               A No Soliciting Simple Mail Transfer Protocol (SMTP)
                            Service Extension

Status of this Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements.  Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol.  Distribution of this memo is unlimited.

Copyright Notice

Abstract

   This document proposes an extension to Soliciting Simple Mail
   Transfer Protocol (SMTP) for an electronic mail equivalent to the
   real-world "No Soliciting" sign.  In addition to the service
   extension, a new message header and extensions to the existing
   "received" message header are described.

Table of Contents

1.  Introduction

1.1.  The Spam Pandemic

   Unsolicited Bulk Email (UBE), otherwise known as spam, has become as
   one of the most pressing issues on the Internet.  One oft-quoted
   study estimated that spam would cost businesses $13 billion in 2003
   [Ferris].  In April 2003, AOL reported that it had blocked 2.37
   billion pieces of UBE in a single day [CNET].  And, in a sure sign
   that UBE has become of pressing concern, numerous politicians have
   begun to issue pronouncements and prescriptions for fighting this
   epidemic [Schumer][FTC].

   A variety of mechanisms from the technical community have been
   proposed and/or implemented to fight UBE:

   o  Whitelists are lists of known non-spammers.  For example, Habeas,
      Inc. maintains a Habeas User List (HUL) of people who have agreed
      to not spam.  By including a haiku in email headers and enforcing
      copyright on that ditty, they enforce their anti-spamming terms of
      service [Habeas].

   o  Blacklists are lists of known spammers or ISPs that allow spam
      [ROKSO].

   o  Spam filters run client-side or server-side to filter out spam
      based on whitelists, blacklists, and textual and header analysis
      [Assassin].

   o  A large number of documents address the overall technical
      considerations for the control of UBE [crocker-spam-techconsider],
      operational considerations for SMTP agents [RFC2505], and various
      extensions to the protocols to support UBE identification and
      filtering [danisch-dns-rr-smtp][daboo-sieve-spamtest][crouzet-
      amtp].

   o  Various proposals have been advanced for "do not spam" lists, akin
      to the Federal Trade Commission's "Do Not Call" list for
      telemarketers [FTC.TSR].

Terminology

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in BCP 14, RFC 2119
   [RFC2119].

1.2.  No Soliciting in the Real World

   Municipalities frequently require solicitors to register with the
   town government.  And, in many cases, the municipalities prohibit
   soliciting in residences where the occupant has posted a sign.  The
   town of West Newbury, Massachusetts, for example, requires:

      "It shall be unlawful for any canvasser or solicitor to enter the
      premises of a resident or business who has displayed a 'No
      Trespassing' or 'No Soliciting' sign or poster.  Further, it shall
      be unlawful for canvassers or solicitors to ignore a resident or
      business person's no solicitation directive or remain on private
      property after its owner has indicated that the canvasser or
      solicitor is not welcome" [Newbury].

   Registration requirements for solicitors, particularly those
   soliciting for political or religious reasons, have been the subject
   of a long string of court cases.  However, the courts have generally
   recognized that individuals may post "No Soliciting" signs and the
   government may enforce the citizen's desire.  In a recent case where
   Jehovah's Witnesses challenged a registration requirement in the city
   of Stratton, Connecticut, saying they derived their authority from
   the Scriptures, not the city.  However, the court noted:

      "A section of the ordinance that petitioners do not challenge
      establishes a procedure by which a resident may prohibit
      solicitation even by holders of permits.  If the resident files a
      'No Solicitation Registration Form' with the mayor, and also posts
      a 'No Solicitation' sign on his property, no uninvited canvassers
      may enter his property... " [Watchtower].

   Even government, which has a duty to promote free expression, may
   restrict the use of soliciting on government property.  In one case,
   for example, a school district was allowed to give access to its
   internal electronic mail system to the union that was representing
   teachers, but was not required to do so to a rival union that was
   attempting to gain the right to represent the teachers.  The court
   held that where property is not a traditional public forum "and the
   Government has not dedicated its property to First Amendment
   activity, such regulation is examined only for reasonableness"
   [Perry].

