generated e-mail addresses at common domain names — done by stringing letters and characters together to create e-mail addresses (such as ajones@isp.com, bjones@isp.com, cjones@isp.com, etc., referred to herein as "dictionary derivation") with the expectation that some of the e-mail addresses will lead to real users. To combat these types of activities, the Act prohibits the initiation of unlawful Commercial E-Mail, or the provision of e-mail addresses to which unlawful Commercial E-Mail is sent, with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that: (a) the e-mail

address was obtained using automated means from a third party web site or online service in violation of its posted policies,[152] or (b) the e-mail address was obtained using an automated means that generates possible e-mail addresses by combining names, letters, or numbers into numerous permutations.[153]

The Act also prohibits two other common tactics used to send Commercial E-Mail in an anonymous way. Automated software programs are often used to create multiple e-mail accounts for use in sending Commercial E-Mail. By sending e-mail from different e-mail accounts each time, attempts by internet service providers, vendors of filtering software and individuals to block e-mails from a particular e-mail address will not be effective in blocking future e-mail. Another common tactic is the use of third party "open relays" and "open proxies" to send spam. "Open relays" and "open proxies" are e-mail servers that are configured to allow remote third party computers to "bounce" or route e-mail through them. Entities that send mass e-mails often abuse these servers by sending spam through them. (This conduct is often referred to as "spoofing.") Accordingly, the Act prohibits: (a) the automatic generation of multiple e-mail accounts through which to send unlawful spam,[154] and (b) the unauthorized use of a third party's computer from which to send unlawful spam.[155]

The FTC is invited by the Act to add additional aggregated activities or practices to be covered by the Act that are "contributing substantially to the proliferation of commercial electronic mail messages."[156] The FTC requested public comment on additional aggravated violations that may be appropriate to regulate.[157]

J. Sexually Oriented Material in E-mails

The Act and its regulations[158] provide for heightened obligations, and criminal penalties, with respect to Commercial E-Mail that contains sexually oriented material. Sexually oriented material means "any material that depicts certain sexually explicit conduct, unless the depiction constitutes a small and insignificant part of the whole, the remainder of which is not primarily devoted to sexual matters."[159]

In particular, e-mails that contain sexually oriented material must: (a) include, in the ASCII character set[160] as the first nineteen characters[161] of the subject heading, the phrase "SEXUALLY-EXPLICIT: "[162] (in all caps), and (b) provide that the content in the e-mail that is initially viewable when the e-mail is first opened by the Recipient (absent any further action by the Recipient such as scrolling down or clicking on a link) include nothing more than: (1) the "SEXUALLY-EXPLICIT: " notice described above, (2) the identification of the e-mail as an advertisement (as required and as described in Section IV.A above), (3) the notice of opt-out opportunity and mechanism (as described in Section IV.B above), (4) the physical postal address of the Sender (as described in Section IV.D above) and (5) any necessary instructions on how to access, or activate a mechanism to access, the sexually oriented material, preceded by a statement that to avoid viewing the sexually oriented materials, the

Recipient should delete the message without following such directions.[163] The matter in the e-mail that is initially viewable when the e-mail is first opened (including, without limitation, the subject line) may not include any sexually oriented materials. Additionally, the "SEXUALLY-EXPLICIT: " notice, the identification of the e-mail as an advertisement, the notice of opt-out opportunity and mechanism, the physical postal address of the Sender and the statement of how to avoid viewing the sexually oriented material must each be clear and conspicuous.[164]

The requirements set forth above do not apply if the Recipient has given prior affirmative consent (as defined by the Act) to receive the message.

Criminal penalties under these provisions of the Act are set forth in Section IV.K below.

K. Criminal Provisions of the Act

The Act provides for criminal penalties on anyone who, in or affecting interstate or foreign commerce, knowingly does, or conspires to do, any of the following:

- accesses a computer without authorization and intentionally initiates the transmission of multiple Commercial E-Mails therefrom;
- uses a computer to relay or retransmit multiple Commercial E-Mails with the intent to deceive or mislead Recipients, or any Internet access service (as defined by the Act), as to the origin of such messages;
- materially falsifies header information in multiple Commercial E-Mails and intentionally initiates the transmission of such messages;
- registers, using information that materially falsifies the identity of the actual registrant, for five or more e-mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple Commercial E-Mails from any combination of such accounts or domain names; and
- falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of five or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses.[165]

For purposes of the above, the term "multiple" is defined by the Act to mean "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."[166]

Criminal penalties under these provisions of the Act range from a fine alone, to a fine plus imprisonment for up to five years, depending, among other things, on whether the offense is committed in furtherance of a felony, whether there are any similar past convictions by the offender, the quantity and volume of the offending acts, the amount of monetary loss caused by the offense, the amount of monetary value gained by the offender as a result of the offense and the number of individuals involved in the offense. The United States Sentencing Commission is required by the Act to review and, as appropriate, amend the sentencing guidelines and policy statements to provide appropriate penalties for violation of the criminal provisions of the Act. The Sentencing Commission issued a request for public comments regarding such guidelines and policy statements,[167] and has since proposed amended sentencing guidelines to Congress.[168]

L. State of Mind

Some of the requirements of the Act depend on the state of mind of the actor. For example, many of the Act's requirements, described above, only apply if the actor had knowledge of certain circumstances or facts. However, the Act provides for certain exceptions to these "state of mind" elements while at other times adding state of mind elements in certain situations. For one, with regard to certain of the Act's requirements, the FTC and other federal agencies and state entities that have authority to enforce the Act are given the power to obtain certain cease and desist orders and injunctive relief without regard to the state of mind of the actor that would otherwise be required by the Act.[169] In contrast, with regard to certain of the Act's provisions, state attorneys general and other state officials and agencies that have authority to enforce the Act are required to allege certain "state of mind" elements, when seeking monetary damages, which would not otherwise be required by the Act.[170]

V. APPLICATION OF THE ACT TO WIRELESS MESSAGING

The Act in general applies to at least some types of wireless messages sent to wireless devices.[171] The Federal Communications Commission ("FCC"), in consultation with the FTC, is required by the Act, by September of 2004 (within 270 days after enactment) to promulgate regulations to protect consumers from unwanted mobile services commercial messages.[172] In August 2004, the FCC issued final rules regarding the sending of commercial e-mails to wireless devices.[175]

In summary, the rules require an opt-in approach with respect to commercial e-mails that are sent directly to wireless device e-mail addresses. Regarding such "opt-

in," the rules provide for a special definition of "express prior authorization," which is more rigid than the definition of "affirmative consent" under the Act which applies to non-wireless messages. So, a special permission process is required with respect to wireless addresses.

