Network Working Group
Request for Comments: 3098
FYI: 38
Category: Informational

T. Gavin
Nachman Hays Consulting
D. Eastlake 3rd
Motorola
S. Hambridge
Intel

April 2001

How to Advertise Responsibly Using E-Mail and Newsgroups or - how NOT to $$$$$ MAKE ENEMIES FAST! $$$$$

Status of this Memo

Copyright Notice

Abstract

This memo offers useful suggestions for responsible advertising techniques that can be used via the internet in an environment where the advertiser, recipients, and the Internet Community can coexist in a productive and mutually respectful fashion. Some measure of clarity will also be added to the definitions, dangers, and details inherent to Internet Marketing.

Table of Contents

1. Introduction

The Internet is not a free resource. Access to and a presence on the 'Net comes at a cost to the participants, the service provider, and the recipients of those services made available by the Internet. The more readily available internet has allowed users access to an unprecedented number of people. Due to the rapid growth and "mainstream" acceptance of the 'Net, new opportunities have been found for the distribution of information to the vast and ever-growing community of Internet users. There are groups and individuals who choose to use the 'Net for purposes for which it was not intended, thus defying the consensus among both the practitioners and the unwilling recipients. The aforementioned practice, of course, is the sending of Unsolicited Commercial and Bulk E-Mail messages, posts to Netnews groups, or other unsolicited electronic communication. This condition has caused an awakening on the part of the Internet community-at-large.

There are stereotypes that must be broken before continuing. Not all persons who are new to the Internet are ignorant of the 'Net's history and evolution, or its proper and ethical uses. Nor are all experienced, long-term Netizens against the use of the Internet for advertising, marketing, or other business purposes. Where these two groups can find commonality is in their opposition to the use of the Internet in irresponsible ways. Some of these irresponsible uses include, but are not limited to, the sending of Unsolicited Bulk or Commercial E-Mail to mailing lists, individuals, or netnews groups. In the vernacular, this activity is called "spamming" (the sending of "spam" [1]). To understand why such activities are irresponsible, one must first understand the true cost and ramifications of such actions.

The protocols and architecture upon which the 'Net is built, which are recognized and adhered to as standards, provide for an openness and availability which foster and encourage easy communication.

These standards were developed at a time when there was no need to consider the concept of "rejecting" information. While those standards have evolved, they continue to emphasize open communication. As such, they do not associate costs or impact with the user-initiated activities which may occur. Because of this openness, persons can and do send large volumes of E-Mail, with little-to-no cost or financial impact for the volume of messages sent. Needless to say, this presents the attractive option (to those who would consider such activity) of multiplying the recipients of their marketing material, and presumably, increasing their success-rate. However, and to reiterate an earlier statement in this text, there is a cost to be incurred at some point in this communication relationship. In the case of E-Mail advertising, since the cost of operation does not increase on the part of the sender, it must therefore increase on the side of the recipient.

And it does. Every recipient of every E-Mail message bears a cost, either direct (cost per message received, an incremental increase in connection charges) or indirect (higher service fees to recoup infrastructural costs associated with the additional 'Net traffic which such mass-mailings create). In addition, other resources, such as the disk space and time of the recipient, are consumed.

Because the recipients have no control over whether or not they will receive such messages, the aforementioned costs are realized involuntarily, and without consent. It is this condition (the absence of consent to bear the costs of receipt of a mass-distributed message) that has shaped the Internet Community's viewpoint - that the act of sending spam constitutes a willful theft of service, money, and/or resources. Those who choose to ignore the financial impact, and instead focus on the consumption of indirect resources, have been known to label spam "Internet Pollution".

The Internet provides a tremendous opportunity for businesses, both large and small. There is certainly money to be made using the 'Net as a resource. This paper recommends practices and ways to use the Internet in manners which are not parasitic; which will not, by their mere existence, engender predetermined opposition, litigation, or other negative conditions. This paper does not guarantee freedom from those, or other negative responses - rather, it provides the reader with a framework through which the marketer/advertiser and the 'Net community (and more importantly, the seller's target market) can coexist as well as possible.

2. Image and Perception of the Advertiser

While it may appear to be financially attractive to advertise via the use of Mass-Messaging ("spam"), as a responsible Internet user, ADVERTISERS SHOULD AVOID THIS OPTION. The possibility of income generation and market or business expansion are minuscule when compared to some of the risks:

- The alienation of the vast majority of the recipients of an advertising message [2][3]

- The damage or loss of credibility in the advertisers market [2]

- Loss in advertiser's and/or seller's Internet connectivity (most service providers have strict "zero tolerance" policies which prohibit the use of their systems for the sending of spam, or for encouraging or enabling such activities)

- Civil and Criminal litigation. In the United States, (and progressively in other sovereign states), it has become accepted as fact that the theft-of-service associated with spamming often constitutes an unlawful use of private property and is actionable as trespass to chattels (a civil law term tantamount to "theft") in civil court [4][5][6][7][8].

