

**Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20580**

Regarding)	
)	
The FTC's request for comments)	Project No. R411008
on regulations regarding unsolicited)	RIN 3084-AA96
commercial email, as directed by)	
the CAN SPAM Act of 2004)	

**COMMENTS OF AeA
(THE AMERICAN ELECTRONICS ASSOCIATION)
TO THE FEDERAL TRADE COMMISSION
REGARDING
THE CAN SPAM ACT**

AeA (American Electronics Association)¹ submits these comments in response to the Federal Trade Commission's ("the Commission") request for comments regarding this proceeding under Sections 3(2)(C), 3(17)(B), and 5(c)(1) of the CAN SPAM Act, P.L. 108-187 ("the Act"). All AeA member companies utilize email to communicate with employees, business partners, customers, and prospective customers. Our members realize the importance of protecting American consumers from false and deceptive commercial email or "spam," as it costs both consumers and businesses billions of dollars in lost productivity and unnecessary expenditures each year. Because of Congress' efforts to control false and deceptive commercial emails, and the Commission's task to further define the extent of those rules, we express support for the Commission's approach in this NPRM and submit the following answers to the Commission's questions.

¹ AeA is the nation's largest high-tech trade association, representing more than 3,000 companies with 1.8 million employees. These 3000+ companies span the high-technology spectrum, from software, semiconductors, medical devices and computers to Internet technology, advanced electronics and telecommunications systems and services. With 17 regional U.S. councils and offices in Brussels and Beijing, AeA has been the accepted voice of the U.S. technology community since 1943. For more information, please visit us at www.aeanet.org.

The Relationship of Third Parties in Marketing Efforts and Establishing a Safe Harbor

The CAN SPAM Act defines the “sender” of a commercial electronic email message generally as a person who initiates such a message and whose product, service, or Internet website is advertised or promoted by the message. AeA commends the Commission’s clarification of the definition of “sender” to contemplate co-branded or joint marketing communications as evidenced in its latest NPRM. However, AeA requests the Commission to establish a safe harbor for those co-branding partners whose products are advertised by third party marketing partners.

It is common practice for businesses to co-brand certain product lines with products offered by other entities that they believe will offer their customers additional convenience, functionality, and savings. Usually a business may include the logo of its co-branding partner in a customer communication. Because the proposed rules are silent on co-branding liability, a question is created as to who is ultimately responsible for compliance with the Act – the sender of the email, the co-branded business partner, or both. Because this dilemma creates confusion for both the business and the consumer alike, AeA respectfully offers its proposal on this issue.

We have suggested that in the situation of a co-branded commercial communication, the Commission employ a control test as to who is to be subject to the Act. Elements that would be indicative of who the controlling entity is, and thus amenable to the Act, would include the determination of:

- Which business partner controls the development of the overall message;
- Which business partner sends the message, or causes it to be sent; and
- Which business partner controls the relationship with the recipient customer – or in the case of the NPRM’s language, the person identified in the “from” line as the sender of the message.

Determining which business partner is the controlling entity would greatly decrease customer frustration as to who is disseminating the commercial communication. Further, establishing who is in control of the message would additionally allow the consumer to better manage who they receive communications from. Businesses, in turn, would gain greater certainty over their legal responsibilities to their customers, while eliminating the chances that a consumer may inadvertently opt-out of valuable business communications they *want* to get. We would also respectfully request that the FTC develop a reasonable definition of “control” and would submit that where the only activity relates to consent regarding usage of brand name or image, control is not present.

However, a question arises as to the responsibility of those who are in a relationship with third-party marketers. AeA respectfully recommends that the Commission adopt a safe harbor for persons who

employ third-party marketers who fall under the definition of “sender,” as long as good-faith efforts are taken to monitor the third-party entities as to their compliance with the Act. By establishing this safe harbor, the Commission will enable businesses to free up resources to ensure compliance with the Act, while creating legal certainty as to ultimate responsibility that will benefit both consumer and business alike.

