Federal Register

Thursday,
May 12, 2005

Part IV

Federal Trade Commission

16 CFR Part 316

Definitions, Implementation, and Reporting Requirements Under the CAN–SPAM Act; Proposed Rule

FEDERAL TRADE COMMISSION

16 CFR Part 316

[Project No. R411008]

RIN 3084–AA96

Definitions, Implementation, and Reporting Requirements Under the CAN–SPAM Act

AGENCY: Federal Trade Commission (FTC).

ACTION: Notice of Proposed Rulemaking; request for public comment.

SUMMARY: In this document, the Federal Trade Commission (''Commission'' or ''FTC'') proposes rules pursuant to several distinct provisions of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (''CAN–SPAM'' or ''the Act''). Specifically, section 7702(17)(B) grants the FTC discretionary authority to prescribe rules modifying the Act's definition of ''transactional or relationship message.'' Section 7704(c)(1) authorizes the Commission to adopt a rule modifying the ten-business-day period senders (and those acting on their behalf) have under the Act to process recipients' ''opt-out'' requests with respect to ''commercial electronic mail messages.'' Section 7704(c)(2) authorizes the Commission to adopt a rule specifying activities or practices that would be considered ''aggravated violations'' by section 7704(b) of the Act, in addition to the aggravated violations already specified in the statute. Finally, section 7711(a) gives the FTC discretionary authority to ''issue regulations to implement the provisions of [the] Act.''

This document invites written comments on issues raised by the proposed Rule and seeks answers to the specific questions set forth in Part VII of this NPRM.

DATES: Written comments must be received by June 27, 2005.

ADDRESSES: Interested parties are invited to submit written comments. Comments should refer to ''CAN–SPAM Act Rulemaking, Project No. R411008'' to facilitate the organization of comments. A comment filed in paper form should include this reference both in the text and on the envelope, and should be mailed to the following address: Federal Trade Commission, CAN–SPAM Act, Post Office Box 1030, Merrifield, VA 22116–1030. Please note that courier and overnight deliveries cannot be accepted at this address. Courier and overnight deliveries should be delivered to the following address: Federal Trade Commission/Office of the Secretary, Room H–159, 600 Pennsylvania Avenue, NW., Washington, DC 20580. Comments containing confidential material must be filed in paper form, must be clearly labeled ''Confidential,'' and must comply with Commission Rule 4.9(c), 16 CFR 4.9(c) (2005).[1]

Comments filed in electronic form should be submitted by clicking on the following Weblink: *https://secure.commentworks.com/ftc-canspam/* and following the instructions on the Web-based form. To ensure that the Commission considers an electronic comment, you must file it on the Web-based form at *https://secure.commentworks.com/ftc-canspam/* Weblink. You may also visit *http://www.regulations.gov* to read this proposed Rule, and may file an electronic comment through that Web site. The Commission will consider all comments that regulations.gov forwards to it.

The FTC Act and other laws the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. All timely and responsive public comments, whether filed in paper or electronic form, will be considered by the Commission, and will be available to the public on the FTC Web site, to the extent practicable, at *http://www.ftc.gov.* As a matter of discretion, the FTC makes every effort to remove home contact information for individuals from the public comments it receives before placing those comments on the FTC Web site. More information, including routine uses permitted by the Privacy Act, may be found in the FTC's privacy policy, at *http://www.ftc.gov/ftc/privacy.htm.*

FOR FURTHER INFORMATION CONTACT: Sana Coleman, Staff Attorney, (202) 326–2249; or Catherine Harrington-McBride, Staff Attorney, (202) 326–2452; Division of Marketing Practices, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW., Washington, DC 20580.

SUPPLEMENTARY INFORMATION:

I. Background

A. CAN–SPAM Act of 2003

On December 16, 2003, the President signed the CAN–SPAM Act into law.[2] The Act, which took effect on January 1, 2004, imposes a series of new requirements on the use of commercial electronic mail (''e-mail'') messages. In addition, the Act gives Federal civil and criminal enforcement authorities new tools to combat unsolicited commercial e-mail (''UCE'' or ''spam''). Moreover, the Act allows State attorneys general to enforce its civil provisions, and creates a private right of action for providers of Internet access services.

The Act also provides for FTC rulemaking on a number of topics. The Commission has already published final Rule provisions: (1) Governing the labeling of commercial e-mail containing sexually-oriented material,[3] and (2) establishing criteria for determining when the primary purpose of an e-mail message is commercial.[4] The current Notice addresses the Act's grant of discretionary authority for the Commission to issue regulations concerning certain of the Act's other definitions and provisions,[5] specifically, to:

- Expand or contract the definition of the term ''transactional or relationship message'' under the Act ''to the extent that such modification is necessary to accommodate changes in electronic mail technology or practices and accomplish the purposes of [the] Act'' [6]
- Modify the ten-business-day period prescribed in the Act for honoring a recipient's opt-out request; [7]
- Specify activities or practices as aggravated violations (in addition to those set forth as such in section 7704(b) of CAN–SPAM) ''if the Commission determines that those activities or practices are contributing substantially to the proliferation of commercial electronic mail messages that are unlawful under subsection [7704(a) of the Act]''; [8] and
- ''issue regulations to implement the provisions of this Act.''[9]

[1] The comment must be accompanied by an explicit request for confidential treatment, including the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. The request will be granted or denied by the Commission's General Counsel, consistent with applicable law and the public interest. *See* Commission Rule 4.9(c), 16 CFR 4.9(c).

[2] 15 U.S.C. 7701–7713.

[3] 69 FR 21024 (Apr. 19, 2004).

[4] 70 FR 3110 (Jan. 19, 2005).

[5] The Act authorizes the Commission to use notice and comment rulemaking pursuant to the Administrative Procedures Act, 5 U.S.C. 553. 15 U.S.C. 7711.

[6] 15 U.S.C. 7702(17)(B).

[7] 15 U.S.C. 7704(c)(1).

[8] 15 U.S.C. 7704(c)(2).

[9] 15 U.S.C. 7711(a). This provision excludes from the scope of its general grant of rulemaking authority section 7703 of the Act (relating to criminal offenses) and section 7712 of the Act (expanding the scope of the Communications Act of 1934). In addition, section 7711(b) limits the general grant of rulemaking authority in section 7711(a) by specifying that the Commijssion may not use that authority to establish ''a requirement pursuant to Section 7704(a)(5)(A) to include any specific words, characters, marks, or labels in a commercial electronic mail message, or to include the identification required by Section 7704(a)(5)(A)

B. Advance Notice of Proposed Rulemaking

On March 11, 2004, the Commission published an Advance Notice of Proposed Rulemaking (''ANPR'') which solicited comments on a number of issues raised by the CAN–SPAM Act, most importantly, the interpretation of ''primary purpose.'' In addition, the ANPR requested comment on the modification of the definition of ''transactional or relationship message,'' on the appropriateness of the ten-business-day opt-out period that had been set by the Act, on additional aggravated violations that might be appropriate, and on implementation of the Act's provisions generally.[10] The ANPR set a date of April 12, 2004, by which to submit comments. In response to petitions from several trade associations, the Commission announced on April 7 that it would extend the comment period to April 20, 2004.[11]

In response to the ANPR, the Commission received approximately 13,517 comments from representatives of a broad spectrum of the online commerce industry, trade associations, individual consumers, and consumer and privacy advocates.[12] Commenters generally applauded CAN–SPAM as an effort to stem the flood of unsolicited and deceptive commercial e-mail that has threatened the convenience and efficiency of online commerce. Commenters also offered several suggestions for the Commission's consideration in drafting regulations to implement the Act.

C. Notice of Proposed Rulemaking on CAN–SPAM Issues Other Than the ''Primary Purpose'' of an E-mail Message

Based on the comments received in response to the ANPR, as well as the Commission's law enforcement experience, in this NPRM the Commission proposes rule provisions on five broad topics: (1) Defining the term ''person'' (in Part II.A.1.); (2) limiting the definition of ''sender'' to address scenarios where a single e-mail message contains advertisements from multiple entities (in Part II A. 2.); (3) clarifying that Post Office boxes and private mailboxes established pursuant to United States Postal Service regulations are ''valid physical postal addresses'' (in Part II.A.4.); (4) shortening the time a sender has to honor a recipient's opt-out request (in Part II. B.); and (5) clarifying that a recipient may not be required to pay a fee, provide information other than his or her e-mail address and opt-out preferences, or take any steps other than sending a reply e-mail message or visiting a single Internet Web page to submit a valid opt-out request (in Part II. C.).[13] In Part II of this NPRM, each of these proposed provisions is discussed, section by section. Other topics are also discussed, in response to issues raised in comments responding to the ANPR, regarding CAN–SPAM's definition of ''transactional or relationship message'' (in Part II.A.3.), and the Commission's views on how CAN–SPAM applies to certain e-mail marketing practices, including ''forward-to-a-friend'' e-mail marketing campaigns (in Part II.A.5.), even though the Commission does not propose rule provisions addressing those practices. Finally, in Part II.D., the Commission discusses its determination not to designate additional ''aggravated violations'' under section 7704(c)(2).

The Commission invites written comment on the questions in Part VII to assist the Commission in determining whether the proposed Rule provisions strike an appropriate balance, maximizing protections for e-mail recipients while avoiding the imposition of unnecessary compliance burdens on law-abiding industry members.[14]

II. Analysis of Comments and Discussion of the Proposed Rule

A. Section 316.2—Definitions

Section 316.2—one of the Rule provisions previously adopted under CAN–SPAM—defines thirteen terms by reference to the corresponding sections of the Act that define those terms.[15] This NPRM does *not* reopen the rulemaking process for twelve of these definitions. This NPRM, however, does propose adding a proviso to the previously-adopted definition of ''sender.'' This NPRM also proposes adding definitions of ''person'' and ''valid physical postal address.'' These proposed definitional provisions were not part of the earlier rulemaking proceedings, but are discussed and explained in the sections that follow. (Parts II.A.1, 2 and 4.) This discussion of definitions also covers, in Part II.A.3 and 5, why the Commission is not proposing any change to the Act's definition of ''transactional or relationship message'' and how CAN–SPAM applies to ''forward-to-a-friend'' e-mail campaigns.

* * * in any particular part of such a mail message (such as the subject line or body).''

[10] 69 FR 11776 (Mar. 11, 2004). The ANPR also solicited comment on questions related to four Commission reports required to be submitted to Congress: a report on establishing a ''Do Not E-mail'' Registry, submitted on June 15, 2004; a report on establishing a system for rewarding those who supply information about CAN–SPAM violations, submitted on September 16, 2004; a report setting forth a plan for requiring commercial e-mail to be identifiable from its subject line, to be submitted by June 16, 2005; and a report on the effectiveness of CAN–SPAM, to be submitted by December 16, 2005. The comments related to the ''Do Not E-mail'' Registry are discussed in the Commission's June 15, 2004, Report, and comments related to the informant reward system are discussed in the September 16, 2004, Report. The Commission will consider the relevant comments received in response to the ANPR in preparing the remaining reports.

[11] 69 FR 18851 (Apr. 9, 2004). The associations seeking additional time were the Direct Marketing Association, the American Association of Advertising Agencies, the Association of National Advertisers, the Consumer Bankers Association, and the Magazine Publishers of America. The associations indicated that an extension was necessary because of the religious holidays and the need to consult more fully with their memberships to prepare complete responses.

[12] This figure includes comments received on the ''Do Not E-mail'' Registry, which had a comment period that ended March 31, 2004. Appendix A is a list of commenters who submitted a comment in response to the ANPR cited in this NPRM. Appendix A also provides the acronyms used to identify each commente in this NPRM. A full list of commenters, as well as a complete record of this proceeding, may be found on the Commissioner's Web site: *http://www.ftc.gov/os/comments/conspan/index.htm.*

[13] In addition to proposing several new Rule provisions, this NPRM proposes to renumber certain Rule provisions that were previously adopted. 69 FR 21024 (Apr. 19, 2004); 70 FR 3110 (Jan. 19, 2005). The Commission proposes no other substantive changes to the previously-adopted Rule provisions. The Sexually Explicit Labeling Rule provisions, which were found at 316.4 in the January 19, 2005, **Federal Register** Notice's final Rule, are at 316.6 in the proposed Rule presented in this NPRM. The severability provision, which was 316.5, is now 316.7. The new 316.4 proposes a modification to the amount of time senders (and those acting on their behalf) have to process recipients' opt-out requests. The new 316.5 proposes to regulate how opt-out mechanisms in commercial e-mail messages may work. Sections 316.1, 316.2, and 316.3 (regarding scope, definitions, and ''primary purpose'' criteria respectively) retain their numbering from the January 19, 2005, **Federal Register** Notice.

[14] The August 13, 2004, NPRM was limited to the Commission's proposal for criteria to facilitate the determination of the primary purpose of an electronic mail message, 69 FR 50091. These criteria were finalized in a January 19, 2005, **Federal Register** Notice, and have been adopted as 16 CFR 316.3. *See* 70 FR 3110. Nevertheless, many comments submitted in response to that NPRM addressed issues other than ''primary purpose'' that were not raised in the August 13, 2004, NPRM, but are addressed in the instant NPRM. The Commission will consider comments relevant to discretionary rulemaking issues that were submitted in response to the August 13, 2004, NPRM. Commenters are advised, however, that the instant NPRM proposes rule provisions and seeks comment relevant to the discretionary rulemaking topics. Commenters wishing to respond to this NPRM's proposals and requests for comment should take advantage of this current public comment opportunity.

[15] *See* 16 CFR 316.2; 69 FR 2104 (Apr. 19, 2004); 70 FR 3110 (Jan. 19, 2005).

1. Section 316.2(h)—Definition of ''Person''

The term ''person'' appears throughout CAN–SPAM,[16] and is also used in a number of Rule provisions. The Commission proposes to add a definition of this term under authority granted in section 7711 of the Act, which empowers the Commission to ''issue regulations to implement the provisions of this Act.'' The Commission believes that making it clear that the term ''person'' is broadly construed, and is not limited solely to a natural person, will advance the implementation of the Act. The proposed definition tracks the definition of the term included in the Telemarketing Sales Rule, 16 CFR 310.2(v): ''an individual, group, unincorporated association, limited or general partnership, corporation, or other business entity.''

2. Section 316.2(m)—Definition of ''Sender''

Section 7702(16)(A) of the Act defines ''sender'' as ''a person who initiates [a commercial electronic mail] message and whose product, service, or Internet Web site is advertised or promoted by the message.'' [17] The definitional provisions that the Commission has already adopted under CAN–SPAM [18] incorporate by reference the Act's definition of ''sender.'' Many commenters urged that this definition be modified to provide that when more than one person's products or services are advertised or promoted in a single e-mail message there would be only one sender of a message for purposes of the Act.[19] In response to these comments, the Commission proposes in 316.2(m) to set out the criteria for identifying the ''sender'' in that situation. The Commission proposes this clarification pursuant to its discretionary rulemaking authority to ''issue regulations to implement the provisions of this Act.'' [20] Implementation of the Act requires clarity with respect to who is the ''sender'' of a commercial e-mail message because the ''sender'' is obligated under the Act to honor any opt-out requests. Moreover, the sender, as the initiator of a commercial e-mail message, is also obligated to provide a functioning return e-mail address or other Internet-based opt-out mechanism and provide a valid physical postal address of the sender.[21] Therefore, the proposed definition is:

The definition of the term ''sender'' is the same as the definition of that term in the CAN–SPAM Act, 15 U.S.C. 7702(16), *provided that*, when more than one person's products or services are advertised or promoted in a single electronic mail message, each such person who is within the Act's definition will be deemed to be a ''sender,'' *except that*, if only one such person both is within the Act's definition and meets one or more of the criteria set forth below, only that person will be deemed to be the ''sender'' of that message:

(i) The person controls the content of such message;

(ii) The person determines the electronic mail addresses to which such message is sent; or

(iii) The person is identified in the ''from'' line as the sender of the message.

Under this proposal, only one of several persons whose products or services are advertised or promoted in an e-mail message would be the ''sender'' if the person initiated the message *and* was the only person who controlled the content of the message, determined the e-mail addresses to which it would be sent, or was identified in the ''from'' line as the sender.[22] If no one person who meets the Act's definition of ''sender'' satisfies the latter part of this proposed definition (*i.e.*, if no one person controls the content of the message, determines the e-mail addresses to which the message would be sent, or is identified in the ''from'' line as the sender), then all persons who satisfy the definition will be considered senders for purposes of CAN–SPAM compliance obligations.

A hypothetical example can illustrate this proposal. If X, Y, and Z are sellers who satisfy the Act's ''sender'' definition, and they designate X to be the single ''sender'' under the Commission's proposal, *among the three sellers*, only X may control the message's content, control its recipient list, or appear in its ''from'' line. X need *not* satisfy *all three* of these criteria, but *no other seller* may satisfy *any* of them. The sellers may use third parties to be responsible for any criteria not satisfied by X. For example, if X appears in the ''from'' line, the sellers may use third parties—but *not* Y or Z—to control the message's content and recipient list.

a. Comments on the Definition of ''Sender''

The Act's definition is clear with respect to a scenario where a person tries to hide his identity or escape responsibility by having someone else send commercial e-mail on his behalf. Indeed, the legislative history indicates an intent that the definition of ''sender'' reach any entity that either sends its own e-mail messages or contracts with one or more third parties [23] to transmit messages on its behalf.[24] The Senate Report states:

> Thus, if one company hires another to coordinate an e-mail marketing campaign on its behalf, only the first company is the sender, because the second company's product is not advertised by the message. If the second company in this example, however, originates or transmits e-mail on behalf of the first company, then * * * both companies would be considered to have ''initiated'' the e-mail, even though only the first company is considered to be the ''sender.'' [25]

However, commenters argued strongly that the Act's definition is unclear when applied to more complex marketing arrangements involving multiple advertisers and e-mail service providers.

Several commenters claimed to find support in the Act and its legislative

[16] *See, e.g.,* 15 U.S.C. 7702(8), (12), (15), (16); 7704(a)(1), (2) and (3).

[17] 15 U.S.C. 7702(16)(A).

[18] 16 CFR 316.2(m).

[19] The ANPR asked whether it would be helpful to clarify the obligations of the parties when more than one seller's products or services are advertised in a message. The responders to the ANPR's web-based questionnaire overwhelmingly supported clarifying the obligations of multiple senders—seventy-seven percent of responders favored clarifying the obligations and eighty-two percent supported having the Commission issue regulations clarifying who meets the definition of ''sender.'' Commenters who submitted written comments also strongly supported clarification. *See, e.g.*, ABA; IAC; Moerlien; PMA; USTOA; and Visa. Nevertheless, some commenters opined that e-mail messages may have multiple senders and that each should comply with the opt-out requirements. *See, e.g.*, ABM at 6–7 (''[E]ach business whose products are advertised should be considered a sender of the e-mail * * * provided that they are truly 'initiators' and that a reasonable recipient would perceive each of the businesses equally as a sender of the mail.'') ABM proposed a drop-down menu from which recipients could choose whether to opt-out from future commercial e-mail from all, one, or several senders. *See also* ERA; Time Warner (joint marketing effort where two or more companies send out joint e-mail messages).

[20] 15 U.S.C. 7711(a).

[21] 15 U.S.C. 7704(a)(3), (a)(4), and (a)(5).

[22] This proposed definition does not eliminate the possibility that a message may have more than one ''sender.'' However, advertisers can use the criteria set forth in the proposed definition to establish a single sender and avoid a multiple-sender situation. If advertisers fail to structure the message to avoid multiple senders under the proposed definition, then each sender is obligated to comply with CAN–SPAM requirements, notably, to provide an Internet-based opt-out mechanism and a valid physical postal address, and to honor any opt-out requests.

[23] This would include arrangements where numerous so-called ''affiliates'' are induced to send commercial e-mail messages on behalf of a seller to drive traffic to the seller's Web site, and the affiliates are paid based on the number of individuals who ultimately purchase the seller's product or service, or visit the operator's Web site through referral from the affiliate.

[24] *See, e.g.*, Bankers; IAC; Microsoft.

[25] S. Rep. No. 108–102, at 16 (2003).

history for the theory that CAN–SPAM provides for only one sender. For example, IAC, MBNA, and Microsoft pointed out that the statute, throughout, refers to a singular entity: ''the sender'' or ''that sender.'' [26] By comparison, CAN–SPAM's definition of ''initiate'' expressly provides that more than one person may *initiate* a message.[27] These commenters also noted that the Senate Report cited immediately above refers exclusively to messages with one sender.[28] The Commission is not persuaded by these arguments. The Act's definitions of ''initiate'' and ''sender'' are intertwined and must be read together. Every ''sender'' must also satisfy the ''initiate'' definition, so the Act's provision for multiple initiators can apply to multiple senders as well. Moreover, based on the Senate Report excerpt cited above, the Commission believes that CAN–SPAM's drafters apparently had only one scenario in mind—a single seller hiring a third party to transmit messages on its behalf. It is not uncommon, however, for a particular commercial e-mail message to include promotions or advertisements from more than one seller. Under the Act's definition of ''sender,'' each advertiser in an e-mail message may be a ''sender'' of the message because each: (1) ''Initiates'' the message [29] (*i.e.*, has ''procured'' the initiation of the message by paying, providing consideration to, or inducing another person to initiate the message on its behalf); [30] and (2) has products or services that are promoted or advertised in the message.[31]

Responding to the possibility that multiple senders in a single message may have to comply independently with CAN–SPAM, commenters claimed that implementation of the Act may be impeded in single message/multiple advertiser scenarios because of four significant problems the commenters identified regarding a regime that holds more than one party responsible for being the sender of a single e-mail: the difficulty of providing multiple opt-out mechanisms and valid physical postal addresses in a single message; the burden of maintaining multiple suppression lists; the possible violation of privacy policies and statutes; and frustration of consumer expectations. Each of these problems is discussed below.

