

June 27, 2005

Federal Trade Commission
CAN-SPAM Act
Post Office Box 1030
Merrifield, VA 22116-1030

Re: CAN-SPAM Act Rulemaking, Project No. R411008

Dear Secretary,

On behalf of the Email Service Provider Coalition (“ESPC”), I am submitting the following comments to the FTC in response to the Notice of Proposed Rulemaking (“NPRM”) for the CAN-SPAM Act.

The ESPC is made up of over 60 leading companies – all of which are struggling with the onslaught of spam, as well as the emerging problems related to the deliverability of legitimate email. Email service providers (ESPs) enable their customers to deliver volume quantities of email messages. These messages originate from the full spectrum of the US economy – large and small businesses, educational institutions, non-profits, governmental agencies, publications, and affinity groups – who use the services of ESPs to communicate with their customers, members, and constituents. While ESPs serve the marketing needs of the business community, it is by no means the only customer group served. Email service providers also deliver transactional messages (such as account statements, airline confirmations, and purchase confirmations); email publications; affinity messages; and relational messages.

The ESP industry is robust and growing. Within the ESPC, we estimate that our members provide volume email services to over 250,000 customers. These customers represent the full breadth of the U.S. marketplace: from the largest multi-national corporations to the smallest local businesses; from

local schools to national non-profit groups and political campaigns; from major publications with millions of subscribers to small affinity-based newsletters.

Earlier this year, the ESPC broadened our membership criteria to include many other companies involved in the email industry. Notably, our membership now includes many companies involved in email authentication and reputation systems. We also have welcomed mail transfer agents (MTAs) and large Internet Service Providers (ISPs) to the ESPC. In many ways, the ESPC now represents the full email industry.

Given the significant breadth and scope of our connections to the email industry, the ESPC has a deep understanding of the implications and effects of the CAN-SPAM Act. Our membership has spent a great deal of time reviewing the Act and the NPRM. We are happy to provide the following comments and would welcome the opportunity to discuss our views further.

Our comments follow the format of questions presented in the NPRM. We have not prioritized our comments. However, our concerns regarding the reduction in the opt-out processing period, the definition of Sender, and the definition of Transactional and Relationship messages are significant.

1. Section 316.2

a. Definition of Person

The FTC has proposed a clarification in the definition of Person that would ensure that corporations and individuals are subject to the Act. The proposed definition tracks the definition of person found in the Telemarketing Sales Rule, 16 CFR 310.2(v): “an individual, group, unincorporated association, limited or general partnership, corporation, or other business entity.” The ESPC supports this proposal. We believe strongly that both individuals and organizations should be subject to the provisions of the CAN-SPAM Act.

b. Definition of Sender

The FTC has proposed a clarification of definition of sender that will allow greater delineation of responsibilities when a commercial message contains promotions for more than one advertiser (and therefore has more than one Sender). Specifically, the Commission has proposed that a single Sender may be responsible for complying with CAN-SPAM where one entity has satisfied the Act's definition of Sender and at least one the following criteria: (1) control of the content of the message; (2) determination of the email addresses to which the message is sent; or (3) identification in the "from" line as the sender of the message. The Commission's proposal would also require that the single Sender be the only entity that possesses any of these three characteristics.

Under the CAN-SPAM Act, it is possible to have more than one Sender – and therefore, more than one person responsible for compliance – within a single commercial message. This multiple-sender issue can create daunting compliance challenges for businesses. In addition, it may be confusing to consumers if there are multiple opt-out links and multiple postal addresses for the various Senders of a commercial message. Due to these concerns, the ESPC has requested additional guidance on this issue in past comments to the FTC. We support the Commission's efforts to further clarify this issue under the Act and specifically endorse the criteria related to selection of email addresses and reference in the "from" line of a message. However, the issue of "control" over the content of a message raises some important questions that we feel require additional guidance or clarification.

The first criterion provided by the Commission is that a single Sender may be found if the definition of Sender is satisfied and the "person controls the content of the message." The use of the word "control" in this context requires further clarification. Specifically, the ESPC feels that the FTC should clarify that list owners should be considered "the" Sender in certain circumstances, and should not be disqualified from being designated a single Sender due to the fact that they may not "control" the ad copy in a message.