Further, although FTC uses the word “affiliate” in the rule, it does raise certain concerns. The Act neither contemplates the term, nor is it defined anywhere. The key test in the Act has to do with entities that hold themselves out under a different name under a separate line of business. Many companies have very few affiliates and most do business under the larger corporate name—which would not hold them out to a separate standard. Unaffiliated third parties are a very different issue.

For these reasons, AeA respectfully recommends that the term “affiliate” be adequately defined, and that the definition of “sender” be clarified to include a safe harbor, so as to eliminate any questions of amenability and liability with regard to the Act.

The Definition of “Transactional or Relationship Message” Needs Clarification With Regard to Employer Communications

The CAN SPAM Act primarily defines the term “Transactional or Relationship Message” as an electronic mail message the primary purpose of which is to facilitate, complete or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender. The Commission has further defined the term in its NPRM, but in doing so, has included employer communications.

AeA believes that employer to employee communications should not be included in the definition of a “transactional or relationship message” as it opens a Pandora’s Box by attempting to categorize individual emails between those in an employer/employee relationship. Classifying such communications that occur over employer-provided and maintained networks will ultimately result in more harm to the employee – and ultimately the consumer – as they may be denied critical information that is beneficial but not necessarily tied to their continuing employment with the employer. Further, the privacy paradigm that surrounds the employment relationship is far different than the one surrounding the consumer relationship, with different privacy issues at stake. To commingle the two would result in a decreased flow of critical information internally that will inevitably be to the detriment of the employee.

AeA respectfully submits that the answers to all of the Commission’s questions in this area are yes and that it not further limit employer-employee communications.

Forward-To-A-Friend Programs

The NPRM requests comments regarding “Forward-To-A-Friend” email messages. AeA agrees with the Commission’s belief that making available the means for forwarding a commercial email message would not rise to the level of “inducing” the sending of an email, but more under the domain of “routine conveyance,” as someone else – the recipient’s friend – has identified the new recipient, provided their email address, and caused the message to be sent.

Many online service providers do not offer rewards or compensation for the forwarding of a commercial email – other than providing consumers an opportunity to have the pleasant feeling of knowing they have passed on a “good deal” to a friend. As such, the sending of the email would not rise to the level of an inducement for the purposes of the definition of “procure.”

It would also be fair to say that it would not rise to the level of an inducement should a seller offer a reward to an individual that has sent an email along once their “friend” has subsequently taken action on the forwarded email, as it is outside the either party’s ordinary course of business to maintain such a transaction. The term “procure,” as contemplated by the Act and referenced in the legislative history, was specifically defined to prevent third-party “renegade” behavior by e-mail marketers and the willful ignorance of those unscrupulous businesses who engage them.² Although it does not mention “Forward-to-a-Friend” programs either specifically or generally, it is apparent that the CAN SPAM Act was not crafted to imply or establish an email marketing business relationship between online service providers and their customers should they forward a “good deal” to a friend. For this reason, the sending of such an email should not rise to the level of an inducement for the purposes of the definition of “procure” even if the promise of reward contingent upon subsequent action was offered.

It should also be noted that many online service providers do not retain forwarded emails during this routine conveyance; only when the ultimate recipient takes action on the forwarded email does it get retained or stored. Should the individual in fact purchase a product or service, only then would they be incorporated into a database and subject to the protections of the CAN SPAM Act and the rules as set by the Commission.

² “*Procure*.—The term “procure”, when used with respect to the initiation of a commercial electronic mail message, means intentionally to pay or induce another person to initiate the message on one’s behalf, while knowingly or consciously avoiding knowing the extent to which that person intends to comply with this Act. ***The intent of this definition is to make a company responsible for e-mail messages that it hires a third party to send, unless that third party engages in renegade behavior that the hiring company did not know about.*** However, the hiring company cannot avoid responsibility by purposefully remaining ignorant of the third party’s practices. The “consciously avoids knowing” portion of this definition is meant to impose a responsibility on a company hiring an e-mail marketer to inquire and confirm that the marketer intends to comply with the requirements of this Act.” (*Emphasis added*). S. Rep. No. 108-102, at 15 (2003), http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_reports&docid=f:sr102.108.pdf.

For the preceding reasons, AeA respectfully recommends that the Commission include “Forward-to-a-Friend” programs within the “routine conveyance” exception.

