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

Comments of the International Council of Online Professionals
in response to Notice of Proposed Rulemaking request for public comments

Definitions, Implementation and Reporting under the CAN-SPAM Act
Project No. R411008

Federal Register Notice (16 CFR Part 316)
dated June 27, 2005

The International Council of Online Professionals (iCop™) is pleased to be presented this opportunity to comment on behalf of our members on the proposed rulemaking contemplated by the Federal Trade Commission under the Controlling the Assault of Non-Solicited Pornography And Marketing Act (the "CAN-SPAM Act" or simply the "Act"). The International Council of Online Professionals is a membership organization composed of the owners of small enterprises whose business operations are conducted entirely or predominantly on the Internet. The mission of the organization is to promote the legal, ethical and responsible operation of business enterprise among its members.

Once again iCop applauds the Commission for its ongoing and lengthy efforts to promulgate a rational regulatory regime in order to facilitate compliance with the CAN-SPAM Act. However, **we feel the Commission has been burdened with accomplishing that which cannot be done as the Act currently stands.**

In the Notice of Proposed Rulemaking (NPRM) the Commission asks two questions which highlight this point.

1. Section 316.2 – Definitions

…

d. Should the Commission adopt a "safe harbor" with respect to opt-out

and other obligations for companies whose products or services are advertised by affiliates or other third parties? If not, why not? If so, what would be appropriate criteria for such a safe harbor?

…

2. Section 316.2(o) – "Transactional or Relationship Message"

…..

j. Where a recipient has entered into a transaction with a sender that entitles the recipient to receive future newsletters or other electronically delivered content, should e-mail messages the primary purpose of which is to deliver such products or services be deemed transactional or relationship messages?

….

The very need to ask these types of questions underscores the difficulty with the CAN-SPAM Act, which is the failure to focus on the core problems and draw the necessary clear lines.

In an effort to cater to the interests of opt-out marketers, ("spammers") and those who believe networks should have a totally free hand, given the legislative thrust of the CAN-SPAM Act, the Commission is obliged to develop rules which end up micro-managing commercial behavior without addressing the real issues, while leaving it within the total discretion of Internet access services as to how to handle Internet mail.

The simple truth is that "spamming" is big business. As long as Congress only **regulates** the sending of unwanted commercial e-mail, while trying to exempt other types of e-mail, the Act serves no useful purpose except to make the lives of permission based marketers more difficult. This is especially true for iCop members who carry out their online businesses in accordance with best practices and now find themselves struggling to

ensure compliance with a regulatory regime which simply does not fit their business model, but instead caters to spammers.

The Act needs to define spam as the sending of unsolicited **bulk** commercial e-mail (UBCE). Bulk means sending one e-mail to more than one recipient at the same time.

The emphasis on bulk is important. An individual forwarding a piece of list e-mail to a friend, a salesman sending one e-mail to a potential customer, introducing himself to that specific customer, or a publisher sending one e-mail to another publisher seeking to do a joint venture are not examples of abuse of e-mail communication, but rather carrying on business in the ordinary course. However, if the salesman or publisher sends the same e-mail to a number of different contacts, then the message is being sent in bulk, and if sent without either express or implied consent, constitutes abuse.

The Act must prohibit the sending of UBCE. At the same time, the Act can give commercial the widest meaning, while structuring the definition of consent to allow for express and implied consent. In turn, it can require that those who grant implied consent are given the opportunity to opt-out from receiving commercial e-mail when their e-mail address is collected.

This will ensure that the Act does not impede accepted forms of ordinary commerce by e-mail. It also avoids the need to try and distinguish between commercial, transactional and relationship e-mail.

In addition the Act should require that commercial e-mail have a ready mechanism to allow recipients to withdraw their consent at any time, without cost, which must be immediately honored in accordance with accepted practice among permission based marketers.

The whole approach of focusing on consent, rather than content avoids the need to get into the myriad of issues involving multiple senders, suppression lists, whether the opt-out obligation should apply to this type of mail or that, extending the opt-out obligation to list providers, any need to distribute suppression lists to third parties or affiliates, while prohibiting the misuse of opt-out requests.