It is a fundamental tenet to any Internet presence that a party will be responsible for their Internet "image", or the personae that they create. If an advertiser sells a product which is enjoyed by many, and the advertiser has not alienated, offended or angered a disproportionately larger number of uninterested recipients, that advertiser could be viewed as a hero. Conversely, an advertiser broadcasting their product to millions of uninterested parties, at the parties' cost, will earn the advertiser the moniker of "spammer", thief, or other less attractive names. The advertiser will be held responsible for those actions, and the effects those actions have in the marketplace, which is to say, the 'Net community.

"On the Internet, nobody knows you're a dog." [9] That was the caption to an illustration published in the 1990's. The message is clear - the Internet renders all parties anonymous. The methods used to sell products in the traditional sales channels - language, image, relationships, eye contact or body language - no longer apply when measuring an Internet sale. Reputation, reliability, honesty, trustworthiness, and integrity have taken the place of the more

direct sales approaches that have been previously used. These are dictated by the rate at which both information and misinformation travel on the Internet. And, just as an Internet user cannot control what messages are sent to them, neither can the Internet marketer control the information that is disseminated about them, or their activities. Some information will circulate that is not accurate. Perhaps there will be cases where there will be information circulating which is downright incorrect. But, a successful market reputation, based on ethical behavior, will render the inevitable piece of misinformation meaningless. For an advertiser to exist responsibly on the Internet is for the advertiser and seller to take active responsibility for their actions.

3. Collateral Damage

As this paper has pointed out, there is ample reason to expect that the sending of spam will result in a significant level of undesirable reactions, targeted at the advertiser and/or the seller. Death threats, litigation and retaliatory actions are commonplace. For these reasons, "spammers" (and in particular, those entities providing mass-mailing services for third-party businesses) will frequently take steps to ensure their anonymity. These actions take various forms, and have been known to include:

- Forging the sender name, domain name, or IP Address of the sender (called "spoofing")

- Sending messages through any type of hardware, software or system which belongs to an uninvolved third-party (called "relaying")

Each of these activities, as well as numerous others, are criminal acts in many countries. It is unethical to use the resources of any other party without their express permission. To do so breaches the laws of numerous jurisdictions and international agreements - offenders have been successfully prosecuted in numerous jurisdictions.

4. Caveat Mercator

"Let the Seller beware." Advertisers and Sellers can be held responsible for the appropriateness (or lack thereof) of the messages they send when applied to the recipients to whom the advertisements are sent. For this reason, all prospective advertisers must first be absolutely certain that the recipients of their advertising are appropriate. For example, sending an advertisement which contains a link to a website where content of an overt sexual nature is displayed can have many undesirable consequences:

- In many countries, providing such material to under-age minors is a crime. As the provider of the link, the advertiser's position is tenuous.

- In some countries, such material is a crime to view, possess, or distribute ("trafficking"). As the website owner or advertiser, a party engaging in such activities must consider the ramifications of international law.

To prevent such risk, advertisers should qualify the recipients of their advertising. However, it must be noted that E-Mail addresses provide little useful information to that end. Remember, "On the Internet, nobody knows you're a dog." Advertisers will have no way to qualify a prospective recipient as an adult with complete discretionary and plenipotentiary authority. In other words, an advertisement targeting a high-income population in need of property investment opportunities may be sent to a group of school children. Or a dog.

How then, does the prospective advertiser/seller determine the quality of their leads? The essential requirement is that the advertiser "know" their audience.

As with all sales leads, the ones which are developed and generated by the advertiser who will use them are of the most value. There is an inherent value to collecting the data first-hand; by collecting the data directly from the prospective recipient, the advertiser can accomplish two important goals:

- The advertiser ensures that the recipient is genuinely interested in receiving information. Thus, the advertiser can protect themselves from the negative impact of sending Unsolicited E-Mail ("spam").

- The advertiser maintains the ability to "pre-qualify" the lead. One interested lead is worth more, from a sales and marketing perspective, than millions of actively uninterested potential recipients.

If an advertiser maintains an active website or uses other mass-marketing tools (such as direct-mail), and they are interested in pursuing Internet Advertising, the advertiser can add a mechanism to gather sales lead data in a relatively simple manner. From the perspective of Responsible Use, the only such mechanism to be discussed in this text will be the "Opt-In" concept, to be discussed in detail later in this document.

Regardless of the manner in which the information is gathered, there are certain steps which the advertiser must follow. The advertiser must inform the person that data is being collected. In addition, the reason why the information is being collected must be clearly stated. BE AWARE! There are jurisdictions which restrict the collection of Personal Data. The laws addressing collection and future handling of Personal Information will vary from place to place; advertisers must take steps to gain an understanding of those laws.

Prudence should be the advertiser's guide. If an advertiser is unsure as to the applicability or legality of an action, both in the jurisdiction of the advertiser as well as that of the recipients, the action must be avoided entirely. Advertisers would be well advised to realize that, if they engage in spamming, they will inevitably break the laws of some jurisdiction, somewhere.

