symantec.
赛门铁克

24 February 2006

Communications and Technology Branch
Commerce, Industry and Technology Bureau
2/F Murray Building
Garden Road
Hong Kong

Attention: Assistant Secretary (B)
[Fax: +852 – 2511 1458]

COMMENTS ON LEGISLATIVE PROPOSALS TO CONTAIN THE PROBLEM OF UNSOLICITED ELECTRONIC MESSAGES

Symantec Corporation[1] is hereby pleased to respond to the Bureau's request for comments to the above legislative proposals.

Overall, we feel that this is a very comprehensive piece of legislation, and the spirit of the legislation, as articulated in its guiding principles, deserve our full support.

We hope our attached comments will be of assistance to the Bureau; in its deliberation over various aspects of the legislative proposals.

Should the Bureau feel a need for any further clarification on our comments or other related issues, please do not hesitate to contact us. We would be most pleased to make ourselves available at your disposal.

Yours sincerely,

Chua Kay Chuan
Regional General Manager
Asia-Pacific & Japan Government Relations
Symantec Corporation

[1] Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries.

Rec'd on 2.3.06

COMMENTS ON THE UNSOLICITED ELECTRONIC MESSAGES BILL

1. Background

1.1 Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, California, Symantec has operations in more than 40 countries.

1.2 Symantec has been at the forefront of the fight against spam (unsolicited electronic messages in the forms of e-mails). We consider spam to be more than just annoying e-mails; but a serious security risk, because it is a conduit by which viruses, trojans, phishing attempts and other threats may be delivered into systems.

1.3 Through the Symantec Probe Network, comprising more than two million decoy e-mail accounts - configured to attract a large stream of spam attacks by simulating a wide variety of Internet e-mail users - Symantec is able to collect global data with true representation of the spam messages that are circulating on the Internet at any one time.

2. Overall: Well-Thought Through and Comprehensive Proposals

2.1 We feel that, overall, the legislative proposals for the Unsolicited Electronic Messages Bill ("the UEM Bill") ***is well-thought through and comprehensive*** in addressing the various key issues related to spam/spim (spam through mobile devices) or other unsolicited electronic messages (UEMs); and ***Symantec would like to congratulate the Bureau to this end.***

3. Guiding Principle[2]: Legislation as Part of a Basket of Measures

3.1 While we fully support the six articulated guiding principles of the Unsolicited Electronic Messages Bill, we feel that it should also add, explicitly as one of its core guiding principles, that this legislation can only be partially effective in addressing the problem of UEMs.

3.2 While this fact is acknowledged at the end of the introductory section of the Consultant Paper[3], ***it is important that the UEM Bill explicitly recognizes the limits of legislation in effectively addressing the problem; and put the legislation in the correct context of being a part - albeit of great importance - of a concerted solution to the problem,*** comprising a basket of measures that include the use of all forms of

[2] Page 15, Part II: Objectives and Guiding Principles (Para 12 – 18)
[3] Page 14, Part I: Introduction (Para 10)

available technology (e.g. IP filtering and traffic shaping by ISPs), public awareness-building and education, international collaboration, etc.

4. Enhancement of Enforcement Resources[4]: Addressed

4.1 In fact, another key component of this basket of measures would be the enhancement of enforcement and investigative resources, which is a pre-requisite to ensuring the effectiveness of this legislation. ***We are pleased to note that the proposal addressed this through allowing the Court to order a convicted offender to pay up to the entire costs and expenses of relevant investigative/enforcement work.***

5. Extra-Territorial Jurisdiction[5]: An Enlightened Approach

5.1 We support the incorporation of extra-territorial jurisdiction into the UEM Bill, thereby giving Hong Kong's law enforcement a formal basis for seeking international co-operation

5.2 ***We feel that this is an enlightened approach, giving recognition to both the fundamental cross-border nature of the global UEM problem, in particular spam; and the need for international cooperation in its resolution.***

6. "Opt-Out" Regime[6]: Privacy and Security Risks to End-Users

6.1 ***In principle, we would urge against the adoption of an "opt-out" regime***, as this poses the risk of having recipients "confirming" their e-mail addresses to spammers, and may result in their "verified" addresses (which are more valuable after verification) being sold to others, and thus ensuring that the same recipients being sent even more spam messages.

6.2 ***Instead, we would encourage the greater use of technology to block such spams, and methods involving a "trusted" third-party***, for example, where requests are submitted instead to the ISP to block such spams. Such methods would much better address the dual concern of allowing compliant commercial electronic messages, whilst ensuring that the security and privacy of end-users are not compromised. A dispute resolution process could then be put in place to handle any non-spam messages blocked by mistake, but in good faith.

---

[4] Page 48, Part VIII: Powers of Investigation [Para 84(d)]
[5] Page 20, Part III: Scope of Application (Para 28)
[6] Page 24, Part IV: Rules About Sending Commercial Electronic Messages (Para 31 - 35)

7. 10 Working Days to Honour Unsubscribe Request [7] : Additional Unproductive Costs for Legitimate Businesses

7.1 For legitimate/compliant commercial electronics messages, we feel that ***it is onerous on legitimate commercial entities to have to honour any unsubscribe request within the proposed 10 working days***, as this would require businesses to update their mailing lists more than once a month, resulting in additional, unproductive costs for businesses. ***A more reasonable duration would be 20 working days,*** which would allow businesses to do a monthly update of their entire mailing lists, the usual current practice amongst business entities.

