Thanks for seeking comments on the issue of sexually explicit material. I'm glad to see the FTC (and the Congress) taking action against sexually objectionable material in email. I would like to comment on a few things:

1. As ever, I'm not sure what the definition of "pornographic material" is. What is pornographic to me may not be to the transmitter of the material, leading to confusion to be settled in the appellate courts. While I understand that it is not the FTC's job to supply this definition, it is certainly the job of the congress.

2. Is there any technical definition of the "brown paper wrapper"? It is mentioned on the abstract, but not in the proposal.

3. It is possible that the brown paper wrapper the sender might choose would be to use JavaScript to hide the explicit content until the user clicked a disclaimer or some such. Users are encouraged to disable JavaScript in their mail reader to avoid security breaches. By disabling JavaScript, the mail reader might display explicit content by default, possibly making a loophole for the sender. Likewise if the sender is using a text-based email reader, techniques using JavaScript or HTML to hide explicit content might fail. Whose fault would it be if the content was displayed? The users, the senders, or the author(s) of the mail reader?

4. The proposal should specify the character encoding (ASCII or 8859-1), to avoid issues where messages are sent in, for example, two-byte unicode characters. The phrasing in the proposal specifies that the proposed mark be present in the first 27 characters, but fails to specify any encoding, leaving a potential loophole where messages may be sent in, say, ROT-13 encoding, rendering the proposed mark unintelligible in most email readers. Perhaps the best way to manage this would be to include a definition of "characters" in 316.1(c).

5a. In 316.1(a), reads, "Any person who initiates, to a protected computer, the transmission of a commercial electronic mail message..." If the sender of the message sends it to an open SMTP relay, do they meet this criteria? The open relay could be considered an unprotected computer if it relays messages from any sender to any recipient.

5b. Following up on 5a, referencing 316.1(a), when an open SMTP relay sends the message to the recipient's mail server, does the owner of the open SMTP relay meet this criteria?

I would appreciate any feedback the Commission has.

Brad Koehn