   The courts have consistently held that the state has a compelling
   public safety reason for regulating solicitation.  In Cantwell v.
   Connecticut, the Supreme Court held that "a State may protect its
   citizens from fraudulent solicitation by requiring a stranger in the
   community, before permitting him publicly to solicit funds for any
   purpose, to establish his identity and his authority to act for the

cause which he purports to represent" [Cantwell].  And, in Martin v.
City of Struthers, the court noted that "burglars frequently pose as
canvassers, either in order that they may have a pretense to discover
whether a house is empty and hence ripe for burglary, or for the
purpose of spying out the premises in order that they may return
later" [Martin].  The public safety issue applies very much to email,
where viruses can easily be delivered, in contrast to telephone
solicitations where public safety is not nearly as much an issue.

This analysis is U.S.-centric, which is partly due to the background
of the author.  However, the concept of prohibiting unwanted
solicitation does carry over to other countries:

o  In Hong Kong, offices frequently post "no soliciting" signs.

o  In the United Kingdom, where door-to-door peddlers are fairly
   common, "no soliciting" signs are also common.

o  In Australia, where door-to-door does not appear to be a pressing
   social problem, there was legislation passed which outlawed the
   practice of placing ads under wipers of parked cars.

o  In France, which has a long tradition of door-to-door
   solicitation, apartment buildings often use trespass laws to
   enforce "no solicitation" policies.

o  In the Netherlands, where door-to-door solicitation is not a
   pressing issue, there is a practice of depositing free
   publications in mailboxes.  The postal equivalent of "no spam"
   signs are quite prevalent and serve notice that the publications
   are not desired.

1.3.  No Soliciting and Electronic Mail

Many of the anti-spam proposals that have been advanced have great
merit, however none of them give notice to an SMTP agent in the
process of delivering mail that the receiver does not wish to receive
solicitations.  Such a virtual sign would serve two purposes:

o  It would allow the receiving system to "serve notice" that a
   certain class of electronic mail is not desired.

o  If a message is properly identified as belonging to a certain
   class and that class of messages is not desired, transfer of the
   message can be eliminated.  Rather than filtering after delivery,
   elimination of the message transfer can save network bandwidth,
   disk space, and processing power.

This memo details a series of extensions to SMTP that have the
following characteristics:

o  A service extension is described that allows a receiving Mail
   Transport Agent (MTA) to signal the sending MTA that no soliciting
   is in effect.

o  A header field for the sender of the message is defined that
   allows the sender to flag a message as conforming to a certain
   class.

o  Trace fields for intermediate MTAs are extended to allow the
   intermediate MTA to signal that a message is in a certain class.

Allowing the sender of a message to tag a message as being, for
example, unsolicited commercial email with adult content, allows
"good" spammers to conform to legal content labelling requirements by
governmental authorities, license agreements with service providers,
or conventions imposed by "whitelist" services.  For senders of mail
who choose not to abide by these conventions, the intermediate trace
fields defined here allow the destination MTAs to perform appropriate
dispositions on the received message.

This extension provides a simple mean for senders, MTAs, and
receivers to assert keywords.  This extension does not deal with any
issues of authentication or consent.

2.  The No-Soliciting SMTP Service Extension

Per [RFC2821], a "NO-SOLICITING" SMTP service extension is defined.
The service extension is declared during the initial "EHLO" SMTP
exchange.  The extension has one optional parameter, consisting of
zero or more solicitation class keywords.  Using the notation as
described in the Augmented BNF [RFC2234], the syntax is:

    No-Soliciting-Service = "NO-SOLICITING"
        [ SP Solicitation-keywords ]

As will be further described below, the "Solicitation-keywords"
construct is used to indicate which classes of messages are not
desired.  A keyword that is presented during the initial "EHLO"
exchange applies to all messages exchanged in this session.  As will
also be further described below, additional keywords may be specified
on a per-recipient basis as part of the response to a "RCPT TO"
command.

2.1.  The EHLO Exchange

   Keywords presented during the initial exchange indicate that no
   soliciting in the named classes is in effect for all messages
   delivered to this system.  It is equivalent to the sign on the door
   of an office building announcing a company-wide policy.  For example:

       R: <wait for connection on TCP port 25>
       S: <open connection to server>
       R: 220 trusted.example.com SMTP service ready
       S: EHLO untrusted.example.com
       R: 250-trusted.example.com says hello
       R: 250-ENHANCEDSTATUSCODES
       R: 250-NO-SOLICITING net.example:ADV
       R: 250 SIZE 20480000

   The "net.example:ADV" parameter to the "NO-SOLICITING" extension is
   an example of a solicitation class keyword, the syntax of which is
   described in the following section.

