

Addressing FTC DIARRUCA Concerns draft-malamud-diarruca-concerns-00

Status of this Memo

This document is an Internet-Draft and is CONFORMANCE UNDEFINED.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress".

The list of current Internet-Drafts can be accessed at <<http://www.ietf.org/ietf/lid-abstracts.txt>>.

The list of Internet-Draft Shadow Directories can be accessed at <<http://www.ietf.org/shadow.html>>.

This Internet-Draft will expire in September 2004.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

The U.S. Congress, having hit a home run with the do-not-call list, has decided that since computers are like telephones, a do-not-email list ought to win them the pennant. You have an opportunity to block that metaphor. The FTC has issued an Advanced Notice of Proposed Rulemaking and has given the public until March 31, 2004 to respond. This document tells you how and explains the issues.

Terminology

The key words "Good Thing™", "Bad Thing™", "Feature©", and "Bug©" in this document are to be interpreted as described in [4].

1 Introduction

The U.S. Federal Trade Commission (FTC) has issued an Advanced Notice of Proposed Rulemaking (ANPR), which is a formal agency action of notice and comment prior to rulemaking pursuant to the U.S. Administrative Procedures Act [6] and is in response to the passage of the CAN-SPAM Act of 2003 [15] The ANPR is entitled "Definitions, Implementation, and Reporting Requirements Under the CAN-SPAM Act." [7]

The request for public comment lists a variety of issues pertaining to implementation and reporting requirements of the CAN-SPAM Act of 2003. This document only addresses a subset of the issues raised, including:

- Section 9(a) and §9(b) of the CAN-SPAM Act of 2003 mandates that the Commission submit a report "setting forth a plan and timetable for establishing a nationwide marketing Do Not E-mail Registry." In response, the Commission has already issue a pre-procurement call for contractors to build this Do Not E-mail Database and operate that system on behalf of the Commission.[8] The Commission has solicited comments from the public on "practical, technical, security, privacy, enforceability and other concerns" with respect to establishment of such a registry.
- Section 6(I) of the DIARRUCA requests comments from the public on the use of an "ADV" label in the subject line of non-adult commercial messages and further inquires whether senders could add additional information such as "ADV:Automobiles."
- Additionally §6(H)(3) and §(4) of the DIARRUCA request commentary on the issues of "analysis and recommendations concerning how to address commercial email that originates in or is transmitted through or to facilities or computers in other nations." and "options for protecting consumers, including children from the receipt and viewing of commercial email that is obscene or pornographic."

2 How to Submit Comments

Congress thinks the Do-Not-Mail list is great. Senator Schumer calls the list the last hope for consumers. The Chairman of the FTC has said this is your basic Bad Idea.TM [5]

To submit your comment electronically, go here:

http://www.regulations.gov/AGCY_FEDERALTRADECOMMISSION.cfm¹

You then have to scroll down to get to CAN-SPAM, then click on "Submit a Comment." That leads you to a snazzy form to fill out. You can skip the survey if you want and enter your comments directly in the text area, or you can attach a document.

Note: The author apologizes for not furnishing a direct link to the relevant proceeding. That is actually a Feature© not a Bug© at [Regulations.gov](http://www.regulations.gov)², the "e-gov" (sic) operation that the FTC outsources these functions to. There is no permanent URL for a given comment action and the search forms only support `method=POST`.

The reason for this appears to be because [regulations.gov](http://www.regulations.gov) is further outsourcing the comment sub-function to facilities located on the other shore at CommentWorksTM.com. Perhaps [regulations.gov](http://www.regulations.gov) is taking the "customer" analogy a bit too far, attempting to force consumers through the front door so they view all the pretty merchandise available. After all, somebody hurrying in to comment on some mundane trade regulation, might well succumb to an "impulse buy" and take the time to comment on a forthcoming environmental ruling.

In your comments, make sure to identify who you are and why your comments are relevant. For example:

- *Tell them who you are:* "I am the author of several Internet RFC's including [3], 'A Standard for the Transmission of IP Datagrams on Avian Carriers' which defines the fundamental characteristics used for electronic mail when transported over an infrastructure composed of avian carriers."
- *Tell them about any Bad ThingsTM:* "I believe a centralized do-not-email registry poses a significant security and privacy threat to consumers. I do not believe that mechanisms such as SHA-1-based one-way hash will provide adequate security for a centralized database and the non-standard use of labels in messages violates some key assumptions about the mail architecture as detailed in [17] and [18]."
- *Tell them about any Good ThingsTM:* "I believe a decentralized approach, such as that outlined in the IETF No-Soliciting Proposed Standard will provide greater benefit to consumers and provides a much better solution for the international environment in which electronic mail, particularly spam, functions."

