CB(1)1071/05-06(04)

Hong Kong
Internet Service
Providers Association
HKISPA

By post and by email (uem@citb.gov.hk)

Communications and Technology Branch
Commerce, Industry and Technology Bureau
2/F Murray Building
Garden Road
Hong Kong
(Attention: Assistant Secretary (B))

10 March 2006

Dear Sirs,

Response to the January 2006 Consultation Paper (Consultation) on Legislative Proposals to Contain the Problem of Unsolicited Electronic Messages (UEMs)

We submit our response to the Government's Consultation herein.

We acknowledge the alarming problems of UEMs and the absence of existing Hong Kong statutory measures to specifically tackle UEMs.

As a general comment, compared to the previous 2004 consultation paper on UEMs and the July 2005 draft UEMs legislative framework, the January 2006 UEMs legislative proposals contained in the Consultation have been improved and demonstrate the Government's sincerity in drawing up a HK anti-UEM law which is sufficiently extra territorial, advanced and fitting for our unique international economy. For example, we note the expanded definition of "Hong Kong link" which not only encompass UEMs with a Hong Kong origin as in the previous July 2005 draft legislative framework, but is now made broadly to cover extra jurisdictional arena, which given the extra territorial nature of UEMs, is welcome.

We are particularly pleased that the Government has accepted our prior proposal and now stated in Paragraphs 91 and 100(g) of the Consultation that the liability of a telecommunications service provider who by nature merely provide a service and exercise no control over the content or use of such service should not be treated as if it has sent, or has caused to be sent, the message. The Spam Act 2003 of Australia has a similar provision and we agree that our UEM Bill should be on par with that.

We find a number of issues which deserve further consideration and we set out our specific proposals and comments to the Consultation as well as our new proposal now lacking in the Consultation as follows. Unless otherwise stated, the references to paragraphs stated in the sub headings below are to the paragraphs of the Consultation.

1. Scope of Application – Unsolicited Commercial Electronic Messages – Paragraphs 19, 20 and 29(c)

Hong Kong
Internet Service
Providers Association
HKISPA

We agree that, in view of the rapid development of information and communications technology, the UEM Bill should cover generally all forms of e-communications unless it is specifically excluded to cater for future developments in technologies and services.

We also agree that the UEM Bill should regulate commercial UEMs only. Most UEMs, as a matter of fact, are commercial in nature. In addition, our UEM Bill should be made in line with most of the anti-spam legislation in overseas jurisdictions (such as South Korea, Japan, Australia, U.K. and the USA) which also adopt such scope of governance. Given the intrinsic extra-territorial nature of UEMs and given Hong Kong's positioning as an international city, our anti-spam law should be created on par with the majority to minimize the potential cross jurisdictional conflicts.

Notwithstanding the foregoing, we wish to ask the Government to consider whether limiting our UEM Bill to regulating commercial UEMs only would effectively legitimatize spamming where the primary purpose is non-commercial. The negative consequences of receiving unsolicited e-messages whether of commercial or non-commercial nature may be the same to spammed victims and hence deserve consideration for possible regulation.

ISPs generally must transmit what they have been instructed to. Because the UEM Bill in effect blesses the spamming of non-commercial UEMs, the transmission of non-commercial messages may grow. The UEM law will indirectly cause the ISPs to have to transmit larger quantity of spam e-mails claiming to be non-commercial in nature, even when the recipients consider the relevant ISP to exceed the limit with the possible consequence that the said ISP ending up blacklisted. The vicious cycle then follows. It will be difficult for ISPs to judge what nature the spam emails belong to nor is it their duty to do so. The services of the blacklisted ISP will in turn be adversely affected. Our customers will not get the services they expect, causing them dissatisfaction, delays and possibly economic loss.

We therefore propose the Government to consider ways in which the public users can opt out of the receiving e-messages even of a non-commercial purpose and to possibly impose measures to control bulk spamming of non-commercial e-messages. We appreciate this is a sensitive issue and we do not have the perfect solution. Nonetheless, the Government should give it some thought.

Speaking from the point of view of local ISPs, we agree with the Government that the present Section 24 of the Telecommunications Ordinance needs to be amended because of the new anti UEM rules. The Section 24 provides that a person performing a telecommunications service shall be guilty of an offence if he willfully destroys, alters, intercepts, or abstains from transmitting any message, should be amended to clarify that it does not apply to acts done for the purpose of facilitating compliance with the UEM Bill or any other law or implement the terms of contract made between a telecommunications service provider and its customer. This will help protect the ISPs' actual operation to comply with the UEM Bill or other laws, for example, for implementing a spam filter to block e-messages contravening the UEM Bill or for providing service for blocking

Hong Kong
Internet Service
Providers Association
HKISPA

telephone calls from callers not revealing their originating telephone numbers against the UEM Bill.