5. Targeting the Audience

Advertisers have something to sell. It may be a product, service, or other tangible or intangible item. And, of course, the advertiser needs to get the word out to the market - quickly. After all, neither the seller or the advertiser are making sales and earning profits if nobody is buying the product. However, before advertisers can advertise the product, they must first determine to WHOM the product will be advertised.

There are considerations in determining the answer to that question. This text has already addressed how the sending of Unsolicited Commercial E-Mail ("spam") can generate a number of negative effects. In addition, numerous surveys cited herein show that the vast majority of publicly-available mailing lists and Netnews groups similarly abhor spam. The advertiser's first step should always be to determine which avenues are appropriate for advertising. Then, advertisers must determine which avenues are appropriate for EACH SPECIFIC ADVERTISEMENT. Advertisers are faced with the task of determining which Netnews groups accept ads, then of those, which groups are of a topic to which the proposed advertising is relevant. Similarly, the same work should be done for mailing lists. Advertisers should take some level of comfort in the fact that there *are* Netnews groups and mailing lists which welcome advertising - finding them is a worthwhile investment of the advertiser's time and resources.

For assistance in locating such advertising-friendly websites, mailing lists, and Netnews groups, advertisers can consult existing ethical and responsible Internet advertisers. Alternatively, any low- or no-cost research resource or search engine can be employed to

find those groups and lists. BUT UNDER NO CIRCUMSTANCES SHOULD AN ADVERTISER PURCHASE A MAILING LIST AND START MAILING! There are other reasons which will be addressed further into this document, but to engage in such activity opens the advertiser to the liabilities and negative ramifications previously stated. Such negative conditions cause increased costs to the seller/advertiser, when the risks (loss of connectivity, defense against litigation, avoiding discovery, etc...) are factored into an advertiser's overall operation. In short, it is in the best interests of the seller and advertiser to ensure that the proper audience is targeted, prior to any further steps.

6. Reaching the audience

Once the prospective advertiser has determined a target market for a specific advertisement, a manner of advertising must be selected. While these are too numerous to mention, this document concerns itself only with those that apply to the ethical use of Internet resources. Of those, the pertinent ones to be examined (in order of desirability and effectiveness) are:

- A dedicated website or web page
- Advertisement placed on a "shared" advertising site (placing an advertisement on an established web-page which caters to people that indicate a potential for interest in (a) specific type(s) of product(s). Such advertisements can take the form of text, links,

  "Click-Through Banners", or other.
- Netnews posting
- Targeted E-Mail messages

Note that any manner of blind broadcast (distribution-based) advertising which does not involve the targeting of the recipients is not considered responsible.

Once the advertiser has determined the medium for reaching their target audience, there are key points to be considered, each being specific to the medium of advertisement:

A. Dedicated website or web page

Advertisers have the option of creating a dedicated website, or a page within another site for their advertisement. If, from a technical standpoint, an advertiser is unsure of the process for

creating such a website, there are numerous resources available to provide assistance. From no-cost avenues such as instructional websites; to low-cost resources such as books, videotapes or classes; to full-service businesses and consultants who can advise advertisers throughout the entire scope of the website/web page design, implementation and hosting process (or any part thereof), there is a solution available for every type of site and cost-structure.

B. "Shared" Advertising website

Advertisers have the option of placing their advertisements on a website operated by a third-party. For advertisers with an immediate need, such sites (also called "Electronic Malls", "E-Shops" or other names) have several advantages. In some cases, a shared site can be more cost-efficient than building a dedicated website. Many sites will target a specific market (refer to Section 5 of this document). By using existing resources, advertisers can avoid the cost and burden of owning their own site. Many websites will target a specific advertisement to a specific audience, thus providing much of the research for the prospective advertiser, and providing the advertiser the means with which to reach the most receptive audience. Additionally, advertisements from such advertising sites can be integrated into a larger context, such as supporting free e-mail services, Internet access, or news broadcasts. Such integration can lend a level of credibility to an advertising effort that might not exist otherwise.

Some notes on the use of any type of website for advertising:

Regardless of what method an advertiser chooses to use for for advertising on the Web, there are some specific caveats regarding customer interactions:

First, the advertiser must ensure that their contact information - name, phone, e-mail address - are all clear and available;

Second, advertisers should take care in creating forms which gather information about customers, as there is concern in the United States and other countries about gathering information from minors without parental consent. There is also concern about grabbing dynamic information via persistent state information, such as through the use of "cookies" or through data collection software resident on the user’s computer without their knowledge.

Information should only ever be gathered in a voluntary and informed fashion, as opposed to the use of cookies, forms, or other methods that may be available;

Third, if advertisers DO gather information about people and plan to use it for marketing in ANY way, advertisers must be VERY clear to specify their plans as people submit their information.

C. Netnews and E-Mailing list group postings

If an advertiser has selected newsgroups as a targeted medium, there are critical preliminary determinations to be made. The accepted presumption should be that a Netnews group will not welcome spam, although there are newsgroups which are advertising-friendly. However, the only way to determine whether a group welcomes a particular type or form of advertising is to either:

- read the Frequently Asked Questions (FAQ) to determine what is specifically permitted or prohibited on that particular group.

  or

- ask the group by posting a message which briefly notes how you intend to advertise your product. Do not mention any product details in this message, merely ask if the group would object.

  or

- if it is a "moderated" newsgroup, send an e-mail to the group's moderator. Many group moderators will have a specific preference for how to deal with advertising, through compilation, "digest" formats, or other.