The new wireless spam rule generally applies if either: (i) the sender has knowledge that the e-mail address is that of a wireless device, or (ii) the domain name of the e-mail address is contained on a list of wireless address domain names that will be maintained by the FCC. Therefore, senders of Commercial E-Mails should scrub their address list against the FCC-maintained list of wireless domain names, at least every thirty (30) days, unless the means by which "opt-in" has been obtained meets the requirements of the FCC's regulatory definition of "express prior authorization." Additional requirements also apply to e-mails that are sent to wireless devices, similar to those imposed on non-wireless messages, such as inclusion of a functioning electronic return address and honoring of opt-out requests.

VI. PREEMPTION OF STATE LAW

The Act serves to preempt, in part, state laws regulating unsolicited commercial e-mail. However, such state laws continue to be effective to the extent that they prohibit falsity or deception in any portion of a Commercial E-Mail.[178] A number of state spam laws remain effective with regard to their provisions relating to falsity or deception. In addition, a number of states have begun to propose bills that are drafted specifically to fall outside of the Act's preemptive affect. For example, such a law was enacted in Maryland in May 2004.[179]

Also, generally applicable state trespass, contract, tort, fraud and computer crime laws may continue to be enforced. Prior to the Act's enactment, these types of state laws were often used by aggrieved parties as well as governmental enforcement agencies to challenge spam-related activities. It is expected that enforcement under these types of state laws will continue in parallel with enforcement activities under the Act. In July 2004, for example, the New York State Attorney General settled a suit brought against e-mail marketer OptInRealBig.com under state laws prohibiting fraud, deception and illegality in the conduct of business. Under the settlement the company paid $50,000 in penalties and investigative costs and agreed to a series of marketing restrictions, including a permanent injunction against the sending of commercial e-mail messages containing false or misleading header information, subject lines or sender information, the initiation of commercial e-mail messages with the intent to deceive or mislead recipients or an ISP with respect to their origin, registering a domain name using false information; and the making of false representations concerning the right to use an ISP address.[180]

VII. ENFORCEMENT OF THE ACT

A. Enforcement Powers

1. In General

The FTC, or, as applicable, the federal agency that has authority over the entity in question,[181] has the authority to enforce the Act as if a violation of the Act is an unfair or deceptive act or practice under the Federal Trade Commission Act and the Federal Trade Commission trade regulation rule.

In general, in connection with FTC enforcement of the Act, the remedies applicable to a violation of the Act are the same as those that apply to a violation of the Federal Trade Commission Act.[182] In connection therewith, civil penalties may be up to $11,000 for each violation.[183]

On April 29, 2004, the FTC announced the first governmental actions under the CAN-SPAM Act: One against Detroit-based Phoenix Avatar, and another against Global Web Promotions operating out of Australia and New Zealand. These companies are viewed as among the largest spammers in the world, with Phoenix Avatar generating four hundred and ninety thousand consumer complaints to the FTC, and Global Web Promotions generating three hundred and ninety-nine thousand consumer complaints to the FTC. In both cases, government officials were assisted by private entities, such as anti-spam organizations and ISPs, in identifying, and substantiating claims against, these companies. Additional cases have since been brought by the FTC under the Act.

Federal Trade Commission v. Phoenix Avatar, LLC; United States v. Daniel J. Lin et al. Claims brought against Phoenix Avatar center around its e-mails promoting diet patches that, the Government maintains, have no clinical value. It is alleged that these e-mails contained false claims, spoofed header information and no opt-out mechanism. Both civil and criminal actions have been initiated against Phoenix Avatar. Civil claims have been brought by the FTC under the Federal Trade Commission Act and the CAN-SPAM Act. Criminal action has been initiated by the United States Attorney's office out of the Eastern District of Michigan under both the criminal provisions of the CAN-SPAM Act as well as federal mail fraud statutes. The court issued first a temporary restraining order and then a preliminary injunction against Phoenix Avatar and froze the company's assets.[184]

Federal Trade Commission v. Global Web Promotions Pty Ltd. Similar civil claims against Global Web Promotions have been brought by the FTC, with the cooperation of the Australian Competition & Consumer Commission and the New Zealand Commerce Commission.[185] These claims center around the company's e-mails promoting diet patches and human growth hormone products.

Federal Trade Commission v. Harry, d/b/a/Hitech Marketing, Scientific Life Nutrition, and Rejuvenation Health Corp. The FTC obtained a restraining order and a freeze on assets under the Act in federal court against an individual and various companies alleged to have sold bogus "human growth hormone" products over the Internet through spam.[186]

2. State Enforcement

In addition to the FTC and other federal agencies, a state attorney general or another official or agency of a state has limited enforcement powers under the Act with regard to false or misleading header information, misleading subject headings, sexually oriented e-mail, or a pattern or practice of violating those provisions of the Act requiring opt-out mechanisms and notices, identification of an e-mail as an advertisement, inclusion of physical postal address in e-mails and honoring opt-out requests.[187]

When a state entity is enforcing the Act, the Act provides for specific penalties to be applied.[188] In addition to injunctive relief, a state entity can impose damages on behalf of its residents of the greater of: (a) the actual monetary loss suffered by such residents, or (b) the number of separate e-mail addresses to which unlawful e-mail was sent to residents of the state multiplied by up to $250 but not to exceed $2,000,0000 in the aggregate, except in the case of false or misleading header information in which case there is no cap.[189] These specified damages may be tripled in the event of willful and knowing violations or in the event of certain aggravated violations.[190] The damages may also be reduced if the defendant has established and implemented, with due care, commercially reasonable practices and procedures designed to effectively prevent violations of the Act, or if the violation occurred despite commercially reasonable efforts to maintain compliance with such practices and procedures.[191] Attorneys' fees are also available.[192]

The first state action under the CAN-SPAM Act was brought in July 2004 by the Massachusetts Attorney General. Suit was brought under the Act and Massachusetts state laws against a Florida resident who allegedly sent spam advertising cut-rate mortgages to Massachusetts residents.[193]

3. Internet Access Service Providers

"Internet access service providers" that are adversely affected by a violation of certain provisions of the Act have the authority to bring a civil action to enjoin further violation and to recover damages. The definition of "Internet access service provider" under the Act is very broad, and could be read to include more than just a true internet service provider. It includes any provider of "a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers."[194] As a result of this broad definition, employers that provide e-mail accounts to their employees,

universities, some web site operators, and even an individual with an e-mail server in his basement, could theoretically have authority to bring action under the Act.