8. "Do-Not-Call" Registers[8]: Presents Inherent Risks to Information Privacy and Security

8.1 The implementation of "do-not-call" registers ***inherently represents risks to information privacy and security.*** This is compounded by the proposal[9] for the TA to make available such registers for public inspection in the form of an online record.

8.2 We would therefore strongly urge the TA (which has been tasked with its implementation) to ***be relentless in its deployment of adequate safeguards - in the forms of technology, resources and security protocol - in the maintenance of such a database.*** Only then could the risks to information privacy and security be sufficiently mitigated.

8.3 ***We are pleased to note that there is currently no plans for a "do-not-call" register for e-mail addresses***, although the proposed legislation does not preclude the possibility of implementing such a register.

9. Form of Electronic Messages Covered by UEM Bill [10] : Technology Neutrality is Forward-Looking

9.1 We are pleased to note the proposal that the UEM Bill should take a technologically-neutral stance, and cover generally all forms of electronic communications, unless specifically excluded. ***We believe that this stance is a forward-looking one, and is better suited to its objective of regulating activities related to the sending of commercial UEMs for the long-term.***

9.2 As further evidence of the need for this technologically neutral stance, we are already seeing spam being propagated through newer technologies

[7] Page 27, Part IV: Rules About Sending Commercial Electronic Messages (Para 40)
[8] Page 28, Part IV: Rules About Sending Commercial Electronic Messages (Para 44)
[9] Page 33, Part IV: Rules About Sending Commercial Electronic Messages [Para 58(b)]
[10] Page 18, Part III: Scope of Application (Para 22 – 23)

like Instant Messaging (IM, spim), instead of the traditional e-mail medium. According to the Pew Internet & American Life Project survey, one-third of the 52 million American citizens who use IM have already received spim; whilst Bropia and Kelvir worms have been known to attack MSN Messenger users; while "Osama Found" adware worm has been found circulating amongst users of AOL Instant Messenger. Another recent example found through Yahoo! Messenger is as follows:

"desire_more_7j:
Hi, <xxxxxx - account name edited> Hi again. This is my other ID. I made $38 in the last hour by investing $2 in the following site. Tomorrow I will have made about $800 dollars. It only costs $2 total. You can make good money also. Just go read this site and sign up. If you dont have $2 to spend, please ignore this."

10. Other Provisions[11]: Additional Proposals for Inclusion

10.1 Finally, there are two other issues that we felt had not been adequately addressed by the proposed UEM Bill. In our experience with legislation in other countries, including the US CAN-SPAM Act 2003, as well as some state legislation in the US, these issues are usually overlooked in the legislative process, and only surfaces in the implementation phase of the legislation and through tests in Courts.

10.2 **Issue (1): Relief from Liability for Spam Filter and Anti-Spam Technology Providers**

(a) Security companies such as Symantec work closely with Internet Service Providers (ISPs)/Telecom Service Providers (TSPs) to guard end-users from the threats of cyber crime, and spam has proven itself to be a potential medium for the proliferation of cyber crime. As such, security companies and ISPs/TSPs has an obligation to end-users to adopt a conservative stance in the calibration of its filters or other anti-spam technological measures; and in some cases, this may lead to the blocking and filtering out of legitimate (as defined by the Bill) messages, solicited or otherwise.

(b) ***It is therefore important that the legislation include explicit relief from liability for security companies/ISPs/TSPs and other providers of spam filters and anti-spam technologies***, otherwise, it would significantly discourage the deployment and development of such effective anti-spam filters/technologies, which is already recognized as one of the key component of the basket of measures required to tackle the UEM/spam problem.

[11] Page 51, Part IX: Other Provisions

(c) At the same time, in order to address any unintended filtering/blocking of legitimate messages, ***a dispute resolution process be put into place***, perhaps with the TA acting as the final arbitrator in the resolution process.

10.3 **Issue (2): Relief from Liability for Real Brand/Product Owners for Spam Sent Without Due/Express Consent**

(a) Real brand and product owners - whose brands, products and services may be sold through spam, without their intent nor express consent - have often fallen victim to civil/statutory actions taken against them. Such spam often includes false advertisements and even pirated products of the real brand and product owners.

(b) Whilst the potential for such an offence is partially alluded[12] to in the proposals – and is further governed by Section 16A, Sub-Section (1)(b) of the Theft Ordinance (CAP 210) – we are concerned with the issue of where the onus of proof should lie, in particular, since there is a corresponding proposal[13] that "principals" would be treated as having committed the same offence.

(c) We are therefore of the opinion that this legislation ***should provide for explicit relief from liability for real brand and product owners, with the onus of proving due/express consent being placed on the people/entities transmitting the spam.*** Previous experiences in the US has shown that it is very costly for legitimate businesses, especially when they own brands and products that are the popular with spammers, to continually go the Courts to defend themselves and prove that they had not given the necessary due/express consent to the spammer - even though such truth may already be common sense. Without such relief, the cost impact (of doing business) to legitimate commercial concerns and brand/product owners would be significantly raised.

Submitted By: Chua Kay Chuan
Regional General Manager
Asia-Pacific & Japan Government Relations

for **SYMANTEC CORPORATION**

[12] Page 43, Part VI: Offences Relating to the Sending of Commercial Electronic Messages [Para 76(d)(ii)]
[13] Page 55, Part IX: Other Provisions [Para 100(d)]