It is a recommendation that prospective advertisers read the groups to which they choose to post for a period before posting. Generally, an extended period of reading the messages in the group will give the advertiser an indication as to how their advertisement will be viewed or accepted on the group in question.

However, this period of reading should not be used as a substitute for the suggestions above. Many groups will have specific instructions and/or requirements for posting

advertisements. Advertisers who fail to meet those requirements will be undertaking irresponsible behavior, and will be subject to the effects thereof.

D. Compiled E-Mail Lists

It bears repeating at this point: Let the Seller Beware. The material discussed in Section 4 of this document is particularly relevant in the consideration of E-mail, and the use of compiled lists of e-mail addresses for advertising. Advertisers should understand that they bear the responsibility for ensuring the proper targeting of their recipients; the proper display of their or their seller's identities; and the use of resources or systems only with the express permission of the owners of those systems.

When faced with the task of collecting and compiling recipient information, one option that is frequently presented is that of pre-compiled mailing lists. Most often, these are advertised using the very method which is irresponsible, that of Unsolicited E-Mail. There are numerous reasons why these lists should not be used.

Many suppliers create mailing lists from addresses which they have gathered in mildly to extremely unethical ways. Many of these list-makers rely on grabbing volumes of addresses without checking their legitimacy. In other words, they send out software robots to grab addresses they find in News or Mailing List archives which may be many years old! In addition, many list owners create addresses using a "dictionary", creating vast numbers of invalid addresses which are then sold to unsuspecting purchasers. People change jobs, change ISPs, and change everything about themselves over time; trusting a third party for a mailing list is just not wise.

It is known that some mailing list providers have created mailing lists from E-mail addresses of people who have asked to be REMOVED from their mailing lists. They then sell these lists to other advertisers who think they're getting a list of people who will welcome the unsolicited information.

Regardless of the source, however, advertisers and sellers bear the responsibility for maintenance of their lists. Purchasing a list from a third-party shifts the maintenance costs of that list onto the advertiser who uses it. Needless to say, this is only economical for mailing list vendor.

Given these conditions, all evidence points to the fact that the greatest level of control of an advertiser's own success and liability rests with the advertiser themselves. This being the case, advertisers are faced with the task of compiling their own lists of willing recipients of Advertising-related E-Mail messages. As discussed previously, those leads which are generated by the advertiser are the most likely to have an interest in the advertisement, so they are also the least likely to protest the receipt of such advertisements via E-Mail. It is this circumstance that makes the use of an "Opt-In" list (refer to Section 7 of this text) to be perhaps the most successful method of advertising distribution on the Internet.

It must be noted here - for the same reasons that apply above, if an advertiser has compiled their own mailing list for their purposes, that list must NEVER be sold to another party. Just as it is considered unethical to purchase a third-party mailing list, it is equally so to be the provider of that list. Customers who wish to receive information about your product are not likely to respond favorably when contacted in an unsolicited fashion by your business associates; protect your reputation from the backlash of bad-faith that can occur in such cases.

7. Opt-In Mailing Lists

This document has laid out the basic facts of Internet Marketing; the advertiser bears the responsibility of their actions; there will always be recipients of that advertising who do not wish to receive it; there are reactions to every responsible and irresponsible act. Given these considerations, and taking into account the central message of this document; that Internet Advertising *can* be a successful venture for everyone involved; there remains a key tool for the Internet advertiser to harness. Opt-In mailing lists provide the prospective Internet advertiser with the control they need over the list of their prospective target audience (validity of e-mail address; applicability to the intended product; willingness to receive advertising via e-mail).

Opt-In mailing lists are consistently shown to be more effective in starting and maintaining customer relationships than any other type of Internet advertising; studies have shown Opt-In mailing to be Eighteen (18%) Percent more effective than Banner advertising [10], which has a response rate of only 0.65%. It is so successful because the recipients of those E-mailed advertisements made a specific effort to receive them, thus indicating their interest in receiving information about products which the recipient felt were of interest to themselves.

Advertisers wishing to employ Opt-In mailing lists in their advertising can turn to several resources for assistance. If an advertiser operates their own website or web page, they already possess the most important facet, a web presence with which to invite participation in the Opt-In list. If the advertiser chooses to use a shared website for their product, they can also utilize an Opt-In data gathering mechanism. There are numerous forms and technologies that can be employed to build an Opt-In list - this document will not address them individually. Rather, the purpose of this section is to provide the advertiser with information which, when used, will help protect the advertiser, and make the advertising experience a successful one.

