Before the Federal Trade Commission
Washington, D.C. 20580

In the Matter of Definitions, Implementation, and Reporting Requirements Under the CAN-SPAM Act	Project No. R411008 RIN 3084-AA96

COMMENTS

These comments are submitted pursuant to the Notice of Proposed Rulemaking[1] released March 10, 2004, by the Federal Trade Commission ("FTC" or "the Commission") regarding the implementation of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "CAN-SPAM Act" or the "Act").[2]

BACKGROUND AND INTRODUCTION

I am an attorney in private practice in Los Angeles. My firm represents many entities that employ the Internet and e-mail messages in order to market and provide services. For over a decade, I have lectured and written extensively about Internet legal issues, both to the industry and to attorneys representing it. In all, I have probably given more than a dozen lectures and published roughly 75 articles on the subject.

Several of my clients have developed relationships, generally by contract, with third-party e-mail services (known as "affiliates") that send commercial content on their behalf. Those clients have expressed concern regarding the application of the CAN-SPAM Act and, specifically, whether they are liable under the Act for the conduct of third-party affiliates. As explained herein, the Commission should limit such liability in accordance with general theories

---

1 Published at 69 Fed. Reg. 11775 (Mar. 11, 2004) ("Notice").

2 Pub. L. No. 108-187, 117 Stat. 2699 (Dec. 16, 2003).

of agency and vicarious liability, to ensure and confirm that entities will not be liable under the Act when third-party affiliates send emails that are unsolicited, or otherwise in violation of the Act, without authorization.

As explained in these comments, several provisions of the CAN-SPAM Act are unclear as to which entities may be liable for violations of the Act and how such liability may be avoided. Strictly construed, any person whose content is transmitted in an unsolicited e-mail is liable for all resultant violations of the Act. Such liability is avoided if the person "prevent[s] the transmission" or "report[s] it to the Commission" but, as a practical matter, in the majority of instances that action is not possible, especially in the context of affiliates who have sole control over their e-mail facilities. If the Commission implements the Act in such a way that compliance becomes unreasonable or impossible, the result will be to discourage entities from attempting to comply and will likely lead to increasingly deceptive practices to mask e-mail origination and to transport spamming operations to locations outside the United States where enforcement, as well as jurisdiction, becomes problematic. In other words, unreasonably harsh rules will generate more spam, not less. That obviously undesirable result can be avoided by adopting the limiting constructions to the Act proposed in these comments.

In addition, I address the Commission's request for comment on the establishment of a "rewards" program to encourage parties to report CAN-SPAM Act violations. Although such a program may be beneficial in this context, it is also vulnerable to abusive or anticompetitive activity. The Commission should address the potential for false reports submitted to gain competitive advantage, and should impose sanctions or penalties for such

conduct. The Commission has authority to adopt such sanctions under the Federal Trade Commission Act,[3] and the exercise of that authority is consistent with sound public policy.

I. THE COMMISSION SHOULD CLARIFY THE DEFINITION OF "INITIATE" TO EXCLUDE MESSAGES SENT BY A THIRD PARTY WITHOUT AUTHORIZATION

The Notice seeks comment on the scope of the definition of "sender" under the CAN-SPAM Act. Notice at 23, Section E. The Act applies to all "senders" of e-mail, which include both those who "initiate" messages and those who advertise or promote their product through such messages. Act § 3(16)(A). To "initiate" a message means to "originate or transmit" it or to "procure the origination or transmission" of the message. *Id.* § 3(9). The Commission's construction of the definition of "initiate" — what it means to "procure" the sending of a message — is of crucial import. "Procure" is itself defined as "intentionally to pay ... or induce" another to send a message. *Id.* § 3(12). Yet it is possible that those statutory definitions may be read to mean that any entity whose product or service is promoted by a third party is as liable under the Act as the sender itself. Indeed, the Act states that more than one entity may be deemed to "initiate" an e-mail. *Id.* § 3(9).

In electronic marketing, it is common for commercial entities to retain, typically by contract, third-party e-mail affiliates to advertise goods and services. In those arrangements, the commercial entities will supply retained affiliates with content that they wish them to advertise. For compensation, the affiliate e-mails content provided by the commercial entities to persons on lists that the affiliate independently owns or obtains.

