Nanyang Business School
Nanyang Technological University
Singapore 639798

September 13, 2005

Mr Andrew Haire
Assistant Director-General (Telecoms)
Infocomm Development Authority of Singapore
8 Temasek Boulevard #14-00 Suntec Tower Three
Singapore 038988
Fax: (65) 6211-2116
E-mail: spamcontrol@ida.gov.sg

Dear Mr. Haire:

I have read the proposed spam control bill at http://www.ida.gov.sg/idaweb/doc/download/I2883/2nd_Joint_IDA-AGC_Consultation_Paper.pdf and have the following comments.

I am excited to know that I can not only sue the sender of the SPAM, but the company being advertised. This is an excellent idea, as the sender is frequently hard to detect. In contrast, the company selling the product must make itself known in the commercial e-mail.

However, I note the excessive technology focus of the proposed bill. The crux of SPAM is the social problem of criminals advertising their products at the cost of recipients. Make a law that criminalizes such activity. Do not make a law that criminalizes technology. I will illustrate how the technology focus damages the bill below.

First, I fail to see why unsolicited commercial (e-)mail should be narrowly defined as either e-mail or mobile phone mail. Junk faxes, unsolicited commercial telephone calls, and physical junk mail all cause similar kinds of inconveniences. Why not make the law applicable to all forms of business to consumer telecommunications and to postal mail? Essentially, such a law should criminalize the transmission of advertising where the cost of the advertising is partly or wholly borne by the recipient.

Second, the definition of sender (clauses 3(3)b and 7(2)b in the proposed act) isn't very clear. One emerging trend is 'spacking,' i.e., the sending of unsolicited commercial e-mail (UCE) through hacked accounts or open ports on home computers. If my computer sends UCE, am I responsible for it? Intent should be a critical part of the definition of sender. If I did not intend to send the mail, I should not be liable.

For example, assume hacker A in the Philippines uses a computer with an open port owned by B in Singapore to send SPAM. (1) Is B liable, since B sent the SPAM? (2) Is the SPAM governed by the act, since A is in the Philippines, and does not have central management and control in Singapore?

Now, what if Organization A with central management and control in the Philippines routes the SPAM through a small subsidiary office in Singapore. The system is automated so that no human agent in Singapore sends the SPAM. Is the SPAM subject to the spam control bill?

Third, some kinds of forums are handled through e-mail (e.g., ListServs), while others are not (e.g., Usenet News). If I am a member of a forum handled via e-mail and I receive SPAM through it, I can sue the sender. However, if I am a member of another kind of forum, I cannot sue the sender. Why? Note that some ListServs are handled by e-mail, but viewed by recipients on the web. Thus, to the recipient, there may be no distinction between an e-mail based and non-e-mail based forum.

Fourth, the definition of "unsolicited" is unclear. The definition identifies particular kinds of unsolicited e-mails, but does not articulate when an e-mail is solicited. If I have a prior business transaction with an organization, can they send me commercial e-mail?

Fifth, civil suits are insufficient to reduce SPAM. The act frequently cites the US CAN-SPAM act. However, in the US, SPAM is also a criminal offense. One can be arrested, fined, and jailed by the US government.

Sixth, the combination of an opt-out clause and public education could potentially increase the suffering of SPAM recipients. Many modern SPAMs employ sophisticated deceptive strategies. It will be pragmatically impossible to teach e-mail users about all (or even most of) these deceptive strategies. If this bill becomes law, it will become increasingly difficult to distinguish legitimate opt-out sites and disguised mail-harvesting sites. While the law makes mail harvesting illegal, the fact is that most spammers/mail harvesters are practically impossible to track down and apprehend.

Seventh, the law does not take into account EDI systems run by Small and Medium Enterprises (SMEs). Many of these organizations cannot afford EDI (or even XML based) systems. Their data is thus sent over e-mail. Easy to construct computer systems (COM-based e-mail programming libraries now come with many commercial e-mail clients) extract the e-mail to throw into databases. Such systems can easily send over 100 messages a day or 10,000 messages a year. If two SMEs sever their ties, one SME could send the other "UCE," even though there was no "intent" to do so.

I hope you take these issues into account.

Sincerely,

Cecil Chua