It is very common for list owners to approve or disapprove a certain ad for delivery to their lists; however they typically do not have 'control' over the specific creative content within an approved ad. The great majority of advertisers or marketers that provide advertising copy to a list owner for delivery to a list demand that no changes be made to the advertisement. In such situations, we feel strongly

that the list owner's inability to edit the content of the ad should not disqualify the list owner from being identified as the single Sender of the message. In other words, we feel that fundamental control is exercised by saying "yes" or "no" to an advertisement within a message being delivered to a list of email addresses. And, further, that merely creating the advertisement is not control for purposes of the Act when a list owner exercises the type of fundamental control described above.

We believe that control over the content of a message can be determined by certain factors, including the ability to:

- determine whether the message is sent, or
- approve or reject content to be included in the message (but not necessarily the ability to edit or control the content itself).

It may be possible to clarify the issue of control by defining "control" according to these two criteria. In other words, "control" for purposes of the regulation could be found when one of the two criteria is satisfied.

In addition to the issue of control, the members of the ESPC are concerned that the ability to designate a single Sender in list rental situations may be limited by the lack of clarity around the words "advertise or promote" in the definition of Sender. Our comments below describe the issue of list owners and their responsibilities for providing an opt-out under the CAN-SPAM Act. One method to ensure that a list owner has the ability to be considered the Sender of a message is to clarify the concepts of "advertise or promote" in the definition of Sender.

We feel that this issue could be clarified by considering certain common practices in email marketing to be advertising or promotion. Specifically, in list rental situations, we feel that the following should be considered promotional content:

- reference to the list owner in the from line of the message;
- inclusion of a logo or other reference to the list owner; or
- a statement in the message that the message is being delivered through the list owner.

Such a clarification would allow list owners to properly take responsibility for the opt-out function (and CAN-SPAM compliance generally) in those messages that are delivered to the addresses on their list.

c. Opt-out obligations for third-party list providers

The FTC has requested comments on the issue of opt-out obligations in list rental, or third party list sharing, situations. We firmly believe that list owners should be responsible for providing an opt-out function, as described in the Act, in every message. However, the CAN-SPAM Act creates a scenario where a list owner may not be a Sender if they are not advertising within the message. As a result, a list owner may not be required to offer an opt-out, even though the message was generated from their list. This creates a perplexing situation where consumers may not be able to unsubscribe from the actual list that generated the message.

The members of the ESPC feel strongly that list owners should be responsible for providing an opt-out function in every message sent through their lists. We also recognize that the CAN-SPAM Act may be unfortunately limited to requiring only Senders (meaning those advertising within a message) to provide an opt-out function. As a result, we are currently considering an update to our industry best practices document, the ESPC Pledge, that would require list owners to provide an opt-out in every message sent to their lists.

d. Creation of a Safe Harbor

The ESPC is generally supportive of safe harbor programs. We feel that companies should have an opportunity to go beyond mere compliance with legislative and regulatory demands and offer additional dispute resolution and auditing safeguards. In the email industry, the use of a safe harbor for affiliate marketing or list rental could be a valuable tool to build consumer trust.

We feel strongly that any safe harbor program should include benefits for those companies that voluntarily agree to participate. Such participation is always accompanied by additional costs and burdens on a company, so it is appropriate to create an incentive to participate. One possible, and valuable incentive, is the creation of a presumption of compliance for companies within a safe harbor program. The ESPC would be very interested in further discussion of such programs.

e. Definition of Valid Physical Postal Address

The Commission has proposed a definition for the term “valid physical postal address” under the Act. Currently, no such definition exists and confusion has ensued as to appropriate compliance with this provision. Specifically, it is not clear if post office boxes, private mail boxes, or corporate mail stops would satisfy the Act.

The proposed definition would clarify that a “valid physical postal address” includes: 1) the sender’s current street address; 2) a Post Office box registered with USPS; or 3) a private mailbox that the sender has registered with commercial mail receiving agency.

The ESPC is strongly supportive of this proposal. It provides the necessary clarity and gives industry explicit guidance on the types of addresses that are satisfactory under the Act.

f. Email sent to online groups

Online groups – also known as discussion lists, “list serves,” mailing lists, and chat groups -- constitute a thriving and active community engaging in both commercial and non-commercial speech via email. The ESPC counts among its members some of the largest providers of such fora – including one which hosts over 40,000 different lists. Such lists provide a dizzying array of opportunities for individuals to connect with others who share their interests.

Many of these lists are volunteer efforts, even though they may sometimes involve commercial content. Although ESPs that host mailing list services are generally considered to be engaged in “routine conveyance,” it is not clear what obligations mailing list operators and moderators face under the Act. Therefore, it is especially important to consider whether ambiguity or vagueness in the CAN-SPAM Act would cause list operators to limit such fora for discussion. Because many of these community lists are operated by volunteers with no budget for legal assistance, lack of clarity regarding CAN-SPAM compliance obligations could have a chilling effect, causing operators to cease such community fora, especially if the activities of list participants expose them to legal risk.