Internet access service providers have the authority to challenge violations of the Act involving false or misleading header information, certain aggravated violations, sexually oriented e-mail, or patterns or practices of violating those provisions of the Act prohibiting misleading subject headings and requiring opt-out mechanisms and notices, identification of an e-mail as an advertisement, inclusion of physical postal address in e-mails and honoring opt-out requests.[195]

To bring an action against an Initiator or Sender of Commercial E-Mail that did not, itself, directly transmit or originate the e-mail messages in question (*e.g.*, where the defendant procured a third party to transmit or originate the e-mail), an Internet access service provider must allege a "knowledge" element not required in governmental actions under the Act. The plaintiff must allege that the defendant had actual knowledge, or consciously avoided knowing, whether the third party procured to transmit or originate the e-mail was engaging, or would engage, in a pattern or practice that violates the Act.[196] The effect of this additional "knowledge" requirement is to make an advertiser less likely to be liable to an Internet access service provider for e-mails that are not transmitted directly by the advertiser, but are instead transmitted by a third party on the advertiser's behalf.

An Internet access service provider can bring an action seeking injunctive relief and monetary damages equal to the greater of: (a) the actual monetary loss incurred by the provider as a result of the violation, and (b) the number of separate e-mail addresses to which unlawful e-mail was transmitted, or attempted to be transmitted, through the provider's facility, or to an e-mail addresses harvested from the provider, multiplied by up to $25 but not to exceed $1,000,000 in the aggregate, except in the case of false or misleading header information in which case the number of e-mail addresses is multiplied by up to $100, with no upper limit.[197] These specified damages may be tripled in the event of willful and knowing violations or in the event of certain aggravated violations.[198] The damages may also be reduced if the defendant has established and implemented, with due care, commercially reasonable practices and procedures designed to effectively prevent violations of the Act, or if the violation occurred despite commercially reasonable efforts to maintain compliance with such practices and procedures.[199] Attorneys' fees are also available.[200]

Hypertouch, Inc. v. BVWebTies, LLC. Just under three months after the Act's effective date, the first litigation was initiated under the Act. In *Hypertouch, Inc. v. BVWebTies, LLC,*[201] Hypertouch Inc., an ISP, filed a claim against two parties, BVWebTies, LLC, the owner of the bobvillas.com domain name, and BlueStream Media, an online marketing company. The complaint alleges that the defendants sent Commercial E-Mail messages through the plaintiff's e-mail servers that: (i) contained or were accompanied by header information that was materially false or materially misleading in that the machines identified as originating the e-mails did not match up

with the IP addresses of the machine that actually sent the messages, (ii) used a domain name that was registered to a false non-existent entity obtained by means of false representation, (iii) were sent despite opt-out requests, (iv) did not contain a valid physical postal address of the sender, (iv) were sent to e-mail addresses that were harvested from a domain name registry web site, and (v) were sent to addresses generated using automated means (*i.e.*, a dictionary attack). The plaintiff seeks actual or statutory damages, aggravated damages, preliminary and permanent injunctions, attorneys' fees and costs.

The America Online, Earthlink, Microsoft and Yahoo! Litigation. Also within three months of the Act's effective date (and within one week of the Hypertouch filing), America Online Inc., Earthlink Inc., Microsoft Corp and Yahoo! Inc., coordinated with each other in filing six Internet access service provider lawsuits against over one hundred known spammers that they identified though a collaborative effort.[202] In their collaborative lawsuits, these ISPs allege, for example, (i) deceptive solicitations for various products including get-rich-quick schemes, prescription drugs, pornography, instructions for conducting spam campaigns, banned CDs, mortgage loans, university diplomas, cable descramblers and other common types of unsolicited mail, (ii) the use of open proxies to send e-mails, (iii) falsified header information, (iv) the failure to include a physical postal address in e-mails, and (v) the failure to provide an opt-out mechanism in e-mails.[203] Subsequently, in June 2004, Microsoft filed similar CAN-SPAM Act suits against eight additional alleged spammers.[204]

4. Private Right of Action by Recipients

There is no civil private right of action under the Act. However, some state laws provide for a private right of action, on behalf of the general public of that state, under any statute that may be enforced by a state attorney general.[205] Therefore, it is possible that in some states and in specific circumstances, an individual could bring an action under the Act against a company on behalf of the general public of that state.

B. Criminal Violations

Penalties under the criminal provisions of the Act are discussed *supra*, pp. 18-19.

VIII. FTC ACTIVITY

A. Rulemaking

The FTC generally has the authority, and in some cases is required, to issue regulations to implement the provisions of the Act.[206] For example, the FTC is required to issue regulations defining the relevant criteria to facilitate the determination of the primary purpose of an e-mail (applicable in connection with the definitions of Commercial E-Mail and Transactional or Relationship Message under the Act).[207] The FTC is also invited, but not obligated, to issue regulations: (i) refining the definition of Transactional or Relationship Messages,[208] (ii) altering the amount of time a Sender has to honor opt-requests,[209] (iii) expanding upon the Act's aggravated violations,[210] and (iv) regarding the implementation of the Act generally.[211]

B. Do-Not-E-Mail Registry

By June of 2004, the FTC was required by the Act to submit a report to Congress that sets forth a plan and timetable for establishing a Do-Not-E-Mail registry, including an explanation of any concerns of the FTC regarding such a registry, and an explanation of how the registry would apply to children's e-mail accounts. The FTC is authorized, but not required, by the Act to implement such a registry.[215] In its report issued in June 2004, the FTC, citing the security, privacy and enforcement difficulties of a Do-Not-E-Mail registry, proposed a plan to require the implementation of a technological method of authentication of the true origin of e-mail messages prior to further consideration of a Do-Not-E-Mail registry.

C. Rewards for Information About Violations

By September of 2004, the FTC is required by the Act to submit a report to Congress setting forth a system for rewarding those who supply information about violations of the Act.[216] The FTC has requested public comment on such a "bounty" system,[218] and is compiling and reviewing expert testimony on the bounty plan.[219]

D. Labeling of Commercial E-Mail

By June of 2005, the FTC is required by the Act to submit a report to Congress setting forth a plan for requiring that Commercial E-Mail 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 FTC has that cause the FTC to recommend against such a plan.[220] The FTC requested public comment on these issues for its consideration in connection with such report.[221] In particular, the FTC requested comments regarding a requirement that Commercial E-Mails be labeled with the "ADV" characters.

E. Study of Effects on Commercial E-Mail

By December of 2005, the FTC is required by the Act to submit a report to Congress providing a detailed analysis of the effectiveness and enforcement of the Act and the need, if any, for Congress to amend the Act.[222] The FTC requested public comment on these issues for its consideration in connection with such report.[223]

IX. TECHNOLOGICAL AND OTHER SOLUTIONS

It is widely agreed that the problem of spam cannot be successfully combated by the law alone. Technology will have a large part to play in effectively preventing unwanted e-mail messages from reaching users' e-mail inboxes. In addition to the many server and client-based spam filtering products available on the market (which have weaknesses in that they do not yet have a reliable means of authenticating the true source of an e-mail message, *i.e.*, identifying "spoofed" e-mails), several technologies are in the works:

"**DomainKeys**," proposed and supported by Yahoo!, is designed to authenticate the "from" header in an e-mail by attaching encrypted "keys" or tags to every e-mail sent. One key is held in a public database in a manner so that it is attributed to a particular ISP and the other key (a private key) is linked to the message. Upon delivery of the message, the receiving server can match the private key to the pubic key to verify that the e-mail was sent from the ISP from which it was purported to have been sent. If the public key does not corroborate the purported "from" address, the message is identified as "spoofed," and therefore filtered as spam.

