July 24, 2004

Submitted by: Ms Lau Yeong Shoon

Re: **Anti-Spam Law Public Consultation**

Any cases cited for examples in the following are real and experienced, and not made up. They have all been communicated to the ISP I use, Pacific Internet, and I have spoken and sent these cases to the attention of Mr Kenneth Goh of PacNet. This submission has three parts: General Concerns, Concerns regarding the Paper, Questions in the Paper.

General Concerns:

1. **Definition of Spammer / Unsolicited Email Sender**—Those who ***violate*** this legislation should be defined as those (even "commercial") senders/organisations that ***do not already*** have our email addresses in their database by virtue of ***our having given*** our email addresses to them in any form, perhaps in our engagement with them in a sales transaction or communication, we filled in their forms or something with our email addresses.

   Currently the spate of spammers are mainly those who '**stole**' our email addresses by whatsoever means we do not know, but certainly including those who bought from "email lists sellers" who promise hundreds of thousands of private and public email (from now shortened to 'em') addresses. These current spammers (at least those I received) are people or organisations whom ***I don't know*** anything about, many a time don't even know their existence; including spammers who attempt to sell to me em lists of hundreds of thousands of em addresses,—local and foreign, private, personal or company.

   For example, if a person makes a transaction at a company who asks him to give his em address, and he did. This could be taken by the company to mean it can send him unsolicited em till he opts out. He could have chosen in the first place not to give his em address. When an em address is not given in this manner, the company should have utterly no right to send unsolicited em to all others whose em addresses it have found by other means, by buying lists, or stealing them from watching the internet, etc.

   Such should **not** be included as valid spammers even if they abide by all the requirements of using "[ADV]" etc., or make claims that we subscribe to them, which claims they have employed before in their gimmicks too. In these latter cases, where they claim we subscribe to them, the ISPs should be empowered to take legal actions against them when the subscriber affirms that he has not "subscribe" to the spammer.

   Furthermore, ***individuals should not*** be allowed to spam, even if they comply with all the use of "[ADV]" etc. That is, only commercial (legal) organisations can send unsolicited em by complying with all the requirements; the failure of which is a violation of this legislation.

2. The legislation must empower the ISPs or the authority to take legal actions against those who **sell** em addresses, as well as those who violate intellectual property rights (a persistent spammer is now selling "primary school examination papers"), whether by this law or any other laws.

3. I am not sure if the currently drafted legislation would penalise those who employ such tricks as, for example, "bu_yFurni_ture AT Cheap_0utlets" in subject line. Notice that underscores are embedded to make words not valid for filtering out, as well as zero (0) are used in place of 'oh' (O) or vice versa.

4. The requirements of valid spams should require that the Subject line must start with "[ADV] "—a space must follow "[ADV]" and no other punctuation marks or tricks be allowed.

5. The legislation should **Exclude** all "commercial" communications of obscene, undesirable, vexing, lewd 'commodities and services' [*sic*]. Those who sell enlargements of body parts are **objectionable, obscene and lewd** and must **not** be allowed as valid spammers; and be *immediately* and *automatically* taken to legal actions by ISPs and the authority, the moment an ISP subscriber sends the complaint. Please note that the gender of the recipients are not known from em addresses, so that these become even monsters and tormentors of the recipients; and should be additionally charged as harassers, besides all the other laws that they have violated.

In my opinion, if the above considerations are properly fenced by the legislation, the opt-out could be a valid option to protect em users as well as genuine commercial activities.

Concerns in the Proposed Legislation Framework for Control of Email Spams:

Pt. 10, p. 2: Please see my note no. 5 under "General Concerns" above.

Pt. 2.10, p. 9: Spammers can frequently be traced by their names and/or mobile phone numbers or websites included in their contents. So that within Singapore, these spammers can be blacklisted by having their identities, which the first ISP they use have, circulated to all the other ISPs to stop their subscription with the others. Also, their mobile nos., etc., listed in their contents allow the tracing of them to be taken to court for legal actions. They should include those from Singapore who use other countries to send their spams.

Pt. 3.8, p. 12: (feedback) those free downloads are for trials only, subsequent uses require payments. Question should be who pays? Spammers pay to spam; or users pay money to block them and pay time to remove those not blocked? In any case, one of the free trials was such that if one does not have another of their products, their anti-spam cannot be used. Another of the free trial has a long-winded way of accessing their site to download, such that it cannot be found and cannot be downloaded.

Pt. 3.15, p. 14: Does this mean that CASE will prosecute those spammers, or that a reporting of them to CASE will empower CASE to prosecute these as well?

This also concerns Question 13 of the paper.