   Historical Note:

       A similar proposal was advanced in 1999 by John Levine and Paul
       Hoffman.  This proposal used the SMTP greeting banner to specify
       that unsolicited bulk email is prohibited on a particular system
       through the use of the "NO UCE" keyword [Levine].  As the authors
       note, their proposal has the potential of overloading the
       semantics of the greeting banner, which may also be used for other
       purposes (see, e.g., [Malamud]).

2.2.  Solicitation Class Keywords

   The "NO-SOLICITING" service extension uses solicitation class
   keywords to signify classes of solicitations that are not accepted.
   Solicitation class keywords are separated by commas.

   There is no default solicitation class keyword for the service.  In
   other words, the following example is a "no-op":

       R : 250-NO-SOLICITING

   While the above example is a "no-op" it is useful for an MTA that
   wishes to pass along all messages, but would also like to pass along
   "SOLICIT=" parameters on a message-by-message basis.  The above
   example invokes the use of the extension but does not signal any
   restrictions by class of message.

The initial set of solicitation class keywords all begin with a
domain name with the labels reversed, followed by a colon.  For
example, the domain name "example.com" could be used to form the
beginning of a solicitation class keyword of "com.example:".  The
solicitation class keyword is then followed by an arbitrary set of
characters drawn from the following construct:

```
    Solicitation-keywords = word
         0*("," word)
         ; length of this string is limited
         ; to <= 1000 characters
    word = ALPHA 0*(wordchar)
    wordchar = ("." / "-" / "_" / ":" / ALPHA / DIGIT)
```

A solicitation class keyword MUST be less than 1000 characters.  Note
however that a set of keywords used in the operations defined in this
document must also be less than 1000 characters.  Implementors are
thus advised to keep their solicitation class keywords brief.

Any registrant of a domain name may define a solicitation class
keyword.  Discovery of solicitation class keywords is outside the
scope of this document.  However, those registrants defining keywords
are advised to place a definition of their solicitation class
keywords on a prominent URL under their control such that search
engines and other discovery mechanisms can find them.

While this document defines solicitation class keywords as beginning
with a reversed domain name followed by a colon (":"), future RFCs
may define additional mechanisms that do not conflict with this
naming scheme.

2.2.1.  Note on Choice of Solicitation Class Keywords

This document does not specify which solicitation class keywords
shall or shall not be used on a particular message.  The requirement
to use a particular keyword is a policy decision well outside the
scope of this document.  It is expected that relevant policy bodies
(e.g., governments, ISPs, developers, or others) will specify
appropriate keywords, the definition of the meaning of those
keywords, and any other policy requirements, such as a requirement to
use or not use this extension in particular circumstances.

During discussions of this proposal, there were several suggestions
to do away with the solicitation class keywords altogether and
replace the mechanism with a simple boolean (e.g., "NO-SOLICITING
YES" or "ADV" or "UBE").  Under a boolean mechanism, this extension
would have to adopt a single definition of what "YES" or other label

means.  By using the solicitation class keywords approach, the mail
infrastructure remains a neutral mechanism, allowing different
definitions to co-exist.

2.3.  The MAIL FROM Command

"SOLICIT" is defined as a parameter for the "MAIL FROM" command.  The
"SOLICIT" parameter is followed by an equal sign and a comma
separated list of solicitation class keywords.  The syntax for this
parameter is:

```
    Mail-From-Solicit-Parameter = "SOLICIT"
                          "=" Solicitation-keywords
    ; Solicitation-keywords, when used in MAIL FROM command
    ; MUST be identical to those in the Solicitation: header.
```

Note that white space is not permitted in this production.

As an informational message, the "550" or "250" replies to the "RCPT
TO" command may also contain the "SOLICIT" parameter.  If a message
is being rejected due to a solicitation class keyword match,
implementations SHOULD echo which solicitation classes are in effect.
See Section 2.4 for more on error reporting.