First, commenters argued that if the law holds more than one party responsible for being ''senders'' of a single e-mail message, the message would have to contain a welter of opt-out mechanisms and physical postal addresses, likely resulting in consumer confusion.[32]

Second, commenters argued that treating each advertiser in an e-mail as a ''sender'' would require multiple suppression lists—*i.e.*, when a list owner advertises its products in an e-mail, along with advertisements of other companies, the list owner and each advertiser would have to add each person that opts out to their ''suppression'' lists and check each list against those of each of the others before sending additional messages.[33] Commenters argued that this result would add unnecessary administrative costs and complexity for legitimate e-mail marketers.[34] A list owner would have to develop a mechanism for receiving suppression lists from every advertiser with which it deals, and for comparing its own mailing list against multiple suppression lists for each message it sends.[35] In addition, a list owner would have to develop a mechanism for managing multiple opt-outs, *i.e.*, ensuring that the consumer can opt out from each advertiser and that all opt-outs sent to the list owner are forwarded to the advertisers from whom the consumer no longer wishes to receive commercial e-mail.[36] Commenters therefore argued that multiple suppression lists would increase costs and time delays.[37] Commenters also noted that, in the case of online newsletters or similar publications, the need for multiple suppression lists could endanger the existence of such newsletters because it would be impossible to create a different newsletter tailored for each recipient, containing only advertisements for companies to which that recipient had not sent an opt-out request.[38] In this regard, some commenters indicated that requiring multiple suppression lists also would threaten the type of joint marketing arrangements that are common in industry and chill electronic commerce.[39]

Third, commenters contended that the need for multiple suppression lists leads to another problem with treating each advertiser as a ''sender'': Multiple suppression lists could force a business to divulge customer names to list owners and other advertisers, even when the business has promised to protect that information under its privacy policy.[40] In addition to contravening privacy policies, a requirement to check names against multiple lists would necessitate passing lists back and forth among several parties, increasing the risk that consumers' private information may be shared with inappropriate entities, or subjected to greater vulnerability from hackers.[41]

Fourth, some commenters stated that, in some situations at least, a requirement that each separate advertiser in a single e-mail message be treated as a separate sender would run counter to consumer expectations.[42] Commenters noted that, when consumers have subscribed to an online newsletter or similar service, they would expect to submit an opt-out request to that newsletter publisher, not to each advertiser in the newsletter.[43] In other words, consumers would expect to send an opt-out request to the party with whom they have previously done business, and to whom they have provided affirmative consent to receive e-mails, not to advertisers that may be included in that party's message.[44]

[26] *See, e.g.*, 15 U.S.C. 7704(a)(3), 7704(a)(5), 7702(17)(a).

[27] *See* 15 U.S.C. 7702(9).

[28] IAC; MBNA; Microsoft. *See* S. Rep. No. 108–102.

[29] 15 U.S.C. 7702(9).

[30] 15 U.S.C. 7702(12).

[31] 15 U.S.C. 7702(16)(A).

[32] *See, e.g.*, Bankers; DMA; ERA; IAC; MPAA; Microsoft; PMA; Time Warner.

[33] *Id.*

[34] *See, E.g.,* Bankers; ASTA; DMA; MPAA; Microsoft; SBA pointed out that this would be particularly injurious to small businesses.

[35] *See, e.g.,* DMA; ERA; Microsoft; PMA.

[36] *See, e.g.,* Microsoft.

[37] *See, e.g.,* Bankers; DMA; ERA; MPAA; Microsoft.

[38] *See, e.g.,* NAA; OPA; Time Warner.

[39] *See, e.g.,* NAA; Time Warner.

[40] *See, e.g.,* Bankers; ASTA; ACB; DMA; IAC; MPA; Microsoft; Time Warner. Of course, to the extent permitted by law, an advertiser could change its privacy policy to reflect the need to share opt-out information with other advertisers. Such a change, however, would not necessarily be in the bets interests of consumers who do not want their e-mail addresses shared among third parties.

[41] *See, e.g.,* DMA; IAC; MPAA; Microsoft; Time Warner.

[42] ABM; DMA; Time Warner.

[43] AMB; Microsoft; Midway; Time Warner.

[44] *See, e.g.,* Time Warner. Arguments regarding consumers' opt-out expectations are complicated by the fact that, in some situations, the party to whom consumers would expect to submit an opt-out request would not be a ''sender'' under the Act. For example, commenters raised the case of an e-mail address list owner who sends commercial messages on behalf of others but does not advertise any products or services of its own. *See, e.g.,* IAC; Microsoft (also arguing that the Act's regulation of this arrangement decreases consumer choice and control). If consumers have asked the list owner to send them commercial messages, they may expect to be able to opt out of that party's messages. This party would not be a ''sender'' under the Act and thus would not have to honor opt-out requests if its own products or services are not advertised in the message. List owners who send messages on a seller's behalf, however, may satisfy the Act's ''initiate'' definition. 15 U.S.C. 7702(9). Persons

Continued

b. Proposal To Modify Definition of ''Sender''

Based on the arguments discussed above, the Commission believes there is merit in the argument that an interpretation of ''sender'' that would not allow multiple advertisers in a single message to designate one as the ''sender'' could impede implementation of CAN–SPAM by placing undue compliance burdens on businesses and endangering the privacy of consumers' personal information. Therefore, the Commission believes that to implement CAN–SPAM, the definition of ''sender'' should be modified so that in situations when more than one person's products or services are promoted or advertised in a single e-mail message, those sellers may structure the sending of the e-mail message so that there will be only one sender of the message for purposes of the Act.

If there is only one sender, the question remains how to determine who is the sender in messages with multiple advertisers. Commenters proposed a variety of criteria for designating a single ''sender'' of such e-mail messages. Most commenters focused on two principal indicia for determining the identity of the sender: (1) Control of the message and (2) recipient expectations.[45]

(1) Control of the Message

Commenters cited several factors evidencing control that would be useful in determining the sender's identity, including:

- Who entity holds itself out as the sender? Who is in the ''from'' line? [46]
- Who originates or transmits the e-mail? Who sends it or causes it to be sent? [47]
- Who collects the recipients' e-mail addresses? Who is the list owner? [48]
- Who provides the list of recipients' e-mail addresses? Who controls the recipient list? [49]
- Who provides the content? Who controls the development of the message content? [50]
- Who, if anyone, has an existing relationship with the recipient? Who, if anyone, received affirmative consent to e-mail the recipient? Who controls the relationship with the recipient? [51]
- Who is the recipient directed to contact if he or she wants more information or to purchase the product or service advertised? [52]

(2) Recipient Expectations

Other commenters urged the Commission to use a ''net impression'' test, in which the ''sender'' would be determined in a way that would be consistent with the recipient's reasonable expectations, *i.e.*, the entity that a reasonable recipient would expect to be the ''sender.'' [53] Commenters suggested that, under such an approach, the Commission would evaluate a message using a variety of factors, like those listed above, that may evidence control.

The Commission believes that the factors highlighted by commenters are relevant to the issue of who should be considered the ''sender.'' These factors can be distilled to three elements, any one or more of which may be the deciding factor as to who is the sender in situations when more than one person's products or services are advertised or promoted in a single e-mail message. The proposed Rule provides that in such situations, the sellers may structure the sending of the e-mail message so that there is but one ''sender''—a person who not only meets the Act's definition, but who also controls the content of the message, determines the e-mail addresses to which such message is sent, or is identified in the ''from'' line as the sender of the message.[54] This proposal would ameliorate what some commenters argued was an overwhelming obstacle to multiple-advertiser messages while preserving e-mail recipients' rights under CAN–SPAM. Sellers who do not avail themselves of this opportunity, in effect, to designate one ''sender'' will each be considered a sender of an e-mail message advertising products or services offered by multiple sellers.

c. ''Sender'' Definition Issues Other Than Single Message/Multiple Senders

Commenters raised additional issues that relate to the definition of ''sender.'' These comments fall into three broad topics: (1) An entity's ''sender'' obligations under CAN–SPAM when its separate lines of business or divisions transmit e-mail messages; (2) an entity's ''sender'' obligations under CAN–SPAM for e-mails transmitted by its affiliates or other similar parties; and (3) content of the ''from'' line as it relates to the identity of the ''sender.'' Comments on each of these topics are discussed in the sections immediately below.

(1) Separate Lines of Business or Divisions

Proposed 316.2(m) incorporates by reference the Act's language regarding obligations under CAN–SPAM when an entity's separate lines of business or divisions transmit e-mail messages.[55] Thus, when a separate line of business or division initiates a message in which it holds itself out to be that line of business or division rather than the entity of which it is a part, the ''sender'' of the message will be considered to be the line of business or division.

Some commenters asked the Commission to provide further clarification of the Act's language with regard to separate lines of business or divisions.[56] The Commission believes, however, that the elements of the definition of ''sender'' adequately clarify obligations in such situations and no additional Rule provision is needed.

Other commenters raised different concerns with how the ''sender'' definition's approach to separate lines of business or divisions would apply to various business models in e-mail

who ''initiate'' commercial e-mail must comply with the Act. *See, e.g.,* 15 U.S.C. 7704(a) and (b).

[45] Nevertheless, a small group of commenters recommended that the Commission use a ''but for'' test. *See, e.g.,* Bankers; ASTA; DMA; Discover; IAC; MPAA; Microsoft; Time Warner. Under such a test, if an e-mail message would have been sent regardless of whether a particular advertisement was included, then the advertiser would not be a sender. The Commission does not believe that such a test is workable from the perspective of law enforcement because it relies on gauging the intent of the sender, an approach that is contrary to the Commission's traditional analysis of advertising or marketing claims. In its final primary purpose criteria, the Commission similarly declined to adopt a ''but for'' test for determining a message's ''primary purpose,'' instead opting to look at the message from the recipient's perspective. 70 FR at 3118. The Commission noted that its decision to use the recipient's perspective is based on the analytical approach the Commission traditionally has taken with advertising, where claims are judged from the consumer's perspective not the marketer's. *Id.* Therefore, the Commission declines to adopt a ''but for'' test, or any other approach that focuses on a sender's intent, in determining the identity of the ''sender.''

[46] Bankers; DMA; ERA; Experian; Go Daddy; MPAA.

[47] *See, e.g.,* ABM; AeA; ACB; ERA; Experian; Go Daddy; IPPC; MMS; NAR; Coalition; Time Warner; USTOA.

[48] *See, e.g.,* DMA; Experian; ERA; IAC; IPPC; Microsoft; Moerlien; Time Warner. IAC and Microsoft also recommended that the list owner or broker be required to identify itself and the role it plays in sending the e-mail.

[49] *See, e.g.,* Bankers; AeA; DMA; ERA; MPAA; IAC; IPPC; MPAA.

[50] *See, e.g.,* AeA; DMA; ERA; Go Daddy; NAR.

[51] *See, e.g.,* AeA; Experian; IAC; Coalition.

[52] *See, e.g.,* Coalition (suggesting one test would be who derives the primary value from the message); USTOA.

[53] *See, e.g.,* ABM; IAC; Microsoft; NAR; Coalition; USTOA.

[54] See ''from'' line discussion in this NPRM, below, for explication of the requirements of CAN–SPAM and section 5 of the FTC Act with respect to the ''from'' line.

[55] 15 U.S.C. 7702(16)(B).

[56] *See, e.g.,* DSA; IFA; Go Daddy (suggesting that ''sender'' should not include affiliates unless companies are so closely intertwined that a reasonable person would conclude they were the same entity); IPPC; MMS; USTOA; Weston.

marketing. These commenters argued that third-party list providers or e-mail services should be considered akin to separate lines of business or divisions and asked that the Commission incorporate the concept of ''third-party advertising service'' or list provider into the definition of ''sender.'' [57] These commenters expressed concern that the definition of ''sender'' does not encompass third-party advertising services, e-mail list service providers, or similar services that compile lists of e-mail addresses, have an established relationship with the recipients, and often use their own lists of e-mail addresses to transmit messages on behalf of advertisers.[58] Some commenters disagreed, urging the Commission to hold responsible the entity whose products or services are advertised or promoted in an e-mail, not the facilitators of the transaction such as list owners/brokers/managers, broadcast services, and other entities not promoting their own products and services in the e-mail.[59]

The Act is quite clear that the definition of ''sender'' includes two elements: one must initiate a message *and* advertise one's own product, service, or Web site in order to be a ''sender.'' [60] Thus, the Act reflects Congress's determination that the obligations of the ''sender'' will fall only on an entity whose products or services are advertised in the message, even though other parties may also transmit or procure the transmission of the message. The Act's definition of ''sender'' simply does not apply to entities that do nothing more than provide a list of names or transmit a commercial e-mail message on behalf of those whose products or services are advertised in the message. Of course, if an e-mail service provider or list compiler or owner initiates messages that advertise or promote its *own* product or service as well as the products or services of others, the list owner may be considered to be the sender. Given this framework, the Commission is not inclined to expand CAN–SPAM's regulation of who must honor opt-out requests to entities whose products or services are *not* advertised or promoted in a message. However, pursuant to section 7709, which requires the Commission to report to Congress on its analysis of the effectiveness and enforcement of the Act, the Commission includes questions in Part VII on the benefits and burdens of such an expansion.

(2) Sender Liability for Practices of Affiliates or Other Similar Entities

Some commenters asked the Commission for a ruling that content providers are not responsible for e-mail messages advertising their product or service if the messages are sent by affiliates or other third parties over which they have no control.[61] The Commission declines to issue so broad a statement—especially because, in other contexts, it has specifically held sellers liable for the actions of third-party representatives if those sellers have failed to adequately monitor the activities of such third parties and have neglected to take corrective action when those parties fail to comply with the law.[62] The Commission believes it inappropriate to excuse content providers in advance from the obligation to monitor the activities of third parties with whom they contract. However, the Commission includes questions in Part VII on whether a ''safe harbor'' provision should be added to the Rule and, if so, what criteria such a safe harbor might include.

(3) Content of the ''From'' Line as It Relates to the Identity of the ''Sender''

Several commenters requested guidance on CAN–SPAM's regulation of ''from'' line content. CAN–SPAM provides that ''a 'from' line * * * that accurately identifies any person who initiated the message shall not be considered materially false or misleading.'' [63] Although this seems fairly straightforward on its face, a number of commenters expressed the view that clarification is needed as to what may be acceptable in the ''from'' line and what would be considered materially false or misleading.[64] Commenters noted that many of the problems with deceptive or fraudulent commercial e-mail involve ''spoofing,'' where the sender pretends to be someone else to induce the recipient to open the e-mail message.[65] Commenters also urged the Commission to use caution and retain a flexible standard, allowing the use of any name in the ''from'' line as long as the name is not deceptive or misleading.[66] In this regard, they indicated that guidelines that are too specific may be overly restrictive because any particular sender might use a variety of names, none of which is deceptive.[67] Commenters suggested that each of the following could be non-deceptive when used in the ''from'' line: Advertiser's name, product being promoted, user ID, screen name, trade name, corporate division, e-mail service provider, third-party advertising service, or marketing company or list used.[68]

Because a significant number of commenters sought guidance on this issue, the Commission believes it helpful to set forth its interpretation of this portion of the Act, although it is not proposing rule provisions in this regard. The analysis must begin with section 7704(a)(1)(B), quoted above, which establishes that ''a 'from' line * * * that accurately identifies any person who initiated the message shall not be considered materially false or misleading.'' [69] Section 7704(a)(6) of the Act is also important because it defines ''materially'' in this context, stating that:

> For purposes of [the Act's prohibition on false or misleading header information, including the ''from'' line], the term ''materially,'' when used with respect to false or misleading header information, includes the alteration or concealment of header information in a manner that would impair the ability of an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation, or the ability of a recipient of the message to respond to a person who initiated the electronic message.

Reading these two provisions together reveals that the test of whether a ''from'' line of an e-mail message runs afoul of CAN–SPAM entails resolution of two issues:

[57] *See, e.g.*, Experian; Coalition (suggesting the Commission could interpret the Act as providing that a ''third party advertising service'' which ''holds itself out to the recipient throughout the message as that particular [third party advertising service] rather than as the [advertiser itself], shall be treated as the sender of such message for purposes of this Act'').

[58] *See, e.g.*, Experian.

[59] *See, e.g.*, MMS.

[60] S. Rep. No. 108–102.

[61] *See, e.g.*, ACB; IFA MPAA; Time Warner; Weston.

[62] *See, e.g.*, 310.4(b)(3)(v) of the Telemarketing Sales Rule, which requires sellers and telemarketers to monitor and enforce compliance with the do-not-call policy and procedures. *See also U.S.* v. *Richard Prochnow,* No. 1:02–CV–917–JOF (N.D. Ga. June 9, 2003).

[63] 15 U.S.C. 7704(a)(1)(B).

[64] *See, e.g.*, Experian; Go Daddy; Jaffe; ValueClick. On the other hand, NFCU considered the Act's language to be perfectly clear. Several commenters asked that the Rule prohibit deceptive or misleading routing or ''reply to'' information. *See* Bahr; K. Krueger. The Commission believes that this practice is already prohibited by section 7704(a)(1) and no further prohibition is needed.

[65] *See, e.g.*, Bahr, Giambra; Potocki; SIIA.

[66] *See, e.g.*, ASTA; EDC; EFF; Experian; Gilbert; Go Daddy; Jaffe; MBNA; NetCoalition; Richardson; SIIA; ValueClick.

[67] *See, e.g.*, ASTA; EFF; Experian; Gilbert; Go Daddy; Mead; NetCoalition; SIIA; ValueClick.

[68] *See, e.g.*, ASTA; Bank; Calvert; Countrywide; EDC; EFF; Experian; K. Krueger; MBNA; NetCoalition; Reed; Richardson; SIIA.

[69] 15 U.S.C. 7704(a)(1)(B).

• Whether the ''from'' line has been altered or concealed in a manner that would impair the ability of an ISP or a law enforcement agency to identify, locate, or respond to the person who initiated the message; and

• Whether the ''from'' line ''accurately identifies any person who initiated the message.''

The first element of this analysis demands little explication. It focuses on the typical spammer's favorite device—falsifying or manipulating header information to thwart efforts to identify and locate the originator of the e-mail. As to the second element, if the ''from'' line accurately identifies the person who initiated the message, then the ''from'' line would not be deceptive. The Commission believes that this does not mean that the ''from'' line necessarily must contain the initiator's formal or full legal name, but it does mean that it must give the recipient enough information to know who is sending the message. For example, if John Doe, marketing director for XYZ Company, sent out commercial e-mails for the company and the ''from'' line indicated that the message was from ''John Doe'' or from ''XYZ Company,'' the ''from'' line would have accurately identified the person who initiated the message. Whether any other name—such as the user ID, corporate division, e-mail service provider, or others suggested by commenters—would be legally sufficient depends on whether such name ''accurately identifies'' a person who ''initiated'' the message, as that term is defined by the Act. For additional guidance on what information in the ''from'' line is acceptable, e-mail senders should consider their messages from their recipients' perspective. If a reasonable recipient would be confused by the ''from'' line identifier, or if a reasonable recipient would not expect the ''from'' line identifier that is provided, those are indications that the sender is not providing sufficient information.

3. Section 316.2(o)—Definition of ''Transactional or Relationship Message''

CAN–SPAM designates five broad categories of messages as ''transactional or relationship messages.'' [70] The Act excludes these messages from its definition of ''commercial electronic mail message,'' [71] and thus excludes them from most of the Act's substantive requirements and prohibitions.[72]

The Act authorizes the Commission ''to expand or contract the categories of messages that are treated as transactional or relationship messages for purposes of [the Act] to the extent that such modification is necessary to accommodate changes in e-mail technology or practices and accomplish the purposes of [the Act].'' [73] Rule provisions previously adopted under CAN–SPAM [74] include 316.2(o), which incorporates the Act's definition of ''transactional or relationship message'' by reference. The Commission proposes no modification to this Rule provision. While many commenters made a number of thoughtful suggestions, none advanced any of them with sufficient evidentiary support for the Commission to conclude that any suggested modification ''is necessary to accommodate changes in electronic mail technology or practices and accomplish the purposes of [the Act],'' as CAN–SPAM requires.[75] Nevertheless, the Commission has considered all the comments on this issue and sets forth its analysis below. The following sections discuss, in turn: (a) CAN–SPAM's regulation of ''transactional or relationship'' e-mail messages as compared with that of ''commercial'' e-mail messages; (b) the Act's standard for modifying the ''transactional or relationship message'' definition; and (c) commenters'' suggestions for expanding the statutory categories of ''transactional or relationship messages.'' Commenters' suggestions regarding each of the ''transactional or relationship'' categories as designated by the Act are discussed below, category-by-category.

a. CAN–SPAM's Regulation of ''Transactional or Relationship'' E-mail Messages as Compared to That of ''Commercial'' E-mail Messages

As noted, CAN–SPAM's requirements and prohibitions are mainly applicable to commercial e-mail messages. The Act defines commercial e-mail messages as those the ''primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet Web site operated for a commercial purpose).'' [76] Commercial e-mail messages are subject to the Act's requirements that the sender or initiator include in the message: (1) A clear and conspicuous notice that the message is an advertisement or solicitation, if the message is sent without the ''affirmative consent'' of the recipient; (2) clear and conspicuous notice of the recipient's right to opt out of subsequent commercial messages from the same sender; and (3) a valid physical postal address of the sender.[77] The Act further prohibits false or misleading transmission information and deceptive subject headings, and requires that a sender provide a mechanism through which opt-out requests may be made online and honor a recipient's opt-out preference.[78]

Messages categorized as ''transactional or relationship'' are subject only to the Act's prohibition on false or misleading transmission information.[79] If a sender's e-mail message, however, is *not* considered as having a ''transactional or relationship'' primary purpose under one of the statutorily established categories, but instead is deemed to have a primary purpose that is commercial, the consequences are relatively modest. In such a case, the sender must comply with requirements of CAN–SPAM—most importantly (from the recipient's

[70] Section 7702(17)(A) of the Act defines a ''transactional or relationship message'' as ''an electronic mail message the primary purpose of which is—

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

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

(iii) To provide—

(I) Notification concerning a change in the terms and features of;

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

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

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

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

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

[71] The Act defines a ''commercial electronic mail message'' as one ''the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet Web site operated for a commercial purpose).'' 15 U.S.C. 7702(2)(A).