Community mailing lists are often aimed at allowing any subscriber to communicate with the rest of the group *en masse*. Such mailing lists are implemented using tools that span the range from simple aliases or automated address systems to complex mailing list software that provides sophisticated features about the level of control the list owner has and what safeguards there are regarding postings by people other than the list owner. The content can vary for each message distributed, carrying commercial or non-commercial content.

Industry best practices are to subscribe someone to a discussion group only if they have given permission in advance. In fact, ESPs that offer community mailing lists that support such communications generally require not just an initial opt-in but also that a subscriber additionally confirm the subscription from their email address before the subscription becomes active (a so-called “confirmed opt-in”). It is possible to have addresses added to a list without permission, however, either by intentional choice on the part of the list owner, through forgery and fraud, or by typographical error.

When ESPs offer mailing list services, they sometimes charge for the service and other times offer the service free of charge to subscribers. Frequently, free services are associated with including advertising in messages to subscribers on the list, or the advertisements may be sent separately (without normal list content).

Mailing list software can offer the list owner a range of choices for controlling who subscribes and what content is sent through a list. Here is a general description of the types of mailing lists that exist today:

- **Alias (a/k/a address exploder):** A simple form of community mailing list, an alias maps an address such as myfriends@domainname.com or volleyball-team@domainname.com to a list of recipients so anyone knowing the email address can send to the alias and have mail automatically reach all members of the group. The list owner exerts some control over what addresses are added to the alias but typically has no ability to pre-screen content; subscribers typically have only an all-or-nothing choice of being included in the distribution list on an on-going basis or being removed entirely.
- **Announcements Only:** only the list owner may post items for distribution to the list's

recipients; the “from” address is usually the list owner’s, even if s/he is forwarding a message.

- **Moderated:** each message by a subscriber requires approval by the list owner or other designated moderators before it can be distributed to the list. This provides the greatest control but introduces inherent delay which is problematic for high-volume lists or lists that broadcast breaking news or other time-sensitive information; the “from” address is usually that of the person who sent it for distribution, even though the list owner receives it and approves it.

Within each of the categories above, the list owner may configure the discussion forum with additional controls, including:

- List owner approval for all new subscribers;
- Limitations on who can post to the list (i.e., only subscribers); and
- Limitations on access to the list of addresses.

The decision whether to use these tools is frequently a function of the kind of group dynamic the list owner wants to support (i.e., censorship, bottlenecks, and extra labor on the part of a list owner operating a list on a volunteer basis).

It is exceedingly rare for even the most sophisticated mailing list software to allow subscribers to choose from which senders they wish to receive email. A subscriber’s choice is usually limited to deciding whether they want to be on the list or not. Given the current state of tools for community mailing lists, asking list owners or moderators to accumulate opt-out requests specific to an advertiser or sender would be a significant burden that would inhibit operators of community mailing lists, especially where list operators or moderators are providing services on a volunteer basis.

The ESPC believes that list owners or moderators of a discussion group should not be considered “senders” under CAN-SPAM if they are acting to facilitate online discussion or other types of community mailing lists. Indeed, most list owners will be considered to be engaged in routine conveyance under the Act – and therefore not included in the definition of Sender.

2. Section 316.2(o) – Transactional or Relationship Message

a. Legally mandated notices – transactional or relationship messages

The Commission has asked for comments on the issue of legally mandated notices. Specifically, the Commission asked if such messages should be considered transactional or relationship messages under the Act.

The CAN-SPAM Act includes a definition for Transactional and Relationship Messages that focuses on commercial transactions such as purchases, provision of product information, employment, or delivery of goods or services. The definition does not offer a clear category for legally mandated notices that fall outside of these commercial transaction concepts. As a result, it is unclear whether legally mandated notices are Transactional or Relationship Messages. It could be argued strongly that such messages are indeed not a part of the definition.

Similarly, it is likely that legally mandated notices will fall outside of the definition of Commercial Electronic Mail Messages, as they do not usually advertise or promote a particular product or service. This raises the important question as to how legally mandated notices should be classified under the Act.