The receiving system may decide on a per-message basis the
appropriate disposition of messages:

```
R: <wait for connection on TCP port 25>
S: <open connection to server>
R: 220 trusted.example.com SMTP service ready
S: EHLO untrusted.example.com
R: 250-trusted.example.com says hello
R: 250-NO-SOLICITING net.example:ADV
S: MAIL FROM:<save@example.com> SOLICIT=org.example:ADV:ADLT
S: RCPT TO:<coupon_clipper@moonlink.example.com>
R: 250 <coupon_clipper@moonlink.example.com>... Recipient ok
S: RCPT TO:<grumpy_old_boy@example.net>
R: 550 <grumpy_old_boy@example.net> SOLICIT=org.example:ADV:ADLT
```

In the previous example, the receiving MTA returned a "550" status
code, indicating that one message was being rejected.  The
implementation also echoes back the currently set keywords for that
user on the "550" status message.  The solicitation class keyword
which is echoed back is "org.example:ADV:ADLT" which illustrates how
this per-recipient solicitation class keyword has supplemented the
base "net.example:ADV" class declared in the "EHLO" exchange.

It is the responsibility of a receiving MTA to maintain a consistent
policy.  If the receiving MTA will reject a message because of
solicitation class keywords, the MTA SHOULD declare those keywords
either in the initial "EHLO" exchange or on a per-recipient basis.
Likewise, a receiving MTA SHOULD NOT deliver a message where the
"Solicitation:" matches a solicitation class keyword that was
presented during the initial "EHLO" exchange or on a per-recipient
basis.

Developers should also note that the source of the solicitation class
keywords used in the "MAIL FROM" command MUST be the "Solicitation:"
header described in Section 2.5 and MUST NOT be supplemented by
additional solicitation class keywords derived from the "Received:"
header trace fields which are described in Section 2.6.

## 2.4.  Error Reporting and Enhanced Mail Status Codes

If a session between two MTAs is using both the "NO-SOLICITING"
extension and the Enhanced Mail Status Codes as defined in [RFC3463]
and a message is rejected based on the presence of a "SOLICIT"
parameter, the correct error message to return will usually be
"5.7.1", defined as "the sender is not authorized to send to the
destination...  (because) of per-host or per-recipient filtering."

Other codes, including temporary status codes, may be more
appropriate in some circumstances and developers should look to
[RFC3463] on this subject.  An example of such a situation might be
the use of quotas or size restrictions on messages by class.  An
implementation MAY impose limits such as message size restrictions
based on solicitation classes, and when such limits are exceed they
SHOULD be reported using whatever status code is appropriate for that
limit.

In all cases, an implementation SHOULD include a "Mail-From-Solicit-
Parameter" on a "550" or other reply that rejects message delivery.
The parameter SHOULD includes the solicitation class keyword(s) that
matched.  In addition to the solicitation class keyword(s) that
matched, an implementation MAY include additional solicitation class
keywords that are in effect.

## 2.5.  Solicitation Mail Header

Per [RFC2822], a new "Solicitation:" header field is defined which
contains one or more solicitation class keywords.

    Solicitation-header = "Solicitation:" 1*SP Solicitation-keywords

An example of this header follows:

```
   To: Coupon Clipper <coupon_clipper@moonlink.example.com>
   From: Spam King <save@burntmail.example.com>
   Solicitation: net.example:ADV,org.example:ADV:ADLT
```

Several proposals, particularly legal ones, have suggested requiring
the use of keywords in the "Subject:" header.  While embedding
information in the "Subject:" header may provide visual cues to end
users, it does not provide a straightforward set of cues for computer
programs such as mail transfer agents.  As with embedding a "no
solicitation" message in a greeting banner, this overloads the
semantics of the "Subject:" header.  Of course, there is no reason
why both mechanisms can't be used, and in any case the
"Solicitation:" header could be automatically inserted by the
sender's Mail User Agent (MUA) based on the contents of the subject
line.

2.6.  Insertion of Solicitation Keywords in Trace Fields

The "Solicitation:" mail header is only available to the sending
client.  RFCs 2821 and 2822 are quite specific that intermediate MTAs
shall not change message headers, with the sole exception of the
"Received:" trace field.  Since many current systems use an
intermediate relay to detect unsolicited mail, an addition to the
"Received:" header is described.