"**Sender Policy Framework**" (SPF), already implemented by AOL and Google, is designed to change the DNS database so that operators of e-mail servers can publish which internet protocol addresses they use to send e-mail. As a result, receiving e-mail servers would be able to automatically identify a "spoofed" e-mail by checking the DNS database to determine whether the IP address from which the e-mail actually came correlates with an IP address that is associated with the purported domain name in the e-mail. If not, the message is identified as "spoofed," and therefore filtered as spam.

"**Caller ID for E-mail**," developed by Microsoft, is similar to SPF in that it is designed to authenticate e-mail through the DNS database, but it targets the author-header information in the message rather than the return path information.

Since the SPF and Caller ID proposals are similar and compatible, they have been merged together and are sometimes now referred to as "Sender ID." The merged proposal would require that organizations set up e-mail servers so that they automatically verify the domain names from which e-mail messages were sent. There is also a potential that the Sender ID proposal will be merged with Yahoo's DomainKeys proposal, since they are also compatible with one another. The Anti-Spam Research Group of the Internet Engineering Task Force is in the midst of

evaluating the various technologies to combat spam, with the intent that one or more of them will be adopted and implemented as a standard on the Internet worldwide.

Microsoft has also touted the "e-Stamp" framework, in which all senders of e-mail would be required to pay per e-mail sent. Assuming that the per e-mail fee structure can be developed such that it would cost the "normal" subscribers no more money than they currently pay under the monthly flat fee structure, the e-Stamp proposal would only affect spammers, and not legitimate consumers and companies.

Some anti-spam groups such as the Spamhaus project are proposing the establishment of a new ".mail" domain that would be spam-free. An anti-spam organization would survey e-mail sent from .mail addresses and vouch for their non-spam nature, thereby assuring ISPs transmitting such messages of their legitimacy.

Some Internet Service Providers are using available, low-tech tools to combat spam. Cable provider Comcast, the largest provider of broadband Internet access, responded to reports that its system was one of the largest sources of outgoing spam by joining other ISPs in implementing the selective blocking of "port 25," the network gateway that allows computers to send and receive e-mail based on the Simple Mail Transfer Protocol. Comcast reported in June 2004 that blocking port 25 on the accounts of users suspected of being the source of deliberate spam or an inadvertent source of relayed spam resulted in a 35% drop in the amount of spam coming from its system.

CONCLUSION

The CAN-SPAM Act raises significant issues with respect to a company's e-mail marketing campaigns. Since the Act is relatively new, with little interpretive legislative history, regulations or judicial precedent to date, we are left with a literal reading of the Act to interpret its applicability and requirements. The FTC is required to promulgate rules to further define the Act's obligations, and may soon provide additional insight and guidance.

There are a number of practical steps a company can, and should, take to protect itself from potential liability under the Act. Such measures include the following:

1. Establish and implement written internal compliance policies reflecting practices and procedures designed to effectively prevent violations of the Act. The Act specifically provides that having such policies in place will serve to reduce a company's exposure to damages under the Act even if a violation occurs despite such policies.[224] Policies should take into consideration not only the CAN-SPAM Act, but also any promises made in operative privacy policies pertaining to the use of e-mail addresses and e-mailing practices, any contractual obligations the

company has to third parties and all other applicable laws. As part of the implementation of these policies, the policies should be circulated within the company and employees and agents should be educated about their requirements.

2. Regularly audit internal e-mail marketing practices and enforce compliance with applicable policies.

3. Review and re-evaluate published privacy policies, in particular with regard to opt-in and opt-out practices and use of e-mail addresses.

4. Create a "standard" template for use as applicable in all the company's requests for consent to receive e-mail messages.

5. Review the use of "pre-checked" consent boxes on company web sites.

6. Create a template for use in all the company's Commercial E-Mails containing the required information, notices and opt-out mechanisms.

7. Review e-mail address collection practices, including the compliance of third party e-mail lists. Instruct employees not to harvest e-mail addresses or use dictionary derivation to obtain e-mail addresses in any manner contrary to the restrictions of the Act.

8. Review, re-evaluate and, if necessary, revise or amend existing contracts and form agreements for e-mail-based advertising, affiliate marketing and e-mail-related services.

9. Keep abreast of FTC and FCC rulemaking, and consider submitting comments on proposed rules.

10. Monitor new technological tools for managing compliant e-mail marketing campaigns.

ENDNOTES

[1]Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, codified at 15 U.S.C. § 7701 et seq (2003).

[2]State laws continue to be effective only to the extent that they prohibit falsity or deception in any portion of a commercial e-mail. In addition, generally applicable state trespass, contract, tort, fraud and computer crime laws remain in effect. *See* Section VI below for a further discussion of surviving state law.

[3]Because the Act has only been effective since January 1, 2004 and because the Federal Trade Commission has only commenced its rulemaking process as required under the Act, this paper reflects a present understanding of the Act and may be subject to change as rulemaking is completed, enforcement activity continues and case law develops.

[4]CAN-SPAM Act §§ 5(a)(3) and 5(a)(5)(A)(ii).

[5]CAN-SPAM Act § 5(a)(4).

[6]CAN-SPAM Act §§ 5(a)(5)(A)(i) and 5(a)(5)(B).

[7]CAN-SPAM Act § 5(a)(5)(A)(iii).

[8]CAN-SPAM Act §§ 4 and 5(a)(1)-(2).

[9]CAN-SPAM Act § 5(b)(1). E-mail addresses can be harvested (or extracted) from public newsgroup and chat room postings, web sites and other on-line areas using automated "spider" or "robot" programs. Dictionary attacks are mass e-mail dispatches sent to automatically-generated e-mail addresses at common domain names with the expectation that some of the addresses will lead to real users.

[10]CAN-SPAM Act § 4.

[11]CAN-SPAM Act § 5(b)(3).

[12]CAN-SPAM Act § 4.

[13]CAN-SPAM Act § 4.

[14]CAN-SPAM Act § 5(b)(2).

[15]CAN-SPAM Act § 4.

[16]CAN-SPAM Act § 5(d).

[17]CAN-SPAM Act § 7. *See* pp. 23-25, *infra*, for a discussion of actions that have been initiated by the FTC, the U.S. Attorney's office and the State of Massachusetts.