In many cases, legally mandated notices may be associated with a commercial transaction. In such situations, it would seem appropriate to connect the legal notice to the underlying transaction and consider the legal notice to be a Transactional or Relationship message. However, it is also possible that such messages are not associated with a commercial transaction of any kind. In such situations, the CAN-SPAM Act would not seem to apply. This possibility was considered by the Commission in the regulations regarding “primary purpose” under the Act. In these regulations, the Commission recognized that there could be messages that were neither Commercial Electronic Mail Messages nor Transactional or Relationship messages. It would seem that legally mandated notices that are not associated with an underlying commercial transaction would fall into this undefined “other” category and fall outside of the scope of the CAN-SPAM Act.

b. Debt collection – commercial or transactional or relationship messages

The Commission has asked for comments on the issue of email messages that are associated with demands for payment, or debt collection notices. Specifically, the Commission has asked if such messages should be considered Commercial messages or Transactional or Relationship messages under the Act.

While the members of the ESPC are not specifically engaged in delivering debt collection notices via email, we do feel it is important to interpret the CAN-SPAM Act consistently. Demands for payment and debt collection notices are always associated with an underlying commercial transaction. The fact that an agent of the creditor may be sending the notice should not change the determination as to the status of the message. We feel that such messages are properly categorized as Transactional or Relationship messages under the Act.

To consider such messages Commercial would require a finding that there is something being advertised or promoted within the email. Debt collection messages do not advertise products or services; they demand payment for products or services previously delivered. It is very clear that such messages are associated with a commercial transaction. Any distinction based upon the use of an agent for delivery of the message could create significant confusion in many other ecommerce business models (e.g., many ecommerce vendors use agents for billing, shipping, and product fulfillment).

It should be noted that if a debt collection notice happened to include advertising or promotional copy, the Commission's guidance with regards to the primary purpose of the message would apply.

e. Scenarios – Transactional or Relationship Messages and Third Parties

The Commission has asked for comments on the issue of agents (or third parties) that are acting on behalf of a principal in sending a Transactional or Relationship message. Specifically, the Commission has asked whether messages sent by such third parties should be considered Transactional or Relationship messages.

The ESPC feels strongly that agents acting on behalf of a principal should be considered to have the same status as the principal. Thus, if a message sent by a person would be considered to be a Transactional or Relationship message under the Act, the same message sent by an agent of that person should be afforded the same status. In other words, the fact that an agent sent the message should not be relevant to an analysis of the content of the message.

Many business models online today rely upon third parties to perform many functions. Indeed, much of the ecommerce transacted today is passed through agents, service providers, enablers, and others. Jurisprudence has long recognized that an agent acts on behalf of, and within the powers granted by, a principal. It would contravene this long-standing doctrine to find that email messages sent by an agent were in some way different than those sent by the principal.

k. Modification of Definition of Transactional or Relationship Message

One of the compliance challenges presented by the CAN-SPAM Act comes from the multi-faceted use of email in the workplace today. Sales departments within large, distributed organizations send many low-volume messages to contacts and potential prospects every day. These messages may indeed be commercial in nature. But they do not rise to the level of public policy concern (spam) to which the Act was targeted.

Similarly, the CAN-SPAM Act does not include any standards for the volume of email sent from an organization. In other words, a single email sent by an employee could be deemed a violation of the Act. The ability of a large organization to police the individual use of email by employees is very limited. And it would seem unfortunate for an otherwise compliant organization to be embroiled in a costly legal action as a result of a very small number of email messages being out of compliance with the Act.

As an example, a large financial institution may have a multitude of affiliates that operate around the country. Some of these affiliates could have local branches. And some local branches could have loan officers, business development professionals, or other employees charged with selling services

to the community within which their branch resides. Presume that a loan officer from a bank wants to send a personalized note to the owner of a business within the same town. The purpose of the message may indeed be commercial and the content of the message could indeed be promotional. Should such messages need to be reviewed against a global opt-out list maintained by the parent organization? Such a result would hinder the free flow of business relationship communications.

Due to this concern, we feel that a new category of Transactional or Relationship messages is necessary: *business relationship messages*. Such messages would be exempted from the definition of Commercial Electronic Mail Messages (as they would be considered Transactional or Relationship messages). We feel that business relationship messages may have some, but not necessarily all, of the following attributes:

1. Low volume (the message is sent to a limited number of email addresses and is not part of a systematic campaign to many email addresses)
2. Limited volume over time;
3. Personalization is involved (the message may include content that makes clear the message was intended for a specific person);
4. The messages may be unique (and not part of a larger campaign);
5. An existing relationship between sender and recipient may exist;
6. The message is relevant to the recipient;and
7. The message is relevant to the relationship between the sender and recipient.