A. Privacy

As stated previously, advertisers should take care in gathering information from Opt-In participants. First and foremost, the person providing the information must be aware that they are doing so. By taking these preliminary steps, an advertiser decreases the risk of having any messages interpreted as spam. If, in submitting information for any purpose, the advertiser intends to use the submitted or inferred data for any mailings, there should be clear language indicating so. Furthermore, persons submitting data must be given the choice to "Opt-Out"; that is, to choose to submit the data but NOT receive any advertisements. A safe course of action is for the advertiser to configure their data-gathering so "Opt-Out" is the default; that is, to ensure that any members of the list have made a concerted effort to get onto said list. In nearly all cases, merely having a "check-box" available with the caption

> "Please send me E-Mail advertisements or announcements about your products."

is sufficient.

It is crucial that advertisers be aware that different jurisdictions deal with the collection of personal data differently - the burden of verification of these laws rests on the advertisers. For additional information on privacy, refer to Appendix B of this document.

B. Integrity

When maintaining a list where names can be submitted via some type of public or semi-public resource, such as a website, advertisers should take steps to verify every subscription to

that list. There are key pieces of data that can be used to verify the integrity of a particular subscription request, but the only person who can attest to the genuineness of the actual act of subscribing is the owner of the E-Mail address which has been submitted.

To protect themselves from the risk of inadvertently spamming an unsuspecting recipient, advertisers should immediately confirm any submission. In doing so, advertisers can satisfy all requirements for responsible confirmation of a subscription request. In addition, if a person's E-Mail address has been submitted to a list without the knowledge or permission of the owner of that E-mail address, immediate notification of that, and the receipt of supporting data, enables the owner of that account to act accordingly to protect their account from future wrongdoing.

When generating confirmations, the following information must be provided to the subscriber:

- the E-Mail address subscribed
- the manner in which it was subscribed (website or mailing list address)
- the Date and Time of the subscription request (via NTP, for uniformity in future reference)
- the IP Address of the host which submitted the request
- the full headers of the subscription request (where applicable, such as mailing lists)
- the Name, website address, and contact E-Mail address of the advertiser
- instructions to the recipient as to how to permanently remove themselves from the list

In addition, a well-represented business will make an effort to communicate this material in a way which the average recipient can understand and relate to, such as the following example [11]:

- - - - - - C O N F I R M A T I O N - - - - - - - - - - - -

Thank you for your interest in Widget Sales!

This is confirmation of your subscription request for the Widget Sales E-mail list.

You are currently subscribed with this address:

foo@bar.example

Your request was received via our website at

http://www.example.com/input.html

If you did not submit this request, someone may have submitted it for you, or may be pretending to be you.

If you wish to be removed from this list, Reply to this message with the word UNSUBSCRIBE as the body of the message.

If you feel you were added to the list without your permission, the information below should be forwarded to your ISP's Administrative staff for follow-up, with an explanation of your concern.

As stated in RFC-2635, "you can do this by sending mail to "Postmaster@your-site.example". Your postmaster should be an expert at reading mail headers and will be able to tell if the originating address is forged. He or she may be able to pinpoint the real culprit and help close down the site. If your postmaster wants to know about unsolicited mail, be sure s/he gets a copy, including headers. You will need to find out the local policy and comply."

```
Widget Sales, Inc.            |      http://www.example.com
Responsible Internet          |            info@example.com
Marketing - Made Easy!        |       cust-serv@example.com
--------------------------------------------------------------
```

Submission Information:

Request received for foo@bar.example from 192.168.0.1 at 06:41:55:13(GMT) on 07.03.1999 via

http://www.example.com/input.html

E-Mail headers follow:

```
Received: from 01.anytown.dialup.example.net
   ([192.168.0.1]) by adshost.example.com
   (FooBarMail v01.01.01.01 111-111) with SMTP
   id <19990703054206.VDQL6023@77.anytown.dialup.example.net>
   for <marcel@example.com>; Sat, 3 July 1999 01:41:55 +0000
From: Customer <foo@bar.example>
To: mail-list@example.com
Subject: Submission Request
Date: Sat, 03 July 1999 01:41:55 -0400
Organization: Zem & Zem Bedding Company, Inc.
Reply-To: foo@bar.example
Message-ID: <k???12qelNxp7Q=??3dbgLHWTLv@4??.bar.example>
X-Mailer: FooBarMail HTTPMailer Extension 1.0.532
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: quoted-printable
```

C. Protection

Advertisers should be advised of certain measures they can take to protect themselves. Frequently, and especially when the traffic on a particular mailing list is low, a subscriber may forget that they had requested membership on that list. When a new message is sent and subsequently received, said recipient may lodge a complaint of spamming. If this situation is multiplied by several recipients, the advertiser and/or seller risks losing their Internet access, even if they have acted responsibly throughout the process.

For this reason, advertisers should keep an archive of all submission requests which are received. This archive should be kept as diligently as the advertiser’s operational data, and should be similarly safeguarded. Having such requests available will protect the advertisers from any reports of spamming, whether they are malicious, or the result of a genuine misunderstanding. For reasons that should be obvious, those messages should remain archived for a period that lasts AT LEAST as long as the list remains active. While this is not necessarily a requirement for responsible behavior, it is a measure of safety for the responsible advertiser.