Quite frankly, approaches requiring the sharing of opt-outs with third parties or affiliates are an anathema to any permission based marketer or online publisher whose first instinct is to respect the privacy of list members, which is part of the fundamental relationship between a responsible list administrator and his, her or its list members and who speaks of list members unsubscribing, not opting out, which is spammer terminology.

The Act must also prohibit all activities that facilitate the sending of UBCE. This means:

- Knowingly selling bandwidth to those who send UBCE

- Software used to harvest e-mail addresses in bulk, or carry out dictionary attacks

- Software used to send UBCE which is specifically designed to allow the sender to hide his, her or its identity, by taking advantage of open proxies or relays or other technical means used to hide the sender's identity

- Knowingly providing hosting or bandwidth to those who provide tools or services specifically designed to aid those who send UBCE

- Knowing providing hosting to web sites that are promoted or advertised by sending UBCE

Why? As matters now stand without these prohibitions, the Act allows bandwidth providers to sell bandwidth to spammers and those who provide services that facilitate spamming.

At the same time, because at present UBCE can legally continue, Internet access services must continue to put up high barriers against the receipt of the ongoing tsunami of un-requested bulk e-mail, while being under no obligation to facilitate the delivery of requested, needed or vital e-mail communications.

This makes a mockery of the entire effort to control online abuse of e-mail communication, while weakening e-mail as a viable medium for online commerce.

Without the appropriate legal framework:

- There is no incentive for Internet access services to exercise appropriate security to stop the use of their networks as UBCE sources

- Bandwidth providers are free to sell bandwidth to spammers and those who provide the tools needed by spammers

The result? The worst abusers will to continue to ignore the law and send UBCE through the use of zombie computers, open proxies and relays.

In the meantime, we are fussing over an Act and related rules that do nothing to support and promote permission based marketing, but instead facilitate the ongoing activities of so called "legitimate" opt-out commercial e-mailers, or spammers.

In addition, the Act discourages Internet access services from making the needed investment in network security, while foregoing revenues from supporting spamming.

Rather, the Act encourages Internet access services to continue to rely on technical efforts to control spamming such as e-mail authentication, filtering, block lists and sender reputation schemes, all of which are doomed to fail. Why? Simply put, **none of these technical approaches stops spam at the source.**

The result? The Act places those organizations that decide to enforce network security at a competitive disadvantage.

At the same time, the Act encourages certain backbone providers to continue with business as usual and play both sides of the street, acting as arms merchants by selling bandwidth to spammers, while providing down-stream Internet access services and consumers with filters and other technical means to stop UBCE.

This means the Act as presently written is simply mocking the entire effort to properly control online abuse of e-mail communications.

Congress passed an Act which says to e-mailers: "You can send Government approved spam, as long as you are transparent in your actions and honor opt-out requests."

The same Act says to ISPs: "You can do anything necessary to decline to have Government approved spam on your network, if you choose to operate in that fashion, or you can fully support the sending and receipt of Government approved spam to and from your network. You can also choose to reject any e-mail, whether or not you have reason to believe it is spam, and even though its delivery may be necessary or vital for one of your users."

You cannot build an approach to control online abuse of e-mail communications based on a law that has at its heart such blatant contradictions.

Any legal framework designed to support the necessary policies to control online abuse of e-mail must involve mutual accountability and responsibility.

For those who wish to use e-mail for commercial purposes, this primarily means: being transparent, so that if there are problems, you can be held accountable, and you must only send bulk email with prior informed consent, express or implied, while fully respecting your list members' right to automatically unsubscribe.

As to ISPs this means: taking the necessary steps to prevent your networks from being sources of unsolicited bulk email, which includes investing in network security, not supporting spamming operations or related activities using your network space, and facilitating the delivery of bulk email as requested by your users to their inboxes.

For all these reasons, iCop calls upon the Federal Trade Commission to ask Congress to re-write the Act, so establishing a legal framework which supports the use of electronic mail for permission-based commerce only, while properly facilitating the needed efforts to bring online abuse of electronic mail under control through enforcement of network security.

ALL of which is respectfully submitted, this 27th day of June, 2005.

International Council of Online Professionals
1002 Pine Lake Drive
Pineville, LA 71360
318-445-9931
http://www.i-cop.org

by: jl scott, Phd., Director

and: John Glube, Legal Analyst