We feel that this addition to the definition of transactional and relationship messages is critical to the compliance efforts of organizations with employees that may create low-volume messages to prospects and clients on a regular basis. The lack of such a definition leaves such organizations with the very real prospect of preventing, limiting, or drastically delaying such communications in order to ensure compliance with the standards of the CAN-SPAM Act, and this restriction does not promote the purposes of the Act, i.e., limiting spam.

3. Forward-To-A-Friend Email Messages

The Commission has asked for comments on the common practice of offering a “forward to a friend” function within commercial email. Such messages can be forwarded by the original recipient of an email message and may be delivered through systems provided by the Sender, or through the email application used by the original recipient. It is also common for website publishers to provide a web-based mechanism for the forwarding of content, where a recipient may enter additional email addresses to which the web page content will be sent.

It should be noted that a Sender should never have responsibility for a message that is forwarded directly from a recipient’s own email application, regardless of whether the Sender has encouraged such forwarding. Senders have no interaction with the act of forwarding from a recipient’s email application. A recipient takes such action independently. It would be inappropriate to create compliance obligations under the Act where the Sender has no control over the distribution of the message. In other words, if a recipient decides to forward a message through her/his desktop email application, the original Sender of the message (the advertiser) should not bear CAN-SPAM obligations – even if the Sender has encouraged the recipient to forward the message.

Where a website publisher offers a web-based mechanism for forwarding commercial content (the message is forwarded through a service offered or hosted by the Sender), the Sender may have obligations under the CAN-SPAM Act under certain circumstances [e.g., where the website offers a benefit to the consumer to send the content and the website collects the friends’ email addresses].

The Commission has opined that the Act’s definition of Procure would include “forward to a friend” mechanisms if the Sender acted to “induce” the recipient to forward the message. In other words, if the Sender provides some inducement to the act of forwarding, the forwarded message would fall within the scope of the Act and the Sender would be responsible for CAN-SPAM compliance for the message.

The Commission has adopted an unfortunately broad interpretation of the word “induce.” Essentially, the Commission has suggested that any persuasion beyond a mere recitation of the availability of a forwarding function will be considered an inducement.

The ESPC agrees that mere statements regarding the availability of a forwarding function do not create the necessary inducement contemplated under the Act. However, we are greatly concerned that the Commission has used such an expansive interpretation of inducement. Indeed, it would appear from the Commission’s examples that the mere inclusion of an exclamation point (“Forward to a Friend!”) could be considered undue persuasion and, thus, inducement. This is an extreme and unfortunate result. The members of the ESPC agree with the Commission that inducement may be found whenever consideration is exchanged for the act of forwarding. But finding that inducement exists whenever a Sender uses anything more than *de minimis* persuasion or influence unnecessarily limits an important business communication channel and creates undue compliance burdens. Inducement should only be found where an exchange of consideration has occurred.

To be clear, forwarded messages are not a source of spam. The ESPC is not aware of any study or report that has shown such messages to be considered problematic by consumers. Anecdotally, it seems that such tools are embraced by consumers as an efficient way to share information. Unnecessarily impeding the use of this feature does little if anything to stop spam and will frustrate consumers and businesses alike. We therefore encourage the Commission to consider only an exchange of consideration as inducement and to adhere to intent of the CAN-SPAM Act’s general purpose: to staunch the continued proliferation of spam.

4. Section 316.4—Prohibition against Failure to Honor Opt-Out Requests within Three Business Days of Receipt

a. Opt-out request timing

The Commission has proposed a reduction in the time period permitted for processing opt-out requests, from 10 days to 3 days. The Commission supports this proposal by finding that “current technology allows for processing such opt-out requests more expeditiously than the current ten-business-day time frame.”

The members of the ESPC agree that technology permits opt-out requests to be processed quickly. In many cases, opt-out requests are processed instantaneously. However, such processing speed is

limited to situations where only a single delivery channel and business are involved. Most ESPC members provide immediate opt-out processing services on behalf of their customers. In other words, if an ESPC member is sending volume email on behalf of a client, an opt-out request is processed immediately.

However, all email is not sent through a single software application or service provider, marketing channel, or business unit. And the time required to process opt-out requests *across* service providers, marketing channels, or business units often takes more than three days. In most cases, the cross-channel or business unit suppression processes have taken significant resources simply to be in compliance with the current 10 day period.

To provide clarity on this point, the ESPC asked members to provide examples of opt-out processes that take more than three days in their current operations. The following examples show clearly the legitimate need for the Commission to preserve the current 10 day opt-out period.