[RFC2821] documents the following productions for the "Received:"
header in a mail message:

```
   ; From RFC 2821
   With = "WITH" FWS Protocol CFWS
   Protocol = "ESMTP" / "SMTP" / Attdl-Protocol
```

Additionally, [RFC2822] defines a comment field as follows:

```
   ; From RFC 2822
   comment        =       "(" *([FWS] ccontent) [FWS] ")"
   ccontent       =       ctext / quoted-pair / comment
```

The "Mail-From-Solicit-Parameter" defined in Section 2.3 above is a
restricted form of ctext, yielding the following production:

```
   With-Solicit = "WITH" FWS Protocol
             "(" [FWS] comment [FWS] ")"
   comment       =       "(" *([FWS] ccontent) [FWS] ")"
   ccontent = ctext / quoted-pair /
             comment / Mail-From-Solicit-Parameter
```

```
                     ; The Mail-From-Solicit-Parameter
                     ; is a restricted form of ctext
```

An example of a Received: header from a conforming MTA is as follows:

```
   Received: by foo-mta.example.com with
       ESMTP (SOLICIT=net.example:ADV,org.example:ADV:ADLT) ;
       Sat, 9 Aug 2003 16:54:42 -0700 (PDT)
```

It should be noted that keywords presented in trace fields may not
agree with those found in the "Solicitation:" header and trace fields
may exist even if the header is not present.  When determining which
keywords are applicable to a particular exchange of messages,
implementors SHOULD examine any keywords found in the "Solicitation:"
header.  Implementors MAY examine other keywords found in the trace
fields.

2.7.  Relay of Messages

The "NO-SOLICITING" service extension, if present, applies to all
messages handled by the receiving Message Transfer Agent (MTA),
including those messages intended to be relayed to another system.

Solicitation class keywords supplied by a client on a "SOLICIT"
parameter on a "MAIL FROM" command SHOULD be obtained from the
"Solicitation:" field in the message header.  An SMTP client SHOULD,
however, verify that the list of solicitation class keywords obtained
from the "Solicitation:" field uses valid syntax before conveying its
contents.  An SMTP server SHOULD set this parameter after detecting
the presence of the "Solicitation:" header field when receiving a
message from a non-conforming MTA.

2.8.  No Default Solicitation Class

Implementations of "NO-SOLICITING" service extension SHOULD NOT
enable specific solicitation class keywords as a default in their
software.  There are some indications that some policy makers may
view a default filtering in software as a prior restraint on
commercial speech.  In other words, because the person installing and
using the software did not make an explicit choice to enable a
certain type of filtering, some might argue that such filtering was
not desired.

Likewise, it is recommended that a system administrator installing
software SHOULD NOT enable additional per-recipient filtering by
default for a user.  Again, individual users should specifically
request any additional solicitation class keywords.

The mechanism for an individual user to communicate their desire to
enable certain types of filtering is outside the scope of this
document.

3.  Security Considerations

This extension does not provide authentication of senders or other
measures intended to promote security measures during the message
exchange process.

In particular, this document does not address the circumstances under
which a sender of electronic mail should or should not use this
extension and does not address the issues of whether consent to send
mail has been granted.

This might lead to a scenario in which a sender of electronic mail
begins to use this extension well before the majority of end users
have begun to use it.  In this scenario, the sender might wish to use
the absence of the extension on the receiving MTA as an implication
of consent to receive mail.  Non-use of the "NO-SOLICITING" extension
by a receiving MTA SHALL NOT indicate consent.

4.  IANA Considerations

There are three IANA considerations presented in this document:

1. Addition of the "NO-SOLICITING" service extension to the Mail
   Parameters registry.

2. Documentation of the use of comments in trace fields.

3. Creation of a "Solicitation:" mail header.

4.1.  The Mail Parameters Registry

The IANA Mail Parameters registry documents SMTP service extensions.
The "NO-SOLICITATION" service extension has been added to this
registry as follows.

| Keywords | Description | Reference |
| ----------- | ------------------------------ | --------- |
| NO-SOLICITING | Notification of no soliciting. | RFC3865 |

The parameters subregistry would need to be modified as follows:

| Service Ext | EHLO Keyword | Parameters | Reference |
| ----------- | ------------ | ----------- | --------- |
| No Soliciting | NO-SOLICITING | Solicitation-keywords | RFC3865 |

The maximum length of Solicitation-keywords is 1000 characters.  The
"SOLICIT=" parameter is defined for use on the MAIL FROM command.
The potential length of the MAIL FROM command is thus increased by
1007 characters.