Needless to say, use the language you feel is appropriate to express the views you hold. Just remember, you are speaking to a non-technical audience which is under a full-court press from some very eager contractors and is very anxious to be shown to be "doing something" about the problem.

¹ http://www.regulations.gov/AGCY_FEDERALTRADECOMMISSION.cfm

² <http://www.regulations.gov/>

3 No-Soliciting in a Nutshell

The No Soliciting SMTP Service Extension[16], a Proposed Standard, is being advanced by the author as an alternative to centralized, non-standardized approaches such as the do-not-email list and the use of labels on the subject line of a message. The extension does the following:

- Anybody can define a solicitation class keywords and attach meaning to them. Solicitation class keywords begin with your domain name in reverse order, followed by a colon, followed by arbitrary text. For example: `org.media:ADV:ADLT`. Solicitation class keywords can be up to 1000 characters long although, as with many things in life, brevity is better.
- A `Solicitation:` header is defined, which is available to the sender of a message to insert a solicitation class keyword.
- The `received:` header may be used by an Message Transfer Agent (MTA) to insert solicitation class keywords while the message is in transit.
- The `MAIL FROM` command in SMTP and responses may include solicitation class keywords.
- As a message recipient, you can filter on solicitation class keywords at either your message reader or your MTA, taking actions you feel are appropriate.

If the FTC wished to used this extension:

- They would define their solicitation class keywords. For example:
`gov.ftc:SEXUALLY-EXPLICIT-CONTENT`.
- The FTC could still require a label on the subject line if they feel that is necessary as a visual clue or for political reasons. But, with this extension they have choices and could instead/also require that information to be present in the body of the message as part of the "Brown Bag" requirement adopted by the Congress.
- The FTC might require any sender of a particular class of mail to use a `Solicitation:` header with the appropriate solicitation class keyword inserted.
- The FTC might also require high-volume senders of a particular class of mail to use the SMTP service extension.
- The FTC could concentrate on enforcement of violations instead of having to manage yet another large MIS project.

4 Background on the Centralized Do-Not-Email Registry

Metaphors can be as powerful as a herd of cattle upwind in late spring, but inappropriate metaphors can tempt lawmakers into using policies as mismatched to the problems they are trying to solve as a NASA Metro Map.[1]

In response to a public perception of widespread abuses by the telemarketing industry, the U.S. Congress passed legislation requiring the FTC and FCC to coordinate the establishment of a do-not-call list.[10] The FTC and FCC both issued regulations [11] [12] and those regulations were upheld by the U.S. Court of Appeals.[13]

The do-not-call program proved to be immensely popular, drawing a record number of registrants. Consumer surveys indicate that the program has been highly effective, reducing the number of unwanted calls dramatically. For example, a poll by Harris Interactive showed that "more than half of all adults (57%) say they have signed up and most of these people say they have either received no telemarketing calls since then (25%) or far less than before (53%)."[14]

The analogy between one highly successful program, the Do-Not-Call list, and the pressing public concern over spam was just too easy to make. If it works for telephone, why not for spam?

The analogy is flawed. The technologies are different. A simple illustration of the difference is the economics of what happens if the list gets out into the wild and some violator wishes to reach the people on the list. Assume a do-no-call list of 50 million numbers and an equivalent do-not-email list of electronic mail addresses:

- To reach the 50 million telephone consumers, a substantial investment in telemarketing equipment, personnel, and time is needed. Even if the average amount of time to reach a consumer and attempt to conduct a transaction is just one minute, the do-not-call list would require 833,333 hours of personnel time and telecommunications charges. At \$5/hour for people that's \$4,166,166 for labor. At \$0.05/minute for telecommunications, that's \$2,500,000 in telephone charges. And, these are only the variable costs.
- In sharp contrast, reaching 50 million consumers by electronic mail can be done in minutes, requires no capital investment, and there are numerous service providers who will send mail at a cost of approximately \$50 per million messages. The variable costs for reaching everybody on the do-not-spam list is \$2500, less than 1/5000th of the cost for the do-not-call list.