Example 1:

An advertiser places a media buy through an advertising agency or list broker. The list broker places list rental orders on behalf of their client with email list vendors.

When the list broker places the orders with each list vendor, it sends a creative (advertising copy) and a suppression file (a list of email addresses from which the advertiser has received opt-out requests) for the order. The campaign is tested over a 24 hour period with different creative examples to determine optimal performance and then on the day it is set to mail, the advertiser determines the final creative advertising copy to be deployed.

The list broker now has to coordinate the final creative change with each list vendor, operational tests have to be sent, the advertiser has to approve the final tests with the list broker, and then the list broker has to give approval to each list vendor.

It is estimated that these and other last-minute creative changes occur with 70% of orders for this ESPC member. This process of changes can take at least 1 to 2 days to complete, and often times even longer. The ESPC member sometimes needs to request new suppression

files from list brokers who have to go back to the advertisers because more than 10 business days have passed from the time the order was placed to the time the tests are ready to mail.

In such situations, processing an opt-out request within 3 business days is not possible as campaigns are typically set to launch for longer than three business days.

Example 2:

Many large advertisers require list vendors to scrub (or merge/purge) their lists through a third party service (analogous to bonded mail houses in the direct mail industry). This actually requires technical resources to extract list data from an order, encrypt it, send it to the merge/purge provider, then upload it back to the list vendor's database and run against the order.

Also, the list vendor will usually need to secure non-disclosure agreements (NDAs) with third parties to ensure privacy of the data they are sending outside of its database. There are frequently delays in negotiating these NDAs. The delays experienced with NDA agreements usually occur when the broker has possession of the advertiser's suppression file. By the time the campaign is tested and the NDA language negotiated, the suppression file could be at least 5 days old.

More importantly, the actual processing time for suppression list scrubbing often takes at least a day, and is often complicated through the provision of multiple suppression files across affiliates and business units.

During our discussions of the opt-out processing issue, our members described companies that demanded to send an encrypted CD containing a suppression file through a courier. This was done due to concerns about security. The use of a courier and processing the encrypted disk could easily take more than three business days – making compliance impossible.

It should be noted that there is no evidence that the period currently provided for opt-out processing creates more spam. Indeed, legitimate businesses do not perceive an opt-out request as an invitation to send more email. To do so would be damaging to their brands. It is in the best interests of organizations to process such opt-out requests as quickly as possible.

Moreover, other marketing channels have been afforded far greater leeway in processing requests to unsubscribe under Commission rules. Specifically, the telemarketing industry has been given 31 days to process new listings on the national do-not-call list¹. The use of a single suppression file arguably provides an easier path to compliance for telemarketers than the highly distributed and fragmented email environment. It seems incongruous that email marketing would then be provided just one-tenth of the amount of time afforded to telemarketers for processing removal requests.

d. Suppression of addresses – technical procedures

The Commission has requested technical information regarding suppression functions in email. The Technology Committee of the ESPC has taken each of the questions presented by the Commission and prepared the following responses:

What specific technical procedures are required to suppress a person's email address from a sender's directory or distribution list?

1. Compare a list of suppression addresses against the list of active addresses. For each address on the suppression list, check to make sure it is not on the active list. This can be done before scheduling the message (so that no messages are generated for suppressed addresses) or could be implemented as an outbound gateway filter (so that the messages are generated, but then stopped before they get sent out).
2. Compare a list of MD5 encoded suppression addresses against a list of MD5 encoded active addresses. This allows you to match the addresses shared by both lists without revealing addresses on the suppression list that were not already on the active list.

¹ 16 CFR § 310.4(b)(3)(iv) The seller or a telemarketer uses a process to prevent telemarketing to any telephone number or any list established pursuant to §§ 310.4(b)(3)(iii) or 310.4(b)(1)(iii)(B), employing a version of the “do-not-call” registry obtained from the Commission **no more than thirty-one (31) days** prior to the date any call is made, and maintains records documenting this process. (emphasis added)

3. Upload the list to a third party data processor that holds both lists and performs the above comparison. The data processor then returns either A) a list of addresses already on the active list that should not be sent email or B) a list of valid addresses from the active list that can be sent email.

All of the 3 methods above result in a list of addresses that should not receive a message, which then must be uploaded to the email software in order to prevent sending email to those addresses. Most email software today supports uploading suppression list files to prevent emailing them.

What are the specific time requirements and costs associated with those procedures?