[72] One provision, section 7704(a)(1), which prohibits false or misleading transmission information, applies equally to ''commercial electronic mail messages'' and ''transactional or relationship messages''; otherwise, CAN–SPAM's prohibitions and requirements cover only ''commercial electronic mail messages.''

[73] 15 U.S.C. 7702(17)(B).

[74] 69 FR 21024 (Apr. 19, 2004); 70 FR 3110 (Jan. 19, 2005).

[75] *Id.*

[76] 15 U.S.C. 7702(2)(A). *See* Rule Provisions Establishing Criteria for Determining When the Primary Purpose of an E-mail Message is Commercial, 70 FR 3110 (Jan. 19, 2005).

[77] 15 U.S.C. 7704(a)(5)(A)(i)–(iii).

[78] 15 U.S.C. 7704(a)(1); (a)(2); (a)(3); and (a)(4).

[79] 15 U.S.C. 7704(a)(1).

standpoint), to provide an opt-out mechanism and to honor opt-out requests received. These requirements do not prohibit transmission of ''transactional or relationship'' content. Even if a recipient opts out of receiving messages with a commercial primary purpose from a particular sender, that sender may continue to transmit other types of messages. Therefore, recipients who invoke their rights under the opt-out mechanism required by CAN–SPAM will continue to receive valuable ''transactional or relationship'' messages. This is important because transactional or relationship messages are communications that Congress has determined to be *per se* valuable to recipients. Nevertheless, to ensure that the protection from unwanted commercial e-mail CAN–SPAM affords recipients not be eroded, the Commission believes the partial exemptions from the Act's provisions established in the definitions of ''commercial electronic mail message'' and ''transactional or relationship message'' should be interpreted narrowly.

b. CAN–SPAM's Standard for Expanding or Contracting the Categories Designated as ''Transactional or Relationship'' Messages

CAN–SPAM authorizes the Commission to expand or contract the statutory definition of ''transactional or relationship message'' if two criteria are met: (1) The modification must be necessary to accommodate changes in e-mail technology or practices; and (2) the modification must accomplish the purposes of the Act. More than 120 commenters recommended specific modifications to expand or constrict the categories of transactional or relationship messages.[80] Nevertheless, it is striking that only a single commenter asserted that modification was necessary to accommodate changes in e-mail technology or practices.[81] Even this lone commenter did not assert that the change had occurred since the passage of the Act.[82] A handful of commenters suggested that their proposed modifications were necessary to accomplish the purposes of the Act, but these commenters did not claim that any change in technology or practice necessitated their suggested modifications.[83] Therefore, the Commission proposes no substantive modification to expand or contract coverage of the definition of ''transactional or relationship message.'' Although it appears that no such changes are warranted at this time, the Commission did consider all of the comments received on this issue. The various proposals for modification are summarized below.

c. Commenters' Proposals With Respect to Transactional or Relationship Messages

In general, business commenters urged expansion of the definition of ''transactional or relationship message'' to ensure that it includes the messages that these commenters believe do not warrant the opt-out rights and disclosures that CAN–SPAM requires of commercial e-mail. Some commenters recommended modifying the existing statutory transactional or relationship categories explicitly to encompass certain types of e-mail messages. Others recommended specifying whole new categories. Still others sought clarification that particular e-mail messages would be deemed by the Commission to fall into one of the existing specified types. Some consumer commenters, however, believed that the specified categories of transactional or relationship messages were too broad. One such commenter opined that a message should only be considered transactional or relationship if the ''recipient has given an e-mail address to the sender *and* requested that the sender use this method to send these messages.''[84] Commenters' proposals regarding the five categories of transactional or relationship messages established by the Act are discussed immediately below, category by category, followed by a discussion of commenters' proposals for new categories of transactional or relationship messages.[85]

(1) Section 7702(17)(A)(i)—Messages To Facilitate, Complete, or Confirm a Commercial Transaction That the Recipient Has Previously Agreed To Enter Into With the Sender

Of the five categories of messages included in the Act's definition of transactional or relationship messages, the first is messages ''to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender.''[86] Although numerous commenters suggested modifications—predominantly that this part of the definition be expanded—the Commission proposes no modification to the Act's definition of ''transactional or relationship message'' in this area. As noted above, the Commission finds insufficient support in the comments to meet the statutory standard for modifying this definition. Commenters did not demonstrate that any modification is needed to accommodate changes in e-mail technology or practices, and to accomplish the purposes of the Act. Nonetheless, the Commission believes it worthwhile to summarize briefly the kinds of modifications suggested by commenters, and to explain its views regarding certain of this section's provisions. These suggested modifications fall under four basic topics: (a) What constitutes a ''commercial transaction'' under section 7702(17)(A)(i)? (b) How many confirmation messages under section 7702(17)(A)(i) may a sender transmit pursuant to a single transaction? (c) May an e-mail sender use a third-party to send messages under section 7702(17)(A)(i) on its behalf? and (d) Do messages negotiating a commercial transaction satisfy section 7702(17)(A)(i)? Comments relating to each of these topics are discussed in the sections below.

[80] A smattering of other commenters discussed technological changes that do not necessitate modification of the transactional or relationship definition. For example, a few commenters noted that new spam-blocking techniques used by ISPs to filter spam should not be allowed to filter out transactional or relationship messages. Jaffe; CMOR. Another commenter noted that ''the use of ICQ, IM and text messaging via phone and blackberry has increased the source of UCE.'' Shaw. (ICQ is a type of instant messaging program. Instant messaging is defined by Webopedia.com as ''a type of communications service that enables you to create a kind of private chat room with another individual in order to communicate in real time over the Internet, analogous to a telephone conversation, but using text-based, not voice-based, communication.'')

[81] Discover.

[82] Discover cited a purportedly ''recent'' development in online marketing whereby ''companies increasingly use e-mail to facilitate or complete transactions as to which the recipient has made an inquiry or application, but has not yet entered into a contract.''

[83] Lenox; Visa. In fact, Go Daddy opined that there were no technological changes of which it was aware that would necessitate modification of this definition. Go Daddy.

[84] Marzuola.

[85] A variety of commenters claimed that some e-mail messages are neither commercial nor ''transactional or relationship,'' and therefore should be considered exempt from the Act and the proposed Rule. *See, e.g.*, CBA; CMOR (messages sent to conduct marketing and opinion research); BMI (copyright infringement notices). *See also* ACA (claiming that debt collection e-mail messages are not commercial, and are ''at most, 'transactional or relationship messages' ''). The Commission agrees that certain types of messages may not satisfy either the ''commercial'' or ''transactional or relationship'' definitions, and thus are not regulated by CAN–SPAM. The Commission has posed questions in this NPRM asking whether certain types of messages are beyond the scope of the Act, and whether CAN–SPAM should be modified to address these messages.

[86] 15 U.S.C. 7702(17)(A)(i).

(a) What Constitutes a ''Commercial Transaction'' Under Section 7702(17)(A)(i)?

IAC urged the Commission to opine that a ''commercial transaction,'' as used in section 7702(17)(A)(i) , need not involve the exchange of consideration.[87] IAC noted that in the definition of ''commercial electronic mail message'' the term ''commercial products or services'' includes ''content on an Internet Web site operated for a commercial purpose.'' Based on this, IAC argues that registering for a free Internet service such as Evite (a Web site through which registrants may send electronic invitations to events) constitutes a commercial transaction. Microsoft also advocated this position, raising the specter that if the Commission does not adopt this view, it would only encourage ''many more online businesses to charge for their services.'' [88]

The Commission believes that this reading of section 7702(17)(A)(i) is unnecessary because the types of e-mail messages that prompt the concern of IAC and Microsoft would likely be deemed ''transactional or relationship messages'' under a separate subparagraph of section 7702(17)(A). Specifically, under section 7702(17)(A)(v), it seems likely that a message sent from Evite or a similar entity to one who had registered to use its services would be considered a message ''to deliver goods or services * * * that the recipient is entitled to receive under the terms of a transaction'' between the recipient and Evite. The Commission believes that the modifier ''commercial'' has been deliberately omitted from this provision of CAN–SPAM to accommodate just the sort of scenario that IAC and Microsoft raise. The Commission seeks comment on whether messages sent pursuant to a relationship in which no consideration passes may be considered to be a ''commercial transaction'' under section 7702(17)(A)(i), or would more appropriately be considered a transactional or relationship message under section 7702(17)(A)(v), or under some other theory.

(b) How Many Confirmation Messages Under Section 7702(17)(A)(i) May a Sender Transmit Pursuant to a Single Transaction?

IAC also requested that the Commission expressly allow each confirmation message pursuant to a single transaction to be a transactional or relationship message, even if more than one such message is sent. As an example, IAC cited a scenario in which one confirmation is sent immediately after a consumer completes an online transaction (such as booking an airline flight or hotel room) and another is sent in close proximity to the travel time to remind a recipient of her reservation.[89] The Act is silent as to the number of times a sender may transmit to a particular recipient a message to facilitate, complete, or confirm a single commercial transaction. Nevertheless, the Commission believes that, given the purposes of the Act, a standard of reasonableness is implied, and that senders must meet that standard.[90] IAC's scenario would appear to meet this standard, but other scenarios would not. As an extreme example to illustrate the point, if a company sent hourly confirmations of a transaction that warranted merely a single such notice—particularly if the message also contained content advertising or promoting products or services—the Commission would likely view such messages as commercial and not transactional.

(c) May an E-mail Sender Use a Third Party To Send Messages Under Section 7702(17)(A)(i) on Its Behalf?

IAC also urged the Commission to opine that when an entity with whom a recipient has done business uses a third party to send a message confirming a transaction, the message would still be considered a transactional or relationship message.[91] By way of example, IAC argued that when a consumer books an airline reservation using Expedia, the consumer should be considered to have entered into a transaction not only with the airline, but also with Expedia.[92] NAIFA asked that the Commission opine that e-mail messages from an insurance agent to a customer should be considered transactional or relationship messages even though the customer pays the premium to the insurer, not the agent.[93]

These comments raise the question of whether the language of section 7702(17)(A)(i) supports allowing such transactional or relationship messages only from the sender, or also from affiliated third parties if they are facilitating, completing, or confirming a transaction. In the examples cited—when Expedia processes sales on behalf of an airline, and when an insurance company uses agents to sell policies—a message confirming the transaction would qualify as a transactional or relationship message under section 7702(17)(A)(i) whether, in the first example, it came from either Expedia or the airline, and whether, in the second example, it came from either the insurance company or the selling agent. These examples seem fairly straightforward; the Commission seeks comment on whether other situations involving transactional or relationship messages from an entity purporting to be acting on behalf of a sender might be more problematic for consumers or cooperating sellers, or present opportunities for evasion of CAN–SPAM's consumer protections.

(d) Do Messages Negotiating a Commercial Transaction Satisfy Section 7702(17)(A)(i)?

Some commenters asked that the Commission ensure that e-mail messages sent to negotiate a transaction be included in the definition of transactional or relationship message.[94] The Commission believes that, to the extent that negotiation may be considered a ''commercial transaction'' that a recipient has previously agreed to enter into, it would seem that such messages likely would be considered transactional or relationship as long as they were sent to facilitate or complete the negotiation. On the other hand, the Commission would not interpret the term ''transactional or relationship message'' to include an initial unsolicited message that proposes a transaction and attempts to launch a negotiation by offering goods or services. Rather, such a message would likely be categorized as a commercial e-mail message, and would be required to comply with all prescriptions of the Act. The Commission seeks more information about whether e-mail messages sent to effectuate or complete a negotiation might be considered ''transactional or relationship messages'' under section 7702(17)(A)(i), and if so, under what circumstances that may or may not be the case.

[87] IAC.

[88] Microsoft.

[89] IAC.

[90] *See* Go Daddy (advocating requiring contact via transactional or relationship messages to be reasonable).

[91] IAC.

[92] According to IAC, absent such an interpretation, if a consumer were to forward an opt-out request to Expedia pursuant to section 7704(a)(3)(A)(i) prior to the time Expedia had transferred the customer's e-mail address to the airline, such transfer could be considered a violation of section 7704(a)(4)(A)(iv).

[93] NAIFA.

[94] *See, e.g.*, Mellon; SIA; Wells Fargo.

(2) Section 7702(17)(A)(ii)—Messages To Provide Warranty Information, Product Recall Information, or Safety or Security Information With Respect to a Commercial Product or Service Used or Purchased by the Recipient

Commenters had relatively few suggestions for modification to this category, but NADA requested that the Commission opine that scheduled maintenance notifications be considered safety or security information and covered by this definition.[95] To the extent that scheduled maintenance is designed to ensure the safe operation of a product, the Commission believes that reminders of this nature would be considered safety information under the ''transactional or relationship'' partial exemption from CAN–SPAM's requirements. Scheduled maintenance that is *not* necessary for safe operation of a product, however, would not satisfy this ''transactional or relationship'' category. A message notifying recipients when such scheduled maintenance is due could satisfy section 7702(17)(A)(v)—covering, among other things, delivery of product updates or upgrades—if recipients previously agreed to receive such notices from the sender. Section 7702(17)(A)(v), the fifth ''transactional or relationship'' category, is discussed below.

Two other comments requested expansion of this category to cover additional messages. First, Ford Motor recommended that ''product service'' information be expressly included in this category. It is not clear from the comment what kinds of messages might fall outside the existing categories in this section, but within the ''product service'' category. Nor does the comment contain sufficient evidence that this suggested modification is necessary to accommodate changes in e-mail technology or practices and accomplish the purposes of the Act. As a result, the Commission declines to incorporate this language into the proposed Rule.[96] Second, Countrywide recommended expansion of ''security information'' to include ''security-related notifications or education.'' The language of the Act is clear that messages relaying ''security information'' will be categorized as ''transactional or relationship,'' and the Commission finds that the comments contain insufficient justification for altering this language.

(3) Section 7702(17)(A)(iii)—Messages To Provide—(I) Notification Concerning a Change in the Terms or Features of; (II) Notification of a Change in the Recipient's Standing or Status With Respect To; or (III) at Regular Periodic Intervals, Account Balance Information or Other Type of Account Statement With Respect to, a Subscription, Membership, Account, Loan, or Comparable Ongoing Commercial Relationship Involving the Ongoing Purchase or Use by the Recipient of Products or Services Offered by the Sender

The Commission received many comments related to the three sub-categories that comprise this provision. Most business commenters recommended expanding these sub-categories or interpreting them broadly to include more (or even all) messages between a sender and any customer with whom the sender has an established business relationship.[97] Some commenters who endorsed this expansion suggested that the proposed Rule require that the frequency with which recipients are contacted must be reasonable.[98] Some consumers expressed concern about the volume of e-mail messages they might receive if this transactional or relationship category were interpreted too broadly.[99]

The recommendations for expansion were couched in a variety of terms. Some commenters requested that any e-mails regarding a transaction that formed the basis of a relationship between the seller and consumer be considered transactional or relationship messages. Others suggested that messages about an ongoing service that the customer has requested or consented to receive be considered ''transactional or relationship.'' [100] Still others recommended adding a new category for messages ''concerning information, products, or services that the recipient has received or will receive from the sender.'' [101]

Some of the comments focused on specific elements of the language of section 7702(17)(A)(iii). For example, some comments advocated interpreting ''an ongoing commercial relationship'' as beginning when a person opts in to receiving future messages, even in the absence of a purchase.[102] Others suggested removing the restriction that account balance information and statements be sent at regular intervals, noting that certain account statements are ''sent following a transaction, rather than on a 'regular' temporal schedule.'' [103] Some sought a specific articulation that billing statements are transactional or relationship messages, even if some advertising content is included because ''billing statements would be sent irrespective of the inclusion of an advertisement.'' [104] One commenter recommended allowing not only account balance but also ''account-related'' information to be considered transactional.[105] Another inquired whether offerings of related or alternative financial relationships could be categorized as transactional or relationship messages.[106]

The Commission is not inclined to adopt any of these suggestions. As noted above, the Commission believes that the ''transactional or relationship'' provision should be interpreted narrowly to prevent erosion of the protection CAN–SPAM affords recipients from receiving unwanted messages. The categories delineated in the ''transactional or relationship'' provision of the statute are clear and comprehensive, representing Congress's judgment as to the kinds of messages that should be exempt from most provisions of the Act, including its opt-out requirements. Furthermore, the statute provides that the Commission can modify these categories only if the modification is necessary to accommodate changes in e-mail technology or practices and accomplish the purposes of the Act. Because there is inadequate support in the comments to support such a finding, the Commission is not inclined to expand this category of transactional or relationship messages as suggested by commenters.

A small number of the comments focused on narrowing the category to prevent abuses in instances when marketers continue to send commercial

[95] NADA.

[96] If recipients agreed to receive such messages, however, they could satisfy section 7702(17)(A)(v) in the same way that messages reminding recipients of scheduled maintenance could. *See* discussion of section 7702(17)(A)(v) below.

[97] *See, e.g.*, Cendant.

[98] Go Daddy.

[99] Jensen (noting that merely purchasing a single item from a company should not ''allow the company to then inundate the customer with sales pitches, nor should a bank be able to send messages for its many services unrelated to a customers [sic] checking account if that is the only relationship that exists between the parties'').

[100] MPAA; Lenox.

[101] Wells Fargo.

[102] *See, e.g.*, MPAA (noting that a ''subscription or 'preferred customer' loyalty program where special discounts and event opportunities are routinely promoted'' often do not involve the exchange of consideration).

[103] CBA. The Commission believes that if such notices are routinely sent at a certain interval following a transaction that this may well meet the regular interval standard.

[104] Reed. This issue is addressed in the January 19, 2005, **Federal Register** Notice. 70 FR at 3117.

[105] Countrywide.

[106] Visa.

e-mail messages under the guise of transactional or relationship messages even after a loan is paid off, claiming to be changing the status of the recipient from ''paid off'' to ''inactive.'' [107] In a similar vein, NCL expressed concern about the use of dual-purpose messages not only to transmit the recipient's bank balance, but also to advertise additional financial products or services, noting the ''potential for abuse'' if the advertising content overwhelms the transactional or relationship content. As noted above, application of the Commission's primary purpose criteria [108] will allow for proper categorization of such messages. Moreover, as noted in relation to section 7702(17)(A)(i), the Commission interprets the Act as implying a standard of reasonableness. As a result, the Commission may evaluate whether the frequency of contact with which messages purported to be ''transactional or relationship'' are sent exceeds what would be reasonable for such communications in determining whether the message is delivering *bona fide* transactional or relationship content. The Commission therefore is not inclined to propose a rule provision that departs from the statutory language of section 7702(17)(A)(iii).

(4) Section 7702(17)(A)(iv)—Messages To Provide Information Directly Related to an Employment Relationship or Related Benefit Plan in Which the Recipient Is Currently Involved, Participating, or Enrolled

The Commission received a relatively small number of comments on this part of the definition of transactional or relationship message. A consistent theme in the few comments received was the concern that employers be able to send messages to their employees promoting discounts or other offers available to them because of their status as employees.[109] As noted above, the Commission believes that the categories within the definition of transactional or relationship message should be interpreted narrowly. It is unclear from the comments received in response to the ANPR, however, how narrowly this provision must be construed to ensure that e-mail recipients are not unduly burdened by unwanted commercial e-mail messages in the context of an employer-employee relationship. The Commission therefore poses questions in this NPRM soliciting data about classifying messages that offer employee discounts or other similar messages as transactional or relationship messages on the ground that they ''provide information directly related to an employment relationship * * *.''

One commenter urged the Commission to opine that a message sent by a third party on behalf of an employer would be considered transactional.[110] The Commission believes that it is reasonable to interpret the Act to allow an employer to retain a third party as its agent to send a message that would otherwise fit within the confines of this definition; such a message would not be excluded from the definition merely because the third party initiated the e-mail. Nevertheless, the Commission does not interpret this provision as providing blanket treatment as ''transactional or relationship'' for any e-mail message sent on behalf of a third party, even with the permission of an employer. Thus, if a third party were to market its own goods and services to the employees of another company on its own behalf, rather than on behalf of the employer, those messages would not be deemed ''transactional or relationship'' under section 7702(17)(A)(iv). The Commission welcomes further comment this issue.

A few commenters suggested that the Commission depart from the language of the Act by deleting the term ''directly,'' to require only that a message be ''related to an employment relationship or related employee benefit plan.'' [111] Others suggested that the term '' 'directly related to an employment relationship' is not sufficiently clear,'' and recommended that the proposed Rule provide that ''[e]ven commercial messages are employment related when delivered over employer-provided computers.'' [112] The Commission believes such departures from the statute are unwarranted because the comments provide insufficient evidentiary basis that the modification would meet the statutory standard—*i.e.*, necessary to accommodate changes in e-mail technology or practices and to accomplish the purposes of the Act. Moreover, such a modification would diminish the protections provided to recipients of unwanted commercial e-mail messages. For the same reasons, the Commission declines to interpret the phrase ''employment relationship'' so broadly as to allow *any* messages sent by an employer to an employee to qualify as transactional or relationship messsages. The language of the statute clearly delineates this category of transactional or relationship messages as those ''to provide information directly related to an employment relationship * * *'' and the Commission finds no basis in the comments to expand this category.