The economics is simple: this is a large financial disincentive to violate the do-not-call list. The returns would have to be very large to justify the risk. Spamming the do-not-spam list, on the other hand, has a low entry cost, requires a negligible return, and has low risk.

A do-not-email list would be impossible to secure. The list must be consulted by all legitimate marketers. And, as we've seen with DVDs distributed to members of the Academy of Motion Picture Arts and Sciences, distribution of secrets to a large population, no matter how august that population, is an inherently insecure activity.

The FTC, as part of the rule-making process, has issued a "Request for Information" (RFI) [8] in which contractors no doubt expended significant energy responding how they would protect the security of such a database. Unfortunately, requests for copies of those proposals by prospective contractors have not been released for public scrutiny due to "concerns about proprietary information," so it is not possible to point out the security flaws in any specific proposal (but see [Appendix A](#)).

In the RFI, the FTC expressed interest in a variety of proposals. The core do-not-email database was specified as having a capacity of 300 million electronic mail messages, and vendors had to price out solutions of up to 450 million entries. Three of the variants solicited by the FTC are noteworthy:

- A list that only has domain names and not individual electronic mail addresses. Such a list might work well for sophisticated users with their own domains, but would disenfranchise those users who use large Internet Service Providers such as Time Warner's AOL or Microsoft's MSN.
- A list that includes the addresses of telemarketers, flipping the onus to register from those who do not want email to those who sent the unwanted email. While this idea may seem clever, just imagine the burden this places on millions of individual mail users who would have to download the list frequently, and install mail

filters to match each of the addresses.

- One idea that has caught the imagination of some members of the press is the proposal by UNSPAM®, LLC (<http://www.unspam.com/>³), which bills itself as the "the no-spam registry experts" who are "paving the way towards a spam-free future." Their approach uses a one-way hash based on SHA-1. Their schtick is that means you can't read the list, but can only use it to verify an email address. There is a fundamental problem here. Finding email addresses is easy: you can use Google, build your own scraper, buy a list, or do a dictionary attack. The key to the global "spamonomy"—a term coined by noted author Danny Goodman in his forthcoming book analyzing spam, how it works, and how you can try to stop it²—is verifying that an email address is real and active. Wouldn't it be handy to have a single source you could use to scrub your lists to find out which addresses are valid? This is a really Bad Idea™.

We should note in passing that the RFI also includes provisions for charging consumers for the privilege of being included on the list.

A do-not-email list is not practical to secure, nor is it practical to run. It is a highly centralized solution requiring intense government supervision and large contracts to the private sector to operate the computers.

Most importantly, the centralized database does not take into account our international world. Most spam, even that originating from U.S. citizens, goes through facilities in many countries. It is hard to imagine the European Union and the U.S. agreeing how to merge separate do-not-email databases to provide a unified solution, let alone agree on what privacy standards should be imposed by such a large collection of individual information aggregated in one place.

In contrast, it is very possible to imagine both entities imposing labeling requirements that can coexist in a common header, much as food that crosses national boundary has labeling requirements imposed by multiple jurisdictions.

Why should a private citizen have to register with the federal government in order to be left alone? A large centralized database is a security threat, a privacy threat, and will do little to solve the problem. In contrast, a decentralized solution stands a chance of being adopted by different jurisdictions and is flexible enough to handle the wide variety of people who use electronic mail.

Finally, John Klensin has pointed out that even if the list was successful for the classes of mail it attempts to regulate, such a large volume of mail falls outside of those classes that any unilateral centralized solution is bound to fail:

"It might perhaps also be worth pointing out that, unlike the pre-'do-not-call' telemarketing situation, there is a high volume of nuisance spam today, traffic that has no obvious commercial purpose, since it does not contain any solicitation in any characters or language that the recipient can read. Whether that traffic is deliberate or accidental remains a matter of debate, but it almost all originates from offshore servers and would almost certainly be insensitive to 'do-not-email' lists."

³ <http://www.unspam.com/>

5 Background on Labels

Section 5(d) of the [CAN-SPAM Act](#) [15] directs the FTC, within 120 days of the promulgation of the act, to "prescribe ... clearly identifiable marks or notices to be included in or association with commercial e-mail that contains sexually explicit material." In a notice of rulemaking on this subject,[19] the mechanism proposed for such identification would be the insertion of the phrase `SEXUALLY-EXPLICIT-CONTENT`: as "the first 27 letters in the subject line."

