

FEDERAL TRADE COMMISSION
Marketing Practices Division
Washington, DC

CAN SPAM Act Advanced Notice of Proposed Rulemaking
Project No. R411008
April 20, 2004

INTRODUCTION

MCI, Inc. (“MCI”) hereby submits these comments to assist the Commission in setting forth rules as required by the CAN SPAM Act (the Act). As one of the largest global providers of Internet service MCI is severely impacted by the rising tide of spam. As a provider of a broad scope of communications products and services, MCI uses electronic mail to communicate with its customer base and limits all commercial communications to consent based messages.

MCI has a long standing history of empowering consumers to control the amount and content of messages coming into their in-boxes and has been an advocate for laws and policies that accomplish these goals. We believe that every effort must be taken to insure that electronic mail continues to be considered a reliable and efficient communications tool for all who use it for legitimate purposes. MCI applauds the strict criminal sanctions set forth under the Act for fraudulent and deceptive messages, and encourages the Commission to devote greater enforcement efforts on combating such illegal practices. In addition, we hereby provide input on other key sections of the Act, as requested by the Commission’s Advanced Notice of Proposed Rulemaking (ANPRM).

Subject Line Identification

As set forth under the Act, the Commission must prepare a report on the practicality of requiring commercial messages to be identified as such in the subject line. This is generally seen as requiring the letters “ADV” being affixed as the first three letters of the subject line in all spam messages. MCI does not see this as a useful or practical way to enforce the provisions of the Act. A subject line label does not make it any easier or more likely for our ISP units to filter out unwanted messages and thereby reduce the amount of spam going to end users.

The reason for this is that, like many other proposed remedies, only legitimate organizations will abide by this rule. These organizations respect their intended recipients’ choices, obtain permission prior to sending commercial messages, provide opt-out and contact information, implement customer service processes to address any possible complaints and readily cooperate with enforcement agencies to resolve any issues that may arise. For those organizations, this requirement has no added value or

benefit. The actual targets of a labeling requirement and the types of individuals or organizations that undertake nefarious practices in sending spam are the exact ones that would never comply with the majority of the Act's requirements anyway, and this is just one more requirement they would ignore. This concept is based on a false premise that spammers are law abiding individuals. Moreover, this label does not make enforcement actions any more fruitful or less problematic. Ultimately, because of the ADV stigma, this requirement would make it more likely for consumers to ignore the messages sent by companies they actually want to do business with and instead, open messages from disreputable spammers who would fail to abide by the condition.

Of course, the ADV labeling requirement is not a new idea. It is a requirement that several states have imposed over the course of the past few years when passing their respective spam laws. California, Colorado, Nevada and Tennessee are just a few of the states that passed such labeling provisions, and it is useful to look to those and all other states that have passed this requirement into law for a possible reduction in the number of spam messages, complaints to ISPs or overall improvement in the annoyance level related to spam. After making inquiries, requesting studies and otherwise researching the results of this requirement, we have been unable to obtain any evidence from the respective states agencies, academia or independent research entities that would show the usefulness or benefit of this requirement. Thus, MCI does not see this as a practical tool for fighting spam or enforcing the Act.

Determining the Primary Purpose

The provisions of the Act apply to “any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service.” MCI encourages the Commission to provide as much guidance as possible to marketing organizations on how this primary purpose standard will be defined and applied. The ANPRM sets forth several suggested options on determining the primary purpose of an electronic message.

MCI believes that when there is a dual purpose to an electronic message, the “net impression” standard, as outlined in the ANPRM, is the most practical and reasonable method of determining the primary purpose. This method allows for the consideration of all material contained within the body of the email to be taken into consideration rather than portions dedicated to commercial advertisements.

In addition, MCI provides the following examples where the primary purpose should not be defined as commercial advertising. If an e-mail would still be sent absent the commercial advertisement, its primary purpose should not be considered to be commercial in nature. If it contains educational material to help inform recipients on certain industry sectors or technology improvements, its primary purpose should not be considered to be commercial in nature. If sponsors' or advertisers' logos are included in what is otherwise an event agenda or newsletter, its primary purpose should not be considered to be commercial in nature. Finally, if it invites recipients to join in ongoing

discussions or events to which they have indicated an interest in attending, its primary purpose should not be considered to be commercial in nature.

Essentially, to fall within the primary purpose definition, a message should be sent for the purpose of promoting a specific product or service, and that promotion should be more important than all other purposes in the body of the message in order for its primary purpose to be commercial in nature.

Transactional or Relationship Messages

Under the Act, transactional or relationship messages are specifically exempted from the definition of a commercial electronic message. However, as the Commission has indicated in its ANPRM, it is necessary to examine the scope and definition of a transactional or relationship message. MCI encourages the expansion of this type of message to include messages that are sent out on an as needed basis by an entity's account teams to representatives of enterprise level customers with whom they have a pre-existing relationship. In order to adequately control the scope of such emails and not unduly loosen the controls of the Act, MCI proposes a differentiation between messages sent to individual consumers and those sent to owners or representatives of business entities.

Consumers often use their personal email addresses for commercial communications, read e-mails on their personal time and are not usually engaged in a constant exchange of business e-mails. For e-mails sent to consumers, we believe a more narrow definition of the relationship or transactional message is appropriate and to limit such e-mails to instances where an account or specific service is at issue, and as otherwise defined under the Act.

However, in the normal course of any business, it is necessary and practical for a company's representatives to keep in touch with their enterprise level customers for a variety of needs, and these needs often include updating customers on improved services, technology launches or industry gatherings. While the end goal of these communications may be commercial in nature, they are part of an ongoing relationship, the recipient is familiar with the sender and the parties are engaged in a continual exchange of information related to their business or profession. In addition, the entity that is the recipient of such messages has specifically named the representatives or job functions that are the points of contact to the vendor and has provided their e-mail address for all communications related to the business relationship. In such instances, the transactional or relationship exemption should be expanded to include communications where there is a pre-existing business relationship *and* the communications are between representatives of business entities.