Other comments focused on when an employment relationship begins. MPAA requested clarification that an '' 'employment relationship' begins at the time when an offer of employment is tendered.'' [113] This transactional or relationship category includes ''provid[ing] information directly related to an employment relationship.'' Information submitted to a prospective employee who has received a *bona fide* offer of employment after actively seeking such employment could be considered information ''directly related to an employment relationship,'' provided such information regards only the prospective employment relationship. As discussed above, the Commission narrowly interprets the scope of the employment relationship. Therefore, e-mail messages sent in regard to the initiation of such an employment relationship present little risk of abuse. At this time, the Commission believes that there is little likelihood that prospective employees would be subject to unwanted commercial e-mail messages from their prospective employers between the time an offer of employment is made and the time it is either accepted or rejected. Questions regarding this interpretation are posed in this NPRM.

As discussed above, since no comments suggested changes that would meet the statutory standard, the Commission declines to propose a rule that would depart from the statutory language.

(5) Section 7702(17)(A)(v)—Messages To Deliver Goods or Services, Including Product Updates or Upgrades, That the Recipient Is Entitled To Receive Under the Terms of a Transaction That the Recipient Has Previously Agreed To Enter Into With the Sender

The Commission received many comments on this provision, most of which addressed application of the act to: (a) E-mail messages delivered pursuant to an electronic subscription; (b) e-mail sent in response to a request for information from a recipient; or (c) messages from an association to its

[107] *See, e.g.*, Ford.

[108] 16 CFR 316.3.

[109] Wells Fargo; CBA; NADA.

[110] SVM (''This definition should be modified to acknowledge that a message is transactional or relationship message, regardless of whether it is sent directly by the employer or with the consent of the employer or on behalf of the employer by a third party or by a service in which the employer of the recipient has enrolled on behalf of the recipient.'').

[111] *See, e.g.*, Countrywide.

[112] Ford Motor.

[113] MPAA.

membership. Each of these is discussed below.

(a) E-mail Messages Delivered Pursuant to an Electronic Subscription

Several commenters recommended considering subscriptions (to newsletters, membership clubs, or other similar electronically delivered content) ''transactional or relationship'' because such messages deliver goods or services the recipient is entitled to receive under the terms of a transaction that the recipient previously agreed to enter into with the sender.[114] According to one of these commenters, section 7702(17)(A)(v)'s reference to a previously agreed-to transaction is satisfied when a recipient opts in to a sender's mailing list, whether or not the recipient provided consideration.[115] Similarly, Microsoft suggested ''where the underlying transaction specifically includes the receipt of promotional e-mails, such as a subscription to a free online service that is supported in whole or in part through the transmission of promotional messages to subscribers,'' such promotional messages should be considered ''transactional or relationship.'' [116]

CAN–SPAM's regulation of a message delivered pursuant to a subscription depends on whether or not the message contains exclusively commercial content. The Commission addressed this distinction in the ''primary purpose'' rulemaking proceeding. In that proceeding, the Commission stated that an exclusively commercial message does *not* satisfy section 7702(17)(A)(v).[117] Rather, CAN–SPAM treats such a message, when it is sent pursuant to a subscription, as a commercial e-mail message delivered with the recipient's ''affirmative consent.'' [118] In that case, all of CAN–SPAM's provisions regulating commercial e-mail apply, except a recipient's ''affirmative consent'' overrides his or her previously-submitted opt-out request, and a message sent with a recipient's affirmative consent does not have to provide clear and conspicuous identification that the message is an advertisement or solicitation.[119] When a subscription calls for delivery of a message that is not exclusively commercial, then the message is ''transactional or relationship'' under section 7702(17)(A)(v) as long as ''the recipient is entitled to receive [the message] under the terms of a transaction that the recipient has previously agreed to enter into with the sender.'' [120] The sender is not required to receive consideration from the recipient for the message to fall within this category.

(b) E-mail Messages That Respond to a Recipient's Request for Information

Some commenters suggested that messages containing information specifically requested by the recipient be considered ''transactional or relationship.'' [121] ValueClick noted that absent such an interpretation, a consumer visiting a travel Web site and requesting information about a specific destination might be unable to receive messages about the destination about which she inquired.[122] Justasmallthing.com echoed this sentiment, stating that if a request for a catalog is made by a recipient, a company should have the right to respond by e-mail, unless the recipient has requested not to be contacted in that manner.[123] ABM argued that messages sent in response to a specific request for information should be allowed even if the requestor had previously opted out of commercial mail messages.[124] These commenters were consistent in their belief that the intent of the Act is not to regulate solicited e-mail messages, and that failure to state expressly that such messages are included in the definition of transactional or relationship message would lead to decreased productivity and unnecessary restrictions on consensual communication.[125]

The Commission believes that the concerns raised by these commenters are already addressed by section 7704(a)(4) of the Act, which makes clear that even commercial e-mail messages may be sent to a recipient who has previously opted out ''if there is affirmative consent by the recipient subsequent to the opt-out request.'' [126] In each of the scenarios posed by commenters, consumers who request information or consent to receive it would, presumably, have provided ''affirmative consent,'' thus enabling the sender to respond.[127]

(c) E-mail Messages From an Association to Its Members

Many membership associations argued that e-mail messages sent by associations to their members should be considered transactional. ABA requested that the definition of transactional or relationship messages be modified to expressly ''include all e-mail communications, whether commercial or informational, that are sent by associations and other tax-exempt nonprofit organizations to their own members.'' [128] As ABA noted, ''[t]he act of procuring membership in an organization has long provided explicit and implicit consent to communication from that organization regarding that membership, especially when the individual voluntarily provides his or her e-mail address fully anticipating receipt of e-mail communications.''* * * [129]

[114] P&G United; Speer (noting that the language of the Act should be expanded to allow for the delivery of ''information'' as well as goods or services); SIA (requesting that the FTC clarify that certain informational messages, including ''newsletters, reports, and others that provide information to customers, concerning such things as investments or advice, do not have a primary purpose that is commercial in nature''); Lunde; Lenox; Venable; NEPA; Comerica.

[115] Edgley.

[116] Microsoft.

[117] 70 FR at 3118, n. 91.

[118] *See* 15 U.S.C. 7702(1) for the Act's definition of ''affirmative consent.''

[119] *See* 15 U.S.C. 7704(a)(4)(B); 7704(a)(5)(B).

[120] 15 U.S.C. 7702(17)(A)(v).

[121] *See* Edgley; ESPC; Fredrikson; Mellon.

[122] *See also* Discover; KeyCorp; PMA; SIA. ASA made a similar argument in the business-to-business context regarding messages responding to an invitation from a general contractor to bid on a project. According to ASA, if bid proposals sent in response to such invitations were not considered transactional, subcontractors wishing to reply could have to determine if the general contractor has opted out before doing so.

[123] *See also* Edgley; Fredrikson.

[124] *See also* KeyCorp; NADA (analogizing to the Telemarketing Sales Rule, which permits telemarketing calls in response to an inquiry or application even if the individual called is on the National Do Not Call Registry). This is permissible under section 7704(a)(4)(B) of the Act.

[125] *See, e.g.*, ABA (noting that the Act was ''intended to apply primarily to unsolicited communications sent by for-profit businesses, not to e-mail communications between associations and other tax-exempt nonprofit organizations and their respective members'' and that members ''expect—and value—the receipt of such information'' as renewals, seminar notices, and educational materials); UNC; United (arguing that since messages a recipient ''knowingly chooses to receive'' are not unsolicited, they should be treated as transactional or relationship messages); Lenox; ClickZ; ICOP; Aspects.

[126] 15 U.S.C. 7704(a)(4)(B). Section 7702(1) presents the Act's definition of ''affirmative consent.'' Of course, any commercial e-mail message sent with a recipient's affirmative consent must provide an opt-out mechanism that complies with sections 7704(a)(3) and 7704(a)(5).

[127] 15 U.S.C. 7702(1)(A) (defining ''affirmative consent'' to mean ''the recipient expressly consented to receive the message, either in response to a clear and conspicuous request for such consent or at the recipient's own initiative'').

[128] ABA. *See also* RTCM; AAOMS; IAAMC; ABM; AOC (suggesting that while existing categories of transactional or relationship message may include communications between organizations and their members, the expansion of either category or the creation of a new category that explicitly delineates such messages as transactional or relationship would be preferable).

[129] One consequence of categorizing such opt-in mail as transactional or relationship is that those who receive it would not have a legally-mandated opportunity to make an opt-out request pursuant to sections 7704(a)(3)(A) and (a)(4)(A). Some

Continued

The Commission believes it is likely that many such messages may have a primary purpose that fits within the existing categories of transactional or relationship messages. However, the Act does not provide an explicit exemption for communications by membership associations with their members, nor do any of the comments argue that modifying the definition of ''transactional or relationship message'' to include comments from associations to their membership is necessary to accommodate changes in e-mail technology or practices and accomplish the purposes of the Act. Thus, to the extent that application of the primary purpose criteria yields the conclusion that a membership association's e-mail message sent to its membership has a commercial primary purpose, then the association, as a sender, would need to comply with the provisions of the Act relating to commercial e-mail messages.

Lastly, some commenters requested expanding the section 7702(17)(A)(v) category to include messages about service updates or upgrades, in addition to product upgrades.[130] One suggested that the provision should be framed around messages the sender is entitled to send, rather than those a recipient is entitled to receive.[131] As neither of these suggestions was supported by evidence that the proposed change is necessary to accommodate changes in e-mail technology or practices and accomplish the purposes of the Act, the Commission is not inclined to adopt them.

(6) New Categories of Transactional or Relationship Messages Recommended by Commenters

Commenters proposed a variety of new transactional or relationship categories for specific market segments or types of campaigns. These include messages from educational institutions to their faculty, staff, students, alumni, and friends;[132] communications between franchisors and franchisees;[133] messages sent by cemeteries and funeral homes;[134] all messages sent by businesses to their existing customers;[135] business-to-business communications,[136] including what some commenters termed ''business relationship messages'''; [137] messages sent by non-profit organizations;[138] messages that provide legally mandated notifications to customers;[139] and messages reminding consumers ''that they are included in the sender's database or have been added to such database and how they may opt-out.''[140] As discussed above, because no comments suggest that the recommended changes are necessary to accommodate changes in e-mail technology or practices and accomplish the purposes of the Act, the Commission declines to adopt these recommendations. If a message contains the commercial advertisement or promotion of a commercial product or service, it contains ''commercial'' content under the Act. If a message providing non-commercial content (such as a legally mandated notification) also contains commercial content, then it will be governed by the Commission's primary purpose criteria as a dual-purpose message.[141] The Commission has included in this NPRM questions that solicit further information on the topic of new transactional or relationship categories.

4. Section 316.2(p)—Definition of ''Valid Physical Postal Address''

The proposed Rule defines the term ''valid physical postal address'' to clarify that a sender may comply with section 7704(a)(5)(A)(iii) of the Act by including in any commercial e-mail message any of the following: (1) The sender's current street address; (2) a Post Office box the sender has registered with the United States Postal Service; or (3) a private mailbox the sender has registered with a commercial mail receiving agency (''CMRA'') that is established pursuant to United States Postal Service regulations. This proposed definition is important because section 7704(a)(5)(A)(iii) of the Act requires any commercial e-mail message to include ''a valid physical postal address of the sender.''[142]

In its ANPR, the Commission noted that many senders of commercial e-mail seeking compliance advice had questioned the scope of the term ''valid physical postal address,'' suggesting rulemaking under section 7711 might be appropriate to clarify this issue.[143] Accordingly, the ANPR asked whether the term ''valid physical postal address'' could fairly be read to encompass a Post Office box or private mailbox,[144] and

commenters noted that association members, and others who receive transactional or relationship messages, are afforded the right to ''opt out'' as part of their membership. *See, e.g.,* AOC; AWWA. There is, however, no legal compulsion for associations to grant this right to members.

[130] SVM.

[131] SVM.

[132] KSUF; UNC (arguing that ''CAN–SPAM compliance language'' requiring an opt-out mechanism in every message deemed to be commercial would negatively impact the recipients' view of the message, and ''reduce drastically the size'' of their e-mail contact list).

[133] Cendant (arguing that the primary purpose of these messages, even those offering business seminars, is not to sell such services, but rather to ''timely communicate and offer business seminars to our franchisees'').

[134] ICFA (arguing that the CAN–SPAM Act ''never intended to restrict'' messages sent by cemeteries and funeral homes to alert families to special events or services, or changes in cemetery rules).

[135] NEPA. *See also* Comerica; ACB; PMA (''[A]ny e-mail relating to the goods or services which formed the basis of the transaction or relationship between the sender and the consumer should be considered a transactional or relationship message.'').

[136] *See, e.g.,* Visa (noting that the Commission had included a business-to-business exemption in the Telemarketing Sales Rule); ACLI (noting the definition of ''Pre-Existing Business Relationship'' in § 214 of the FACT Act, Pub. L. 108–159, 117 Stat. 1952); MMS; Harte; RMAS; SIA. Courthouse agreed that such a preexisting or current business relationship exemption is desirable, but noted that it may be appropriate to limit it to relationships where there has been a ''prior monetary payment by the recipient to the sender.''

[137] Some commenters mentioned a special category of ''business relationship'' messages: those that are individualized and sent from one employee of a company to an individual recipient (or small number of recipients). *See, e.g.,* ESPC; Wells Fargo (stating that if each e-mail sent by an employee of a business has to be scrubbed against that business's suppression list it would be ''extraordinarily burdensome and expensive''). The Commission has asked questions in Part VII of this NPRM about whether such a carve-out is warranted due to changes in e-mail technology and practices, and whether such a carve-out is necessary to accomplish the purposes of the Act.

[138] *See, e g.,* ASAE; AWWA; ABA; RTCM; AAOMS; IAAMC; ABM; AOC. Several of these commenters argued that all e-mail communications from non-profit organizations to their current members should be deemed ''transactional or relationship messages.'' Others claimed that messages by nonprofits might be considered ''commercial'' only if the messages' content related to an activity not substantially related to the organization's tax-exempt, non-profit purposes. The main justification offered by these commenters was that a nonprofit's messages to its members are intended to provide information in connection with an organization or association membership and/or to deliver goods and services under the terms of an existing member, donor or customer relationship.

[139] According to commenters, these include privacy notices, billing error notices, and change in terms notices. *See* IBAT; RMAS (urging that e-mails including a service deliverable, obligatory notice, or other contracted-for advice, product, or service should be transactional); SIA (recommending that notices mandated under Gramm-Leach-Bliley be considered transactional); Wells Fargo (suggesting that the Commission coordinate with banking regulators regarding the overlap in regulations regarding legal notices); Comerica.

[140] ValueClick.

[141] *See* 16 CFR 316.3. For a detailed discussion of the Commission's primary purpose criteria, *see* 70 FR 3110.

[142] 15 U.S.C. 7704(a)(5)(A)(iii). It is noteworthy that other anti-spam legislation introduced in the 108th Congress contained a requirement that the valid physical address of the sender be included in each e-mail message. *See* SPAM Act, S. 1231, section 206 (introduced June 11, 2003). Still other bills required inclusion of the sender's valid physical street address. *See, e.g.,* Reduction in Distribution of Spam Act of 2003, H.R. 2214, section 101(a)(1)(D) (introduced May 22, 2003).

[143] 69 FR at 11781.

[144] This NPRM uses the term ''private mailbox,'' a term of art used in the regulations of the United States Postal Service, in place of the term commercial mail drop, which the ANPR used.

whether it would be desirable for the Commission to adopt rule provisions clarifying the scope of the term.[145]

Dozens of commenters responded on this issue.[146] A significant majority of these comments urged the Commission to clarify that a sender could satisfy the Act's valid physical postal address disclosure requirement by providing a Post Office box or private mailbox address. The Commission is persuaded by the arguments these commenters advanced, and therefore has defined the term in the proposed Rule to include the sender's street address, Post Office box, or private mailbox, duly registered with the United States Postal Service or a CMRA. These comments address a valid physical postal address as a means of identifying and locating the sender; the statutory intent reflected in the use of the term ''physical'' in the Act's reference to ''valid physical postal address;'' and practical concerns regarding the potential burdens on e-mail senders if Post Office boxes and private mailbox addresses were not considered to satisfy this requirement. Comments relating to each of these topics are discussed in turn immediately below.

a. A Valid Physical Postal Address as a Means of Identifying and Locating the Sender

Commenters uniformly agreed that one intent of CAN–SPAM is to allow recipients and law enforcement officials to easily identify and locate senders of e-mail.[147] These commenters were split, however, on the issue of whether inclusion of a street address is necessary to effectuate this intent. Arguing that Post Office boxes and private mailboxes have been used by criminals in the past as a means of preserving their anonymity, NFCU opposed reading the term ''valid physical postal address'' to include those alternatives.[148] Other commenters opposed defining ''valid physical postal address'' to include private mailboxes on the grounds that they are more likely than Post Office boxes to be used to mask the identity of a rogue spammer because the United States Postal Service typically has more rigorous identification procedures than private mailbox companies.[149] ASTA opined that allowing a Post Office box or commercial maildrop to be a ''valid physical postal address'' would frustrate the purpose of the Act because, if the sender falsified his or her registration information, the address would not help recipients or law enforcement authorities locate the sender.[150]

Many commenters took the opposite tack, arguing that allowing a Post Office box or private mailbox to be a ''valid physical postal address'' would make it possible to identify and locate senders because renters of Post Office boxes must provide their street location to the Post Office as a condition for obtaining a box address.[151] ERA also suggested that since very few recipients would ever visit the sender in person, a Post Office box or private mailbox address would be useful even if it only allowed the recipient to contact the sender by conventional mail.[152] Experian opined that for the Commission to limit the definition of ''valid physical postal address'' by excluding Post Office boxes and private mailboxes would exceed the agency's mandate under the Act.

The Commission is aware from its own law enforcement experience that those who orchestrate illegal schemes typically seek to remain anonymous to law enforcement officials and the irate public affected by their schemes. Nevertheless, CAN–SPAM and the FTC's regulations under it will impact the business practices of many legitimate companies that send commercial e-mail messages, and the Commission is reluctant to require such entities to alter their mail handling procedures unnecessarily. As SIIA noted, ''[a]n individual or entity seeking to evade identification can just as easily use inaccurate street addresses'' as hide behind a Post Office box or private mailbox.[153] Such a seller would simply tell the same lies in a different way. Thus, allowing the use of Post Office boxes and private mailboxes creates no greater risk that a sender will falsify information to thwart the purposes of the Act. Moreover, the regulations of the United States Postal Service require verification of the street address of any person seeking to rent a Post Office box or a private mailbox through a CMRA.[154] Therefore, the proposed Rule defines the term ''valid physical postal address'' to include Post Office boxes and private mailboxes duly registered pursuant to regulations of the United States Postal Service.[155]

b. Statutory Intent Reflected in the Use of the Term ''Physical''

A second issue raised by several commenters was the meaning of the term ''physical'' in this section of the Act. Some commenters argued that the inclusion of the word ''physical'' must be given weight and that this word must be seen as a delimiter of the rest of the phrase, ''valid * * * postal address,'' thus requiring a street address.[156] These

When a commenter is quoted, however, the term the commenter actually used is reproduced.

[145] 69 FR at 11781.

[146] One commenter suggested requiring that information provided to a domain name registrar be valid and include a confirmed physical address. Vandenberg. Such a requirement is unnecessary as obtaining a domain name by false or fraudulent representations is already prohibited by section 7704(a)(1)(A) of the Act. *See* 15 U.S.C. 7704(a)(1)(A).

[147] A few commenters on either side of this issue were particularly precise, focusing on the value of a valid physical postal address to law enforcement authorities and potential plaintiffs seeking to accomplish service of legal process. *See* AT&T; K. Krueger. *But see* DoubleClick (''If the purpose of this provision were to identify where companies could be served with legal process, then the law would have required the listing of a sender's corporate headquarters or legal 'place of doing business.' '').

[148] *See* NFCU (noting that ''such addresses are often used in fraud schemes and effectively shield their owners from identification''). *See also* Sachau (''[W]e have too many fly by nights with post office boxes—here today and gone tomorrow.''); ValueClick; ICC.

[149] Gilbert (''P.O. Boxes require identification etc. Many private mailboxes do not.''); NCL (noting that since some individuals' and businesses' ''only mailing address * * * is a post office box,'' inclusion of a P.O. box would be acceptable, but that private mailbox addresses should be excluded because they ''are often used to obscure [senders'] real physical locations''); Shaw (no ''mail drops'').

[150] ASTA (also noting that a street address is desirable ''to have a locus about which complaints could be filed if necessary''). *See also* RDS (noting that recipients and law enforcement officials must ''have access to the persons responsible for sending the e-mail''); NetCoalition (A physical address is necessary to ''ensur[e] that a sender can be physically located.'').

[151] *See, e.g.*, SIA; Discover; IAC; DMA (suggesting that a Post Office box should be included as a valid physical postal address ''[w]here the sender is otherwise locatable as a result of being a registered entity under corporate law or federal securities regulation''); ABA; DoubleClick. *But see* Gilbert (claiming that many private mailboxes do not require identification).

[152] ERA (noting that a requirement that the street location be disclosed could result in sender's having to train staff to handle customer visits).

[153] *See* SIIA. *See also* Coalition (noting that this provision is likely to impact legitimate marketers who do not misrepresent their identity rather than spammers who might as easily falsify a street address as hide behind a falsely registered Post Office box or private mailbox).

[154] A CMRA must confirm that an applicant for a private mailbox resides or conducts business at the permanent address shown on the application submitted to the CMRA. Applicants have a duty to file a revised application if any of the information provided changes. D042.2.6 (governing procedures for delivery of mail to a CMRA). Similarly, an application for a Post Office box ''may not be approved until the applicant's identity and current permanent physical address where he or she resides or conducts business is verified.'' D910.2.1–2.2 (DMM Issue 58 plus Postal Bulletin changes through PB 22130 (6–10–04)). Furthermore, criminal or civil sanctions for providing false or misleading information on either application accrue, pursuant to 18 U.S.C. 1001.

[155] Proposed Rule 316.2(p).

