Dear sir,

Spam is a technological problem and I believe that the solution lies in technology and not legislation. This is not to say that legislation may not be useful in compelling ISP's to implement technological solution to this scourge of the internet. Licensing terms may be another mechanism.

A quick review of the various strategies that had been used.

a. Black listing - this doesn't work as the spammer can easily change their ip and anme

b. White listing - Very useful but still require the user to scan through all the emails to pick out all the non-spammers.

c. Heuristic keyword search - success rate low though Microsoft security experts said that it holds promise.

d. Opt-in list / Opt-out list -- Doesn't work with cross border spammers. May even flag the validity of the email.

I would like to propose another mechanism that can be implemented quite easily by the ISPs.

What I propose is the use of key access. This means when I give out my email I also give a key for the user. Only those emails that has a valid keycode in the subject line will find its way into my e-mail box. The user can set various categories of keycodes for different uses. Some categories come to mind are:

a. Public keycode. This is like not having code but can stop bots
   from havesting.
b. Public keycode with expiry date.
c. Single use keycode - to be used only once.
d. private keycodes - different people can be given different keycodes.

All keycodes can be removed at the discretion of the user. With keycode access the responsibility of stopping spam lies with the user but the delivery agent at the ISP's server has to be configured/written to handle this. Technologically this is not very difficult.

When the scheme is widely adopted email client may allow the setting to be done in the email client software. As this is new a special client or web-based mechanism for setting the keycodes must be provided by the ISP.

Hope this helps.

Regards,
-kok chee chiong-