Thus, the affiliate controls the recipient lists as well as the servers that send the e-mails. If the affiliate configures its systems to send unauthorized, unlawful e-mails, the affiliate

---

[3] 15 U.S.C. §§ 41 *et seq.* ("FTC Act").

cannot be precluded from engaging in that practice, even if the service contract does not permit it. Unfortunately, affiliates have used this system to extract additional compensation or more favorable contract terms. For example, commercial advertisers and content providers have been threatened by affiliates that the affiliates will engage in widespread, blatant spamming if they do not receive whatever benefit they request. Were these affiliates to make good on their threats and send unlawful e-mails, it certainly could not be said that these e-mails were authorized by the content provider/advertiser or that the content provider/advertiser should be held responsible for them. Even a single incident of this type could be devastating for an advertiser, particularly a small one, because of the cost of defending an allegation and, especially, because of the huge penalties authorized by the Act.

On its face, however, the CAN-SPAM Act could assign liability to the content provider/advertiser when affiliates willfully and without consent send unlawful e-mails containing the advertiser's content.[4] As such, the Act would impose what is essentially strict liability on any entity whose content appears in a spam e-mail. That result is unacceptable. The law generally abhors strict liability, especially where, as here, criminal penalties are contemplated. *E.g.*, *United States v. X-Citement Video, Inc.*, 513 U.S. 64, 70 (1994) (construing a federal statute prohibiting exploitation of a minor to require proof that defendant was aware of victim's age); *Staples v. U.S.*, 511 U.S. 600, 618-19 (1994) (overturning conviction on gun offense on grounds that prosecutor failed to prove defendant's knowledge that gun was among those that must be registered); *United States v. United States Gypsum Co.*, 438 U.S. 422 (1978) (intent is necessary element of criminal antitrust offense). Even where the unlawful conduct is

[4] Several provisions of the CAN-SPAM Act require a scienter showing in order to support a state enforcement action. Act, § 7(f)(9). There does not appear to be an analogous scienter requirement with respect to actions brought by the FTC. Thus, an entity may be deemed liable under CAN-SPAM in a federal enforcement action for all violations, without regard to whether the defendant had actual or implied knowledge that the unlawful conduct took place.

considered more an affront to "public welfare" rather than a violent act, courts do not readily accept strict liability. *Morissette v. United States*, 342 U.S. 246, 256 (1952) (overturning conviction for conversion of Government property for lack of *mens rea*). At the least, a defendant must know the practical nature of his actions, even if he is not aware of their legal significance. *See United States v. Bailey*, 444 U.S. 394, 408-09 (1980) (affirming convictions for escape where defendant prisoners affirmatively took actions to leave prison without authorization).

In addition, at civil common law one is responsible for the actions of another only if those actions are authorized. *See* RESTATEMENT SECOND OF AGENCY § 1 ("RESTATEMENT"). Thus, for example, a principal is liable for the actions of an agent only if the agent obtained authority for those actions. "Authority is the power of the agent to affect the legal relations of the principal by acts done in accordance with the principal's manifestations of consent to him." *Id.* § 7. An agent also has "apparent authority" if the principal communicated his consent to the third party affected by the agent's actions. *Id.* § 8.

Agents that willfully violate the law — for example, by committing an intentional tort — do not confer liability on their principal unless the violation was ordered or was a necessary means of satisfying an order. *See, e.g., Denlinger v. Brennan*, 87 F.3d 214, 216 (7th Cir.1996) ("intentional torts outside the scope of employment usually do not lead to an employer's vicarious liability"); *Whalen v. Allers*, 302 F. Supp. 2d 194 (S.D.N.Y. 2003) (employer not liable for employee's violation of 28 U.S.C. § 1983); *Haybeck v. Prodigy Svcs. Co.*, 944 F.Supp. 326 (S.D.N.Y. 1996) (Internet company not liable for employee's infecting another employee with HIV). *See also* RESTATEMENT § 228(1)(c) (principal liable if act was "actuated, at least in part, by a purpose to serve his master"). Nor is the principal liable for

actions committed that are outside the scope of the agency. *See* RESTATEMENT §§ 229, 235. Thus, for example, employers are not vicariously liable for the actions of employees that are on "frolic and detour." *E.g., Kirchoffner v. U.S.*, 765 F. Supp. 598 (D.N.D. 1991) (government not vicariously liable for automobile collision involving federal employee acting outside his employment).

