

Comments
On
Joint IDA-AGC Consultation Paper

**Proposed Legislative Framework for the Control of E-mail
Spam**

Pacific Internet Limited

89 Science Park Drive
#02-05/06 The Rutherford
Singapore 118261
Tel: 6872 0322
Fax: 6872 5912

COMMENTS ON PROPOSED LEGISLATIVE FRAMEWORK FOR THE CONTROL OF E-MAIL SPAM

Introduction

Pacific Internet Limited (PacNet) welcomes the opportunity to provide our comments on the joint IDA-AGC consultation paper on the proposed legislative framework for the control of e-mail spam.

PacNet supports the legislative initiative in minimizing spam. This is in line with the on-going measures taken by both the industry and its denizens. However, the proposed spam bill needs to be flexible enough to accommodate and withstand the rapidly evolving Internet landscape.

Q1. What are the considerations that should determine whether a communication is solicited or unsolicited?

We are of the view that emails sent by a merchant pursuant to a user's consent provided directly to the merchant, whether generic or specific, should be deemed solicited.

Q2. What are the considerations that should determine whether a communication is commercial?

Q3. Should there be exclusions from the definition of spam?

The definition of spam might also include communications which are not intended to promote or sell products or services but represents a form of propaganda (e.g. soliciting support for political or religious groups, chain letters, etc.). Appeals for donations should only be limited to those from registered charitable bodies.

Q4. Do you agree that the proposed legislation should apply to all e-mail messages regardless of the technology used to access them?

Yes. A technology neutral approach is in accord with the ITU's definition of electronic mail (i.e. correspondence in the form of messages transmitted between user terminals over a computer network). However, the distinction between SMSs & emails may not be clear as emails are increasingly retrieved or downloaded using alternative mobile means e.g. via SMS over a cellular phone, through a PDA, among others. In these instances, the costs of retrieval or download to the user are much higher than traditional means. Hence, we would urge IDA and AGC to expedite the study on mobile spam.

Q5. Do you agree that the proposed legislation should apply only to spam transmitted in bulk?

Q6. What are the considerations that determine whether e-mail messages have been transmitted in bulk?

Yes. However, the parameters should be clear, objective, transparent and easy to apply. The US approach would serve as a useful guideline in the implementation of Singapore's definition of bulk although it is proposed that the initial threshold be set lower (e.g. 20-50 emails instead of 100 emails during a 24-hour period). However, a distinction needs to be made between a single spam email targeting one individual and one that is sent to an entire newsgroup or mailing list.

Q7. Do you agree that the proposed legislation should apply to spam sent from or receive in Singapore?

We believe that the application of the proposed legislation should be limited to the jurisdiction where the offence was perpetrated i.e. Singapore. This serves the objective of preventing Singapore from becoming a spam haven. Further extra-territorial application should be dependent on treaties agreed to between countries supporting combat of spam.

Q8. Do you agree that the person commissioning or procuring spam should also be liable under the proposed legislation?

Q11. Are these minimum standards sufficient?

Yes. We support the spirit in making the ultimate perpetrator of the spam responsible. However, consideration should be given to the extra cost burden on the victim in proving the causal link.

Q9. Would you agree that the opt-out regime for spam control is more beneficial to Singapore as a regional IT and commercial hub?

Although an opt-out regime is more open to abuse and is likely to result in greater volumes of spam than an opt-in approach, it is probably the best compromise given the consideration of not unduly stifling genuine marketing and entrepreneurial efforts.

Q10. What is a reasonable time period for compliance with opt-out requests?

Compliance with opt-out requests should take place as soon as reasonably possible.

Q12. Are the recommended labeling requirements sufficient? Is '[ADV]' an appropriate label? Should there be any other requirement?

The labeling requirements should remain flexible and meet the demands of the prevailing circumstances since spammers tend to be ingenuous in circumventing legislated requirements. However, in the case of solicited mails, i.e. where consent

has been given by the user (*see Q1 above*), it should be clarified that the mails should not be deemed spam even where they have not been labeled with “[ADV]”.

Q13. Do you agree that ISPs should be empowered to commence legal action for unlawful spam?

Yes. However, ISPs should have full discretion whether to commence legal action and over their conduct of the legal action. In any case, ISPs MUST NOT be compelled to take legal action on behalf of its subscribers or any party suffering damage or loss as a result of the spam. To this end, ISPs should be allowed to retain damages recovered. Individuals should also be permitted to take legal action against spammers to serve as a further deterrent measure. To facilitate such actions, simple procedures (e.g. through the Small Claims Tribunal) can be implemented. Alternatively, collective class action suits may also be instituted.

Q14. What would be an appropriate quantum for the computation of statutory damages? For instance, would \$1 for every unlawful spam e-mail sent be adequate? Should there be a cap on the quantum of statutory damages that can be awarded by the court?

A minimum punitive amount should be imposed as a S\$1 per spam email damage would not serve to discourage spammers. Under the US threshold, a daily breach would attract only S\$100 damages, a monthly breach, S\$1,000 and yearly breach, S\$10,000. These amounts are insignificant compared to the costs of other modes of advertising/marketing (e.g. in the newspapers, television, radio). Statutory damages should be in addition to damages for economic loss and the ISP should not be required to prove actual damage. Damages awarded should also include both direct and indirect costs of investigation.

Q15. Do you agree that ISPs should be allowed to take legal action against the spammer who uses dictionary attacks or automated spamming tools without having to prove that the emails fail to comply with legal requirements?

Yes. All recipients of the spam should also be allowed to take legal action.

Q16. Who do you think should draft the code of practice?

Q17. What should the code of practice cover?

Q18. Who should enforce the code of practice?

We support the introduction of a code of practice. Individual ISPs are already taking various measures to minimize spam and protect their subscribers against spam. It is laudable to consolidate such efforts. However as industry players such as ISPs are not regulatory bodies without vested powers of prosecution against offenders, it will not be appropriate to mandate a statutory duty to implement a self-regulatory code. As the core competencies of ISPs are not in enforcement, it will also not be appropriate to

cast the duty of enforcement on ISPs. To give the code of practice greater authority, it is proposed that an authority (such as the IDA) be the party having ultimate control over the code. Notwithstanding, input should be sought from all parties concerned including ISPs, independent organizations, marketers and Internet users. Under the code, ISPs will provide necessary and reasonable co-operation and support in investigations.

Other Comments

(a) We urge IDA to craft the proposed Telecom Competition Code to be consistent with the proposed spam legislation so that telecommunications licensees are not placed in a more onerous or restrictive position viz-a-viz other merchants. For example, paragraph 3.2.6.2 of the proposed Telecom Competition Code continues to retain an opt-in approach in contrast to the opt-out regime in the proposed spam bill.

(b) Spammers should also be subjected to criminal liabilities under the proposed spam legislation (especially under Q15 above).