[18]CAN-SPAM Act § 7(g). *See* p. 24, *infra*, for a discussion of actions that have been filed by Internet access service providers. Also, *see* p. 24, *infra*, for a discussion of the potential for an individual private right of action under the Act.

[19]Norman H. Roos, *HIPAA's Privacy Standards May Apply to You*, CT. LAW TRIBUNE, Nov. 25, 2002, at 3; Kristen J. Mathews, *FTC Bans on Marketing Use of Consumer Info By Credit Reporting Agencies Are Upheld*, E-COMMERCE LAW & STRATEGY, Aug. 2002, at 6; Richard Raysman and Peter Brown, *Protecting Consumer Privacy: Are You Prepared?*, N.Y. LAW JOURNAL, April 11, 2000, at 3. Other causes of action under United States law that can and have been used to combat unsolicited and bulk e-mail include: (i) state fraud and deception statutes, regulations and common law, (ii) breach of ISP acceptable use policies, (iii) trespass to chattels, (iv) the Computer Fraud and Abuse Act, (v) state spam laws (to the extent surviving), and (vi) trademark infringement, false designation of origin, dilution and unfair competition. A case may be brought under foreign law (subject to jurisdictional requirements) such as a European Community Member State's law implementing the European Commission's Electronic Communications Directive, which, in general, permits commercial e-mail to be sent to natural persons only on an opt-in basis. *See* Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201, 31/07/2002 P. 0037 – 0047.

[20]The Act generally applies to e-mail messages that are sent to "protected computers," which means a computer which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States. CAN-SPAM Act § 3(13); 18 U.S.C. § 1030(e)(2)(B). This definition, as interpreted by the courts, will serve to define the jurisdictional scope of application of the Act.

[21]The Act's provisions regarding false or misleading header information apply to Transactional or Relationship Messages (as defined by the Act) even though they do not constitute Commercial E-Mail.

[22]CAN-SPAM Act § 3(2).

[23]CAN-SPAM Act § 3(2)(D).

[24]CAN-SPAM Act § 3(2)(C).

[25]Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act, Notice of Proposed Rulemaking and Request for Public Comment, 69 Fed. Reg. 50091 (Aug. 13, 2004) (to be codified at 16 C.F.R. §§ 3.16.1-316.5). This is a continuation of the agency's effort to solicit public comment on this issue, see Advance Notice of Proposed Rulemaking and Request for Public Comment, 69 Fed. Reg. 11776 (March 11, 2004).

[26]*See* Proposed 16 C.F.R. § 3.16.3(a)(2) & (3) (referring to "content that pertains to one of the functions listed in paragraph(b) of this section," i.e., content that pertains to a "transactional or relationship function"). Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act; Notice of Proposed Rulemaking and Request for Public Comment, 69 Fed. Reg. 50091, 50106 (Aug. 13, 2004).

[27]Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act; Notice of Proposed Rulemaking and Request for Public Comment, 69 Fed. Reg. 50091, 50106 (Aug. 13, 2004) (to be codified at 16 C.F.R. §§ 3.16.1-316.5).

[28]CAN-SPAM Act § 3(2)(B).

[29]There is an argument that a subscription-based e-mail newsletter constitutes a "service" that would meet this definition of a Transactional or Relationship Message, despite the fact that the Act's language provides as examples "product updates and upgrades."

[30]CAN-SPAM Act § 3(17)(A).

[31]Those requirements of the Act regarding false or misleading header information apply to Transactional or Relationship Messages.

[32]*See* S. Rep. No. 108-102, p. 16 (July 16, 2003) ("[Transactional or relationship] messages could also include some promotional information about other products or services, but only if the promotional material is truly ancillary to a primary purpose listed in this definition."). See also Section II.A.2 below.

[33]Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act; Proposed Rule, 69 Fed. Reg. 11776 (2004) (to be codified at 16 C.F.R. pt. 316) (Advance notice of proposed rulemaking, request for public comment Mar. 11, 2004).

[34]Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act; Proposed Rule, 69 Fed. Reg. 11776 (2004) (to be codified at 16 C.F.R. pt. 316) (Advance notice of proposed rulemaking, request for public comment Mar. 11, 2004).

[35]*See* Proposed 16 C.F.R. § 3.16.3(a)(1)-(3) (distinguishing advertising and promotional content and transactional or relationship content from "other content"). Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act; Notice of Proposed Rulemaking and Request for Public Comment, 69 Fed. Reg. 50091, 50106 (Aug. 13, 2004).

[36]*Id*.

[37]*Id*.

[38]*Id*.

[39]*Id*.

[40]*See* CAN-SPAM Act § 3(2).

[41]The fact that recipients of a company's newsletters have "opted-in" to receive the newsletters has only limited impact on the analysis of their coverage by the Act. If the nature of the individual's "opt-in" meets the standards of the Act's definition of "affirmative consent," then the e-mail would not be required to be clearly and conspicuously identified as an advertisement or solicitation. CAN-SPAM Act § 5(a)(5)(B). All the other requirements of the Act (with the exception of some of the requirements pertaining to sexually oriented e-mail) would nonetheless apply despite the recipient's affirmative consent to receive the newsletter. However, to the extent an e-mail newsletter falls within the definition of a Transactional or Relationship Message, it would be excluded from the definition of Commercial E-Mail. (*See* n. xxix *supra*) Note that the Act's provisions regarding false or misleading header information apply to Transactional or Relationship Messages as well as Commercial E-Mails.

[42]*See* Proposed 16 C.F.R. § 3.16.3(a)(1). Definitions, Implication, and Reporting Requirements

Under the CAN-SPAM Act; Notice of Proposed Rulemaking and Request for Public Comment, 69 Fed. Reg. 50091, 50106 (Aug. 13, 2004).

[43]*See* Proposed 16 C.F.R. § 3.16.3(a)(2)-(3) (distinguishing advertising and promotional content and transactional or relationship content from "other content"). Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act; Notice of Proposed Rulemaking and Request for Public Comment, 69 Fed. Reg. 50091, 50106 (Aug. 13, 2004). *See also* S. Rep. No. 108-102, at 14 (July 16, 2003) ("... the definition is not intended to cover an e-mail that has a primary purpose other than marketing, even if it ... contains an ancillary marketing pitch").

[44]*See* Proposed 16 C.F.R. § 3.16.3(a)(2). Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act; Notice of Proposed Rulemaking and Request for Public Comment, 69 Fed. Reg. 50091, 50106 (Aug. 13, 2004). As noted above, the argument has been made that a subscription-based e-mail newsletter constitutes a "service" that would meet this definition of a Transactional or Relationship Message, despite the fact that the Act's language provides as examples "product updates and upgrades." The agency itself has requested comment on this point in the NPR. *See* Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act; Notice of Proposed Rulemaking and Request for Public Comment, 69 Fed. Reg. 50091, 50105 (Aug. 13, 2004): "q. Where a recipient has entered into a transaction with a sender that entitles the recipient to receive future newsletters or other electronically delivered content, should such e-mail messages be deemed to be transactional or relationship messages? Why or why not? Should the inclusion of commercial content affect this analysis? If so, how?"