The application of vicarious liability with regard to digital copyright infringement also counsels against an overly broad definition of a an e-mail "sender." Under copyright law, a third party may be liable for copyright infringement if it "has the right and ability to supervise infringing activity," as well as "a direct financial interest in that activity." *Fonovisa, Inc. v. Cherry Auction*, 76 F.3d 259, 262 (9th Cir. 1996). *Accord, A&M Records v. Napster, Inc.*, 239 F.3d 1004, 1023 (9th Cir. 2001); *Arista Records, Inc. v. MP3Board, Inc.*, 2002 WL 1997918, at * 11 (S.D.N.Y. 2002). That liability attaches even to Internet Service Providers that transmit the offending content if they "receive a financial benefit ... in a case in which the service provider has the right and ability to control such activity." Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 512(C)(1)(B). *See also Arista*, 2002 WL 1997918, at 11 (ISP must have "the right and ability to police" the use of their service); *Hendrickson v. Amazon.com, Inc.*, 298 F. Supp. 2d 914, 918 (C.D. Cal. 2003) (Amazon "does not have the right and ability" to control the sale of infringing material by a third party). Thus, unless an entity could have exerted control over the infringer, and derived economic benefit from failing to do so, the DMCA will not impose copyright liability.

The CAN-SPAM Act contains no such limitations of liability.[5] Yet the commercial content providers/advertisers who use affiliates to advertise are in the same position

[5] The Act does exempt those engaged in "routine conveyance" of an e-mail from spam liability, which has been interpreted within the industry to refer to ISPs. Act, § 3(9).

as the ISPs that are deemed immune under certain circumstances under the DMCA — they do not have the ability to control or preclude unlawful activity. Unfortunately, the Act states that anyone who "procures" the transmission of an unlawful e-mail must be treated in equal fashion as the person who actually transmitted it, regardless of whether he had control over such transmission.

Thus, it is incumbent upon the Commission to construe the CAN-SPAM Act in a manner that comports with the construct of agency law and the analogous liability exemptions under the DMCA. It should adopt, in accordance with its express rulemaking authority under Section 13,[6] definitions of "procure" and "initiate" — and, therefore, "sender" — that provide a clear and reasonable limit on the types of entities that may be liable for spam.

Specifically, the Commission should adopt a regulation that where a commercial content provider/advertiser has imposed a policy upon its affiliate for CAN-SPAM Act compliance, an affiliate's violation of that policy renders the offending e-mail an ***un****authorized* transmission that the content provider/advertiser has not, as a matter of law, "initiated." For example, in compliance with the Act, my clients are putting in place policies to instruct affiliates as to how messages shall be sent on their behalf. All messages must contain the requisite disclosures provided in Section 5(a)(5), and must not be "spoofed" to contain false origination identification, or contain false subject lines and headers as proscribed by Section 5(a)(1). In addition, affiliates are being instructed that any "opt-out" message must be honored within 10 days, Section 5(a)(4), and a list of those who opt out must be maintained and forwarded regularly. With that policy, my clients have in effect provided affiliates authority to send e-mails, *but only subject to their compliance with the Act.*

---

[6] "The Commission may issue regulations to implement the provisions of this Act (not including the amendments made by sections 4 and 12)." Act, § 13(a).

A violation of a compliance policy would in effect breach the affiliate's authority. Any non-compliant e-mails would therefore be unauthorized, and thus not fairly attributable to the content provider/advertiser. Such conduct would amount to an intentional violation of the law for which principals and employers ordinarily would not be responsible. *Denlinger*, 87 F.3d at 216. Under such circumstances, then, the commercial entity should not be said to have "initiated" the e-mails, and should not be considered a "sender" under the CAN-SPAM Act. To hold otherwise would render violations of the Act strict liability offenses, which is unreasonable and unwise as a matter of public policy.

If the rules implementing the Act are too draconian, or spread liability to those that had no control over the conduct, the prevalence of spam is likely to increase. Spammers will become more sophisticated at avoiding detection and prosecution, reducing this important legislation to a toothless admonition. By adopting rules that fairly attribute liability to those actually responsible for spam, the Commission will encourage more entities to be aggressive combatants against spam and to structure their marketing practices to be open, transparent, and spam-free. In furtherance of that goal, an entity that has put a compliance policy in place to govern the conduct of an affiliate must not be considered a "sender" when that policy is violated. The Commission should expressly adopt this bright-line test to make clear how advertisers may in good faith comply with the Act.

