Before the
Federal Trade Commission
Washington, D.C.

In the Matter of	)	
	)	**FTC Project No. R411008**
CAN-SPAM Act Rulemaking—Do Not Email	)	

To: The Commission

COMMENTS OF
The Electronic Privacy Information Center
March 31, 2004

Pursuant to the FTC Notice of Proposed Rulemaking[1] dated March 11, 2004, regarding the CAN-SPAM Act and the "National Do Not E-mail" Registry, the Electronic Privacy Information Center submits the following comments, recommending that the Do Not Email Registry must be understood to be one part of a multi-tiered, international approach to protecting consumers from spam, and that the Do Not Email registry should protect individual privacy interests on the Internet by using domain-level listings to protect the privacy of individual email addresses.

The Electronic Privacy Information Center ("EPIC") has a long-standing interest and participation on the complex policy issue of reducing spam. In testimony last year to the Senate Committee on Commerce, Science, and Transportation, EPIC Executive Director Marc Rotenberg discussed the need for a "multi-tiered approach" combining aggressive enforcement, technical solutions (such as filtering and identification of spam), and cooperation at the state and international level.[2] As part of the Privacy Coalition, EPIC joined a group of consumer, civil liberties, computer science, and privacy organizations in recommending a basic policy framework for addressing spam.[3] This policy framework is defined by six principles:

- A clear definition of spam as unsolicited, bulk, commercial email
- Establish Opt-in
- Ensure private rights of action
- Enable technical solutions
- Support international cooperation
- Oppose preemption of state efforts to combat spam

[1] Definitions, Implementations, and Reporting Requirements under the CAN-SPAM Act, 69 Fed. Reg. 48, 11776 (March 11, 2004).
[2] *Hearing on SPAM (Unsolicited Commercial Email) Before the Senate Committee on Commerce, Science, and Transportation Hearing on Spam*, 108th Cong. (May 21, 2003) (Testimony and Statement for the Record of Marc Rotenberg, Electronic Privacy Information Center) *at* http://www.epic.org/privacy/junk_mail/spam/spamtestimony5.21.03.html.
[3] Letter from the Privacy Coalition, Policy Framework for Effective Spam Legislation, to Members of Congress (July 18, 2003) (on file with EPIC).

Further, EPIC has participated in international discussions on spam at the Organization for Economic Co-operation and Development[4] ("OECD"), the Asia-Pacific Economic Cooperation[5] ("APEC"), and the Trans-Atlantic Consumer Dialogue ("TACD"), a forum of 65 consumer groups from the U.S. and the European Union.

SPAM REQUIRES INTERNATIONAL COOPERATION

International cooperation is vital to address the global nature of spam. As TACD recognizes, "concerns about spam are shared by consumers around the world."[6] Just as no one solution exists to spam, no one country can fight the spam problem alone. The Privacy Coalition has emphasized the importance of international cooperation,[7] and both the OECD and TACD emphasize that effective reductions in spam and cross-border enforcement against spammers require that the United States and other countries work together to harmonize legislative approaches[8]. The Do Not Email registry has the potential to be an important part of an international framework and enforcement mechanism against spam. As one piece of the anti-spam puzzle, the effectiveness of the Do Not Email registry on reducing spam depends on cooperation with other spam reduction policies. Specifically, TACD has recommended that the Do Not Email list be created in a manner to provide strong protections for individual users.[9] A domain level Do Not Email registry achieves theses important goals of international cooperation and privacy protection.

DOMAIN LEVEL DISCLOSURE IS NECESSARY FOR THE "DO NOT EMAIL" REGISTRY TO WORK WITH OTHER SPAM REDUCTION EFFORTS

A key element where the Do Not Email registry can cooperate with other spam-fighting policies as part of a multi-tiered, international approach is to focus registry listings at the domain level rather than individual email addresses.