[45]*See* Proposed 16 C.F.R. § 3.16.3(a)(2). Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act; Notice of Proposed Rulemaking and Request for Public Comment, 69 Fed. Reg. 50091, 50106 (Aug. 13, 2004).

[46]*See* Proposed 16 C.F.R. § 3.16.3(a)(3). Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act; Notice of Proposed Rulemaking and Request for Public Comment, 69 Fed. Reg. 50091, 50106 (Aug. 13, 2004).

[47]*See* Proposed 16 C.F.R. § 3.16.3(a)(3). Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act; Notice of Proposed Rulemaking and Request for Public Comment, 69 Fed. Reg. 50091, 50106 (Aug. 13, 2004).

[48]CAN-SPAM Act § 3(14).

[49]CAN-SPAM Act § 3(14).

[50]In any event, if an e-mail address is reassigned to a new user, the new user would not be treated as a Recipient of any Commercial E-Mail sent or delivered to that address before the e-mail address was reassigned. CAN-SPAM Act § 3(14).

[92]CAN-SPAM Act § 3(9). 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. CAN-SPAM Act § 3(15). ". . . a company that merely engages in routine conveyance, such as an ISP that simply plays a technical role in transmitting or routing a message and is not involved in coordinating the recipient addresses for the marketing appeal, shall not be considered to have initiated the message." S. Rep. No. 108-102, at 15 (July 16,

2003).

[93]CAN-SPAM Act §§ 3(9) and 3(12).

[94]CAN-SPAM Act § 3(9).

[95]CAN-SPAM Act §§ 3(9), 3(12) and 3(16).

[96]*See Federal Trade Commission v. Phoenix Avatar, LLC d.b.a. Avatar Nutrition, DJL, LLC, et al*, United States District Court for the Northern District of Illinois, Civ. Action No. 04C 2897 (July 29, 2004). The court's analysis of the definition of "Sender" in this case is discussed in n. 134 below.

[97]CAN-SPAM Act § 3(16)(B).

[98]*See* Sections IV.B and IV.C, *infra*.

[99]CAN-SPAM Act § 3(9).

[100]Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act; Proposed Rule, 69 Fed. Reg. 11776 (2004) (to be codified at 16 C.F.R. pt. 316) (Advance notice of proposed rulemaking, request for public comment Mar. 11, 2004).

[101]CAN-SPAM Act § 5(a)(4)(A)(iii).

[102]CAN-SPAM Act § 5(b)(1)(A).

[103]CAN-SPAM Act § 5(a)(4)(A)(iv).

[104]CAN-SPAM Act § 6.

[105]S. Rep. No. 108-102, at 19 (July 16, 2003). State entities and Internet access service providers do not have authority to enforce this provision of the Act. CAN-SPAM Act § 6(c).

[106]CAN-SPAM Act § 5(b)(2).

[107]CAN-SPAM Act § 5(b)(3).

[108]CAN-SPAM Act § 5(a)(5)(A)(i).

[109]CAN-SPAM Act § 5(a)(5)(B).

[110]CAN-SPAM Act § 3(1).

[111]S. Rep. No. 108-102, at 13-14 (July 16, 2003). *See also State of New York v. Monsterhut, Inc.*, where the Supreme Court of the State of New York, County of New York found that the respondent, Monsterhut.com, had engaged in deceptive business practices and false advertising by falsely representing to consumers that all e-mail addresses were obtained based on permission-based protocols and that consumers had "opted-in" to receive e-mails, when, in fact, consumers had merely failed to remove a check mark from a box which contained such a marking by default. Index No. 402140/02, decision dated Jan. 6, 2002.

[112]S. Rep. No. 108-102, at 14 (July 16, 2003).

[113]CAN-SPAM Act § 3(1)(B).

[114]Such services are frequently referred to as "Append Services."

[115]With regard to sexually oriented Commercial E-Mail, as discussed in Section IV.J., *infra*, the FTC has prescribed marks or notices to be included in the e-mail.

[116]CAN-SPAM Act § 13(b).

[117]Dot Com Disclosures: Information About Online Advertising, http://www.ftc.gov/bcp/conline/pubs/buspubs/dotcom/index.pdf.

[118]CAN-SPAM Act § 5(a)(3)(A).

[119]CAN-SPAM Act § 5(a)(3)(A)(i).

[120]*See* Section IV.F, *infra*, for a discussion of the FTC's request for public comments on this issue in connection with its advance notice of proposed rulemaking.

[121]CAN-SPAM Act § 5(a)(5)(ii). Note that the discussion of the clear and conspicuous requirement in Section IV.A, *infra*, applies equally to the clear and conspicuous opt-out notice.

[122]CAN-SPAM Act § 5(a)(3)(B).

[123]CAN-SPAM Act § 5(a)(3)(B).

[124]CAN-SPAM Act § 5(a)(3)(A)(ii).

[125]CAN-SPAM Act § 5(a)(3)(C).

[126]CAN-SPAM Act § 5(a)(4)(A)(i).

[127]*See* Section IV.F, *infra*, for a discussion of the FTC's request for public comments on this issue in connection with its advance notice of proposed rulemaking.

[128]CAN-SPAM Act § 5(c).

[129] Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act; Proposed Rule, 69 Fed. Reg. 11776 (2004) (to be codified at 16 C.F.R. pt. 316) (Advance notice of proposed rulemaking, request for public comment Mar. 11, 2004).

[130]CAN-SPAM Act § (a)(4)(A)(iv).

[131]S. Rep. No. 108-102, p. 18 (July 16, 2003).

[132]CAN-SPAM Act § 5(a)(4)(B).

[133]CAN-SPAM Act § 5(a)(5)(A)(iii).

[134]*See* Section IV.F, *infra*, for a discussion of the FTC's request for public comments on this issue in connection with its advance notice of proposed rulemaking.

[135]Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act; Proposed Rule, 69 Fed. Reg. 11776 (2004) (to be codified at 16 C.F.R. pt. 316) (Advance notice of proposed rulemaking, request for public comment Mar. 11, 2004).

[136]CAN-SPAM Act §§ 3(9), 3(12) and 3(16).

[137]CAN-SPAM Act §§ 3(9), 3(12) and 3(16).

[138]*See* CAN-SPAM Act § 5(a)(3)-(4).

[139]*See* CAN-SPAM Act § 3(9).

[140]Additionally, to avoid culpability under certain provisions of the Act that apply to promoters in e-mails even if they are not "Senders" or "Initiators" of the e-mail, the company should ensure that the header information in the e-mail is not materially false or misleading. CAN-SPAM Act § 6(a).