In addition, in the DIARRUCA ANPR, the FTC solicited public comment on the use of "ADV", "ADV:ADLT" or similar marks in subject lines, which is the practice adopted by over a dozen state laws previous to the passage of the Can-Spam Act of 2003.

Placing marks on the subject line is a visual clue for a human being, but unfortunately the process is highly error-prone for computers. Even with a human being, the process is ambiguous:

- For a computer, embedding a label in the subject line makes it extremely difficult to reliably filter out unwanted mail. Even with a long label such as `SEXUALLY-EXPLICIT-CONTENT`, there will be collisions. The problem is that the subject line is overloaded: it has to do several different things including the primary task which is conveying the subject of the message in the sender's own words.
- For a consumer, the label is ambiguous. A long label can be confused with real content. And, the definition of short labels are extremely overloaded. For example, over a dozen states passed laws requiring "ADV" in the subject line. Which definition of "ADV" should we think applies to this message? And, what happens when, for example, Korea requires that the Han-gul equivalent be inserted at the beginning of a subject line?
- The purpose of a subject line is for a human being to enter words that convey the subject of the message. Using this for machine-based filtering is silly. A separate header makes much more sense.

An added bonus of using a special `Solicitation:` header is that the same format for solicitation class keywords can be used on on the `received:` headers which are inserted by the Message Transfer Agent. So, if spammers ignore the law about putting in solicitation headers, perhaps your MTA can help compensate by inserting the missing information in a trace field. Of course, it is up to you and your mail reader to decide if you trust that MTA's trace field and what actions to take.

Littering our mail headers with ad-hoc solutions destroys the integrity of the mail system. A more systematic solution will be both more flexible and more effective.

References

- [1] Tufte, E., "[Block That Metaphor! The NASA Space Exploration Map](http://www.edwardtufte.com/bboard/q-and-a-fetch-msg?msg_id=000012&topic_id=1)", <http://www.edwardtufte.com/bboard/q-and-a-fetch-msg?msg_id=000012&topic_id=1>, June 2003.
- [2] Goodman, D., "Be Efraid, Be Very Efraid", SelectBooks (forthcoming), ISBN 1-59079-063-4, 2004.
- [3] Waitzman, D., "[Standard for the transmission of IP datagrams on avian carriers](http://www.rfc.net/rfc1149.html)", RFC 1149, April 1990.
- [4] Howe, D., Ed., "[Free On-Line Dictionary of Computing](http://foldoc.doc.ic.ac.uk/foldoc/index.html)", <<http://foldoc.doc.ic.ac.uk/foldoc/index.html>>, October 2003.
- [5] CBS News, "[FTC: Canning Spam A Tough Chore](http://www.cbsnews.com/stories/2004/03/12/tech/main605558.shtml) ", <<http://www.cbsnews.com/stories/2004/03/12/tech/main605558.shtml>>, March 2004.
- [6] United States Congress, "[US Administrative Procedures Act, Section 553: Rule Making](http://www4.law.cornell.edu/uscode/5/553.html)", <<http://www4.law.cornell.edu/uscode/5/553.html>>, 15 U.S.C. 553, 1946.
- [7] US Federal Trade Commission, "[Definitions, Implementation, and Reporting Requirements Under the CAN-SPAM Act](http://www.ftc.gov/os/2004/03/040309canspamfrn.pdf)", <<http://www.ftc.gov/os/2004/03/040309canspamfrn.pdf>>, Advance Notice of Proposed Rulemaking, Project No. R4110008, RIN 3084-AA96, Billing Code 6750-01-P, March 2004.
- [8] US Federal Trade Commission, "[Request for Information: Federal Trade Commission's Plan for Establishing a National Do Not E-mail Registry](http://www.ftc.gov/ftc/oed/fmo/procure/040224donotemailrfi.pdf)", <<http://www.ftc.gov/ftc/oed/fmo/procure/040224donotemailrfi.pdf>>, February 2004.
- [9] United States Congress, "[The Freedom of Information Act As Amended By the Electronic Freedom of Information Act Amendments of 1996](http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm) ", <http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm>, Public Law 104-231, 110 STAT. 3048, 5 USC 552, October 1996.
- [10] United States Congress, "The Do-Not-Call Implementation Act", Public Law 108-10, 117 STAT. 557, March 2003.
- [11] US Federal Trade Commission, "[Telemarketing Sales Rule](http://www.ftc.gov/os/2000/02/telesalesrule16cfr310.htm)", <<http://www.ftc.gov/os/2000/02/telesalesrule16cfr310.htm>>, 16 CFR 310, January 2003.
- [12] US Federal Communications Commission, "[Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-153A1.pdf)", <http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-153A1.pdf>, FCC 03-153, June 2003.
- [13] U.S. Court of Appeals, Tenth Circuit, "[Mainstream Marketing v. Federal Trade Commission](http://www.ck10.uscourts.gov/opinions/03-1429.pdf)", <<http://www.ck10.uscourts.gov/opinions/03-1429.pdf>>, No. 03-1429, February 2004.
- [14] The Harris Poll, "[Do Not Call Registry Is Working Well](http://www.harrisinteractive.com/harris_poll/index.asp?PID=439) ", <http://www.harrisinteractive.com/harris_poll/index.asp?PID=439>, ISSN 0895-7983, February 2004.
- [15] United States Congress, "[The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 \(CAN-SPAM Act of 2003\)](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf)", <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf>, Public Law 108-187, 117 STAT. 2699, 15 USC 7701, December 2003.
- [16] Malamud, C., "[A No Soliciting SMTP Service Extension](http://trusted.resource.org/no-solicit/draft-malamud-no-soliciting-07.html)", <<http://trusted.resource.org/no-solicit/draft-malamud-no-soliciting-07.html>>, Internet-Draft draft-malamud-no-solicit-07, March 2004.
- [17] Klensin, J., "[Simple Mail Transfer Protocol](http://www.rfc.net/rfc2821.html)", RFC 2821, April 2001.
- [18] Resnick, P., "[Internet Message Format](http://www.rfc.net/rfc2822.html)", RFC 2822, April 2001.
- [19] US Federal Communications Commission, "[Notice of Proposed Rulemaking: Label for E-mail Messages Containing Sexually Oriented Material](http://www.ftc.gov/os/2004/01/canspamfrn.pdf)", <<http://www.ftc.gov/os/2004/01/canspamfrn.pdf>>, RIN 3084-AA96, 16 CFR Part 316, January 2004.