The Do Not Email registry must protect individual privacy by collecting and disclosing only domain names of users that do not wish to receive emails. A Do Not Email registry that collects and discloses individual email addresses frustrates several other spam reduction policies,

---

[4] OECD Spam Conference, Feb. 2-3, 2004. Marc Rotenberg, Presentation of the OECD Spam Workshop: Economic and Societal Impacts of Spam (Feb. 2, 2004) *available at* http://www.oecd.org/dataoecd/47/4/26618949.pdf?channelId=22555297&homeChannelId=33703&fileTitle=Spam+Workshop%3A+Session+2+%28Economic+and+Societal+Impacts+of+spam%29+Presentation.

[5] APEC Conference in Chile, 26-27 Feb. 2004

[6] Trans-Atlantic Consumer Dialogue, Resolution on Unsolicited Commercial Email (Jan. 26, 04) *at* http://www.tacd.org/docs/?id=224.

[7] Letter from the Privacy Coalition, Policy Framework for Effective Spam Legislation, to Members of Congress (July 18, 2003) (on file with EPIC).

[8] Press Release from Organization for Economic Co-operation and Development, OECD Calls on Governments to step up their Fight against Spam (February 2, 2004) *at* http://www.oecd.org/document/17/0,2340,en_2649_37409_26198225_1_1_1_37409,00.html; Trans-Atlantic Consumer Dialogue, Resolution on Unsolicited Commercial Email (Jan. 26, 04) *at* http://www.tacd.org/docs/?id=224.

[9] Trans-Atlantic Consumer Dialogue, Resolution on Unsolicited Commercial Email (Jan. 26, 04) *at* http://www.tacd.org/docs/?id=224.

including consumer approaches promulgated by the FTC itself.[10] The FTC has long recommended that consumers on the Internet protect their email addresses from disclosure to others as a way to reduce spam and prevent potential for fraud and identity theft.[11] This guidance to consumers is designed to protect individual privacy and prevent abuse of email addresses from risks of fraud and identity theft (*e.g.*, "phishing").[12]

An email address-based Do Not Email registry would frustrate and hamper individual privacy interests and the FTC's anti-spam recommendations of non-disclosure of private email addresses.[13] Disclosing individual email addresses to the Do Not Email list would allow spammers to find valid individual email addresses: the FTC has found evidence of email addresses harvesting for spam from email service directories.[14] Further, this list would be subject to abuse from spammers who disregard the CAN SPAM Act or who are beyond the reach of U.S. enforcement; spammers could simply move to countries with little or no anti-spam policy while harvesting email addresses from an email address-based Do Not Email registry. Consumers wishing to reduce spam by using the Do Not Email list should not have to sacrifice their individual privacy by disclosing their individual email addresses in a global list available to spammers.

As a further example of how an email address-based Do Not Email registry could frustrate other anti-spam policy, a Do Not Email registry based on individual addresses unfairly places additional burden on users that change email addresses frequently to avoid spam. The FTC has advised consumers to set up such "disposable" addresses as one way to avoid spam.[15] With an email address-based Do Not Email registry, a consumer following the FTC advice would be burdened by having to reregister the new email address in the registry every time an email address change was made. By unfairly placing an additional burden on consumers, the individual email address Do Not Email registry would frustrate other anti-spam polices.

A DOMAIN LEVEL "DO NOT EMAIL" REGISTRY AS AN ENFORCEMENT TOOL TO REDUCE SPAM

The domain level Do Not Email registry has the potential for being a strong enforcement mechanism for the CAN-SPAM Act by eliminating some of the technical, security, and practical

---

[10] FTC, Don't Want Your Email Address Harvested? (November 2002) *at* http://www.ftc.gov/bcp/conline/pubs/online/dontharvest.htm; FTC, "Email Address Harvesting: How Spammers Reap What They Sow (November 2002) *at* http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm; FTC, Consumer Alert: What's In Your Inbox? (April 2002) *at* http://www.ftc.gov/bcp/conline/pubs/alerts/inbxalrt.htm; FTC, You've Got Spam: How to 'Can' Unwanted Email (April 2002) *at* http://www.ftc.gov/bcp/conline/pubs/online/inbox.htm

