Review of Proposed Legislative Framework For the Control of E-mail Spam

Name: Steven Sim Kok Leong
Job title: IT Security Specialist
Company: Infocomm Security / QA, Computer Centre, NUS

C. - Comment
Q. - Query
C(Q?) - Comment on Annex C questions.

Disclaimer: While some of my comments and queries might strike a similar cord with colleagues in my company, below comments are solely my own and should not be representative of my company's views on this proposed legislative framework.

Executive Summary

1. Application of the proposed legislation

   C. Only an ISP or e-mail provider can ascertain if the spam is transmitted in bulk, not the user. Thus "in bulk" is not a good requirement to facilitate and empower users in dealing with spam.

   Q. Does "received in" cover spam not originating from Singapore companies? What is an example of spam not originating from yet received in Singapore that comes under this legislation? In other words, is "received in" a condition at all necessary (and not redundant) for this legislation?

   Q. Does "originating from" cover local spam relays exploited by non-local companies to spam Singaporeans?

   Q. Does "originating from" cover virus-infected machines exploited for spamming purposes?

   Q. Will there be any attempt to highlight to users that virus-infected emails using spoofed Singapore sender email addresses as well as auto-responses by anti-virus gateways to virus-infected emails using spoofed Singapore sender email addresses cannot be classified as spam? Some of such emails might be commercial in nature depending on whether the virus was created for the intention of spreading UCEs.

2. Requirements for the sending of unsolicited commercial e-mail

   C. Regarding opt-out requests, what is the scope (not stated) of opt-out for future unsolicited commercial e-mails? Can a spammer provide an opt-out for future unsolicited commercial e-mails on only product A? If he/she can, then he could still spam victims with product B, C, D and so forth while still complying with the legislation.

   C. If the spammer is also the email service provider, he/she could easily create multiple email accounts, while genuine, are never used genuinely i.e. he never reads emails in these created email accounts.

3. Legal action

Q. Does ISPs include tertiary education institutes like NUS since NUS performs ISP functions for its users?

4. Civil action for dictionary attacks and use of automated spamming tools

Q. Do automated spamming tools include scripts that mass-mail out the same email and programs such as Excel which allows mass-mailing of contacts listed in a spreadsheet through Outlook client?

5. Co-regulation – codes of practice

Q. Can a company exercise more stringent measures in its self-regulatory code of practice? For instance, can a company classify UCEs with opt-out clauses as spam as well?

Part 2 Prevalence of spam and challenges posted

6. Prevalence of spam and challenges posed

C. Definition of spam is "unsolicited commercial e-mail messages" in the executive summary whereas in 2.1 of Prevalence of spam and challenges posed, it was defined in the broader scope of "unsolicited e-mail messages". There appears a lack of consistency.

Part 3 Legislation in the context of a multi-pronged approach

7. Industry self-regulation

Q. Where can this DMAS Consumer Communications Preference Program be found?

8. Current laws and need for spam control legislation

Q. For spam comprising Nigerian scams, it would constitute the offence of cheating under section 415 of the Penal Code, but who should a user receiving such a spam report this scam to, SPF?

Part 5 Legislative issues

9. Unsolicited communications

Q. If a user receives an e-mail alert or information service to which he could subscribe to, would the e-mail alert be considered spam in the very first place?

10. Commercial communications

Q. If a message described a particular drug but also includes a link e.g. email me for more information or email me to know where to get it, would this be considered a commercial message?

11. E-mail communications

C.(Q1) I feel that if a user submitted his e-mail address during an exhibition or registration of a service to receive commercial offerings, then it is "solicited". However any UCEs (even with an opt-out link) is unsolicited and in my opinion, should be regarded as spam under the legislation.

C.(Q2) I feel that a communication is commercial even if it only tries to introduce a product, apart from attempting to sell a product. Often, the contact for product details is subtly embedded, e.g. an image of the product containing contact information on the product itself.

C.(Q3) Yes, virus-generated emails and antivirus-gateway-generated emails should be excluded from the definition of spam because often the originating system of such spam is infected with a virus.

C.(Q4) Yes, it should apply to all e-mail messages regardless of the technology used to access them. The characteristics of spam stick with the spam e-mail regardless of the technology.

12. Spam transmitted in bulk

C.(Q5) I tend to agree with 5.11 on the New Zealand Discussion Paper. To recipients, unsolicited commercial emails are spam emails regardless of whether they are sent in bulk. This is analogous to port probes and scans. Multiple slow port probes over days can make up a port scan but that does not make any of these port probes any less illegitimate. Thus, I do not think "in bulk" should be a consideration at all.