[156] ValueClick (noting that ''[t]he principal rule of statutory construction is to give meaning to every word''); ICC (''To give some meaning to the term 'physical,' something more than a mere P.O. Box is required.''); AT&T (''[B]y choosing the adjective

Continued

commenters read ''physical'' to mean something more than a mere mailbox. Other commenters countered this argument by citing legislative history to show that Congress intended that the term ''physical'' be viewed in contrast to the term ''electronic,'' and to clarify that it would be insufficient for a sender to simply include an e-mail address to comply with this provision.[157]

The Commission is persuaded that the term ''physical'' can reasonably be read to include not only street addresses, but also validly registered Post Office boxes and private mailboxes. Post Office boxes and private mailboxes have a physical presence, and both are considered legitimate by the United States Postal Service.

c. Practical Concerns if Post Office Boxes and Private Mailboxes Were Not Considered ''Valid Physical Postal Addresses''

Commenters who advocated that Post Office box and private mailbox addresses be considered ''valid physical postal addresses'' also raised several practical concerns about the possible consequences of excluding them from the definition. First, some commenters argued that exclusion of these alternatives could create confusion because there are still some areas within the United States that do not use street addresses, but rather rely on Post Office boxes for the delivery of all local mail.[158] The proposed definition of ''valid physical postal address,'' which includes Post Office boxes and private mailboxes, will resolve the concerns expressed by these commenters.

Other commenters expressed concern that any interpretation of ''valid physical postal address'' that would require a small home-based business to include its street address in commercial e-mail would negatively impact the privacy, and possibly the physical security, of those who run such enterprises.[159] SBA noted that it has long advocated allowing the use of Post Office boxes to protect the security of home-based businesses, which account for more than half of all small businesses.[160] The Commission finds these comments persuasive, and believes that the proposed Rule's definition of ''valid physical postal address'' addresses their concerns.

Finally, commenters cited efficiency as a reason for allowing a Post Office box or private mailbox to be considered a ''valid physical postal address.'' Comerica noted that Post Office boxes are typically used by corporations to speed the process of delivery of mail internally.[161] ACLI and others pointed out that this is not only an efficient business practice, but a common one used for many years by a host of legitimate businesses. Prompted by these and the other considerations discussed above, the Commission proposes to define ''valid physical postal address'' to include such addresses.

5. Implications of Certain Definitions for ''Forward-to-a-Friend'' Scenarios

In the ANPR, the Commission requested comment on the impact of CAN–SPAM on ''forward-to-a-friend'' e-mail marketing campaigns, by which recipients forward a company's message to other persons. In response, the Commission received more than forty comments on the issue of whether forward-to-a-friend marketing campaigns should be required to comply with the Act.

The most clear-cut ''forward-to-a-friend'' scenario involves the situation in which a person receives a commercial e-mail message and forwards the e-mail message to another person. Commenters were also concerned about a similar, but materially different, scenario involving a Web page that enables persons who visit it to send a link to or a copy of that Web page to others via e-mail. CAN–SPAM does not expressly address either of these forward-to-a-friend scenarios, but three of the Act's interconnected core definitions—''sender,'' ''initiate,'' and ''procure''[162]—have an impact on them. Therefore, to assist industry in complying with the Act, this notice discusses the applicability of these definitions to forward-to-a-friend practices.

Industry commenters uniformly opined that forward-to-a-friend campaigns should not be required to comply with the Act, especially when no consideration is provided.[163] They also opined that once a commercial e-mail message is forwarded by the original recipient to a friend or family member, it ceases to be a ''commercial e-mail message'' under the Act.[164] Industry commenters expressed concern that they would be held responsible for CAN–SPAM violations in messages over which they have no control.[165] They cited the fact that when the initial recipient of an e-mail message forwards a company's message, the company has no control over the content or destination of the message, and, thus, lacks the ability to ensure CAN–SPAM compliance.[166] The original recipient could, for example, delete the required opt-out mechanism or the valid physical postal address before forwarding the message to another, or forward the message to someone who, unbeknownst to the original recipient, has previously sent the company an opt-out request. If the company—the original sender or initiator of the e-mail message—is also deemed the sender or initiator of the forwarded e-mail message, then the company may be liable for sending a commercial e-mail message that does not include all the disclosures required by CAN–SPAM[167] or for sending a

'physical,' Congress intended to authorize the Commission to require a more substantial presence than a mere Post Office box.'').

[157] Bahr.

[158] True (noting that ''[i]t would be literally impossible for many legitimate mailers to comply with the Act if a PO Box were not acceptable''); AAR; Jaffe; NAA noting that many smaller newspapers are on rural routes, designated as box numbers); NCL (''[T]he only mailing address that some people have is a post office box.'')

[159] MIS; Consumer; Lunde; Jaffe; Oldaker; ESPC; Bahr (noting that ''junk mailers'' are not required by the Postal Service to include a return address on their mail); DSA: Independent; ERA.

[160] SBA.

[161] Comerica. *See also* Visa; DoubleClick; ESPC; SIA; ABA; MasterCard; Ford Motor; Coalition; SIIA.

[162] The final Rule incorporates by reference these definitions in 316.2(m), (f), and (i).

[163] *See, e.g.*, NRF; Visa; M&F PMA; NAA; DoubleClick; MPAA; Coalition; Time Warner. Commenters tended to discuss two categories of e-mail messages: marketing campaigns that provide consideration for forwarding messages and those that do not. Of course, commenters' concerns were solely about *commercial* e-mail messages. One who transmits a non-commercial e-mail message, including a ''transactional or relationship message,'' is not covered by most CAN–SPAM requirements.

[164] *See, e.g.*, Experian; Visa; M&F PMA; Coalition; DMA; MPA; ERA. These commenters reasoned that what begins as a message with a commercial primary purpose takes on a new *personal* primary purpose once the original recipient forwards it to friends and family. As discussed below, this argument is unavailing. Under the Act, the primary purpose of an e-mail message does not change based on the original recipient's reasons for forwarding it. If the original sender has procured the forwarding of its commercial e-mail message by intentionally paying, providing other consideration to, or inducing the original recipient to forward it, then the message retains its commercial primary purpose. If the original sender does not procure the forwarding of its message, then that entity is no longer the ''sender'' of that message if the original recipient forwards it to other people.

[165] These commenters' concerns regarding CAN–SPAM compliance and control over an e-mail message are not implicated in situations in which the seller/advertiser, rather than the original recipient, actually originates or transmits the message, such as when the recipient submits to the seller/advertiser a list of friends and family to receive commercial messages.

[166] *See, e.g.*, Experian; PMA; ERA.

[167] ''It is unlawful for any person to *initiate* the transmission of any commercial electronic mail message to a protected computer unless the message provides (i) clear and conspicuous identification that the message is an advertisement or solicitation; (ii) clear and conspicuous notice of the opportunity under paragraph (3) to decline to receive further commercial electronic mail messages from the sender; and (iii) a valid physical postal address of the sender.'' 15 U.S.C. 7704(a)(5) (emphasis

message to a person who had already sent the company an opt-out request.[168]

In contrast, a few consumers, consumer groups, and others opined that forward-to-a-friend campaigns should comply with the Act regardless of whether consideration is offered or provided for forwarding an e-mail message.[169] NCL expressed concern that these campaigns may violate the privacy rights of consumers because e-mail may be sent to consumers who have opted out of receiving e-mail from the seller. Go Daddy expressed the opinion that such campaigns should contain an opt-out mechanism that applies to the advertiser.

The analytical starting point for determining the applicability of the Act to forward-to-a-friend scenarios is the Act's definitions. CAN–SPAM's definition of '' 'sender,' when used with respect to a commercial electronic mail message, means a person who *initiates* such a message and whose product, service, or Internet web site is advertised or promoted by the message.'' [170] The term ''initiate,'' in turn, means ''to originate or transmit such message or to *procure* the origination or transmission of such message, *but shall not include actions that constitute routine conveyance of such message.*'' [171] Finally, ''procure'' is defined as follows: ''when used with respect to the initiation of a commercial electronic mail message, ['procure'] means *intentionally to pay or provide other consideration to, or induce,* another person to initiate such a message on one's behalf.'' [172] By operation of these definitions, a person who intentionally pays, provides consideration to, or induces another to send on his or her behalf a commercial e-mail message that advertises or promotes his or her product may be considered to have ''procured'' the origination of that message under the Act, and therefore to be an initiator or sender.[173] That person is therefore legally responsible for ensuring that the message includes an opt-out mechanism and the disclosures CAN–SPAM requires,[174] and for ensuring that opt-out requests are honored.[175]

There are two words used in the definition of ''procure'' that need further explication—''consideration'' and ''induce''—because they are not defined within the Act and are key to understanding the scope of the application of the phrase ''intentionally to pay or provide other consideration to, or induce'' to forward-to-a-friend scenarios.

The term ''consideration'' is generally understood to mean ''something of value (such as an act, a forbearance, or a return promise) received by a promisor from a promisee.'' [176] Nothing in CAN–SPAM's legislative history suggests that Congress intended any meaning different from this common legal definition of the term. Thus, where a person forwards, or uses a Web-based mechanism to transmit, a commercial e-mail message to another, the Commission believes the initiation of the message has been ''procured'' if the person receives money, coupons, discounts, awards, additional entries in a sweepstakes, or the like in exchange for doing so. In such cases, the seller/advertiser would be the sender or initiator and would be responsible for ensuring that the message contains the required opt-out mechanism and disclosures, and that opt-out requests are honored.

On the other hand, where there is no payment or consideration from the sender or initiator, the forwarding of the e-mail will not have been ''procured'' unless the recipient has been ''induced'' to forward the message. To *induce* means ''to lead on to; to influence; to prevail on; to move by persuasion or influence.'' [177] ''To induce'' is much broader than ''to pay consideration'' because it does not require a transfer of something of value. Nevertheless, the modifier ''intentionally'' limits the verb ''induce,'' and the Commission believes that Congress used this language to convey that to ''procure,'' one must do something that is designed to encourage or prompt the initiation of a commercial e-mail.[178] Thus, the Commission believes that in order to ''intentionally induce'' the initiation of a commercial e-mail, the sender must affirmatively act or make an explicit statement that is designed to urge another to forward the message.[179]

The Commission believes that making available the means for forwarding a commercial e-mail message, such as using a Web-based ''click-here-to-forward'' mechanism, would not likely rise to the level of ''inducing'' the sending of the e-mail.[180] The Commission believes that this conduct falls within the ambit of ''routine conveyance,'' defined as ''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.*'' [181] The Act specifies that ''actions that constitute routine conveyance'' do not constitute initiation of a commercial e-mail message.[182]

When a company makes available the means for persons to forward a commercial e-mail message—such as using a Web-based ''click-here-to-forward'' mechanism—the company obviously hopes that its products or services will be advertised by interested viewers.[183] Nevertheless, the Act's legislative history regarding the definition of ''initiate'' explains that a company is engaged in ''routine

supplied). A recipient who forwards a sender's non-compliant commercial e-mail message to one or more people could also face liability as an initiator under CAN–SPAM. 15 U.S.C. 7702(9).

[168] ''It is unlawful for any person to *initiate* the transmission to a protected computer of a commercial electronic mail message that does not contain a functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that (i) a recipient may use to submit, in a manner specified in the message, a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from that sender at the electronic mail address where the message was received. * * *'' 15 U.S.C. 7704(a)(3)(A) (emphasis supplied). A recipient who forwards a sender's non-compliant commercial e-mail message to one or more people could also face liability as an initiator under CAN–SPAM. 15 U.S.C. 7702(9).

[169] K. Krueger; NCL; Go Daddy.

[170] 15 U.S.C. 7702(16)(A) (emphasis supplied).

[171] 15 U.S.C. 7702(9) (emphasis supplied). ''Routine conveyance'' is defined as ''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.*'' 15 U.S.C. 7702(15) (emphasis supplied).

[172] 15 U.S.C. 7702(12) (emphasis supplied).

[173] This, of course, assumes that the activity in question is not routine conveyance. Activity which constitutes routine conveyance is not considered initiating or sending a commercial e-mail. 15 U.S.C. 7702(9) and (15).

[174] *See* notes 167 & 168.

[175] 15 U.S.C. 7704(a)(4).

[176] Black's Law Dictionary 300 (7th ed. 1999).

[177] *Webster's New International Dictionary* 1269 (2nd ed. unabridged 1938).

[178] For example, an e-mail message likely satisfies the Act's definition of ''procure'' when it includes text such as ''Tell-A-Friend—Help spread the word by forwarding this message to friends! To share this message with a friend or colleague, click the 'Forward E-mail' button.''

[179] In most cases, the Commission is not required to prove intent when it alleges a law violation. *See* note 45 above (Commission not required to prove sender's intent); 70 FR at 3118. However, in this case, Congress has specifically included intent as part of the definition of ''procure.''

[180] For example, online retailers may include in their e-mails or on their Web sites a link that simply states ''E-mail to a friend.'' Retailers give consumers who click on such links the opportunity to forward a Web address or content on a Web site via e-mail. The Commission does not believe that these features satisfy the definition of ''induce'' because there is only *de minimis*, if any, persuasion or influence exerted through such a statement.

[181] 15 U.S.C. 7702(15) (emphasis supplied).

[182] 15 U.S.C. 7702(9).

[183] *See, e.g.*, Jaffe (''All companies rely heavily on their happy customers to spread the word of their products or services.''); Register (''There is nothing untoward in a company asking its customers to recommend its goods and services.'').

conveyance'' rather than ''initiating'' a commercial e-mail message when it ''simply plays a technical role in transmitting or routing a message and is not involved in coordinating the recipient addresses for the marketing appeal.'' [184] Based on this legislative history, it seems clear that a seller that simply offers a mechanism on a Web site for forwarding advertising engages in ''routine conveyance'' when someone other than the seller identifies the recipients or provides their addresses. It seems equally clear, however, that a seller who offers payment or other consideration to Web site visitors to use a forwarding mechanism encourages visitors to send commercial e-mail to recipients who otherwise would not receive the e-mail. In such cases, the Commission believes that the seller is ''involved in coordinating the recipient addresses for the marketing appeal.'' Such a seller would not be entitled to avail itself of the ''routine conveyance'' exception to ''initiate.'' Questions concerning the Commission's interpretation of ''routine conveyance'' are included in Part VII of this Notice.

B. Section 316.4—Prohibition Against Failure To Effectuate An Opt-Out Request Within Three Business Days of Receipt

Section 7704(a)(4) of the Act prohibits senders, or persons acting on their behalf, from initiating the transmission of a commercial e-mail message to a recipient more than ten business days after senders have received a recipient's opt-out request.[185] Section 7704(c)(1) of the Act empowers the Commission to modify the ten-business-day opt-out period if it ''determines that a different time frame would be more appropriate after taking into account the purposes of section 7704(a); the interests of recipients of commercial electronic mail; and the burdens imposed on senders of lawful commercial electronic mail.'' [186] Accordingly, the ANPR asked whether ten business days is a reasonable time period for effectuating opt-out requests, or whether the Commission should shorten or lengthen the time frame.

As discussed in greater detail below, 316.4(a) of the proposed Rule tracks section 7704(a)(4) verbatim, with the exception of shortening the time period for implementation to three business days instead of ten. This proposed modification will provide enhanced protection for e-mail recipients' privacy, a key goal of section 7704(a) of the Act, and is supported by the record that current technology allows for processing such opt-out requests more expeditiously than the current ten-business-day time frame.

Section 316.4(b) of the proposed Rule provides that, when enforcing compliance with proposed 316.4(a) through an order to cease and desist or an injunction, the Commission, the Federal Communications Commission, and the attorney general, official, or agency of a State will not be required to allege or prove a defendant's state of mind as required by subsections (a)(2)–(4). Proposed 316.4(b) tracks sections 7706(e) and (f)(2) of the Act, which provide that law enforcement officials need not allege or prove a defendant's state of mind to obtain a cease and desist order or an injunction to enforce compliance with any CAN–SPAM provision that includes a state-of-mind component. The Commission proposes 316.4(b) pursuant to its rulemaking authority under section 7711(a) to ''issue regulations to implement the provisions of [the] Act.'' [187] Proposed 316.4(b) satisfies this rulemaking standard because it will ensure that the Act's regulation of CAN–SPAM enforcement applies equally to enforcement of the Rule and the Act: Whenever a provision of the Act or the Commission's proposed Rule contains a state-of-mind component, that component is waived when a law enforcement official seeks a cease and desist order or an injunction.[188]

Below, the Commission reviews comments on the proper time limit to process opt-out requests and whether recipients' opt-out requests should expire, and explains its proposed requirement that opt-out requests be processed within three business days.

1. Commenters' Proposals Regarding the Appropriate Deadline for Effectuating an Opt-Out Request

Commenters were divided on this issue, with the majority of industry members, including small businesses, recommending that it be kept at ten business days or lengthened, and the majority of individual consumers favoring shortening the period.[189]

a. Comments Suggesting That a Ten-Business-Day Deadline for Effectuating an Opt-Out Request Is Appropriate

Nearly half of consumers who commented, and some e-mail senders who commented, indicated that ten business days is an appropriate time period for processing opt-out requests,[190] opining that this time period provides sufficient time for companies who must synchronize multiple e-mail databases, forward opt-out requests to third parties, or manually process opt-out requests.[191] Other commenters indicated that currently they are able to process opt-out requests in far fewer than ten days, but still support the ten-business-day opt-out period to provide flexibility to accommodate the various ways companies effectuate opt-out requests.[192]

b. Comments Suggesting That Ten Business Days Is Not Enough Time To Effectuate an Opt-Out Request

A substantial number of commenters proposed lengthening the deadline for effectuating an opt-out request, citing complex business arrangements, the use of third-party marketers, and the maintenance of multiple e-mail databases as reasons for doing so.[193] While the time periods proposed by commenters varied, the most common suggestion was thirty-one days.[194] Smaller numbers of commenters suggested extending the opt-out period to fifteen, twenty, or thirty days.[195] Visa suggested that rather than a ''bright-line standard'' for the opt-out time period, the Commission should provide senders with ''flexibility that is consistent with their business operations and [opt-out] processing schedules.'' [196]

The ANPR posed questions about the technical procedures, and the relevant time and costs, associated with processing opt-out requests. The vast majority of commenters who responded

[184] S. Rep. 108–102, at 15.

[185] 15 U.S.C. 7704(a)(4).

[186] 15 U.S.C. 7704(c)(1).

[187] 15 U.S.C. 7711(a).

[188] Pursuant to the Act, this waiver is not available to a provider of Internet access service bringing a civil action pursuant to section 7706(g). 15 U.S.C. 7706(g).

[189] Additionally, of the 3,818 responders to the web-based questionnaire, nearly half (1,700 responders) felt that ten business days was an appropriate time period for processing opt-out requests. Thirty-eight percent (1,449 responders), however, supported shortening this time frame. Only sixteen percent (623 responders) felt that the time period should be extended.

[190] DoubleClick; ClickZ; SVM; NCL.

[191] NetCoalition; MPAA; DoubleClick.

[192] NFCU; NetCoalition; ValueClick.

[193] *See, e.g.*, DMA; ESPC.

[194] *See, e.g.*, ABM; Chamber; Wells Fargo; DMA; Piper CBA; MPA; Bankers. Several commenters argued that thirty-one days is an appropriate time period because it conforms to the recently amended Telemarketing Sales Rule, which requires telemarketers to scrub their telemarketing lists against the National Do-Not-Call Registry every thirty-one days. 69 FR 16368 (March 29, 2004).

[195] *See, e.g.*, Time Warner (recommending fifteen days); BMO (recommending twenty days); NNA (recommending thirty days); ESPC (recommending thirty days).

[196] Visa (noting that in the Gramm-Leach-Bliley Act rulemaking, the Commission ultimately determined that it is appropriate for consumers' opt-out requests to be honored ''as soon as reasonably practicable'').

to these questions, however, provided only the most conclusory information. For example, commenters who asserted that complex business arrangements or the use of third-party marketers impede many senders from effectuating opt-out requests within ten business days omitted details about how or why these complex arrangements affect the time and procedures involved in processing opt-out requests.[197] Nor did they specifically explain the role of third parties as they relate to maintaining and processing suppression lists. Similarly, several commenters who referred to the use of third-party e-mailers as a reason for extending the opt-out period did not specify how long it takes to transfer opt-out requests to these third parties, or the specific technical procedures involved in such a transfer.[198]

Several commenters indicated that the average time to effectuate an opt-out request ''varies'' or that it depends on the size and structure of the sender's business, but did not provide any specific data reflecting the minimum or maximum amount of time it can take to effectuate an opt-out request.[199] Some commenters complained that the Act's ten-business-day time frame has proven burdensome for small businesses with limited staff and resources, or those who lack an Information Technology department, yet these commenters provided no specific data justifying a longer period.[200]

The Commission received very few comments that addressed how long it takes for each step of the opt-out process.[201] Some commenters indicated that many opt-out requests are effectuated almost entirely electronically; other commenters indicated that senders often must process opt-out requests manually, and argued that such manual processing warranted extending the opt-out period.[202] These commenters did not fully explain the circumstances that would require opt-outs to be processed by hand, or precisely what such manual processing entails. As a result, the record lacks anything beyond mere assertions that complex business processes, limited resources, and manual processing may prevent senders from honoring opt-out requests within ten business days. Thus, there is insufficient basis for extending the opt-out period.

Another basis advanced to justify a longer time frame in which to process opt-out requests was the argument that additional time was necessary to enable senders to process requests that are submitted via regular mail or using a method that does not conform to the manner specified in the e-mail message.[203] The Commission notes that section 7704(a)(3)(A)(i) of the Act requires that a commercial e-mail message contain a functioning return e-mail address or *other Internet-based mechanism* that the recipient may use to submit an opt-out request, but does not require requests submitted in other ways be honored within the given time period.[204]

Another concern cited by commenters in support of a longer time period was that unavoidable technical errors occurring during the ten-business-day window could prolong the opt-out process.[205] While this may be a valid concern, the Act already contemplates such unavoidable technical anomalies. Specifically, section 7704(a)(3)(c) of the Act states that an electronic return address or other mechanism used for processing opt-out requests does not fail to satisfy the opt-out requirement if it ''is unexpectedly and temporarily unable to receive messages or process requests due to a technical problem beyond the control of the sender if the problem is corrected within a reasonable time period.''[206] The Commission, accordingly, believes it unnecessary to extend the opt-out period to account for technical errors.