II. THE COMMISSION SHOULD EXPLAIN AND CLARIFY THE MEANING OF "TO PREVENT THE TRANSMISSION" OF A MESSAGE

The CAN-SPAM Act includes specific provisions to address "spoofed" e-mail, that is, messages in which the origination information is falsified to mask the identity of the sender. The Act imposes liability on anyone who derives financial benefit from a spoofed e-mail, reasonably knows of its occurrence, and does not either "prevent" or "report" its

transmission. Act, § 6(a)(1). That provision raises the same issues of authority and vicarious liability as I have discussed in Section I, above. That is, the Act provides no guidance on what it means to "prevent" the transmission of an e-mail.

When an advertiser's content is being e-mailed by third-party affiliates, the advertiser has no actual control over that e-mailing activity. Accordingly, where affiliates engage in spoofing, the advertising entity cannot stop them. But the Act would seem again to hold those entities strictly liable under Section 6(a) when their content appears in a spoofed e-mail.[7] That result is unreasonable, for the reasons I have explained.

It is technologically impossible to prevent affiliates from sending e-mails. Thus, the only available option would be to terminate all contracts with affiliates, which would severely curtail the ability to advertise on the Internet, implicating First Amendment concerns and negatively impacting the growth of Internet commerce.[8] In addition to its effect on commerce and commercial speech, contract termination is, at any rate, unlikely to prevent affiliates from continuing to spoof e-mails, because such termination would not preclude the affiliate from continuing to violate the Act.

Further, any requirement to return or destroy all previously provided commercial content cannot be policed with any degree of assurance. Affiliates may retain the data without detection. Under such circumstances, the entity providing commercial content is powerless to prevent spoofed e-mails containing their content. And as explained above, fundamental

---

[7] Section 6(a) also requires that the entity reasonably knew of the conduct and derived commercial benefit from the spoofed e-mail. Act, § 6(a)(1)-(2). As a commercial entity, the transmission of its advertising conduct is likely to be deemed a benefit, even if the e-mail was unauthorized. And where the e-mail is unauthorized, the entity cannot disgorge any economic benefit it may nonetheless receive. Thus, the only means for avoiding spoofing liability under Section 6(a) is to "prevent" the transmission of spoofed e-mails.

[8] This result would directly contravene Congress's clear goal in fostering the development of e-commerce, as evidenced in its legislative effort to limit taxation on Internet transactions. *E.g.*, Internet Tax Freedom Act, Pub. L. No. 105-277, Div. C, Title XI, 112 Stat. 2681 (1988), *codified at* 47 U.S.C. § 151 note; Internet Tax Nondiscrimination Act, Pub. L. No. 107-75, 115 Stat. 703 (2001), *codified at* 47 U.S.C. § 609.

principles of agency and vicarious liability instruct that an entity that cannot control the actions of a third party should not be liable for the third party's unlawful conduct. Similarly, an entity that did not authorize or send an e-mail should not be civilly or criminally liable for it.

For all of the above reasons, the adoption of a CAN-SPAM Act compliance policy should insulate a commercial entity from liability in the event that an affiliate engages in spoofing. E-mails that are spoofed in violation of a compliance policy are not authorized; they are not fairly attributable to the content provider. Given the practical realities of dealing with third parties, institution of a compliance policy is the most that an entity can do to comport with the Act. Therefore, in accordance with its authority to adopt rules implementing the Act, the Commission should promulgate a regulation stating that commercial entities that impose CAN-SPAM Act compliance policies on their affiliates satisfy the requirements of Section 6(a) and will not be liable for spoofed e-mails.

III. ANY REWARDS PROGRAM MUST BE CONDUCTED IN A WAY THAT PREVENTS OR LIMITS ANTICOMPETITIVE ACTIVITY

The Notice seeks comment on several issues regarding a "rewards system" by which the Commission will provide incentives for reporting violations of the Act. Notice at 26-28, Section G. Although such programs may provide valuable assistance to the Commission, and may deter the sending of spam to some degree, they also carry a dangerous potential for abuse. Accordingly, the Commission should craft any rewards program in order to avoid benefiting parties that make false accusations as a means of gaining competitive advantage.