[11] *See* fn 10, *supra*

[12] FTC, Is Someone 'Phishing' For Your Information (March 2004) *at* http://www.ftc.gov/bcp/conline/pubs/alerts/phishregsalrt.htm; FTC, How Not to Get Hooked by a 'Phishing' Scam (July 2003) *at* http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm;

[13] *See* fn 10, *supra*

[14] FTC, Email Address Harvesting: How Spammers Reap What They Sow (November 2002) *at* http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm. *See* http://www.ftc.gov/bcp/conline/edcams/spam/pubs/harvestchart.pdf.

[15] FTC, Email Address Harvesting: How Spammers Reap What They Sow (November 2002) *at* http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm;

enforceability issues arising under an email address-based Do Not Email registry. Specifically, enforcement of violations of the CAN SPAM Act by ISPs will be simpler under a domain-based Do Not Email registry. By placing a domain on the Do Not Email registry, the ISP can begin to easily establish patterns or practices of violations of § 5(a) of the CAN SPAM Act. By virtue of placing its domain on the Do Not Email registry, an ISP may create the reasonable presumption that all users on its network do not wish to receive spam, and that further spam to that domain is a transmission of spam after objection, in violation of § 5(a) (4) of the CAN SPAM Act.[16] Legitimate businesses are free to rebut this by proving affirmative consent or a transactional or business relationship with an individual user on a domain, as provided by the CAN SPAM Act.

By listing domain names instead of individual email addresses, the Do Not Email registry would become an effective tool for Internet Service Providers ("ISPs") to limit spam, in addition to use of the Do Not Email registry by individual Internet users. ISPs are forced to pay the bandwidth costs of delivering spam mail; ISPs also bear the costs of spam filtering to protect their users. A domain-based Do Not Email registry would allow ISPs to protect their networks against unwanted email, fraud, and identity theft risks. Acknowledging the interests of ISPs in reducing spam, the CAN SPAM Act allows ISPs to pursue enforcement actions against spammers. Listing only domains in the Do Not Email registry, and not individual emails, is consistent with the legislative intent to allow ISPs to protect themselves against abusive spam traffic.

Further, since Congress did not include a private right of action against spammers in the CAN SPAM Act, the Do Not Email registry under the legislation should not include private, individual email addresses. As CAN SPAM may be enforced by ISPs managing at the domain level, but not by individual consumers, then there is no reason to force individuals to disclose individual email addresses since there is no private right to enforce violations of that specific email addresses.

CONCLUSION

The Do Not Email Registry has the potential to be an important part of a global strategy to reduce the spam problem. There is no silver bullet that will solve the complex problem of spam[17]; many groups, including EPIC, the Privacy Coalition, OECD, and TACD have recognized that the most effective strategy to reducing spam is a multi-tiered framework of policy, technical, and legislative tools. A Do Not Email Registry could form part of this strategy and improve enforcement powers of ISPs. However, it should be implemented with domain-level information rather than individuals' e-mail addresses.

Respectfully Submitted,

Chris Jay Hoofnagle
Associate Director

[16] CAN SPAM Act, Pub.L.No. 108-187, § 5(a)(4) (Prohibition of transmission of commercial electronic mail after objection).

[17] Press Release from Organization for Economic Co-operation and Development, OECD Calls on Governments to step up their Fight against Spam (February 2, 2004) *at* http://www.oecd.org/document/17/0,2340,en_2649_37409_26198225_1_1_1_37409,00.html.

Michael Trinh
IPIOP Clerk

Electronic Privacy Information Center
1718 Connecticut Ave. NW 200
Washington, DC 20009
202.483.1140