The Electronic Frontier Foundation

Additional EFF Comments For CAN-SPAM Act ANPR
Docket ID 3084-AA96/16 CFR 316

A.1. MANDATORY RULEMAKING – Determining whether "the primary purpose" of an email message is commercial.

EFF is deeply concerned about this phrase. In order to avoid Constitutional problems, the FTC should interpret it to mean that a message qualifies as having a commercial "primary purpose" only when, if taken as a whole, it cannot be reasonably viewed as containing any noncommercial message. Put another way, if a message taken as a whole can be reasonably said to contain noncommercial content, then it **should not** qualify as having a "primary purpose" that is commercial under the statute. Any other interpretation of this phrase would, by definition, require the statute to reach noncommercial speech. To the extent that the statute reaches noncommercial speech, it should face, and would most certainly fail, strict scrutiny under settled Constitutional law.

EFF is strongly supportive of stopping spam, which we define as unsolicited, commercial, bulk e-mail. In that effort, however, it is unacceptable for noncommercial speech to be sacrificed as a side effect. Any rule that attempts to criminalize e-mails based upon the suggested tests in the ANPR -- the "importance" of the commercial portion, the "net impression" of the e-mail, or whether the commercial portion is "more than incidental" -- creates unacceptable uncertainty and risk for individuals, corporations and organizations engaged in everyday activity online.

For example, a nonprofit organization that solicits donations or sells T-shirts within an e-mail newsletter risks criminal and civil liability if a prosecutor or ISP determines that the "primary purpose" of its newsletter is to raise funds. Similarly, an individual plumber faces uncertainty if he answers a plumbing question posed by someone on a mailing list and includes a paragraph indicating that his services are for hire. Likewise, a fishing club encounters the same anxiety if it recommends specific products (with hyperlinks) to its members.

The legal doctrine underlying EFF's suggested interpretation of the statute is straightforward and settled. "Commercial speech" for purposes of First Amendment scrutiny is an e-mail message that does "no more than propose a commercial transaction," Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 762 (1976), which has been described as "expression related *solely* to the economic interests of the speaker and its audience," Central Hudson Gas & Electric Corp v. Public Service Comm'n of N.Y., 447 U.S. 557, 561 (1980)(emphasis added).

Here, the "primary purpose" clause in the statute is attempting to handle messages that contain both commercial and noncommercial speech. Long ago, the Supreme Court considered the question of mixed commercial and noncommercial speech and expressly rejected the claim that the admixture results in less protection for the noncommercial portion of the speech. Instead,

454 Shotwell Street, San Francisco, CA 94110 USA
+1 415 436 9333 (v) +1 415 436 9993 (f) www.eff.org

the Court held that when the ad or promotional aspects of the message are inextricably intertwined with noncommercial aspects, then the message is noncommercial for purposes of First Amendment analysis. Thus any regulation that reaches such e-mail messages must survive strict scrutiny. Riley v. National Federation of Blind of N. C., Inc., 487 U.S. 781, 796 (1988)(ordinance regulating charitable fundraisers held unconstitutional). In Riley, the Court considered, and rightly rejected, many of the arguments likely to be made in support of expanding the reach of the CAN-SPAM law beyond purely commercial speech. For example, the Court rejected a test that would based liability on whether the speech would have occurred, but for the commercial element, stating: "solicitation is characteristically intertwined with informative and perhaps persuasive speech . . ., and for the reality that without solicitation the flow of such information and advocacy would likely cease." Riley at 796. It also rejected the claim that compelled speech requirements, such as the CAN-SPAM requirements of specific subject line information and compelled return address information, should be subject to reduced constitutional scrutiny than flat bans on the speech. Id. at 796-797.

The Riley case also provides a relatively bright line rule, avoiding the significant vagueness problems that would attend any of the other formulations suggested in the ANPR. Invariably, a test that turned on the "importance" of a portion of a message to the rest or the "net impression" of the message turn on individual predilections of the reader or evaluator. One of the touchstones of First Amendment law is the requirement that rules criminalizing speech, or even discouraging it under pain of civil exposure, be extremely clear and objective. Rules that force the speaker to predict the subjective response of recipients or third party, such as law enforcement, about how "important" the commercial portion of a message was, will force speakers to be more cautious, creating a chilling effect on even legitimate speech for fear of an adverse response. Such rules are rightfully constitutionally suspect.

EFF believes that the Riley court analysis is correct, and that it is appropriately applied to the CAN-SPAM Act. The ability to combine commercial messages with noncommercial ones is one of the chief drivers for the creation of noncommercial speech both online and offline. Television, radio and newspapers are all funded by the inclusion of commercial messages into noncommercial programming. Nonprofit organizations, clubs and societies all utilize fundraising and commercial sales to support their activities. A rule that would potentially subject these activities to the severe penalties of the CAN-SPAM Act will chill these messages and reduce the amount of legitimate speech online.

E.2.1. Do "forward-to-a-friend" and similar marketing campaigns in which marketers rely on their customers to refer or forward the commercial emails to someone else fall within the parameters of "inducing" a person to initiate a message on behalf of someone else?

"Forward-to-a-friend" situations should not create any form of liability under CAN-SPAM. This statute was aimed at the sophisticated commercial vendor and not ordinary people. To allow liability for a consumer who obtains no financial benefit from the e-mail he or she forwards would be a trap for ordinary people. Similarly, it would be unfair to track liability back to the sender based upon the uncontrollable efforts of its customers, who may be overly enthusiastic in their efforts or otherwise unaware of the legal restraints placed by the law. For example, if a customer removed some of the mandated information, like the subject line information, neither the original sender nor the customer should not be liable.

E.4.2. If a sender's email address does not, on its face, identify the sender by name, does that email address comply with § 5(a)(1)?

It may. The Act requires the "from" line to accurately identify the person who initiated the message such that it would not be materially false or materially misleading. While EFF is supportive of this concept generally (misleading and false information in advertisements were rightfully illegal under the Lanham Act as well as other statutes prior to CAN-SPAM), we are concerned about the expanded definition of "materially false or materially misleading" in CAN-SPAM. "Materially false or materially misleading" is defined under the CAN-SPAM statute as altering or concealing of header information in a manner that would impair ability of an ISP or a law enforcement agency to identify, locate, or respond to the sender. A problem arises if a person sends an e-mail with an ad under his nickname instead of his real name. For example, if a subscriber of an allergy discussion listserv sends an e-mail under "DC Asthma" to the discussion group recommending a product or an allergist in the area. The listserv recipients may know the identity of "DC Asthma," but law enforcement or the receiving ISP does not. Accordingly, we suggest that the FTC rule restrict the scope of this to misleading *the recipient*, and not reach situations in which the recipient or the sending ISP know who the sender is, but only law enforcement or a receiving ISP does not. Thus, if the recipient or sender's ISP can identify, locate, or respond to the sender through the nickname or other mechanism, then the sender should still be considered in compliance with § 5(a)(1).