[141]Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act; Proposed Rule, 69 Fed. Reg. 11776 (2004) (to be codified at 16 C.F.R. pt. 316) (Advance notice of proposed rulemaking, request for public comment Mar. 11, 2004).

[142]As this may involve the disclosure of a list of opted-out e-mail addresses, a non-disclosure agreement should be in place to limit the use and disclosure that may be made of such list.

[143]*See* CAN-SPAM Act §§ 5(a)(3) and 5(a)(4).

[144]Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act; Proposed Rule, 69 Fed. Reg. 11776 (2004) (to be codified at 16 C.F.R. pt. 316) (Advance notice of proposed rulemaking, request for public comment Mar. 11, 2004).

[145]As this may involve the disclosure of a list of opted-out e-mail addresses, a non-disclosure agreement should be in place to limit the use and disclosure that may be made of such list.

[146]A services provider retained to send e-mails on a company's behalf, and who, in connection therewith, will receive opt-out requests, should be required to date stamp any opt-out requests received. Additionally, for best practices, a limit should be placed on the frequency at which the services provider can send promotional e-mails on behalf of the company.

[147]CAN-SPAM Act § 5(a)(1). "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." CAN-SPAM Act § 5(a)(1)(C).

[148]CAN-SPAM Act § 3(8).

[149]CAN-SPAM Act § 5(a)(1)(A).

[150]CAN-SPAM Act § 5(a)(1)(B).

[151]CAN-SPAM Act § 5(a)(2).

[152]CAN-SPAM Act § 5(b)(1)(A)(i).

[153]CAN-SPAM Act § 5(b)(1)(A)(ii).

[154]CAN-SPAM Act § 5(b)(2).

[155]CAN-SPAM Act § 5(b)(3). To address "spoofing" as well as other unauthorized uses of third party computers to send spam, the FTC, along with 36 additional agencies in 26 countries, launched the "Operation Secure Your Server" campaign, an international effort to reduce the flow of unsolicited commercial e-mail by urging organizations to close "open relays" and "open proxies." As part of the Operation Secure Your Server initiative, the participating agencies have identified tens of thousands of owners or operators of potentially open relay or open proxy servers around the world, and the agencies are sending letters urging the owners and operators to protect themselves from becoming unwitting sources of e-mail. This year's "Operation Secure Your Server" follows on the heels of last year's campaign against open relays, when the FTC and participating national and international agencies identified businesses with potential open relays, urged them to close the relays, and sent information on how to do so. *See* http://www.ftc.gov/secureyourserver.

[156]CAN-SPAM Act § 5(c)(2).

[157]Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act; Proposed Rule, 69 Fed. Reg. 11776 (2004) (to be codified at 16 C.F.R. pt. 316) (Advance notice of proposed rulemaking, request for public comment Mar. 11, 2004).

[158]On April 13, 2004, the FTC issued a rule to prescribe the notice required to be included in e-mail that contains sexually oriented material, and to further define the Act's obligations with respect to such e-mail messages. 16 C.F.R. § 316.1 (2004). The rule became effective on May 19, 2004.

[159]CAN-SPAM Act § 5(d)(4).

[160]"ASCII" stands for the American Standard Code for Information Interchange. It is the basic character coding system that computers use to communicate with one another. Since computers only recognize numbers, ASCII represents letters and other characters such as "@" as decimal numbers. The requirement that the notice be in the ASCII character set was triggered by a concern that an Initiator would attempt to evade the requirement by including the notice in a different character set that would not be recognized by spam filtering software. [161] The phrase "SEXUALLY-EXPLICIT" comprises 17 characters, including the dash between the two words. The colon (:) and the space following the phrase are the 18th and 19th characters. When an e-mail is forwarded or replied to by a Recipient, the FTC's rule requires that the Recipient delete the "RE:" or "FWD:" designations from the e-mail before it is forwarded or replied to, so that the "SEXUALLY-EXPLICIT: " notice will remain the first nineteen characters of the subject line.

[162]The "SEXUALLY-EXPLICIT: " notice in the subject line is intended to inform the Recipient of the sexually explicit nature of the contents of the e-mail and to facilitate the automated filtering of such e-mail. *See* 16 C.F.R. § 316.1 (2004).

[163]CAN-SPAM Act § 5(d)(1).

[164]Note that the discussion of the clear and conspicuous requirement in Section IV.A above applies equally to these requirements.

[165]CAN-SPAM Act § 4.

[166]CAN-SPAM Act § 4.

[167]Sentencing Guidelines for United States Courts, 64 Fed. Reg. 2169 (2004) (Notice of proposed amendments and request for public comment Jan. 14, 2004).

[168]If Congress does not amend the proposed guidelines by November 1, 2004, they will become effective.

[169]CAN-SPAM Act §§ 7(e) and 7(f)(2).

[170]CAN-SPAM Act § 7(f)(9).

[171]The Act's definitions of "Electronic Mail Address" and "Electronic Mail Message" are broad enough, on their face, to include at least some wireless device addresses and messages. Furthermore, a special section of the Act regarding wireless messages defines "mobile service commercial messages" as a subset of commercial electronic mail messages; in particular, those that are transmitted directly to a wireless device that is utilized by a subscriber of commercial mobile services in connection therewith. CAN-SPAM Act § 14. This interpretation is also supported by the Act's legislative history. *See* 149 Cong. Record H 12854, p. 12860 ("The same type of rules that are applicable to commercial e-mail messages sent to personal computers will clearly also apply to those sent to wireless devices, including mobile phones, and the general provisions of the bill would apply to wireless messages as they would to similar messages sent to a desktop computer. Section 14 of the bill builds upon this legislative foundation and puts in place additional protections and modifications. It requires an FCC rulemaking to assess and put in place additional consumer protections.").

[172]CAN-SPAM Act § 14(b).

[175] In re Rules and Regulations Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, No. FCC 04-194 (Aug. 4, 2004), to be codified at 64 C.F.R. § 64.100 ("Restrictions on Unwanted Mobile Commercial Service Messages")

178CAN-SPAM Act § 8(b).

[179]The "Maryland Spam Deterrence Act" imposes criminal penalties and potential jail time on the: (i) use of another's computer to relay or retransmit multiple (as defined by Maryland's Act) commercial e-mails with the intent to deceive or mislead a recipient or an e-mail service provider as to the origin of the message, (ii) material falsification of header information in multiple commercial e-mails that are intentionally initiated, (iii) registration, under a materially falsified identity, for fifteen or more e-mail accounts or two or more domain names from which multiple commercial e-mails are intentionally initiated, (iv) false representation of the right to use 5 or more IP addresses to intentionally initiate multiple commercial e-mails therefrom, (v) unauthorized access to another's computer to intentionally initiate multiple commercial e-mails therefrom, and (vi) committing of any of the foregoing acts by knowingly providing or selecting e-mail addresses that have been obtained through harvesting or dictionary derivation. Chapter 470, Maryland Laws (2004). Another post CAN-SPAM Act

state anti-spam law has been enacted in Florida.