Finally, some commenters expressed concern that if the Commission adopts an interpretation that a commercial mail message can have more than one sender, ten business days is not a sufficient time to process opt-out requests.[207] These commenters argued that under a ''multiple-sender'' scenario, opt-out requests would need to be communicated to each sender of any given commercial message, a process which could take longer than ten business days to complete. As noted above, the proposed modification of the ''sender'' definition would allow multiple advertisers in a single commercial e-mail message to establish a single ''sender'' for purposes of CAN–SPAM compliance. Therefore, the Commission is not inclined to extend the length of time a sender has to honor opt-out requests to address this concern.

c. Comments Suggesting That the Deadline for Effectuating an Opt-Out Request Should Be Less Than Ten Business Days

Several commenters urged the Commission to set a deadline of less than ten business days to effectuate an opt-out request, because doing so would better protect the privacy interests of e-mail recipients and because the Act's ten-business-day time frame is unnecessarily generous, given the advanced state of technology used to process opt-out requests. Specifically, some commenters expressed concerns that under the current ten-business-day time frame, senders would legally be allowed to ''mail-bomb'' recipients for ten business days during the opt-out period.[208] As one commenter put it, ''Ten days still gives a commercial spammer a LOT of time to send junk.''[209] These concerns were not supported by factual evidence that such practices actually occur, or that these practices would be eliminated by a shorter processing period. The Commission is including questions in Part VII to learn more about the volume of e-mail received from a particular sender after a recipient has submitted an opt-out request to that sender.

Several commenters stated that many senders already have the ability to process opt-out requests in far fewer than ten business days, and that many do so immediately upon receipt of such a request.[210] Go Daddy, a domain name registrar, indicated that it currently honors opt-out requests within seconds, and accordingly, recommended that the Commission shorten the opt-out period.[211] This view was supported by several other commenters who noted that opt-out requests received via an opt-out hyperlink can be added to a suppression list immediately.[212] Still other commenters pointed to currently available mailing list software which will process opt-out requests almost immediately, with delays of only

[197] *See, e.g.*, NNA; ABM.

[198] *See, e.g.*, Visa; ICC; ERA; ABM. *But see* RDS (suggesting that where third parties are used, three to five days is an appropriate time period for processing opt-out requests); Go Daddy (recommending that five days is an appropriate time frame to allow for companies that utilize third parties).

[199] Experian. Generally, commenters indicated that currently there is no industry standard for effectuating opt-out requests. *See, e.g.*, Go Daddy; ACLI.

[200] *See., e.g.*, NNA; BMO.

[201] *See* MBNA.

[202] *See, e.g.*, MPAA; IPPC; KeyCorp; MBA; BMO (suggesting that employees who send out individual commercial e-mail messages often need to collect and circulate opt-out requests manually).

[203] *See, e.g.*, ESPC; BMO; IPPC; KeyCorp; MBNA.

[204] 15 U.S.C. 7704(a)(4)(A).

[205] *See, e.g.*, AeA.

[206] 15 U.S.C. 7704(a)(3)(C).

[207] *See, e.g.*, NetCoalition; Bankers; Chamber.

[208] *See, e.g.*, Giambra; Go Daddy.

[209] Vandenberg (emphasis in original).

[210] *See, e.g.*, RDS; NFCU; NetCoalition; ValueClick.

[211] Go Daddy (''There are very little costs associated with deleting a person's e-mail address from a database, since mailing lists are almost always electronically automated.'').

[212] *See, e.g.*, MBNA.

minutes, or even seconds.[213] Additionally, the Commission is aware of companies that have designed, or are developing, products geared specifically towards complying with this aspect of the CAN–SPAM Act, and which claim to be able to provide fully automated opt-out processing within minutes. Given that such products are in development, it seems likely that the market will yield additional competing technologies in the near future.

2. Commission Proposal Regarding the Appropriate Deadline for Effectuating an Opt-Out Request

Having considered the comments, the Commission believes that while the record does not demonstrate whether fears of ''mail-bombing'' during an opt-out period are well-founded, the fact that many commenters already are able to process opt-out requests virtually instantaneously supports the conclusion that the opt-out period can and should be shortened. The purpose of the opt-out provision in the Can–SPAM Act is to protect recipients from unwanted commercial e-mail. Given that the record suggests that nearly instantaneous processing of a recipient's request not to receive future e-mail messages can be accomplished without an undue burden,[214] the Commission believes that shortening the opt-out period to three business days is appropriate. This furthers the key policy objective underlying Can–SPAM to afford e-mail recipients maximal privacy consistent with reasonable compliance costs. The three-business-day window allows for adequate time for processing, even by those entities whose business practices or technology may not allow for instant removal of e-mail addresses submitted in opt-out requests. This proposed provision will also ensure that law enforcement officials need not allege or prove a defendant's state of mind when seeking a cease and desist order or injunctive relief to enforce compliance with 316.4(a).

3. Commenters' Suggestions Regarding Expiration of Opt-Out Requests

Several commenters noted that the Act does not indicate how long a recipient's opt-out request should remain in effect. Therefore, several commenters were concerned that senders would be required to maintain opt-out lists indefinitely.[215] Commenters argued that without limiting the duration of opt-out requests, suppression lists could grow without limit. Several commenters noted that individuals frequently change their e-mail addresses, or that e-mail addresses often become inactive from non-use, and argued that without putting a cap on the duration of opt-out lists, senders would be required to maintain lists with a potentially large percentage of inaccurate, out-of-date, or inactive e-mail addresses.[216] Therefore, commenters urged the Commission to limit how long opt-out requests remain in effect, and suggested a limit of two to three years.[217]

The Commission has carefully considered these comments, and notes that in the somewhat similar context of the National Do Not Call Registry, the duration of a person's registration is five years, or until the registrant changes his or her telephone number, or determines to take the number off the Registry.[218] In addition, other means exist to minimize the outmoded entries in the Registry—specifically, the existence of relevant databases makes it possible for the Registry's administrator periodically to purge defunct or changed telephone numbers from the Registry. In this way, the process of ''scrubbing'' a call list is limited so that it is no more expensive or time-consuming for industry than is necessary. The Commission is not aware of any similar databases that are available for e-mail marketers to purge defunct e-mail addresses from their distributions lists. On the other hand, the fact that an e-mail marketer's suppression list is likely to have far fewer entries than the 91 million numbers on the National Do Not Call Registry makes the prospect of ''scrubbing'' far less daunting, and tends to vitiate the argument for an expiration of opt-out requests after a certain period of time. Finally, Congress chose neither to impose such a time limit nor to specifically authorize the Commission to do so at this time. In view of all these considerations, the Commission has determined not to propose such a time limit. Nevertheless, the Commission is receptive to submissions of information or data that would show that a provision placing a limit on the duration of an opt-out request would be useful in implementing the provisions of the Act under section 7711(a).

C. Section 316.5—Prohibition on Charging a Fee or Imposing Other Requirements on Recipients Who Wish To Opt Out

Proposed 316.5 broadly prohibits the imposition of any fee, any requirement to provide personally identifying information (beyond one's e-mail address), or any other obligation as a condition for accepting or honoring a recipient's opt-out request. This issue was not addressed in the ANPR, but the Commission now believes it necessary, based on its observation that some senders of commercial e-mail may be encumbering recipients' Can–SPAM opt-out rights with such requirements. The Commission believes that such requirements are entirely inconsistent with the explicit Congressional policy and purposes embodied in the Act.

Section 7704(a)(3)(A) of the Act prohibits any person from initiating ''a commercial electronic mail message that does not contain a functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that a recipient may use to submit * * * a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from [the] sender * * *[219] Section 7704(a)(3)(B) of the Act allows those who initiate commercial e-mail messages to comply with section 7704(a)(3)(A) ''by providing the recipient a list or menu from which the recipient may choose the specific types of commercial electronic mail messages the recipient wants to receive or does not want to receive from the sender, if the list or menu includes an option under which the recipient may choose not to receive any commercial electronic mail messages from the sender.''[220] Section 7704(a)(4), among other things, directs senders, and those acting on a sender's behalf, to honor recipients' opt-out preferences within ten business days of receipt of those preferences.[221]

Can–SPAM requires clear and conspicuous display of the mandatory opt-out mechanism, but imposes no further explicit requirements regarding the manner in which initiators of commercial e-mail comply with these provisions. Nevertheless, the whole thrust of the Act is to ensure recipients can opt out of receiving subsequent

[213] Satchell; K. Kreuger.

[214] *See, e.g.*, Go Daddy.

[215] *See, e.g.*, Wells Fargo; Experian; Coalition.

[216] Piper.

[217] CBA; DMA.

[218] 68 FR 4640 (Jan. 29, 2003).

[219] 15 U.S.C. 7704(a)(3)(A).

[220] 15 U.S.C. 7704(a)(3)(B).

[221] *See* 15 U.S.C. 7704(a)(4)(A). As was explained above, the Commission is proposing to shorten the amount of time senders, and those acting on the sender's behalf, have to honor recipients' opt-out request to three business days. *See* proposed 16 CFR 316.4.

commercial messages from any sender. Indeed, the sole purpose of the Act's opt-out provisions is to protect recipients' privacy from senders of unwanted commercial e-mail; it would be a complete subversion of this privacy protection to allow senders to compel recipients to disclose personally identifying information as the price of opting out. Accordingly, the Commission believes that an e-mail recipient's ability to submit an opt-out request should not be encumbered by any extraneous requirements.

Proposed 316.5 provides: ''Neither a sender nor any person acting on behalf of a sender may require that any recipient pay any fee, provide any information other than the recipient's electronic mail address and opt-out preferences, or take any other steps except sending a reply electronic mail message or visiting a single Internet web page, in order to: (a) Use a return electronic mail address or other Internet-based mechanism, required by 15 U.S.C. 7704(a)(3), to submit a request not to receive future commercial electronic mail messages from a sender; or (b) have such a request honored as required by 15 U.S.C. 7704(a)(3)(B) and (a)(4).''

The Commission intends that this proposed provision apply to all parties involved in processing recipients' opt-out requests: senders of commercial e-mail, those who initiate commercial e-mail, and any third parties that provide assistance to senders in receiving and honoring recipients' opt-out requests. As was explained above, this proposal prohibits these parties from charging a fee to submit an opt-out request, from collecting any information about a recipient other than his or her e-mail address and opt-out preferences,[222] and from requiring recipients to visit more than one Web page to submit an opt-out request.

CAN–SPAM's legislative history supports this proposed regulation. Congressman W. J. (Billy) Tauzin stated that ''We intend that senders of commercial e-mail provide a convenient, clear and simple way for consumers to opt-out of commercial e-mail.'' [223] The Commission's proposal furthers this intent. An opt-out mechanism that requires a fee, unnecessary disclosure of personal information, or access to multiple Web pages would be inconsistent with the demand for a ''convenient, clear and simple'' opt-out mechanism.[224] This proposal also responds to the concerns of the commenter who argued against burdensome opt-out procedures.[225]

As noted above, the Commission is aware that some e-mail marketers are attempting to use the CAN–SPAM opt-out mechanism as an opportunity to collect information about recipients or to subject them to sales pitches before an opt-out request is completed. Conceivably, some e-mail marketers could even attempt to charge recipients a fee for accepting or honoring their opt-out requests. All of these encumbrances are unacceptable, and, pursuant to section 7711 of the Act, which authorizes the Commission to ''issue regulations to implement the provisions of [the] Act,'' [226] the Commission proposes a rule provision that would prohibit these encumbrances.

The prohibitions proposed in this rule provision are not intended to impose any new burden on e-mail marketers beyond those already imposed by CAN–SPAM. Nothing on the record suggests a need or justification for e-mail senders to charge recipients a fee to process opt-out requests. Moreover, there appears to be no reason why an e-mail sender would need to collect any information about a recipient other than his or her e-mail address and opt-out preferences in order to process that opt-out request because, according to CAN–SPAM, opt-out requests are specific to a recipient's *e-mail address*, not his or her name. Finally, the Commission believes that e-mail senders should be able to get all the opt-out information they need from a recipient—namely, the recipient's e-mail address and opt-out preferences—in a single Web page. Requiring a recipient to visit multiple Web pages would frustrate recipients' ability to exercise their opt-out rights under CAN–SPAM, and that is clearly contrary to congressional intent. In Part VII below, the Commission asks questions requesting information regarding this proposed rule provision.

D. Section 7704(c)(2)—Aggravated Violations Relating to Commercial E-mail

Committing an aggravated violation along with a violation of section 7704(a) could subject a defendant to triple damages in a CAN–SPAM enforcement action by a state or an ISP.[227] Section 7704(b) of the Act lists four practices which are to be considered ''aggravated violations.'' [228] According to a Senate Committee Report on an earlier version of the Act, designating specific practices as ''aggravated'' violations is intended to ''apply to those who violate the provisions of the bill while employing certain problematic techniques used to either generate recipient e-mail addresses, or remove or mask the true identity of the sender.'' [229]

Section 7704(c)(2) of the Act authorizes the Commission to specify activities or practices—in addition to the four already enumerated in the statute—as aggravated violations if the Commission determines that ''those activities or practices are *contributing substantially to the proliferation of commercial electronic mail messages* that are unlawful under section 7704(a) of the Act.'' (Emphasis supplied.) Some commenters suggested additional practices that warrant designation as ''aggravated violations.'' After reviewing the comments, the Commission is not inclined to expand the list of aggravated violations because the practices cited by commenters are either already prohibited by the Act, or implicate persons other than those who violate section 7704(a) of the Act and who are therefore beyond the reach of section 7704(c)(2). These proposals are discussed immediately below. Two proposals addressed individually below, regarding manual e-mail address harvesting and exchange of open proxy lists, are not illegal. Nevertheless, the Commission is not inclined to create new aggravated violations regarding these practices.

1. Commenters' Proposals Regarding Aggravated Violations

Numerous commenters recommended that the Commission designate as aggravated violations practices that already are prohibited by other provisions of the CAN–SPAM Act,

[222] The concept of opt-out preferences is introduced in section 7704(a)(3)(B). Pursuant to that provision, people who initiate commercial e-mail messages may ask recipients to specify which types of commercial e-mail they do and do not want from a sender.

[223] Hon. W. J. (Billy) Tauzin, Cong. Rec. E74 (Jan. 28, 2004) (Extension of remarks).

[224] The findings Congress incorporated in the Act reflect concern about the costs that spam imposes on unwilling recipients: ''The receipt of unsolicited commercial electronic mail may result in costs to recipients who cannot refuse to accept such mail and who *incur costs* for the storage of such mail, or for the time spent accessing, reviewing, and discarding such mail, or for both.'' 15 U.S.C. 7701(a)(3) (emphasis supplied). This concern supports the Commission's proposal to prohibit charging or otherwise encumbering the opt-out rights that the Act creates.

[225] *See* O'Connor.

[226] 15 U.S.C. 7711.

[227] 15 U.S.C. 7706(f)(3)(C), (g)(3)(C).

[228] The four practices are: (1) automated e-mail address harvesting; (2) dictionary attacks; (3) automated creation of multiple e-mail accounts; and (4) relay or retransmission of a commercial e-mail message through unauthorized access.

[229] S. Rep. No. 108–102, at 6.

including ''spoofing,''[230] obscuring the origin of an e-mail message, falsifying header information, using non-functional opt-out addresses, and transferring e-mail addresses of persons who have opted-out.[231] Because all of these practices are already prohibited by the Act,[232] designating them as aggravated violations is unnecessary and would neither give greater protection to consumers nor provide a significant new tool to law enforcement. Some commenters urged the Commission to prohibit inaccurate ''Whois'' information.[233] For example, Microsoft, among others, urged that registering a domain name with false or misleading information be added as an aggravated violation.[234] The Commission believes this is already prohibited by the Act. *See* 15 U.S.C. 7704(a)(1)(A) (prohibiting initiation of any e-mail message that includes an originating e-mail address or a domain name that ''was obtained by means of false or fraudulent pretenses or representations'').[235]

A number of commenters suggested that the Commission consider including as an aggravated violation intentionally crafting the content of e-mail messages specifically to evade spam filters.[236] Some commenters mentioned in particular the technique of ''hashbusting,'' where random characters or words are intentionally inserted into the body and/or subject line of the e-mail.[237] Such techniques often go hand-in-hand with other stratagems for hiding the true identity of the sender.[238]

The Commission's view is that hashbusting in the subject line would likely be covered under section 7704(a)(2) of the Act, which prohibits the initiation of any commercial e-mail message where the initiator of that message ''has actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that a subject heading of the message would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message.'' Hashbusting is prohibited under this section because using random characters and meaningless words in a message's subject line can prevent recipients from determining a message's purpose.

The Commission shares the concerns of commenters about hashbusting and like techniques in the body of commercial e-mail messages, the apparent purpose of which is to mislead recipients and frustrate their efforts to filter out unwanted messages. Nevertheless, adding as an aggravated violation the crafting of the content of commercial e-mail messages to evade spam filters appears to be unworkable. Drawing a bright line to distinguish permissible content from content that would violate the Act is fraught with practical difficulties and potentially presents difficult First Amendment issues. Nevertheless, the Commission includes questions in Part VII of this NPRM to solicit further data regarding the prevalence of inserting obfuscating content into commercial e-mail solely to evade spam filters, and to seek views as to whether, as a practical matter, a bright-line guide could be drawn.

A number of commenters complained about various practices that cause annoyance for them in using their computers and requested that such practices be included as aggravated violations. The practices commenters mentioned most often were distributing viruses,[239] hijacking browsers (in other words, manipulating a computer user's ability to navigate the Internet), and using pop-up advertisements.[240] Section 7704(a)(1)(C) already prohibits knowingly using a protected computer to relay or retransmit a commercial or ''transactional or relationship'' message for purposes of disguising the message's origin.[241] Thus, using a computer virus to route messages through someone else's computer is unlawful when doing so disguises a message's origin. Also, CAN–SPAM only reaches e-mail messages that satisfy the Act's definitions of ''commercial electronic mail message'' or ''transactional or relationship message.'' At this time, it is not clear that a message that does no more than distribute a computer virus would satisfy either of these definitions and thus be regulated by CAN–SPAM. Pop-ups and Web browser highjacking are doubtless annoying to consumers, but, based on the record compiled thus

[230] ''Spoofing'' is defined as disguising an e-mail to make it appear to come from an address from which it actually did not originate, such as placing another user's address in the ''from'' or ''reply-to'' lines. *See FTC* v. *GM Funding, Inc.,* SACV 02–1026 (C.D. Cal. filed Nov. 6, 2002).

[231] Richardson (obscuring origin of e-mail); Csorba (forged headers; invalid opt-out); Calvert (non-functional opt-out); Freese (non-functioning opt-out); Safell (spoofing); Innovation (false identification of sender); NetCoalition (deceptive header information); KALRES (mailing after opt-out request); EDC (automated harvesting); Moerlien; St. Saveur; O'Connor; Rospenda; ClickZ; Jensen; Mead; B. Krueger; Discover (transferring e-mail addresses).

[232] *See* section 7704(a)(1)(C) (prohibiting header information that ''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''); section 7704(a)(3) (prohibiting initiation of an e-mail message that does not include a functioning opt-out mechanism); and section 7704(a)(4)(A)(iv) (prohibiting the sale, lease, exchange, transfer, or release of the e-mail address of any person who has opted-out).

[233] ''Whois'' is an Internet program that allows users to query a database of people and other Internet entities, such as domains, networks, and hosts. ''Whois'' databases are maintained generally by the registrars. ''Whois'' data includes the registrant's company name, address, phone number, and e-mail address.

[234] Microsoft; St. Sauveur. *See also* Truth (suggesting ways that accurate Whois information can be used to prevent fraudulent credit card transactions). The Commission has provided testimony to the U.S. House of Representatives Judiciary Committee; Subcommittee on Courts, The Internet, and Intellectual Property regarding the critical importance of accurate Whois information to the integrity of the Internet. *See Accuracy of ''WHOIS'' Internet Database Essential to Law Enforcement, FTC Tells Congress*, May 22, 2002, available at *http://www.ftc.gov/opa/2002/05/whois.htm.*

[235] *See FTC* v. *Global Net Solutions, Inc., et al.*, CV–S–05–0002–PMP (LRL) (D. Nev. filed Jan. 3, 2005) (alleging that, among other things, the defendants violated 15 U.S.C. 7704(a)(1) of CAN–SPAM by initiating commercial e-mail containing an originating e-mail address that was obtained through false representations to the e-mail service provider).

[236] St. Saveur; Danko; ClickZ; Lunde; NetCoalition.

[237] The technique of inserting sometimes strangely eloquent nonsense is favored by spammers as an effective way of defeating spam filters that convert e-mail into ''hashes'' (where characters in words are converted into numbers) (*see, e.g., http://razor.sourceforge.net*) or spam filters that use Bayesian statistical analysis (*see, e.g., http://spamassassin.org*). Computer programs, also known as ''Chomskybots,'' can automatically generate such paragraphs.

[238] *See National Do Not E-mail Registry, A Report To Congress,* FTC, June 2004, at 8 (spammers use many techniques to hide including: spoofing, open relays, open proxies, and zombie drones). Available at *http://www.ftc.gov/reports/dneregistry/report.pdf.*

[239] A ''virus'' is a program or piece of code that is loaded onto one's computer without one's knowledge and runs against one's wishes. Computer viruses can replicate themselves and will quickly use all available computer memory. Some viruses are capable of transmitting themselves across networks and bypassing security systems. *See, e.g., http://www.webopedia.com/TERM/V/virus.html.* Computer viruses comprise a class of ''malicious code'' that can include Trojan horses and worms. A ''Trojan horse'' is a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer. *See, e.g., http://www.webopedia.com/TERM/w/worm.html.* A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs. *See, e.g., http://www.webopedia.com/TERM/T/Trojan_horse.html.*

[240] Richardson; St. Saveur; Keef; ClickZ; Rospenda; Keogh; K. Krueger; Vowles; Maat; B. Krueger.