8. Irresponsible Behavior

Shotgunning a message doesn’t really work in any medium, but it is much easier to do with the Internet than with paper mail or telephone solicitations. The steps which have been provided in this paper will

assist the advertiser in creating a favorable environment for their work; in ensuring that they maintain a responsible presence on the Internet; and in targeting the types of customer and the methods to be used to reach those potential customers. Given these steps, there are some actions which should be avoided as the basis for any Responsible advertising presence on the Internet.

DON'T advertise money-making opportunities that can, in any way, be construed as Pyramid or Ponzi schemes. (For information regarding those types of "investments", refer to Appendix A.1 of this document.)

DON'T forge E-mail headers to make it look as if the messages originate from anywhere other than where they really originate. Many domain owners have won litigation against advertisers who have used their domain name in an effort to conceal their true identity. [12][13][14]

DON'T send out any sort of bogus message to "cover" the intended activity, which is advertising. In other words, don't pretend that a personal message from the advertiser to someone else was sent to a mailing list by mistake so that the body of that message can be used to advertise, as in this example:

> Dear Tony - had a great time at lunch yesterday. Per your request, here's the information on the latest widget I promised [...].

DON'T use overly-general statements such as "Our research shows you're interested in our product." Most recipients know this is usually a bogus claim. Use of it can rob any legitimacy that the advertisement may hold.

DON'T create mailing lists from third party sources (see Section 6; Part D of this document, above).

DON'T SELL MAILING LISTS!!!

Enough negativity! Now for some helpful suggestions.

9. Responsible Behavior

DO create a lively signature which tells the minimum about the product/service. But keep it to 4 lines total (four lines is the maximum recommended length for signatures).

DO participate in mailing lists and newsgroups which discuss topics related to the particular product/service. Advertisers will find people of a similar interest there and many potential customers. So long as an advertiser isn't offensive in their interactions with these groups they can find their participation quite rewarding.

DO ask people if they want to be part of any mailing list that is created. Advertisers must be clear about their intentions of how they plan to use the list and any other information that is collected.

DO tell people how list data has been gathered. If recipients are signed up from a web page, make sure the prospective recipient is aware that they will be getting mail. Many web pages have getting mail selected as default. Our recommendation is that the default be that recipients do NOT wish to receive mailings - even if the prospective recipients find an advertiser's site of interest.

DO respect the privacy of customers. Keep a mailing list private. For an advertiser to sell a mailing list is not responsible or ethical. In addition, if offering any type of online transactions, advertisers should take care to encrypt any sensitive information The addresses of the list members should never be viewable by the list recipients, to protect your list members' privacy.

DO take steps to safeguard all of the personal information that is being taken from customers, such as Credit Card or other Payment information. Provide honest information regarding the methods being used to protect the customer's data.

DO let recipients know how to remove themselves from a mailing list. Advertisers should make this as easy as possible, and place the instructions in every message sent.

DO let people know for what purpose any data is being collected. Advertisers must ensure that their plans regarding data collection are legal.

Advertisers and Sellers can check with the web site of the Better Business Bureau, which operates in the United States and Canada. (www.bbb.org) This organization has several programs and services which can help advertisers in those countries, and has other resources which will benefit advertisers of any nationality.

"Advertisers should advertise responsibly the better mousetrap they have built, and the world will beat a path to their E-mail address."

10. Security Considerations

This memo offers suggestions for responsible advertising techniques that can be used via the Internet. It does not raise or address security issues, but special attention should be paid to the section on "Privacy". While not strictly a network security consideration, privacy considerations can have legal ramifications that deserve special attention.

Appendices

Most readers of this document are probably aware as to why "Pyramid" or "Ponzi" schemes are fraudulent, and in most places, criminal. Appendix "A" describes how these schemes work and some of the risks inherent in their operation and participation.

For a topical review of Privacy law across multiple jurisdictions, including several sovereign nations, Appendix "B" provides some resources for advertisers or other interested parties.

A.1 The classic Pyramid

In the classic Pyramid scheme, there is a list of a few people. A participant sends money to one or all of them, and then shifts that person off the list and adds their own name. The participant then sends the same message to N people....

The idea is that when a recipient’s name gets to the special place on the list (usually at the "top" of the pyramid), they will get lots of money. The problem is that this only works for everyone if there are an infinite number of people available.

As an example, examine a message with a list of four people where each participant sends US$5.00 to each; removes the first name, and adds their own name at the bottom. There may also be some content encouraging the participants to send "reports" to people who submit money. Presume the rules encourage the participants to send out lots of copies until they each get ten direct responses, 100 second level responses, etc., and claim there is a guarantee that the participants will earn lots of money fast if they follow the procedure.

First, some person or group has to have started this. When they did, they were able to specify all four names so it was probably four people working together to split any profits they might get from being the top of the pyramid (or maybe they sent out four versions of the original letter with their name order rotated). In some cases, all names on the list have been proven to be the same person, operating under assumed business names!

While the letters that accompany these things usually have all kinds of language about following the instructions exactly, the most rational thing for a dishonest participant to do if they decided to participate in such a thing would be to;

(1) send no money to anyone else; and

(2) find three other people and replace all the names on the list.