4.2.  Trace Fields

The Mail Parameters registry would need to be modified to note the
use of the comment facility in trace fields to indicate Solicitation
Class Keywords.

4.3.  The Solicitation Mail Header

Per [RFC3864], the "Solicitation:" header field is added to the IANA
Permanent Message Header Field Registry.  The following is the
registration template:

o  Header field name: Solicitation
o  Applicable protocol: mail
o  Status: standard
o  Author/Change controller: IETF
o  Specification document(s): RFC3865
o  Related information:

5.  Author's Acknowledgements

The author would like to thank Rebecca Malamud for many discussions
and ideas that led to this proposal and to John C. Klensin and
Marshall T. Rose for their extensive input on how it could be
properly implemented in SMTP.  Eric Allman, Harald Alvestrand, Steven
M. Bellovin, Doug Barton, Kent Crispin, Dave Crocker, Ned Freed,
Curtis Generous, Arnt Gulbrandsen,  John Levine, Keith Moore, Hector
Santos, Ted Hardie, Paul Vixie, and Pindar Wong kindly provided
reviews of the document and/or suggestions for improvement.
Information about soliciting outside the U.S. was received from Rob
Blokzijl, Jon Crowcroft, Christian Huitema, Geoff Huston, and Pindar
Wong. John Levine pointed out the contrast between this proposal and
"do not spam" lists.  As always, all errors and omissions are the
responsibility of the author.

## 6.  References

### 6.1.  Normative References

   [RFC2119]     Bradner, S., "Key words for use in RFCs to Indicate
                 Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC2234]     Crocker, D., Ed. and P. Overell, "Augmented BNF for
                 Syntax Specifications: ABNF", RFC 2234, November 1997.

   [RFC2821]     Klensin, J., Ed., "Simple Mail Transfer Protocol", RFC
                 2821, April 2001.

   [RFC2822]     Resnick, P., Ed., "Internet Message Format", RFC 2822,
                 April 2001.

   [RFC3463]     Vaudreuil, G., "Enhanced Mail System Status Codes", RFC
                 3463, January 2003.

   [RFC3864]     Klyne, G., Nottingham, M., and J. Mogul, "Registration
                 Procedures for Message Header Fields", BCP 90, RFC 3864,
                 September 2004.

### 6.2.  Informative References

   [Assassin]    Mason, J., "Spamassassin - Mail Filter to Identify Spam
                 Using Text Analysis", Version 2.55, May 2003,
                 <http://www.mirror.ac.uk/sites/spamassassin.taint.org/
                 spamassassin.org/doc/spamassassin.html>

   [CNET]        CNET News.Com, "AOL touts spam-fighting prowess", April
                 2003, <http://news.com.com/2100-1025-998944.html>.

   [Cantwell]    U.S. Supreme Court, "Cantwell v. State of Connecticut",
                 310 U.S. 296 (1940), May 1940,
                 <http://caselaw.lp.findlaw.com/scripts/
                 getcase.pl?court=US&vol=310&invol=296>

   [FTC]         Federal Trade Commission, "Federal, State, Local Law
                 Enforcers Target Deceptive Spam and Internet Scams",
                 November 2002,
                 <http://www.ftc.gov/opa/2002/11/nenetforcema.htm>.

   [FTC.TSR]     Federal Trade Commission, "Telemarketing Sales Rule",
                 Federal Register Vol. 68, No. 19, January 2003,
                 <http://www.ftc.gov/os/2002/12/tsrfinalrule.pdf>.

   [Ferris]       Associated Press, "Study: Spam costs businesses $13
                  billion", January 2003,
                  <http://www.cnn.com/2003/TECH/biztech/01/03/
                  spam.costs.ap/index.html>

   [Habeas]       Habeas, Inc., "Habeas Compliance Message", 2004,
                  <http://www.habeas.com/servicesComplianceStds.html>

   [crocker-spam-techconsider]
                  Crocker, D., "Technical Considerations for Spam Control
                  Mechanisms", Work in Progress, February 2004.