The time and cost varies linearly based on the size of the lists involved. Both the size of the suppression list and the size of the active list affect the processing time and cost. Many senders' suppression lists contain less than 100,000 addresses, in which case the time and cost are fairly negligible. Third party compliance services provide a secure solution for a few hundred dollars per month. A large company with many divisions and marketing partners might pay a few thousand dollars a month for this service.

What, if any, manual procedures are required to suppress a person's e-mail address from a sender's directory or distribution list?

This varies depending on the software used to send the email and the way the suppression is handled.

In the most manual, most secure case, a person must:

1. export their list of email addresses (files range from 1 megabyte to 50 megabytes), standard function of most software
2. upload this list to a third party data processor (30 minutes)
3. wait for the file to be processed (1 minute to 1 hour)
4. download the list of addresses to suppress (1 minute to 3 minutes, typically a small percentage of the addresses uploaded)

5. upload this list of addresses into their email software to suppress (10 minutes)

In the most manual, less secure case, a person must:

1. securely log in to the suppression list system and download an MD5 encoded suppression list (5 minutes to 30 minutes)
2. upload this list of addresses into their email software to suppress (10 minutes)

Some companies today provide plain text files containing their suppression lists to third parties. This is not recommended but included for completeness since it is a practice that is currently in widespread use.

1. anonymously log in to the suppression list system and download a plain text suppression list (5 minutes to 30 minutes, no cost to anyone)
2. upload this list of addresses into their email software to suppress (10 minutes)

Many email providers have integrated CAN-SPAM compliance into their applications. With the most automated solutions, a person simply uses "cut-and-paste" to enter their "secure one-time use key" into their email software and it automatically and securely cleans against the third party suppression list before sending. This entire process adds about 1 minute to the sending process and has been implemented by many of the largest providers.

What, if any, costs are associated with the manual suppression of e-mail addresses?

The hard costs of processing removal requests manually are not large. Such functions primarily represent a labor cost – many hours can be required to properly handle unsubscribe requests manually.

What, if any, circumstances would require manual processing of opt-out requests?

This happens on a daily basis for any large email sender. Requests to unsubscribe come in through many channels other than the automated link provided in the message, such as:

- SpamCop reports
- AOL and other ISP Feedback Loops
- End user phone calls processed by a call center
- End user postal mail requests
- End user emails send to the wrong email address
- Geographically dispersed operations

What are the characteristics of senders that use manual procedures to process opt-out requests?

Only very small senders using an email client such as Microsoft Outlook would do this completely manually. Almost every email software provider and affiliate network has added some level of automated support for opt-out processing.

f. Time limits on duration of opt-out requests

The Commission has stated a reluctance to propose a limit on the duration of an opt-out request. This position is grounded in concerns that consumers will receive unwanted email after submitting an opt-out request (albeit years afterwards). The ESPC urges the Commission to consider a limitation on the duration of opt-out requests due to the unique nature of the email industry. We recommend a time frame of under five years.

Specifically, there is ample evidence that email addresses are recycled rapidly². Consumers do not carry their email address with them when they move from one Internet service provider (ISP) to another. As a result, ISPs frequently reassign email addresses to new customers. This “churn” in email addresses would suggest that an opt-out request should expire after a certain period to ensure

² “It is important to keep in mind that people change ISPs, jobs and email addresses at random resulting in email address turnover of more than 30% per year.”

<http://www.ballyhoomag.com/content/templates/default.aspx?a=12&template=print-article.htm>

“A new study indicates that email addresses are changed at the rate of 31 percent annually, causing 53 percent of those consumers to lose touch with personal and professional contacts, as well as preferred Web sites.”

<http://www.businesswire.com/webbox/bw.101702/222902133.htm>

that recycled email addresses are purged from suppression files. As stated in the CAN SPAM Act, should a subscriber with a previously suppressed address approach that sender to receive a commercial message, the sender must receive affirmative consent prior to doing so. In the case of recycled addresses, the sender would have no way of knowing this fact and are at an unfair disadvantage in acquiring new customers.

It should also be noted that both the National Do Not Call Registry and the Gramm Leach Bliley Act have five year sunset provisions for opt-outs. Providing some parity with these standards would seem appropriate.

g. Suppression Files

The Commission has asked for information regarding the size of email suppression files in comparison to the National Do Not Call List. In an informal survey of ESPC members, we found that many members have suppression lists that exceed the size of the DNC list. Indeed, some members reported files that exceeded the DNC list by over 10 million entries. It should be noted that email is markedly different than telephony. Consumers average many more email addresses than phone numbers. As a result, email suppression files can reach very large numbers for otherwise modest operations.