Author's Address

Carl Malamud

Memory Palace Press

PO Box 300

Sixes, OR 97476

US

E-Mail: carl@media.org

A FOIA Request for Responses to Do-Not-Email Contractor Solicitations

This FOIA request was submitted at [Wed Mar 17 14:10:25 PST 2004] to <<http://www.ftc.gov/cgi-bin/foia.pl>>.

March 21, 2004

Freedom of Information Act Request
Office of General Counsel
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Dear Sir/Madam:

This is a request under the Freedom of Information Act. I request that a copy of the following document(s) be provided to me: Copies of documents submitted in response to the February 23, 2004 Request For Information: Federal Trade Commission's Plan for Establishing a National Do Not E-mail Registry. The responses were sent to the attention of Mr. Daniel Salsburg, Federal Trade Commission, Division of Marketing Practices, 600 Pennsylvania Avenue N.W., Washington, D.C. 20580.

In order to help determine fees, you should know that I am an individual.

I am willing to pay fees up to \$200. If you expect the fees will exceed this, please contact me before proceeding.

I request a waiver of all fees for this request. Disclosure of the requested information to me is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in my commercial interest. Specifically, a national do-not-email registry is a matter of national policy and any proposed contractor-based implementations of such a registry raise numerous issues that the public should be able to examine, particularly in order to be able to submit comments requested by the FTC as part of the Advance Notice of Proposed Rulemaking, Project No. R411008, Definitions, Implementation, and Reporting Requirements Under the CAN-SPAM Act.

If you need to discuss this request, I can be reached at at <<mailto:carl@media.org>>.

Thank you for your consideration of my request.

Sincerely,

Carl Malamud
PO Box 300
Sixes, Oregon 97476

B Document Repository

The source for this document may be found at the following URL:

<<http://trusted.resource.org/no-solicit/response/>>

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Copyright (C) The Internet Society (2004). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC editor function is currently provided by the Internet Society.