[180]The settlement agreement is available at http://www.oag.state.ny.us/press/2004/jul/jul19a_04_attach.pdf.

[181]For example, the Securities and Exchange Commission has authority to enforce the Act against securities brokers and dealers. CAN-SPAM Act § 7(b)(3).

[182]CAN-SPAM Act § 7. *See* 15 U.S.C. § 45 for the applicable provision of Federal Trade Commission Act.

[183]15 U.S.C. § 45(m)(1)(A) and 16 C.F.R. § 1.98(d).

[184]*Federal Trade Commission v. Phoenix Avatar, LLC d.b.a. Avatar Nutrition, DJL, LLC, et al*, United States District Court for the Northern District of Illinois, Civ. Action No. 04C 2897; *United States v. Daniel J. Lin, et al*, United States District Court for the Eastern District of Michigan, Case No. 04-80383. In considering the request for a preliminary injunction in *FTC v. Phoenix Avatar*, the court held that technical evidence tracing e-mail messages back to their "true origin" is not necessary to prove that defendants may be responsible for the sending of spam in violation of the Act. *Federal Trade Commission v. Phoenix Avatar*, supra, (July 29, 2004). The court found that the spam messages in question advertised products sold on Web sites maintained by certain of the defendants, and that the messages themselves contained hyperlinks to the Web sites, leading to the conclusion that the defendants are "likely responsible" for the sending of the messages in question. The court noted expert testimony submitted by both the FTC and the defendants that it was virtually impossible to trace the "true origin" of the e-mail messages in question, and testimony of the FTC expert that the senders likely routed the spam through open proxies in order to disguise its origin. The court concluded, however, that evidence of "true origin" was not necessary to support a preliminary finding, because liability under the CAN-SPAM Act is not limited to senders, but extends to those who "procure the origin" of spam.

[185]*Federal Trade Commission v. Global Web Promotions Pty Ltd., et al*, United States District Court for the Northern District of Illinois, Civ. Action No. 04C 3022.

[186]*Federal Trade Commission v. Harry*, FTC File No. 042-3085, Docket No. 04C 4790 (N.D. Ill. July 12, 2003).

[187]CAN-SPAM Act § 7(f).

[188]CAN-SPAM Act § 7(f).

[189]CAN-SPAM Act § 7(f).

[190]CAN-SPAM Act § 7(f)(3)(C).

[191]CAN-SPAM Act § 7(f)(3)(D).

[192]CAN-SPAM Act § 7(f)(4).

[193]The Attorney General's Press Release announcing the filing of the complaint is available at

http://www.ago.state.ma.us/sp.cfm?pageid=986&id=1257.

[194]47 U.S.C. § 231(e)(4).

[195]CAN-SPAM Act § 7(g). The Act also provides that it shall have no effect on the adoption, implementation or enforcement by an Internet access service provider of a "policy of declining to transmit, route, relay, handle or store certain types of electronic mail messages. CAN-SPAM Act §8(c). In what may be the first judicial decision relying on the CAN-SPAM Act, the District Court of the Western District of Texas found, under this provision, that the University of Texas was allowed to enforce its policy of blocking e-mail messages coming from IP addresses that had been used by the defendant to transmit what qualified as "spam" under the University's policies, even though such e-mail messages were compliant with the CAN-SPAM Act. *White Buffalo Ventures, LLC v. The University of Texas at Austin*, Case No. A-03-CA-296-SS. Some companies that are in the business of sending unsolicited commercial e-mail and comply with the Act's requirements in doing so, argue that ISPs should not be allowed to block their legally-compliant e-mails. *CAN-SPAM law: Little impact so far*, May 20, 2004 <http://www.infoworld.com/article/04/05/20/HNcanspamimpact_1.html>.

[196]CAN-SPAM Act § 7(g)(2).

[197]CAN-SPAM Act § 7(g).

[198]CAN-SPAM Act § 7(g)(3)(C).

[199]CAN-SPAM Act § 7(g)(3)(D).

[200]CAN-SPAM Act § 7(g)(4).

[201]No. C040880MMC, N.D. Cal.

[202]These companies formed an anti-spam alliance in April of 2003, and have since shared information in a joint effort to fight spam. They also collaborate on issues related to technical Internet standards to combat spam, particularly regarding the certification and authentication of e-mail.

[203]On April 27, 2004, AOL obtained a default judgment against three named defendants – one step toward the first final judgment under the CAN-SPAM Act. AOL now must present proof of damages to receive a full default judgment. *See America Online Inc. v. Davis Wolfgang Hawke*, E.D. Va., No. 04-259.

[204]*Microsoft sues eight alleged spammers*, June 11, 2004 <http://www.computerworld.com/softwaretopics/software/groupware/story/0,10801,93784,00.html>.

[205]*See, e.g.*, CAL. BUS. & PROF. CODE § 17204.

[206]CAN-SPAM Act § 13. The FTC has already promulgated rules with respect to sexually explicit Commercial E-Mail. *See* Section IV.J above.

[207]*See* Section II.A, *supra*.

[208]*See* Section II.A.1, *supra*.

[209]*See* Section IV.C, *supra*.

[210]*See* Section IV.I, *supra*.

[211]*See* Sections IV.E and IV.F *supra*. The FTC received approximately 12,000 comments in response to its request for public comment on these issues. Its regulations with regard to the definition of "primary purpose" are expected to be issued by the end of 2004.

[215]CAN-SPAM Act § 9.

[216]CAN-SPAM Act § 11(1).

[218]Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act; Proposed Rule, 69 Fed. Reg. 11776 (2004) (to be codified at 16 C.F.R. pt. 316) (Advance notice of proposed rulemaking, request for public comment Mar. 11, 2004).

[219] *FTC mulls bounty system to combat spammers*, June 30, 2004 <http://www.msnbc.msn.com/id/5326107>.

[220]CAN-SPAM Act § 11(2).

[221]Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act; Proposed Rule, 69 Fed. Reg. 11776 (2004) (to be codified at 16 C.F.R. pt. 316) (Advance notice of proposed rulemaking, request for public comment Mar. 11, 2004).

[222]CAN-SPAM Act § 10.

[223]Definitions, Implication, and Reporting Requirements Under the CAN-SPAM Act; Proposed Rule, 69 Fed. Reg. 11776 (2004) (to be codified at 16 C.F.R. pt. 316) (Advance notice of proposed rulemaking, request for public comment Mar. 11, 2004).

[224]CAN-SPAM Act §§ 7(f)(3)(D) & 7(g)(3)(D).