Reduction of the 10 Day Window for Opt-Out Requests to Three-days

The CAN SPAM Act creates a prohibition against the sending of commercial email messages 10 business days after consumer opt-out of any further messages. The Commission now seeks direction as to whether a three-day period would be more appropriate. AeA respectfully requests that the Commission not reduce the opt-out window from 10 business days to 3 business days, but instead extend it to 30 calendar days.

Under the final and amended Telemarketing Sales Rule (“TSR”)(regarding the National Do-Not-Call Registry), the Commission saw fit to require telemarketer compliance within 30 calendar days, as it best balances the needs of the consumer against the burdens placed upon business.³ Given the organizational complexity of many businesses and the process intricacies inherent in compliance, ten days is proving to be barely adequate, even under the best of situations. Allowing thirty days for opt-out compliance would allow sufficient time for businesses to ensure fulfillment of the requirements, while simultaneously providing the benefit to consumers intended to them by the Act.

However, moving from the period set under the CAN SPAM Act from 10 days to three days will create an impossible threshold for opt-out processing in many common situations. The CAN SPAM Act creates the need for the transfer of suppression lists within and between organizations that are engaged in email marketing and communications. Organizations that either deal with third-party affiliates or are geographically spread out (or both) will be unduly impacted by this arbitrary opt-out time as it will put many well-intentioned companies unnecessarily out of compliance with the Act.

For these reasons, AeA respectfully requests that the Commission extend the opt-out window from 10 business days to 30 calendar days.

³ It should be noted the final and amended TSR requires telemarketers to update and purge their do-not-call lists every thirty business days. The decision was made pursuant to the Commission’s Notice of Proposed Rule Making (69 FR 7329, Feb. 13, 2004) which asked for comments regarding the proposed requirement whether telemarketers be required to scrub their lists every thirty days, or every thirty-one. The scrub period had been reduced to “one month” from every three months in a previous proceeding. Although we are asking the Commission to increase the timeframe for the compliance requirements, the same rationale for selecting a thirty day update/purge requirement is applicable to this proceeding – that of increased flexibility for compliance.

Restriction on Data Collection on Recipients Who Wish To Opt Out

The Commission's NPRM would prohibit the collection of any other information other than the recipient's email address and opt out preferences. Further, it would restrict the opt out process to sending a reply email message or visiting a single Internet Web page. For the following reasons, AeA recommends that the Commission consider excising these requirements from its proposed rule.

AeA's member companies take consumer privacy very seriously and take great steps to ensure that consumer information is both safeguarded and dealt with correctly. As such, many of our companies require that recipients provide more than just their email address for verification purposes. The provision of information other than an email address allows businesses not only to make certain that the person and accounts being deleted are, in fact, the correct ones, but to prevent unauthorized persons from making critical account changes.

AeA is also concerned regarding the restriction of the opt out process to occur on only one Internet Web page. Many online businesses conduct the process using more than one page, to ensure that the process is satisfactorily completed. For instance, a company may send a recipient a page asking the individual to confirm the selection, and then another page in fact confirming that the company had completed the deletion as requested. This multiple step process is for the consumer's benefit as well as the businesses.

As such, AeA respectfully requests that the Commission forbears from including the restrictions against the collection of additional data to confirm the correct deletion, as well as the restriction of performing the opt out process on just one Internet Web page.

We thank you for considering our views, and would be pleased to answer any questions the Commission may have.

Respectfully submitted,

AeA
601 Pennsylvania Avenue
Suite 600, North Building
Washington, D.C. 20004

/s/ Marc-Anthony Signorino

Marc-Anthony Signorino
Director & Counsel, Technology Policy
June 26, 2005

CERTIFICATE OF SERVICE

I, Marc-Anthony J. Signorino, Director and Counsel for Technology Policy for AeA (The American Electronics Association), hereby certify that a true and correct copy of the foregoing Comments of AeA was sent this 26th day of June, 2005, electronically to the Federal Trade Commission via www.regulations.gov.

/s/ Marc-Anthony Signorino .

Marc-Anthony Signorino
Director & Counsel, Technology Policy
AeA