But, presume that not just this participant, but everyone who ever participates decides to follow the "rules". To avoid the start-up transient, assume that it starts with one name on the list and for the next three layers of people, one name gets added and only after the list is up to four does any participant start dropping the "top" name.

What does this look like after nine levels if everything works perfectly? The following table shows, for nine levels, how many people have to participate, what each person pays out, gets in, and nets.

Level	People	Out	In	Net
1	1	0	$55,550	$55,550
2	10	$5	$55,550	$55,545
3	100	$10	$55,550	$55,540
4	1,000	$15	$55,550	$55,535
5	10,000	$20	$55,550	$55,530
6	100,000	$20	$5,550	$5,530
7	1,000,000	$20	$550	$530
8	10,000,000	$20	$50	$30
9	100,000,000	$20	0	-20

So if this scheme ever progressed this far (which is extremely unlikely) over 10,000 people would have made the "guaranteed" $50,000. In order to do that, one hundred million people (or over ten thousand times as many) are out twenty dollars. And it can’t continue because the scheme is running out of people. Level 10 would take one billion people, all of whom have $20 to submit, which probably don’t exist. Level 11 would take ten billion, more people than exist on the earth.

Pyramid schemes are _always_ like this. A few people who start them may make money, only because the vast majority lose money. People who participate and expect to make any money, except possibly those who start it, are being defrauded; for this reason, such schemes are illegal in many countries.

A.2 What about Ponzi?

A Ponzi scheme is very similar to a pyramid except that all of the money goes through a single location. This method of confidence fraud is named after Charles Ponzi, a Boston, Massachusetts "businessman" who claimed to have discovered a way to earn huge returns on money by buying international postal reply coupons and redeeming them in postage for more than their cost. Early "investors" in this scheme did get their promised return on investment, but with money that later investors were investing. Ponzi was actually doing nothing with the money other than deriving his own income from it, and paying latter investors' money to earlier investors.

Notice the similarity to early pyramid participants, who "earn" money from the later participants.

Just as pyramids always collapse, Ponzi schemes always collapse also, when the new people and new money run out. This can have serious consequences. People in Albania died and much of that country's savings were squandered when huge Ponzi schemes that "seemed" to be partly backed by the government collapsed.

A.3 So all multi-levels are evil?

No, all multi-level systems are not the same, nor are they all "evil".

If what is moving around is just money and maybe "reports" or the like that are very cheap to produce, then almost certainly it is a criminal scam. If there are substantial goods and/or services being sold through a networked tier-system at reasonable prices, it is more likely to be legitimate.

If the advertisement says participants can make money "fast", "easy" or "guaranteed", be very suspicious. If it says participants may be able to make money by putting in lots of hard work over many months but there is no guarantee, then it may be legitimate. As always, if it seems "too good to be true", it probably is.

If people are paid to recruit "members" or can "buy" a high "level", it is almost certainly a criminal scam. If people are paid only for the sale of substantial goods and/or services, it is more likely to be legitimate.

It may also be worthwhile to look at the history of the organization and its founders/leaders. The longer it has been around, the more likely it is to continue being around. If its founders or leaders have a history of fraud or crime, a person should think very carefully before being part of it.

B.1 Why Web Privacy?

Directories, lists or other collection sources of personal data are the current informational "gold rush" for Internet Marketers. In the United States and other countries, there is no explicit guarantee of personal privacy. Such a right, under current legislation, stands little chance against certain electronic technologies. Some members of the global community have expressed concern regarding perceived intrusion into their personal privacy. Still, the collection and sale of such information abounds.

Self-regulation by businesses utilizing the Internet is the first choice of legislators, commercial websites, and Internet aficionados.

However, the anticipated profit to be made by selling personal data and by using these lists for advertisement purposes, often dissuades self-regulation.

United States Senator Patrick Leahy, Ranking Minority member of the Judiciary Committee of the United States Senate (at the time of the writing of this document) states very succinctly why we should respect Internet Privacy:

> "Good privacy policies make good business policies. New technologies bring with them new opportunities, both for the businesses that develop and market them, and for consumers. It does not do anyone any good for consumers to hesitate to use any particular technology because they have concerns over privacy. That is why I believe that good privacy policies make good business policies."

The Center for Democracy and Technology suggests Five Conditions that websites should use to be considerate of individual’s rights to privacy:

- Notice of Data Collection
- Choice to Opt Out
- Access to Data to rectify errors
- Adequate Security of Information Database
- Access to contact persons representing the data collector

Notice that the practice of data collection authorization can be accomplished using something as simple as an automated response E-Mail message. Such notices should contain easily understood information about the collecting party's identity, and instructions as to how a customer can remove themselves from the collected population. This will help assure prospective customers that an advertiser is a business of integrity.

Businesses that pursue international trade (do business across national boundaries, overseas, etc...) bear the risk of facing legal prosecution for personal privacy violations. The European Communities have legislation for the flow of Personal Information. If an advertiser is interested in pursuing business interests across borders, and particularly if a business intends to solicit and/or share Personal Information, the advertiser/seller must be able to guarantee the same privacy considerations as a foreign counterpart, or as a business operating in the nation in which the advertiser is soliciting/performing their business.