2. Rules About Sending Commercial Electronic Messages – Misleading Subject Headers – Paragraphs 48, 49 ad 59

We agree with the Government's proposal as stated in Paragraph 49 of Part IV of the Consultation that misleading subject headers be prohibited.

We feel that a general prohibition in the UEM Bill against using misleading subject headings is not enough. Because descriptions in the subject headers vary and it is difficult to state in the statute what and how accurate the descriptions must be, we propose that the UEM Bill requires mandatory labeling of "ADV" for unsolicited commercial e-advertisements.

We note that Article 13(3) of the latest PRC anti-spam regulations 《互联网电子邮件服务管理办法》(which will take effect on 30 March 2006) also impose a mandatory "AD" or "广告" labeling for emails containing commercial advertisements transmitted through the Internet.

3. Legislative Proposals – Exclusions – Paragraph 55

Paragraph 55 reads that with regard to the proposed requirement for a functional unsubscribe facility, the UEM Bill will specify that a person shall not send, or cause to be sent, a commercial e-message that has a "Hong Kong link" to an e-address subject to certain requirements but the said paragraph sub section (d) makes it an exclusion if "the person who sends the message does not know or could not with reasonable diligence have ascertained that the message has a Hong Kong link", amongst other exclusions.

Although the reasonable due diligence caveat may be a commonplace exclusion for many circumstances, this explicit exclusion is not necessary in the UEM's case. We fear that spammers may take advantage of this caveat.

For example, if a popular website, say yahoo.com is not registered in Hong Kong, but there are many yahoo.com e-mail recipients in Hong Kong. Paragraph 55(d) may help a U.S. spammer argue that it has done reasonable due diligence but could not ascertain the message was sent to a yahoo.com's recipient who so happens was physically in Hong Kong at the time of receipt of the e-message. Although we appreciate the complexity due to the cross-border nature of spam, there is no need for our UEM Bill to proactively allowing room for spammers to make excuses.

4. Do Not Call Registers – Paragraphs 44, 45, 58 and 60(a)(i)

The Government's proposed plan is to empower the Office of the Telecommunications Authority (OFTA) with the discretion to set up Do Not Call registers and if so, decide how to implement and operate them.

Hong Kong
Internet Service
Providers Association
HKISPA

However, we comment that:
1. OFTA, being empowered with the discretion to set up Do Not Call registers, should also be vested with the responsibility to device means to protect the Do Not Call registers from being intentionally abused as a source of true electronic addresses by spammers;
2. the Do Not Call registers should operate as a registry, be interactive and user friendly rather than the presently proposed passive online records;
3. the Do Not Call registers should not be open for all to inspect but should be limited to the relevant telemarketers;
4. telemarketers sending or causing to be sent commercial e-messages with a Hong Kong link should first register with the Do Not Call Registry online, set up their profiles and accounts; and
5. the proposed enforcement notice mechanism for pursuing the delinquent is too weak.

According to the proposals, if a telemarketer calls someone in Hong Kong on the Do Not Call register, this could prompt an OFTA investigation. Should the authority see fit, it would issue an "enforcement notice" telling the business to desist such spamming. Should there be further breaches of such enforcement notice, OFTA then has the option of bringing the violator to court, which could lead to a maximum fine of HK$100,000 and further fines for continuing breaches.

Yet history tells us this type of enforcement mechanism is ineffective. Violations of the Personal Data Privacy Ordinance are handled in a similar way, and there has been just one successful court conviction to date. The mandatory giving of second chances of breaching the Do Not Call rules means that telemarketers might find it easy to simply violate the Do Not Call rules and then only quit after receiving an enforcement notice from OFTA.

The USA has set an example in how a national Do Not Call register can be run. Violators are subject to fines for each call made, which count as one separate breach. The fines can reach up to US$11,000 per call, which could easily put out of business any telemarketer that flouts the rules. Hong Kong should adopt a similar plan. To deal with inadvertent mistakes, telemarketers should be required to first register online with the Do Not Call registry to give their identifying information to assist in future enforcement, set up their account to help trace what information they have accessed and also keep good records to ease their own use, and then cross check the numbers in the Do Not Call registers. In addition, all telemarketers should be required to transmit caller ID information so consumers can jot down the number in case of any complaints.