   [crouzet-amtp]
                  Crouzet, B., "Authenticated Mail Transfer Protocol",
                  Work in Progress, May 2004.

   [daboo-sieve-spamtest]
                  Daboo, C., "SIEVE Spamtest and Virustest Extensions",
                  Work in Progress, October 2003.

   [danisch-dns-rr-smtp]
                  Danisch, H., "The RMX DNS RR and method for lightweight
                  SMTP sender authorization", Work in Progress, August
                  2004.

   [Levine]       Levine, J. and P. Hoffman, "Anti-UBE and Anti-UCE
                  Keywords in SMTP Banners", Revision 1.1, March 1999,
                  <http://www.cauce.org/proposal/smtp-banner-rfc.shtml>.

   [Malamud]      Malamud, C., "An Internet Prayer Wheel", Mappa.Mundi
                  Magazine, August 1999,
                  <http://mappa.mundi.net/cartography/Wheel/>.

   [Martin]       U.S. Supreme Court, "Martin v. City of Struthers, Ohio",
                  319 U.S. 141 (1943), May 1943,
                  <http://caselaw.lp.findlaw.com/scripts/
                  getcase.pl?court=US&vol=319&involv=141>

   [Newbury]      The Town of West Newbury, Massachusetts, "Soliciting/
                  Canvassing By-Law", Chapter 18 Section 10, March 2002,
                  <http://www.town.west-newbury.ma.us/Public_Documents/
                  WestNewburyMA_Bylaws/000A1547-70E903AC>

   [Perry]        U.S. Supreme Court, "Perry Education Association v.
                  Perry Local Educators' Association", 460 U.S. 37 (1983),
                  February 1983, <http://caselaw.lp.findlaw.com/scripts/
                  getcase.pl?court=US&vol=460&involv=37>

   [RFC2505]      Lindberg, G., "Anti-Spam Recommendations for SMTP MTAs",
                  BCP 30, RFC 2505, February 1999.

   [ROKSO]        Spamhaus.Org, "Register of Known Spam Operations",
                  November 2003,
                  <http://www.spamhaus.org/rokso/index.lasso>.

   [Schumer]      Charles, C., "Schumer, Christian Coalition Team Up to
                  Crack Down on Email Spam Pornography", June 2003,
                  <http://
                  www.senate.gov/~schumer/SchumerWebsite/pressroom/
                  press_releases/PR01782.html>.

   [Watchtower] U.S. Supreme Court, "Watchtower Bible & Tract Society of
                  New York, Inc., et al. v. Village of Stratton et al.",
                  122 S.Ct. 2080 (2002), June 2002,
                  <http://caselaw.lp.findlaw.com/scripts/
                  getcase.pl?court=US&vol=000&invol=00-1737>

Appendix A.  Collected ABNF Descriptions (Normative)

```
Solicitation-keywords = word
    0*("," word)
    ; length of this string is limited
    ; to <= 1000 characters
word = ALPHA 0*(wordchar)
wordchar = ("." / "-" / "_" / ":" / ALPHA / DIGIT)

; used in the initial EHLO exchange
No-Soliciting-Service = "NO-SOLICITING"
    [ SP Solicitation-keywords ]

; used on the Solicitation: message header
Solicitation-header = "Solicitation:" 1*SP Solicitation-keywords

; used on the MAIL FROM command and replies,
; and on Received: headers.
Mail-From-Solicit-Parameter =
    "SOLICIT" "=" Solicitation-keywords
    ; Solicitation-keywords, when used in
    ; the MAIL FROM command MUST be identical
    ; to those in the Solicitation: header.

; Used on Received: headers
With-Solicit = "WITH" FWS Protocol
        "(" [FWS] comment [FWS] ")"
; From RFC 2822
comment = "(" *([FWS] ccontent) [FWS] ")"
ccontent = ctext / quoted-pair /
        comment / Mail-From-Solicit-Parameter
        ; The Mail-From-Solicit-Parameter
        ; is a restricted form of ctext
; From RFC 2821
With = "WITH" FWS Protocol CFWS
Protocol = "ESMTP" / "SMTP" / Attdl-Protocol
Attdl-Protocol = Atom
```

Author's Address

    Carl Malamud
    Memory Palace Press
    PO Box 300
    Sixes, OR  97476
    US

    EMail: carl@media.org