The Commission's forthcoming order should first explain that liability under antitrust law and for libel may attach for false spam accusations, especially where those accusations do not result in penalties under the Act. False statements to authorities regarding a competitor are not immune from either form of liability. As a matter of antitrust law, while

certain forms of lobbying conduct are immune from antitrust scrutiny under the *Noerr-Pennington* doctrine, based on constitutional concerns with proscribing First Amendment "petitioning" activity,[9] the Supreme Court has expressly rejected the "absolutist position that the *Noerr* doctrine immunizes every concerted effort that is generally intended to influence governmental action." *Allied Tube & Conduit Corp. v. Indian Head, Inc.*, 486 U.S. 492, 503 (1988) (affirming Section 1 judgment against trade association for voluntary standards-setting). For example, misrepresentations and lies made in the course of lobbying can also, in some circumstances, form the basis for antitrust liability. *Allied Tube*, 486 U.S. at 499-500; *California Motor Transport Co. v. Trucking Unltd.*, 404 U.S. 508, 513 (1972) (reversing dismissal of Section 1 civil case on antitrust immunity grounds). In addition, lawsuits brought against competitors that are "objectively baseless," such that "no reasonable litigant could reasonably expect success on the merits," are also subject to antitrust liability. *See Professional Real Estate Investors v. Columbia Pictures Indus.*, 508 U.S. 49, 60 (1993). In accordance with this settled doctrine, the Commission should forewarn that accusations of CAN-SPAM violations against a competitor that prove to be objectively baseless shall remain vulnerable to antitrust liability and are discouraged.

In addition, those falsely accused may have an action in libel and defamation. Those claims are common law torts governed by the precedent in the relevant state. In the District of Columbia, for example, libel is (i) a false and defamatory written statement; (ii) published without privilege to a third party; (iii) involving some fault of the speaker; (iv) that caused the plaintiff special harm. *Messina v. Fontana*, 260 F. Supp. 2d 173, 176-77 (D.D.C. 2003). In the context of spamming, false accusations could have disastrous effects on the

---

[9] *Eastern Railroad Conference v. Noerr*, 365 U.S. 127 (1961); *United Mine Workers of America v. Pennington*, 381 U.S. 657 (1965).

reputation of an entity's goods and services. It would paint the company as untrustworthy, and may raise the appearance that it is capable of far worse abuse, such as fraud and identity theft. It would, therefore, be easy for one falsely accused of spamming to bring a strong claim for libel against his accuser and obtain considerable damages.

A closely analogous case regarding libel was recently decided in Hawaii under the DMCA. *Rossi v. Motion Picture Ass'n of America, Inc.*, 2003 WL 21511750 (D. Hawaii 2003). There, a website owner sued the Motion Picture Association of America ("MPAA") for reporting him as a copyright infringer to his ISP in accordance with the notice requirements of the DMCA. The owner sued under several torts, including libel and defamation. Summary judgment on this claim was granted in favor of MPAA on its defense of privilege. The Court held that the MPAA had reasonable grounds to believe that the website owner had infringed their copyrights by providing downloadable movies and was discharging a public duty to uphold the copyright laws. 2003 WL 21511750, at *4. Those circumstances gave the MPAA a qualified privilege for its statements, precluding liability.

Under that precedent, false spam accusations made without a reasonable basis would enjoy no privilege, inviting liability for libel and defamation. And because accusations may carry competitive advantage, or simply to obtain a reward from the Commission, such baseless accusations are likely to occur. The Commission should, therefore, expressly state in the rules establishing the proposed rewards system that spam reports that would constitute defamation or anticompetitive conduct will not be entertained by the Commission, and that civil liability may result from unreasonable or baseless reports of spamming.

Finally, the Commission should impose penalties on those who falsely report spam. These penalties are within the Commission's authority under Section 5 of the FTC Act, as

they are patently "unfair" and "deceptive." 15 U.S.C. § 45(a). Penalties may include a fine, as well as injunctive relief to prevent the informant from making additional baseless accusations. In that way, the Commission's efforts to combat spam will be more precisely targeted. More importantly, they will not have an unintended harmful effect on the competitive landscape of Internet sales and service.

CONCLUSION

For the reasons explained herein, the Commission should:

- Adopt a definition of "initiate" that excludes unauthorized messages sent by a third party;
- Adopt a definition of "prevent" that clarifies an entity's obligations to prevent violations of Section 5(a)(1) of the Act by third parties; and
- State that objectively baseless reports of violations of the CAN-SPAM Act may result in civil liability as well as Commission fines and injunctive relief.

Respectfully submitted,

Clyde DeWitt
Weston, Garrou & DeWitt
[redacted]
Los Angeles, CA[redacted]

Dated: April 20, 2004