[241] 15 U.S.C. 7704(a)(1)(C). Moreover, section 7704(b)(1)(A)(3) provides: ''It is unlawful for any person knowingly to relay or retransmit a commercial electronic mail message that is unlawful under [section 7704(a)] from a protected computer or computer network that such person has accessed without authorization.'' 15 U.S.C. 7704(b(1)(A)(3).

far in this proceeding, these specific practices do not appear to be contributing substantially to the proliferation of commercial e-mail messages that are prohibited under section 7704(a) of the Act. Where appropriate, however, the Commission will challenge these practices under section 5 of the FTC Act.[242]

2. Manual E-mail Address Harvesting

A coalition of four domain name registrars requested that the Commission consider adding as an aggravated violation the manual harvesting of e-mail addresses.[243] The Act itself designates the *automated* harvesting of e-mail addresses as an aggravated violation. The record amassed to date does not document that manual e-mail address harvesting is a practice that meets the standard specified in CAN–SPAM to be designated as an aggravated violation—*i.e,* there is insufficient evidence that it contributes substantially to the proliferation of unlawful commercial e-mail messages. Therefore, the Commission has not adopted this suggestion, but includes questions in Part VII of this NPRM to solicit further data regarding the prevalence of this practice and to determine whether the manual harvesting of e-mail addresses is contributing substantially to the proliferation of commercial e-mail messages that are prohibited under section 7704(a) of the Act.

3. Open Proxy Lists

Open proxy lists, which are readily available for purchase on the Internet,[244] provide the Internet Protocol address and/or the fully qualified domain name of any computer through which e-mail messages can be routed. Microsoft proposed that the Commission consider adding the sale of such lists as an aggravated violation:

Although the CAN–SPAM Act prohibits the practice of relaying spam through open proxies, drones, or other protected computers, it does not prohibit the means by which spammers can obtain information about these computers. A regulation that prohibits the sale [of lists of such devices] would be a natural analog to Section [7704](b)(1)(A), which creates an aggravated violation for persons who ''assist in the transmission'' of spam through the sale or distribution of harvested e-mail addresses.[245]

Although the Commission believes that Microsoft has a good point, and that this practice serves no legitimate purpose and materially advances the proliferation of spam, the Commission so far has no information showing that the sellers of open proxy lists are the same individuals engaged in sending spam, and violating section 7704(a). If they are not, it would be of dubious value to make the sale of open proxy lists an aggravated violation because an aggravated violation only comes into play in situations where a defendant also is violating section 7704(a). Furthermore, the Commission believes that to *use* an open proxy list may already be an aggravated violation under the Act. Section 7704(b)(3) of the Act states, ''It is unlawful for any person knowingly to relay or retransmit a commercial electronic mail message that is unlawful under subsection (a) from a protected computer or computer network that such person has accessed without authorization.'' [246] As stated above, the purpose of an open proxy is to relay e-mail through a third party's server (a proxy server) so that the recipient cannot trace the sender of the e-mail. Such proxies are almost always accessed without the authorization of the proxy's system administrator.[247] Nevertheless, the Commission seeks additional information on the sale of open proxy lists to determine whether such sales ''are contributing substantially to the proliferation of commercial electronic mail messages that are unlawful under [section 7704(a) of the Act].'' [248] Specifically, the Commission seeks comment on whether prohibiting such sales would give a useful new tool to law enforcement to target unlawful commercial e-mail.

III. Invitation To Comment

All persons are hereby given notice of the opportunity to submit written data, views, facts, and arguments addressing the issues raised by this NPRM. All comments should be filed as prescribed in the **ADDRESSES** section above, and must be received by June 27, 2005.

IV. Communications by Outside Parties to Commissioners or Their Advisors

Written communications and summaries or transcripts of oral communications respecting the merits of this proceeding from any outside party to any Commissioner or Commissioner's advisor will be placed on the public record. *See* 16 CFR 1.26(b)(5).

V. Paperwork Reduction Act

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3506) (''PRA''), the Commission has reviewed the proposed Rule. The proposed Rule does not impose any recordkeeping, reporting, or disclosure requirements or otherwise constitute a ''collection of information'' as it is defined in the regulations implementing the PRA. *See* 5 CFR 1320.3(c).

VI. Regulatory Flexibility Act

The Regulatory Flexibility Act (''RFA''), 5 U.S.C. 601–612, requires an agency to provide an Initial Regulatory Flexibility Analysis (''IRFA'') with a proposed rule and a Final Regulatory Flexibility Analysis (''FRFA'') with the final rule, if any, unless the agency certifies that the rule will not have a significant economic impact on a substantial number of small entities. *See* 5 U.S.C. 603–605.

The Commission requested comment in the ANPR regarding whether CAN–SPAM regulations would have a significant economic impact on a substantial number of small entities. Although the Commission received very few responsive comments, the Commission has determined that it is appropriate to publish an IRFA in order to inquire into the impact of the proposed Rule on small entities. Therefore, the Commission has prepared the following analysis.

A. Reasons for the Proposed Rule

The proposed Rule is advanced pursuant to the Commission's mandate under the CAN–SPAM Act, 15 U.S.C. 7701–7713. The Act seeks to ensure that senders of commercial e-mail not mislead recipients as to the source or content of such messages, and to ensure that recipients of commercial e-mail have a right to decline to receive additional commercial e-mail from a particular source. In that regard, section 7702(2)(C) of the Act requires the Commission to issue regulations defining the relevant criteria to facilitate the determination of whether the primary purpose of an electronic mail message is to advertise or promote a product or service, and is therefore

[242] The Commission has alleged, *inter alia,* that in some instances, pop-ups and Web browser hijacking (a/k/a mouse trapping) may interfere with a user's computer. *See, e.g., FTC* v. *D Squared Solutions LLC,* No. 03–CV–3108 (D. Md. 2003) (pop-ups unfairly interfered with computer use); *FTC* v. *Carlos Pereira,* No. 99–1367–A (E.D. Va. 1999) (manipulating normal functioning of Web browser is unfair).

[243] Register.

[244] *See, e.g., http://www.openproxies.com.* Some Web sites offer a small quantity of ''free'' open proxies but those open proxies have limited value to spammers. For example, the cited Web site offers ten free, but slow, open proxies. A slow open proxy has marginal value to someone who wants to send bulk e-mail because slow connections use too many computer resources. To obtain a list of quality fast open proxies, one must pay a monthly fee.

[245] Microsoft.

[246] 15 U.S.C. 7704(b)(3).

[247] *See http://www.lurhq.com/proxies.html* (most proxies are not supposed to be public).

[248] 15 U.S.C. 7704(c)(2).

commercial.[249] The Act also authorizes the Commission, at its discretion and subject to certain conditions, to promulgate regulations expanding or contracting the categories of ''transactional or relationship messages''; [250] modifying the ten-business-day period prescribed in the Act for effectuating a recipient's opt-out request; [251] and specifying additional activities or practices as ''aggravated violations.'' [252] The Act also authorizes the Commission to ''issue regulations to implement the provisions of [the] Act.'' [253]

B. Statement of Objectives and Legal Basis

The objective of the proposed Rule is to implement the CAN–SPAM Act, 15 U.S.C. 7701–7713. The proposed Rule provisions introduced in this NPRM add a definition of the term ''person''; limit the definition of ''sender''; clarify that Post Office boxes and private mailboxes established pursuant to United States Postal Service regulations are ''valid physical postal addresses''; shorten the time a sender has to effectuate a recipient's opt-out request; and clarify that a recipient may not be required to pay a fee, provide information other than his or her e-mail address and opt-out preferences, or take any steps other than sending a reply e-mail message or visiting a single Internet Web page to submit a valid opt-out request. The legal basis for the proposed Rule is the CAN–SPAM Act, 15 U.S.C. 7701–7713.[254]

C. Description of Small Entities To Which the Proposed Rule Will Apply

The proposed Rule, which incorporates by reference many of the definitions of the CAN–SPAM Act, applies to ''senders'' of ''commercial electronic mail messages'' and, to a lesser extent, to ''senders'' of ''transactional or relationship messages.'' [255] Under the Act, and the proposed Rule, a ''sender'' is ''a person who initiates [a commercial electronic mail message] and whose product, service, or Internet Web site is advertised or promoted by the message.'' [256] To ''initiate'' a message, one must ''originate or transmit such message or * * * procure the origination or transmission of such message.'' [257] The Act does not consider ''routine conveyance'' (defined as ''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'') to be initiation.[258]

Any company, regardless of industry or size, that sends commercial e-mail messages or transactional or relationship messages would be subject to the proposed Rule. This would include entities that use e-mail to advertise or promote their goods, services, or Web sites, as well as entities that originate or transmit such messages. Therefore, numerous small entities across almost every industry could be subject to the proposed Rule. For the majority of entities subject to the proposed Rule, a small business is defined by the Small Business Administration as one whose average annual receipts do not exceed $6 million or who has fewer than 500 employees.[259]

Although it is impossible to identify every industry that sends commercial e-mail messages or transactional or relationship messages, some surveys suggest that an ever-increasing number are using the Internet. A recent Harris Interactive poll, for example, found that about seventy percent of small businesses have an online presence, or plan to have one by 2005.[260] A 2001 study by the National Federation of Independent Business found that, at that time, fifty-seven percent of all small employers used the Internet for business-related activities.[261] While these statistics do not quantify the number of small businesses that send commercial e-mail messages or transactional or relationship messages, they suggest that many small businesses are using the Internet in some capacity. The Commission is aware of at least one survey that suggests that eighty-five percent of small businesses surveyed communicate with existing customers via e-mail, and sixty-seven percent of small businesses communicate with potential buyers via e-mail.[262]

Given the paucity of data concerning the number of small businesses that send commercial e-mail messages or transactional or relationship messages, it is not possible to determine precisely how many small businesses would be subject to the proposed Rule. Accordingly, the Commission believes that a precise estimate of the number of small entities subject to the proposed Rule is not currently feasible, and specifically requests information or comment on this issue.

D. Projected Reporting, Recordkeeping, and Other Compliance Requirements

The proposed Rule would not impose any specific reporting, recordkeeping, or disclosure requirements within the meaning of the Paperwork Reduction Act. Because the CAN–SPAM Act establishes a comprehensive regulatory scheme for commercial and transactional or relationship e-mail messages, and because the Act is enforceable by the FTC as though it were an FTC Trade Regulation Rule, the proposed Rule primarily clarifies the scope of certain definitions within the Act. Specifically, the proposed Rule defines one new term, ''person''; limits the definition of ''sender''; and clarifies that Post Office boxes and private mailboxes established pursuant to United States Postal Service regulations are ''valid physical postal addresses.'' The proposed Rule also clarifies that a recipient may not be required to pay a fee, provide information other than his or her e-mail address and opt-out preferences, or take any steps other than sending a reply e-mail message or visiting a single Internet Web page to submit a valid opt-out request. Only one provision of the proposed Rule imposes substantive compliance obligations, and the Commission does not believe that that provision is likely to impose a substantial impact on significant numbers of small entities. The proposed Rule would require senders to honor recipients' opt-out requests within three

[249] On January 19, 2005, the Commission published a Federal Register Notice promulgating Rule provisions addressing the statutory mandate to establish criteria for determining the primary purpose of an e-mail message. *See* 16 CFR 316.3.

[250] 15 U.S.C. 7702(17)(B).

[251] 15 U.S.C. 7704(c)(1)(A)–(C).

[252] 15 U.S.C. 7704(c)(2).

[253] 15 U.S.C. 7711(a).

[254] Specifically, the authority to modify the ten-business-day period prescribed in the Act for honoring a recipient's opt-out request is 15 U.S.C. 7704(c)(1)(A)–(C). The Act also grants the Commission broad authority to ''issue regulations to implement the provisions of [the] Act.'' 15 U.S.C. 7711(a).

[255] One provision, section 7704(a)(1), which prohibits false or misleading transmission information, applies equally to ''commercial electronic mail messages'' and ''transactional or relationship messages''; otherwise, CAN–SPAM's prohibitions and requirements cover only ''commercial electronic mail messages.''

[256] 15 U.S.C. 7702(16)(A); Proposed Rule 316.2(m).

[257] 15 U.S.C. 7702(9).

[258] 15 U.S.C. 7702(9), (15).

[259] These numbers represent the size standards for most retail and service industries ($6 million total receipts) and manufacturing industries (500 employees). A list of the SBA's size standards for all industries can be found at *http://www.sba.gov/size/summary-whatis.html.* SBA's comment estimates that there are 22.9 million small businesses in the U.S.

[260] *See http://www.ecommercetimes.com/story/35004.htm.*

[261] *See http://www.nfib.com/object/2937298.html.*

[262] *See* Electronic Commerce News, Mar. 15, 2004, ''Gearing Up for Next Front in the War on Spam.'' SBA studies similarly show that eighty-three percent of small businesses use e-mail.

business days rather than the ten business days that the Act would otherwise allow.[263] The Commission anticipates that, in some cases, senders of commercial e-mail may need to purchase software, use an appropriate e-mail service provider, or adopt other business practices or policies to ensure that recipients' opt-out requests are honored. As discussed earlier, comments suggest that software for this purpose is commercially available, is widely used already, and can process opt-out requests instantaneously.[264] If so, the proposal to allow three business days rather than ten for processing opt-out requests would not seem to increase or otherwise adversely affect such compliance costs. Moreover, because the Commission believes legitimate senders may be honoring their recipients' opt-out requests within the proposed three-business-day time frame, the Commission questions whether the proposed Rule imposes any compliance costs beyond those already incurred in the ordinary course of business. The Commission seeks comment and information on software, labor, professional, or other relevant compliance cost issues, if any.

E. Identification of Other Duplicative, Overlapping, or Conflicting Federal Rules

The FTC has not identified any other federal statutes, rules, or policies that would conflict with the proposed Rule's provisions, which, as noted above, add a definition of the term ''person''; limit the definition of ''sender''; clarify that Post Office boxes and private mailboxes established pursuant to United States Postal Service regulations are ''valid physical postal addresses''; shorten the time a sender has to honor a recipient's opt-out request; and clarify that a recipient may not be required to pay a fee, provide information other than his or her e-mail address and opt-out preferences, or take any steps other than sending a reply e-mail message or visiting a single Internet Web page to submit a valid opt-out request.

The FTC seeks comment and information about any statutes or rules that may conflict with the proposed requirements, as well as any other state, local, or industry rules or policies that may overlap or conflict with the requirements of the proposed Rule.

F. Discussion of Significant Alternatives

As discussed above, the CAN–SPAM Act primarily seeks to ensure that senders of commercial e-mail not mislead recipients as to the source or content of such messages, and to ensure that recipients of commercial e-mail have a right to decline to receive additional commercial e-mail from a particular source. The Act, not the proposed Rule, imposes these obligations. The Commission nonetheless has considered and is proposing to adopt clarifications of the statutory definitions suggested in comments by the SBA and other entities advocating on behalf of small business interests, particularly the definitions of ''sender'' and ''valid physical postal address.'' Although the definitions do not impose any compliance burden, the proposed clarifications should help avoid legal or other costs that could otherwise result from uncertainty, if any, about what the proposed Rule covers or requires. As already noted, the Commission is inviting comment on these proposed definitions, including any alternatives that might help further explain or articulate their meaning and scope, consistent with the Act's definitions of those terms. In addition, as explained earlier, the Commission has also considered alternatives to the compliance requirements for receiving and honoring recipients' opt-out requests in deciding to propose: (1) A three-business-day period for honoring opt-out requests rather than the maximum ten-business-day period otherwise allowed under the Act; and (2) a prohibition on e-mail senders' ability to collect a fee, require submission of information other than a recipient's e-mail address and opt-out preferences, or require a recipient to take any steps other than sending a reply e-mail message or visiting a single Internet Web page to submit a valid opt-out request. The Commission believes the proposed alternatives are more likely to protect recipients from unwanted commercial e-mail and, thus, would more fully effectuate the purposes of the Act. Moreover, as noted earlier, the Commission believes the proposed alternatives will not substantially increase compliance costs because of the availability of commercial software that can process opt-out requests well within the proposed compliance period for businesses that send e-mail on their own behalf, and for e-mail service providers who send bulk e-mail on behalf of others, and because the Commission is only proposing to prohibit the extraneous encumbrance of a recipient's ability to submit an opt-out request. Nevertheless, the FTC seeks comment on significant alternatives, if any, to the proposed compliance period and the proposed governance of how opt-out requests are submitted that would further minimize any compliance costs, consistent with the purposes of the CAN–SPAM Act.

VII. Questions for Comment on the Proposed Rule

The Commission seeks comment on various aspects of the proposed Rule. Without limiting the scope of issues on which it seeks comment, the Commission is particularly interested in receiving comments on the questions that follow. In responding to these questions, include detailed, factual supporting information whenever possible.

A. General Questions for Comment

Please provide comment, including relevant data, statistics, or any other evidence, on each proposed change to the Rule. Regarding each proposed provision commented on, please include answers to the following questions:

1. What is the effect (including any benefits and costs), if any, on consumers?

2. What is the impact (including any benefits and costs), if any, on individual firms that must comply with the Rule?

3. What is the impact (including any benefits and costs), if any, on industry?

4. What changes, if any, should be made to the proposed Rule to minimize any cost to industry or consumers?

5. How would each suggested change affect the benefits that might be provided by the proposed Rule to consumers or industry?

6. How would the proposed Rule affect small business entities with respect to costs, profitability, competitiveness, and employment?

B. Questions on Proposed Specific Provisions

In response to each of the following questions, please provide: (1) detailed comment, including data, statistics, and other evidence, regarding the issue referred to in the question; (2) comment as to whether the proposals do or do not provide an adequate solution to the issues they were intended to address, and why; and (3) suggestions for changes that might better maximize consumer protections or minimize the burden on industry.

[263] 15 U.S.C. 7704(a)(4).

[264] *See generally* Part II.B.1.c. above. For example, Go Daddy stated: ''There are very little costs associated with deleting a person's e-mail address from a database, since mailing lists are almost always electronically automated.'' *See also* RDS; NFCU; NetCoalition; ValueClick (indicating that opt-out requests are already being processed quickly).

1. Section 316.2—Definitions

a. Does the proposed definition of ''person'' clarify those individuals and entities that are covered by the Rule and the Act? Should the proposed definition be modified? If so, how?

b. Does the proposed definition of ''sender'' clarify who will be responsible for complying with the CAN–SPAM Act when a single e-mail contains content promoting or advertising the products, services, or Web sites of multiple parties? Should the proposed definition be modified? If so, how? Do the proposed criteria provide adequate guidance to establish who is the sender when there are multiple advertisers?

c. Should opt-out obligations be extended to third-party list providers who do nothing more than provide a list of names to whom others send commercial e-mails? If so, how could this be accomplished, given the statutory language which defines ''sender'' in terms of an entity that both initiates a message *and* advertises its product, service, or Internet web site in the message?

d. Should the Commission adopt a ''safe harbor'' with respect to opt-out and other obligations for companies whose products or services are advertised by affiliates or other third parties? If not, why not? If so, what would be appropriate criteria for such a safe harbor?

e. Does the proposed definition of ''valid physical postal address'' clarify what will suffice under the Act's requirement that a sender include such an address in a commercial e-mail? Should the proposed definition be modified? If so, how?

f. Should CAN–SPAM apply to e-mail messages sent to members of online groups? What types of online groups exist? How are they formed? Does formation typically address the use of unsolicited commercial e-mail with respect to the group? How are e-mail messages transmitted or posted to an online group? Should members be able to opt out of unwanted commercial messages while continuing to receive messages relating to the subject matter of the group? Does this analysis change depending on whether the message is sent by a group member or a source outside the group? Does this analysis change depending on whether the message is unrelated to the subject matter of the online group? Does this analysis change if the online group has a moderator who decides which messages to forward to the group?

2. Section 316.2(o)—''Transactional or Relationship Message''

a. If an e-mail message contains only a legally mandated notice, should this message be considered a transactional or relationship message? Which, if any, of the existing categories of transactional or relationship message would such a message likely fit into? If such a message were considered not to have a transactional or relationship purpose, would it be exempt from regulation under the Act?

b. Should debt collection e-mails be considered ''commercial''? Or, should debt collection e-mails be considered transactional or relationship messages that complete a commercial transaction that the recipient has previously agreed to enter into with the sender? Such an interpretation assumes that the entity with whom the recipient transacted business is the entity sending the collection e-mail, or that the term ''sender'' can be interpreted to encompass a third party acting on behalf of one who would otherwise qualify as a sender. Can a third-party debt collector be considered a ''sender''?

c. Are there any messages that fall outside of the reach of the proposed Rule that should not? If so, how might this be remedied?

d. Can a ''commercial transaction'' under section 7702(17)(A)(i) exist even in the absence of an exchange of consideration?

e. If the primary purpose of an e-mail message is to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender, it is a transactional or relationship message under section 7702(17)(A)(i). Should messages from affiliated third parties that purport to be acting on behalf of another entity (the one with whom the recipient transacted) be considered transactional or relationship messages under this provision?

f. Under what, if any, circumstances should an e-mail message sent to effectuate or complete a negotiation be considered a ''transactional or relationship message'' under section 7702(17)(A)(i)?

g. Is it appropriate to classify messages offering employee discounts or other similar messages as transactional or relationship messages that ''provide information directly related to an employment relationship''? Is a relevant factor the employer's provision of the e-mail address to which such messages are sent to the employee? For example, should all messages sent from an employer to an employee at the employer-provided e-mail address be considered transactional or relationship under section 7702(17)(A)(iv)?

h. The Commission believes that an e-mail message sent on behalf of a third party, even with the permission of an employer, is not ''transactional or relationship.'' Is there any such scenario in which the e-mail message at issue could be considered ''transactional or relationship''? If so, explain.

i. For purposes of section 7702(17)(A)(iv) of the Act, should ''provid[ing] information directly related to an employment relationship'' include providing information related to such a relationship after an offer of employment is tendered?

j. 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 e-mail messages the primary purpose of which is to deliver such products or services be deemed transactional or relationship messages?

k. Should the Commission modify the Act's definition of ''transactional or relationship message'' to include what some commenters call ''business relationship messages,'' which are individualized messages that are sent from one employee of a company to an individual recipient (or a small number of recipients)? If so, what changes in e-mail technology and practices warrant this, and is such a modification necessary to accomplish the purposes of the Act?

l. The Commission believes that e-mail messages from an association or other membership entity to its membership are likely ''transactional or relationship'' in nature, pursuant to section 7702(17)(A)(v). Should messages from such senders to *lapsed* members also be considered ''transactional or relationship'' under that section? Should such messages to lapsed members be considered ''commercial'' when they advertise or promote the membership entity?