We recognise that the above might be too broadly scoped that might affect normal business operations, for example, human sales calls of an ordinary company to their existing customers. Therefore, we propose that the administration consider strengthening the enforcement mechanism for automatic means of electronic message transmission to recipients without an ongoing business relationship, e.g. automatic recorded phone calls and bulk e-mail transmission to random recipients.

Hong Kong
Internet Service
Providers Association
HKISPA

6. Address Harvesting and Dictionary Attacks– Paragraphs 61 to 66

In principle, we agree that address-harvesting in the context of spamming is wrongful. However, we do not agree with Paragraph 64 of the Consultation that address-harvesting, coupled with compliance with the proposed opt-out measures, is not wrongful. Further, we cannot agree with address-harvesting for corporate-wide system administration purposes mean it a "legitimate use" as per Paragraph 64.

We propose that the UEM Bill should make both address harvesting and dictionary attacks offenses as a strict principle. Further, we propose a reverse burden of proof be imposed on e-marketers so that they must show to the recipients upon request that they obtained the address by means other than address-harvesting or dictionary attack, like prior cooperation with ISPs or e-mail service providers. It would then be up to the consumer to decide whether to stay with that ISP or that e-mail service provider.

7. Proposed Changes to Section 24 of Telecommunication Ordinance– Paragraphs 98 and 100 (n)(iii)

We agree with the principle of amending Section 24 of Telecommunication Ordinance to take into account of the operators which comply with the UEM law.

However, we would like to add a further section to the actual wording to the effect that section should also extend to cases where normal network/facility operation would be impeded if the transmission of UEMs were not rejected. This is again speaking from the point of view of our ISP members which are likely to face this problem.

Therefore, we propose that the new Section 24(2) should be worded as follows:
"(2) This section does not apply to any act done for the purpose of (a) facilitating compliance with the Unsolicited Electronic Messages Ordinance or any other law; or (b) implementing the terms of any contract made between a telecommunications service provider and a customer of the telecommunications service provider, *or (c) facilitating normal operation of services by refusing connections or electronic messages from confined set of sources when the network and/or facilities of the service providers may be under risk of failure of operation if they continue to accept connections or electronic messages from those confined set of sources to be decided by the service providers in question. " (NB: our proposed additional wordings are marked in italics)*

8. Right to sue by ISPs – our new proposal

We would like to have similar rights to commence civil actions by local ISPs in the UEM Bill no less than those given under the USA Can-Spam Act.

Section 7(g) of the Can-Spam Act (http://www.spamlaws.com/federal/108s877.shtml) expressly authorizes an ISP which is adversely affected by a violation of certain sections under the Act to bring a civil action in any US district court with jurisdiction over the defendant. Sections upon violation that would give rise to the right to sue by ISPs include

Hong Kong
Internet Service
Providers Association
HKISPA

the prohibition of false or misleading transmission information (Section 5(a)(1)), the requirement of not using deceptive subject headings (Section 5(a)(2)), transmission of commercial emails after objection (Section 5(4)), or inclusion of identifier, opt-out, and physical address in commercial email (Section 5(5)), amongst others.

According to the US law, the aim of bringing a civil action by an aggrieved ISP is to:
1. enjoin further violation by the defendant; or
2. recover damages in an amount equal to the greater of (i) actual monetary loss incurred by the ISP as a result of such violation or (ii) the statutory damages calculated according to the formula in Section 7(g)(3) of the Act.

We also note that Clause 23 of the New Zealand UEM Bill (http://www.brookers.co.nz/bills/new_bills/b052811.pdf) sets out the actions and remedies which service providers can take if a civil liability event is alleged to have occurred. The remedies available to the aggrieved ISPs include seeking injunction from the High Court under stated circumstances, complaining to the enforcement department, joining in court action initiated by the enforcement department made under stated provisions or make an application for compensation from the High Court under stated rules.

We submit for incorporation of similar rights and remedies for aggrieved ISPs in the UEM Bill in case of violation of the UEM law so we can commence civil actions in Hong Kong courts and be clear on what remedies that are available to us. The presently proposed compensation for general victims of spamming is, in our view, insufficient for ISPs who are by our nature different from the general spam victims and hence deserve special treatment as in the US law.

Yours faithfully,

HONG KONG INTERNET SERVICE PROVIDERS ASSOCIATION
香港互聯網供應商協會

Hong Kong Internet Service Providers Association