Other countries and their legislation are shown below:

Germany	-	BundesDatenSchutzGesetz (BDSG)
France	-	Commision nationale de l'informatique et de libertes (CNIL)
UK	-	Data Protection Act (DPA)
Netherlands	-	Wet PersoonsRegistraties (WPR)
Australia	-	Privacy Act of 1998 (OECD DAta Protection Guidelines)
Canada	-	The Personal Information Protection and Electronic Documents Act

References

[1] Hambridge, S. and A. Lunde, "DON'T SPEW: A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*)", FYI 35, RFC 2635, June 1999.

[2] Internet Spam / UCE Survey #1. http://www.survey.net/spam1r.html, July 24, 1997.

[3] ISPs and Spam: the impact of spam on customer retention and acquisition. Gartner Group, San Jose, CA. June 14, 1999. Pg. 7.

[4] CompuServe Inc. v. Cyber Promotions, Inc., No. C2-96-1070 (S.D. Ohio Oct. 24, 1996) (temporary restraining order) [WWW], preliminary injunction entered, 962 F. Supp. 1015 (S.D. Ohio Feb. 3, 1997) [WWW | Lexis | Westlaw], final consent order filed (E.D. Pa. May 9, 1997)[WWW].

http://www.leepfrog.com/E-Law/Cases/CompuServe_v_Cyber_Promo.html
http://www.jmls.edu/cyber/cases/cs-cp2.html
http://www.jmls.edu/cyber/cases/cs-cp3.html

[5] America Online, Inc. v. Cyber Promotions, Inc., No. 96-462 (E.D. Va. complaint filed Apr. 8, 1996) [WWW] (subsequently consolidated with Cyber Promotions' action filed in E.D. Pa.).

[6] Cyber Promotions, Inc. v. America Online, Inc., C.A. No. 96-2486, 1996 WL 565818 (E.D. Pa. Sept. 5, 1996) (temporary restraining order) [WWW | Westlaw], rev'd (3d Cir. Sept. 20, 1996), partial summary judgment granted, 948 F. Supp. 436 (E.D. Pa. Nov. 4, 1996) (on First Amendment issues) [WWW | Lexis | Westlaw], reconsideration denied, 948 F. Supp. 436, 447 (Dec. 20, 1996) [WWW | Lexis | Westlaw], temporary restraining order denied, 948 F. Supp. 456 (E.D. Pa. Nov. 26, 1996) (on antitrust claim) [WWW | Lexis | Westlaw], settlement entered (E.D. Pa. Feb. 4, 1997) [NEWS.COM report].

[7] America Online, Inc. v. Over the Air Equipment, Inc. (E.D. Va. complaint filed Oct. 2, 1997) [WWW] [NEWS.COM report], preliminary injunction entered (Oct. 31, 1997) [NEWS.COM report], settlement order entered (Dec. 18, 1997) [Wired News report].

[8] America Online, Inc. v. Prime Data Worldnet Systems (E.D. Va. complaint filed Oct. 17, 1997) [WWW] [NEWS.COM report].

[9] Steiner, P. "New Yorker". July 5, 1993. p.61.

[10] Spam slam -- opt-in e-mail gains favor.
http://www.zdnet.com/zdnn/stories/news/0,4586,2267565,00.html.
May 28, 1999.

[11] Eastlake, D., Manros, C. and E. Raymond, "Etymology of 'Foo'",
RFC 3092, April 2001.

[12] Parker, Zilker Internet Park, Inc., Parker, Rauch, Texas
Internet Service Providers Association & EFF-Austin v. C.N.
Enterprises & Craig Nowak [WWW]. Available:
http://www.rahul.net/falk/zilkerjudge.txt

[13] Parker, Zilker Internet Park, Inc., Parker, Rauch, Texas
Internet Service Providers Association & EFF-Austin v. C.N.
Enterprises & Craig Nowak [WWW]. Available:
http://www.jmls.edu/cyber/cases/flowers3.html

[14] WebSystems v. Cyberpromotions, Inc and Sanford Wallace [WWW].
Available: http://www.jmls.edu/cyber/cases/websys1.html

Authors' Addresses

Ted Gavin
Nachman Hays Consulting, Inc.
822 Montgomery Avenue, Suite 204
Narberth, PA 19072 USA

EMail: tedgavin@newsguy.com

Donald E. Eastlake 3rd
Motorola
155 Beaver Street
Milford, MA 01757

EMail: Donald.Eastlake@motorola.com

Sally Hambridge
Intel Corp
2200 Mission College Blvd
Santa Clara, CA 95052

EMail: sallyh@ludwig.sc.intel.com

Acknowledgements and Significant Contributors

JC Dill
jcdill@vo.cnchost.com

Barbara Jennings
Sandia National Laboratories

Albert Lunde
Northwestern University

April Marine
Internet Engines, Inc.

Full Copyright Statement

Acknowledgement

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