C.(Q6) Refer to comments at (Q5).

13. Spam sent from or received in Singapore

C.(Q7) Refer to query in 1. I fully agree that it is extremely hard to nap non-local spammers without involving e.g. the Interpol. Therefore, for a good start, I think the legislation should simply cover spam initiated from a Singapore-based company regardless of method used because legislation is only effective on local companies. For instance, a Singapore-based company might engage an overseas company to send spam emails on its behalf. The Singapore-based company should still be liable and guilty of initiating such spam.

14. Person or business commissioning or procuring spam

C.(Q8) I agree that the person commissioning or procuring spam should be liable under the proposed legislation. However, in the event that an open relay server is compromised to send spam under the nose of the owner of the server, the server owner should not be liable under the proposed legislation. Similarly, the owner of a virus-

infected system used to send spam should not be liable, simply because the intention wasn't there, unlike commercial spamming companies.

15. Opt-out regime

C.(Q9) While I disagree that an opt-out regime for spam control is more beneficial (I would prefer an opt-in regime whereby opt-in is defined as a user signing up during an exhibition to receive product offers and NOT the process of receiving an unsolicited commercial email to opt-in as indicated in this process), the inclusion of the [ADV] in the subject header effectively mitigates the risk of spammers exploiting loopholes in the opt-out regime. Loopholes include defining the scope of opt-out, in other words, opt-out of exactly what? If it is an opt-out from further emails from a specific email address or specific product, it does not prevent future spam from a different legitimate email address created by the spammer or for a different product. The use of [ADV] in the subject header should be emphasized here and elsewhere appropriate in this proposal simply because [ADV] empowers the user to decide whether he wants to even receive such advertisements. For instance, by specifying a simple filter rule to delete all emails with subject titles comprising [ADV], the user effectively blocks all unsolicited commercial emails.

C.(Q10) There should only be a minimal time-period defined and should logically take immediate effect. I think one day is a logical deadline because automated scripts can remove users from the database immediately upon either receipt of the opt-out (unsubscribe) email or web form submission. Simply opting-out means the user should no longer receive any further offers on products or services from the COMPANY regardless of whether a different spamming company is engage.

C.(Q11) I like the [ADV] inclusion in the subject title. If this is made mandatory by legislation, users have the choice of filtering off such emails, thus empowering them to customize their preferred actions in dealing with such unsolicited commercial emails.

16. Labeling and other requirements

C.(Q12) I think [ADV] is an appropriate label, unique enough for filtering with little chance of incurring false positives.

17. Legal action

Q. Do ISPs include ISP-like companies like educational institutes managing their own networks and servers and providing services for their staff and students?

Q. What is IDA SingCERT's role in handling spam incidents? If a spam originates from a non-local party or company, should the ISP or user report to SingCERT on the spam? Will SingCERT take action of such spam?

C.(Q13) ISPs should be empowered to commence legal action as this is for the benefit of the users. For non-local spam, SingCERT should perhaps be empowered to engage other national CERTs across borders to resolve such issues.

C.(Q14) Rather than having a monetary amount tied, I think a more effective measure would be to ban the spamming company from sending any commercial email even solicited ones for a fix period of time e.g. 1 year. This is analogous to a driving ban for drivers that flaunt the law.

18. Civil action for dictionary attacks and use of automated spamming tools

C.(Q15) Yes, I agree that ISPs should be allowed to take legal action against the spammer. Impact from dictionary attacks or automated spamming tools is equivalent to DoS attempts which are covered under CMA.

19. Co-Regulation – Codes of Practice

C.(Q16) Industry players should draft the code of practice. ITSC is one excellent organization made up of IDA-independent industry players that could spearhead this.

C.(Q17) It should cover policies and best practices and should also include a grading system for users to easily identify the level of protection covering them.

C.(Q18) Since it is beyond legislation, it should be enforced by the individual organizations themselves. What can be done is to have different grading for organizations implementing various levels of anti-spam security. For instance, an "A" grading could comprise of a very high level of technical spam control measures from preventive to corrective measures and so forth. This is analogous to the hawker stalls with various grading so that users are aware of the level of anti-spam service (or hygiene for food-stalls) they are getting.

Further comments

I think this is a very good start. I have been waiting for this for a very long time.