3. ''Forward-To-A-Friend'' E-mail Messages

a. Does the Commission's discussion in this NPRM of the Act's definitions of ''initiate,'' ''procure,'' and ''sender'' provide sufficient guidance to industry and consumers? Does the Commission's explication of the term ''induce'' provide sufficient guidance to industry and consumers? Does the Commission's discussion of ''routine conveyance'' provide sufficient guidance to industry and consumers? Does the Commission's interpretation of any of these terms impose any undue burdens on industry or consumers?

b. Are there other forwarding mechanisms not discussed in this notice that should be considered ''routine conveyance''? Are there other forwarding mechanisms that should *not* be considered ''routine conveyance''?

c. Does the Commission's reading of ''procure'' to mean something that entails either payment of consideration or some explicit affirmative action or statement designed to elicit the initiation of a commercial e-mail message provide sufficient guidance to industry and consumers? Why or why not?

d. Are there circumstances in which a seller could offer consideration to a person to forward a commercial e-mail that should be included within the ''routine conveyance'' exception?

e. Does the Commission's position on ''routine conveyance'' provide industry with sufficient guidance concerning Web-based forwarding mechanisms? Does it impose any undue burdens on industry or consumers?

4. Section 316.4—Prohibition Against Failure To Honor Opt-Out Requests Within Three Business Days of Receipt

a. Is three business days an appropriate deadline for effectuating an opt-out request? If not, what time frame would be more appropriate? Does the Commission's proposal that multiple advertisers in a single commercial e-mail message may arrange to have only one of those advertisers be the ''sender'' affect what time frame would be appropriate? If so, how?

b. Are some commenters' concerns warranted that under the original ten-business-day provision senders would be permitted to bombard a recipient with e-mail for ten business days following his or her opt-out request? Why or why not? Is this a commonly-occurring practice? If so, what is the evidence supporting this? Providing as much detail as possible, explain whether recipients continue to receive commercial e-mail from a particular sender after submitting an opt-out to that sender. For example, are recipients who submit opt-out requests *targeted* for receipt of additional commercial e-mail? How likely are recipients to continue to receive additional commercial e-mail from a particular sender within ten business days after submission of an opt-out request? How likely *after* ten business days?

c. Some commenters indicated that there are several software products on the market that can effectuate opt-out requests almost immediately. Are such products widely or currently used by e-mail senders? Are these products affordable for small entities? What are the costs and benefits of using such products?

d. What specific technical procedures are required to suppress a person's e-mail address from a sender's directory or distribution list? What are the specific time requirements and costs associated with those procedures? What, if any, manual procedures are required to suppress a person's e-mail address from a sender's directory or distribution list? What, if any, costs are associated with the manual suppression of e-mail addresses? How do such costs compare with costs associated with electronic processing? What, if any, circumstances would require manual processing of opt-out requests? How prevalent is the use of manual procedures to suppress people's e-mail addresses from a sender's directory or list? What are the characteristics of senders that use manual procedures to process opt-out requests? What are the characteristics of senders that use electronic procedures to process opt-out requests? Do small entities process opt-out requests manually or electronically?

e. In marketing agreements involving the use of third parties, what typically is the role of each third party in processing an opt-out request? For example, who typically receives the opt-out request and how? If the opt-out request must be transferred to a third party, how is that transfer accomplished, and how long does such a transfer typically take? Once an opt-out request is received by the third party, what procedures are involved in effectuating the opt-out request, and how long do such procedures typically take?

f. Should there be time limits on the duration of opt-out requests? Why or why not? Does the CAN–SPAM Act give the Commission authority to limit the time opt-out requests remain in effect? If so, how?

g. Is an e-mail marketer's suppression list likely to have far fewer entries than the 84 million numbers on the National Do Not Call Registry? How many recipients receive an e-mail marketer's messages in a typical e-mail marketing campaign? How many of those recipients submit opt-out requests?

5. Section 316.5—Receipt of Requests Not To Receive Future Commercial E-mail Messages From a Sender

a. What are the costs to senders and benefits to recipients of proposed 316.5?

b. Does the Commission's proposal regulating how recipients submit opt-out requests accomplish the goal of removing all extraneous encumbrances that could interfere with a recipient's ability to submit an opt-out request? Do any e-mail senders deprive recipients of any benefit when they submit an opt-out request? Should depriving recipients of a benefit when they opt out be added to the list of encumbrances prohibited by this proposal?

c. Should the Commission's proposal regulating how recipients submit opt-out requests be changed in any way?

6. Aggravated Violations Relating to Commercial E-mail

a. What data are available that would demonstrate that the *manual* harvesting of e-mail addresses is contributing substantially to the proliferation of commercial e-mail messages that are prohibited under section 7704(a) of the Act? Are there legitimate uses of manual harvesting that should be preserved?

b. What evidence is there that the sellers of open proxy lists also engage in sending e-mail messages that are prohibited under section 7704(a) of the Act? Are there any legitimate purposes for selling or distributing for consideration open proxy lists? Are there any circumstances in which an open proxy would be used by a third party with permission of the proxy's operator?

c. Are there practices that contribute substantially to the proliferation of unlawful commercial e-mail messages and are not already prohibited by the Act? For example, is harvesting e-mail addresses from peer-to-peer networks already prohibited by the Act? Is that practice contributing substantially to the proliferation of unlawful commercial e-mail messages? Is harvesting e-mail addresses from newsgroups and other similar online forums already prohibited by the Act? Is that practice contributing substantially to the proliferation of unlawful commercial e-mail messages?

7. Renumbering Provisions of the Sexually Explicit Labeling Rule and Integration of Those Provisions Into The Proposed CAN–SPAM Rule

a. Is the Commission's proposal to renumber and integrate into the Proposed CAN–SPAM Rule the provisions of the previously-adopted Sexually Explicit Labeling Rule a good solution? If not, why not? What other approach would be better? Why?

VIII. Proposed Rule

List of Subjects in 16 CFR Part 316

Advertising, Computer technology, Electronic mail, Internet, Trade practices.

Accordingly, for the reasons set forth in the preamble, the Commission proposes to amend title 16, chapter 1,

subchapter C of the Code of Federal Regulations as follows:

1. Revise part 316 to read as follows:

PART 316—CAN–SPAM RULE

Sec.
316.1 Scope.
316.2 Definitions.
316.3 Primary purpose.
316.4 Prohibition against failure to honor an opt-out request within three business days of receipt.
316.5 Prohibition on charging a fee or imposing other requirements on recipients who wish to opt out.
316.6 Requirement to place warning labels on commercial electronic mail that contains sexually oriented material.
316.7 Severability.

Authority: 15 U.S.C. 7701–7713.

§ 316.1 Scope.

This part implements the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (''CAN–SPAM Act''), 15 U.S.C. 7701–7713.

§ 316.2 Definitions.

(a) The definition of the term ''affirmative consent'' is the same as the definition of that term in the CAN–SPAM Act, 15 U.S.C. 7702(1).

(b) ''Character'' means an element of the American Standard Code for Information Interchange (''ASCII'') character set.

(c) The definition of the term ''commercial electronic mail message'' is the same as the definition of that term in the CAN–SPAM Act, 15 U.S.C. 7702(2).

(d) The definition of the term ''electronic mail address'' is the same as the definition of that term in the CAN–SPAM Act, 15 U.S.C. 7702(5).

(e) The definition of the term ''electronic mail message'' is the same as the definition of that term in the CAN–SPAM Act, 15 U.S.C. 7702(6).

(f) The definition of the term ''initiate'' is the same as the definition of that term in the CAN–SPAM Act, 15 U.S.C. 7702(9).

(g) The definition of the term ''Internet'' is the same as the definition of that term in the CAN–SPAM Act, 15 U.S.C. 7702(10).

(h) ''Person'' means any individual, group, unincorporated association, limited or general partnership, corporation, or other business entity.

(i) The definition of the term ''procure'' is the same as the definition of that term in the CAN–SPAM Act, 15 U.S.C. 7702(12).

(j) The definition of the term ''protected computer'' is the same as the definition of that term in the CAN–SPAM Act, 15 U.S.C. 7702(13).

(k) The definition of the term ''recipient'' is the same as the definition of that term in the CAN–SPAM Act, 15 U.S.C. 7702(14).

(l) The definition of the term ''routine conveyance'' is the same as the definition of that term in the CAN–SPAM Act, 15 U.S.C. 7702(15).

(m) The definition of the term ''sender'' is the same as the definition of that term in the CAN–SPAM Act, 15 U.S.C. 7702(16), *provided that,* when more than one person's products or services are advertised or promoted in a single electronic mail message, each such person who is within the Act's definition will be deemed to be a ''sender,'' *except that,* if only one such person both is within the Act's definition and meets one or more of the criteria set forth below, only that person will be deemed to be the ''sender'' of that message:

(1) The person controls the content of such message;

(2) The person determines the electronic mail addresses to which such message is sent; or

(3) The person is identified in the ''from'' line as the sender of the message.

(n) The definition of the term ''sexually oriented material'' is the same as the definition of that term in the CAN–SPAM Act, 15 U.S.C. 7704(d)(4).

(o) The definition of the term ''transactional or relationship messages'' is the same as the definition of that term in the CAN–SPAM Act, 15 U.S.C. 7702(17).

(p) ''Valid physical postal address'' means the sender's current street address, a Post Office box the sender has registered with the United States Postal Service, or a private mailbox the sender has registered with a commercial mail receiving agency that is established pursuant to United States Postal Service regulations.

§ 316.3 Primary purpose.

(a) In applying the term ''commercial electronic mail message'' defined in the CAN–SPAM Act, 15 U.S.C. 7702(2), the ''primary purpose'' of an electronic mail message shall be deemed to be commercial based on the criteria in paragraphs (a)(1) through (3) and (b) of this section:[1]

(1) If an electronic mail message consists exclusively of the commercial advertisement or promotion of a commercial product or service, then the ''primary purpose'' of the message shall be deemed to be commercial.

(2) If an electronic mail message contains both the commercial advertisement or promotion of a commercial product or service as well as transactional or relationship content as set forth in paragraph (c) of this section, then the ''primary purpose'' of the message shall be deemed to be commercial if:

(i) A recipient reasonably interpreting the subject line of the electronic mail message would likely conclude that the message contains the commercial advertisement or promotion of a commercial product or service; or

(ii) The electronic mail message's transactional or relationship content as set forth in paragraph (c) of this section does *not* appear, in whole or in substantial part, at the beginning of the body of the message.

(3) If an electronic mail message contains both the commercial advertisement or promotion of a commercial product or service as well as other content that is not transactional or relationship content as set forth in paragraph (c) of this section, then the ''primary purpose'' of the message shall be deemed to be commercial if:

(i) A recipient reasonably interpreting the subject line of the electronic mail message would likely conclude that the message contains the commercial advertisement or promotion of a commercial product or service; or

(ii) A recipient reasonably interpreting the body of the message would likely conclude that the primary purpose of the message is the commercial advertisement or promotion of a commercial product or service. Factors illustrative of those relevant to this interpretation include the placement of content that is the commercial advertisement or promotion of a commercial product or service, in whole or in substantial part, at the beginning of the body of the message; the proportion of the message dedicated to such content; and how color, graphics, type size, and style are used to highlight commercial content.

(b) In applying the term ''transactional or relationship message'' defined in the CAN–SPAM Act, 15 U.S.C. 7702(17), the ''primary purpose'' of an electronic mail message shall be deemed to be transactional or relationship if the electronic mail message consists exclusively of transactional or relationship content as set forth in paragraph (c) of this section.

(c) Transactional or relationship content of e-mail messages under the CAN–SPAM Act is content:

(1) To facilitate, complete, or confirm a commercial transaction that the

[1] The Commission does not intend for these criteria to treat as a ''commercial electronic mail message'' anything that is not commercial speech.

recipient has previously agreed to enter into with the sender;

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

(3) 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, to provide —

(i) Notification concerning a change in the terms or features;

(ii) Notification of a change in the recipient's standing or status; or

(iii)At regular periodic intervals, account balance information or other type of account statement;

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

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

§ 316.4 Prohibition against failure to honor an opt-out request within three business days of receipt.

(a) If a recipient makes a request using a mechanism provided pursuant to 15 U.S.C. 7704(a)(3) not to receive some or any commercial electronic mail messages from a sender, and does not subsequently provide affirmative consent to receive commercial electronic mail messages from such sender, then it is a violation of 15 U.S.C. 7704(a)(4):

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

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

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

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

(b) In any proceeding or action pursuant to the CAN–SPAM Act or the CAN–SPAM Rule to enforce compliance, through an order to cease and desist or an injunction, with subsection (a), neither the Commission nor the Federal Communications Commission nor the attorney general, official, or agency of a State shall be required to allege or prove the state of mind required by subsection (a).

§ 316.5 Prohibition on charging a fee or imposing other requirements on recipients who wish to opt out.

Neither a sender nor any person acting on behalf of a sender may require that any recipient pay any fee, provide any information other than the recipient's electronic mail address and opt-out preferences, or take any other steps except sending a reply electronic mail message or visiting a single Internet Web page, in order to:

(a) Use a return electronic mail address or other Internet-based mechanism, required by 15 U.S.C. 7704(a)(3), to submit a request not to receive future commercial electronic mail messages from a sender; or

(b) Have such a request honored as required by 15 U.S.C. 7704(a)(3)(B) and (a)(4).

§ 316.6 Requirement to place warning labels on commercial electronic mail that contains sexually oriented material.

(a) Any person who initiates, to a protected computer, the transmission of a commercial electronic mail message that includes sexually oriented material must:

(1) Exclude sexually oriented materials from the subject heading for the electronic mail message and include in the subject heading the phrase ''SEXUALLY-EXPLICIT:'' in capital letters as the first nineteen (19) characters at the beginning of the subject line; [2]

(2) Provide that the content of the message that is initially viewable by the recipient, when the message is opened by any recipient and absent any further actions by the recipient, include only the following information:

(i) The phrase ''SEXUALLY-EXPLICIT:'' in a clear and conspicuous manner; [3]

(ii) Clear and conspicuous identification that the message is an advertisement or solicitation;

(iii) Clear and conspicuous notice of the opportunity of a recipient to decline to receive further commercial electronic mail messages from the sender;

(iv) A functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that—

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

(B) Remains capable of receiving such messages or communications for no less than 30 days after the transmission of the original message;

(v) Clear and conspicuous display of a valid physical postal address of the sender; and

(vi) Any needed instructions on how to access, or activate a mechanism to access, the sexually oriented material, preceded by a clear and conspicuous statement that to avoid viewing the sexually oriented material, a recipient should delete the e-mail message without following such instructions.

(b) *Prior affirmative consent.* Paragraph (a) of this section does not apply to the transmission of an electronic mail message if the recipient has given prior affirmative consent to receipt of the message.

§ 316.7 Severability.

The provisions of this Rule are separate and severable from one another. If any provision is stayed or determined to be invalid, it is the Commission's intention that the remaining provisions shall continue in effect.

By direction of the Commission, Commissioner Leibowitz not participating.

Donald S. Clark,

Secretary.

Note: Appendix A is published for informational purposes only and will not be codified in Title 16 of the Code of Federal Regulations.

[2] 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.

[3] This phrase consists of nineteen (19) characters and is identical to the phrase required in 316.5(a)(1) of this Rule.

APPENDIX A—LIST OF COMMENTERS CITED IN NPRM AND ACRONYMS ASSIGNED TO COMMENTERS

Acronym	Commenter
AAOMS	American Association of Oral and Maxillofacial Surgeons
AAR	American Air Racing
ABA	American Bar Association
ABM	American Business Media
ACA	ACA International
ACB	America's Community Bankers
ACLI	American Council of Life Insurers
AeA	American Electronics Association
AOC	The Electronic Warfare and Information Operations Association
ASA	American Staffing Association
ASAE	American Society of Association Executives
Aspects	Aspects of Design
ASTA	American Society of Travel Agents, Inc.
AT&T	AT&T Corp.
AWWA	American Water Works Association
Bahr	Law Offices of Susan Bar
Bank	Bank of America Corp.
Bankers	American Bankers Association
BMI	Broadcast Music, Inc.
BMO	BMO Financial Group
Calvert	Thomas Calvert
CBA	Consumer Bankers Association
Cendant	Cendant Corp.
Chamber	United States Chamber of Commerce
ClickZ	ClickZ Network
CMOR	Council on Marketing and Opinion Research
Coalition	National Business Coalition on E-Commerce and Privacy
Comerica	Comerica
Consumer	Consumer World
Countrywide	Countrywide Financial Corp.
Csorba	Frank Csorba
Danko	Danko
Discover	Discover Bank
DMA	Direct Marketing Association, Inc.
DoubleClick	DoubleClick, Inc.
DSA	Direct Selling Association
EDC	EDC Computers, Inc.
Edgley	John Edgley
EFF	Electronic Frontier Foundation
ERA	Electronic Retailing Association
ESPC	E-mail Service Provider Coalition
Experian	Experian Marketing Solutions
Ford	Ford
Ford Motor	Ford Motor Company
Fredrikson	Fredrikson & Byron, PA
Freese	Bill Freese
Giambra	Giambra
Gilbert	Doug Gilbert
Go Daddy	Go Daddy Software, Inc.
Harte	Harte-Hanks, Inc.
IAAMC	International Association of Association Management Companies
IAC	InterActive Corp.
IBAT	Independent Bankers Association of Texas
ICC	Internet Commerce Coalition
ICFA	International Cemetery and Funeral Association
IFA	International Franchise Association
ICOP	International Council of Online Professionals
Independent	Independent Sector
Innovation	Innovation Press
IPPC	International Pharmaceutical Privacy Consortium
Jaffe	Andrew Jaffe
Jensen	Roy Jensen
Justasmallthing.com	Justasmallthing.com
KALRES	KALRES, Inc.
Keef	Carl Keef
Keogh	Jill Keogh
KeyCorp	KeyCorp
Krueger, B.	Brandt Krueger
Krueger, K.	Karl Krueger
KSUF	Kansas State University Foundation
Lenox	Lenox, Inc.
Lunde	Brian Lunde

APPENDIX A—LIST OF COMMENTERS CITED IN NPRM AND ACRONYMS ASSIGNED TO COMMENTERS—Continued

Acronym	Commenter
M&F	Morrison & Foerster LLP
Maat	Ayo Maat
Marzuola	Steven Marzuola
MasterCard	MasterCard International Inc.
MBA	Mortgage Bankers Association
MBNA	MBNA America Bank, N.A.
Mead	Bennett Mead
Mellon	Mellon Financial Corp.
Microsoft	Microsoft Corp.
Midway	Midway Publishing Inc.
MIS	Marketing Idea Shop
MMS	MMS, Inc.
Moerlien	Charles Moerlien
MPA	Magazine Publishers of America
MPAA	Motion Picture Association of America
NAA	Newspaper Association of America
NADA	National Automobile Dealers Association
NAIFA	National Association of Insurance and Financial Advisors
NAR	National Association of Realtors
NCL	National Consumers League
NEPA	Newsletter and Electronic Publishers Association
NetCoalition	NetCoalition
NFCU	Navy Federal Credit Unition
NNA	National Newspaper Association
NRF	National Retail Federation
O'Connor	Clint O'Connor
Oldaker	Oldaker, Biden & Belair
OPA	Online Publishers Association
P&G	Proctor & Gamble
Piper	Piper Rudnick LLP
Potocki	Potocki
PMA	Promotion Marketing Association
RDS	RDS
Reed	Reed Elsevier, Inc.
Register	Register.com, BulkRegister, eNom, Network Solutions, Tucows
Richardson	David Richardson
RMAS	Russell-Mellon Analytical Services
Rospenda	John Rospenda
RTCM	Radio Technical Commission for Maritime Services
Sachau	Barb Sachau
Safell	Jean Safell
Satchell	Stephen Satchell
SBA	Office of Advocacy, U.S. Small Business Association
Shaw	Tom Shaw
SIA	Securities Industry Association
SIIA	Software and Information Industry Association
Speer	Speer
St. Saveur	Joe St. Saveur
SVM	SVM Corporate Marketing
Time Warner	Time Warner
True	THISISTRUE.com
Truth	Dawning Truth
UNC	UNC General Alumni Association
United	United Online
USTOA	United States Tour Operators Association
ValueClick	ValueClick, Inc.
Vandenberg	Michael Vandenberg
Venable	Venable LLP
Visa	Visa USA, Inc.
Vowles	James Vowles
Wells Fargo	Wells Fargo & Company
Weston	Weston, Garrou & DeWitt

[FR Doc. 05–9353 Filed 5–11–05; 8:45 am]

BILLING CODE 6750–01–P