Ten Business Day Period

Pursuant to the authority granted to the Commission by the Act, the ANPRM seeks comment on the time period required for implementing opt-out requests. MCI

believes that in many instances a greater time period would be appropriate and useful. Implementing opt-out requests generally does not require deleting an e-mail address, but rather it requires the e-mail address to be added to a suppression list. Then all future commercial messages are “scrubbed” against the suppression list in order to remove messages going to those who have opted out of receiving such messages.

Often, global companies have multiple databases against which they must scrub an e-mail address from a recipient who has opted out of receiving future commercial communications. Because of differing privacy regimes around the world, it is necessary to keep customer lists separated within various databases, while in many instances, enterprise level customers will be maintained within multiple databases because of their regional and global scope. In addition, if a third party vendor is assigned with the task of sending commercial messages on behalf of a company, both the vendor and the company can do a better job complying with recipients’ opt-out requests if they are given adequate time to do so, and ten days is not sufficient for the communication and implementation between multiple company databases.

MCI supports a time period that is same as that adopted by the Do Not Call rules, which call for a thirty-one calendar day period in order to implement opt out requests. This would be a reasonable period for business entities to adopt their practices and remain compliant, while providing the Commission and other enforcement agencies with a timely enforcement mechanism. Finally, it is a reasonable time frame for the recipient as well because during the course of the thirty calendar days, the recipient is very unlikely to receive so many messages from the legitimate sender that it would cause a consequential burden of time or cost.

Sender of a Commercial Message

The ANPRM recognizes that identifying a single sender for every commercial message poses challenges based on how e-mail is normally generated. In many instances, there may be more than one sender or more than one entity whose commercial message is contained within the body of the message. As requested by the Commission, MCI proposes the following considerations related identifying senders for compliance and enforcement purposes. All the comments below focus on defining the sender as the entity who controls the list of recipients and has the ability to conform its practices to the rules set forth under the Act.

Multiple Advertisers. For instances where there are multiple advertisers within the body of a commercial message, MCI proposes a regulatory mechanism that is focused on the actual entity initiating the message. This would define the sender as the entity that has control over the recipient list and enforce the Act’s rules against that entity. It would be practical in that an advertiser who has no control or ownership over the recipient list would not be held liable for violations, and it would protect recipients’ privacy by not forcing the controlling entity to share email addresses with each advertiser. Examples of this scenario would include entities who purchase space in an advertisement section of a

newsletter or agree to sponsor an event and are thus allowed to display their logo on the advertisements for the event.

Joint Marketing. For instances where a few, usually just two, business entities form a joint marketing campaign and send out commercial advertisements related to the joint campaign, the sender should again be the organization that controls the recipient list. This often means that each organization sends the campaign material to its own customer base, removes all recipients that are contained within its own opt-out lists and remains responsible for forming its respective message in compliance with the Act. Again, this serves the dual purpose of holding the controlling entity liable for violations while protecting recipient privacy by not forcing unnecessary sharing of personal contact information. In fact, to further shore up recipients' privacy protections, the Commission could set forth rules that restrict enforcement to the "single sender" only if there has been no exchange of customer e-mail addresses. Thus, companies would take on greater liability and both be considered a sender if they share their respective customer e-mail information prior to the customers consent to take advantage of the marketing campaign.

Refer a Friend. As indicated in the ANPRM, the practice of forwarding information and commercial messages to friends is a common business practice. In these instances, an individual decides to forward an offer to one or more of their acquaintances, and those recipients will then decide whether or not to take advantage of the commercial offer. A baseline rule in this scenario is that no one can agree to receive commercial messages on behalf of anyone else. Each individual must have control over his own inbox. At the same time, it is impossible to control to whom such messages are sent and to somehow scrub the recipient from an opt-out list when the "sender" is a third party individual and not the business entity itself. Where such "refer a friend" e-mails are forwarded, we propose that if the business entity whose commercial message is being forwarded does not save, use or in any way retain the e-mail address of the friend, there be no opt-out option. Since there is no retention of the recipient's address, the "opt-out" becomes customary and standard. Thus, instead of having to take action to opt-out of receiving such messages in the future the friend does not have to take any further action unless he chooses to take advantage of the commercial offer. This also protects consumer privacy because it does not force individuals to provide their e-mail address to an entity simply to tell that entity not to send them commercial messages.

Other Issues Related to Implementing the Act

Finally, the ANPRM seeks comment on any further issues related to implementation of the Act. MCI applauds the Commission's detailed ANPRM which indicates the level of thought and consideration given to the many challenging issues surrounding implementation of the Act. Aside from those specifically addressed above, MCI proposes one additional item for consideration, especially at this time when the Act is relatively new and its rules are still being formulated. It would be useful for the Commission to implement a detailed series of guidelines which would further assist in bringing organizations into compliance in a timely manner, and serve as a safe harbor of sorts for organizations that take all necessary measures to implement the Act and its

rules. By undertaking a rigorous program of compliance and establishing policies designed to fully comply with the provisions of the Act, companies could qualify for such safe harbor. This would encourage companies to implement more stringent policies, while also serving as a timely and efficient mechanism for the Commission and other enforcement agencies on how to assess subjects of complaints and investigations. Common criteria by which to evaluate an organization's practices would be beneficial to all involved and ultimately, preserve enforcement resources for those whose actions indicate complete abuse and defiance of the law.

Conclusion

In furtherance of the privacy, practicality and enforcement concerns raised above, MCI submits the foregoing comments for consideration.

Respectfully submitted,
MCI, Inc.