The Commission also requested information on “typical” campaign sizes and unsubscribe requests. Again, email is somewhat unique and there is a wide spectrum in campaign sizes. Email is used by the smallest of small businesses up to the top of the corporate world. There is no typical size – email marketing covers the full breadth of marketplace.

Similarly, there is no trend towards a consistent opt-out level in email campaigns. The quality of the offer, the creativity of the content, the frequency of the messages, and the relationship between the sender and the recipients can all have an effect on the opt-out rates. Senders with good practices and creative content will generally see lower opt-out rates.

5. Section 316.5—Opt-out requests

c. Changes to how recipients submit opt-out requests

The Commission has proposed additional standards to guide the functionality and information required to process an opt-out request. Specifically, the Commission has suggested that Senders cannot require: (1) any fees; or (2) any information other than the recipient's email address and opt-out preferences. Additionally, the proposed rule would prohibit any opt-out process that requires more than a reply email or a visit to a single web page to process the opt-out.

The ESPC is generally supportive of clarity and simplicity in opt-out processes. It is inappropriate for Senders to require recipients to navigate through multiple screens in order to request an opt-out. We are strongly supportive of the prohibition on any fees in the opt-out process. Our members are not aware of any such practices in the marketplace today.

We do, however, have serious concerns with the limitations on the data that may be required in the opt-out process. Many messages sent to consumers are mixed messages – they contain both commercial and transactional content. Such messages may, depending on the “primary purpose” analysis promulgated by the Commission, be considered commercial messages under the Act. As a result, it is possible to have mixed messages with significant transactional content that are subject to the requirement to include an opt-out mechanism within the message. In such situations, it may be necessary to gather more data than just an email address and opt-out preference. Indeed, industry standards with regards to security would require a password or other independent identifier prior to such a change in a transactional account.

Many examples exist for this issue. Consider a frequent flyer program that sends a monthly account statement to participants. Such notices usually include a significant amount of promotional content for the airline. It is possible, if not likely, that such messages would be considered commercial under the primary purpose rules. As a result, the message would be required to include an opt-out mechanism. But the transactional nature of the relationship (participation in a frequent flyer program) would suggest that something more than a mere email address would be appropriate to process the opt-out.

Many such programs require entry of a frequent flyer account ID, or a password, or both. This is appropriate due to the fact that more than a marketing message is being sent – the message has significant transactional value.

This concern extends across many, if not most, mixed content messages. Indeed, it is common for transactional messages to include substantial promotional content. When such messages cross the line from transactional to commercial (under the primary purpose test), limitations on the amount of data that may be gathered in an opt-out process become problematic. The ESPC therefore recommends that Commission revise the proposed rule to permit additional data to be gathered in situations where transactional relationships are involved.

Another scenario that would demand additional data in an opt-out process exists when a Sender uses a dynamic link – a special opt-out link that is unique to the recipient – to process the opt-out. In most cases, this allows the recipient to be unsubscribed without entering any data – the dynamic link is associated with the recipient’s email address and thus allows the Sender to recognize and process the opt-out without any additional data.

However, dynamic links can become a problem when a message is forwarded by the original recipient. When this happens, the dynamic link does not change – it is still associated with the original recipient’s email address. If the subsequent recipient clicks on the opt-out link, it is possible that the original recipient’s address will be unsubscribed. Such scenarios suggest that additional data or screens – a confirmation of the email address that is being unsubscribed – would be appropriate. In fact, such confirmations exist today – and frequently require more than one screen in order to confirm and process the opt-out.

It should be noted that dynamic links provide a significant benefit to many consumers. They allow for easy and efficient processing of consumer choice. However, the use of dynamic links does require some level of confirmation to ensure that the correct address is being unsubscribed. The ESPC requests that the Commission clarify that such confirmation processes are acceptable under the rule. As currently proposed, the rule would seriously threaten this valuable consumer tool.

Conclusion

The members of the ESPC have been committed to improving the ecosystem of email since the inception of our organization. We believe strongly in the availability of tools and processes that permit consumers to control their inboxes. For this reason, we have been strong supporters of the CAN-SPAM Act.

We look forward to continued discussions with the Commission on the proposed rules. Our comments are borne from a deep understanding of the technology and business models used in the email industry. We stand prepared to continue the important work of defining appropriate standards under the CAN-SPAM Act.

Sincerely,

J. Trevor Hughes
Executive Director
Email Service Provider Coalition