Pt. 5.12, p. 22: If the definition similar to the US's "multiple" is adopted, such cases as that of Jason and Tony (PacNet knows) who run around repeatedly spamming under many varied different pseudo generated originating return em addresses, should be accumulated together for Jason and Tony as their tally. That is, the tallying should not be based upon a tally of individual return em addresses. In the Jason and Tony case, their contents exposed them as having hidden under varied different probably useless em addresses.

Pt. 5.17, p. 24: Very good, promoters of spams (even sellers of em addresses), procurers and commissioners of spams should all be made responsible for spams generated; or else these may be local personnel who hide by use of foreign spam generators.

Pt. 5.22, p. 25: Take note that 'valid' unsolicited em (complying also with all the requirements of use of "[ADV]" etc.) should only mean organisations with em addresses "**in their database**" (also my point no. 1 under "General Concerns"). This must mean that if we have not given to these organisations our em addresses, we are not "in their database" and should never be sent their unsolicited em.

Pt. 5.28, p. 29: Pt. (b)—should be "must" contain "[ADV]" and a space after it, and in SUBJECT line of em.

Pt. (d)—the sender **must not** further sell or pass on, by whatever means, the em address of the ones who opted out, to anyone else. He must delete them completely from his system.

Pt. (e)—add also telephone contact. *Company names must* be included, that will exclude individuals who spam either for themselves or for others.

This pertains also to Question no. 12 of the paper.

Questions in the Paper:

Qs. 1, 9: If ISPs do not sell or pass their subscribers' em addresses outside of their realms, and commercial organisations respect their clients and customers' privacy and do not sell their clients/customers' em to others, then only those "**in their database**" are opened to receiving unsolicited em, and the opt out system could probably function pretty well to contain spams.

Any em received from organisations or individuals to which the recipient did not given his em address must be taken to task as having violated this legislation. Em addresses bought from em address sellers are not to be treated as "in their database." The legislation should spell this out super clearly.

Q. 2: All objectionable, lewd (even to some but not to others), obscene, pornographic, body-part enlargement, gambling, offensive contents should **not** be regarded as valid "commercial communications," and should be automatically prosecuted. Engagement in such activities have to be chosen by those who want them (i.e., they opt in to these). **None should be assumed and presumed to want it till opted out**. Gambling should also not be presumed (this Singtel presumes!!)

Q. 3: Except for private personal communications and those subscribed by individuals, all others should be treated as spams.

Q. 4: Yes.

Q. 5: NO. PacNet knows that there existed a spammer, even a lewd monster and harasser, who sent to only a list of no more than 10 em addresses, and did so persistently. All spams, whether in bulk or not, are spams.

Q. 6: Please see my comment on Pt. 5.12, p. 22, of your paper, above. Furthermore, I think bulk should be defined not 100 in 24 hours but 100 in 48 hours, so as to make it harder for spammers who try to send in badges. Of course cumulate them as well, similar to that employed by the US for counting "multiple" or "bulk."

Q. 7: Very good, all spammers based in Singapore should be stopped, whether they employ overseas servers or not.

Q. 8: YES, ABSOLUTELY. I had attempted to scold one sender of spam by calling the no. in the spam contents, and the spammer claim that he was not the sender but someone was paid to 'serve' him.

Q. 9: Yes, if the spammers are clearly defined as further suggested above. Otherwise, if the argument of "preponderance of spams from overseas" is used, then an opt-in or opt-out regime is ***equally*** ineffective.

Q. 10: Since the legislation can apply only to local spammers, then it should be few hours, perhaps not more than 10 hours, since within Singapore (unlike the US), there is not time-zone differences at all.

Qs. 11, 12: Please see my comment on Pt. 5.28, p. 29, of your paper, above.

Q. 13, 15: Absolutely agree, but I am concern if the ISP will readily and speedily take the violators to legal task? Can the ISP act base upon complaints by their subscribers, after confirmation of validity of complaints?

Must the ISPs only prosecute only under this Anti-Spam Legislation alone? For example, if the lewd monster strikes, can the ISP also prosecute him under other laws? If not, can the ISP be empowered to report him to the police to take action? In some other cases, can CASE prosecute spammers or ISP report to CASE to prosecute them?

Q. 14: Make it $2 per email, and double at each repeat spamming, i.e., 1st offence: $2 per em, 2nd offence: $4 per em, 3rd offence: $8 per em, 4th offence: $16 per em, etc. Yes, there are spammers who repeat umpteen times.

NO cap to their penalty please. This should be great deterrent, unless there be a billionaire spammer around.

Qs. 16–18: Representatives of users must play a bigger part, e.g., CASE. It appears the whole thing now is in the bigger hand of commercial representatives.