Response to the UEM Proposals

1 Introduction

This response has been prepared by the Hong Kong Computer Society to comment and advise on Government proposals outlined in the document “Consultation Paper on Legislative Proposals to Contain the Problem of Unsolicited Electronic Messages” (**UEM(Eng)-final.pdf**), published January 2005.

In preparing this paper, it has become clear that members of the HKCS hold a variety of views on the issues, particularly the fundamental issue of whether to adopt an opt-in or opt-out regime. This paper tries to include both points of view.

2 Executive Summary

The HKCS strongly supports legislation in Hong Kong to control unsolicited electronic messages. The HKCS believes that the proposals presented in the Consultation Paper provide many positive contributions towards the effective control of SPAM in Hong Kong.

The main areas of concern maintained by the HKCS are as follows:

a. the adoption of an opt-out regime;
b. exemptions for non-commercial messages

In considering these areas, it is important to understand the role of communications in Society, and therefore how electronic messaging interacts with Society.

These areas of concern also lead to the contradictions inherent in the proposals:

a. If it is permitted to send an unsolicited message, why is it an offence to collect addresses with the intent to send unsolicited messages?
b. The problem of UEMs is worst in email; yet the Proposals purposely omit email from the list of do–not–call registers.

The HKCS also advises that UEMs are an automated offence, so efforts should be made to automate our response – this should lead to cost effective investigation and prosecution of offences.

The submission would like to focus on selected key areas as follows:

3 Communication and Society

People communicate in a wide variety of ways, and communication is fundamental to Society. Without communication, Society cannot exist. Feedback is an important, but not universal, feature of communication: people expect to know when a message arrives, or fails to arrive, and people send messages with the intention of receiving messages. Some forms of communication are not symmetrical: a speaker at a conference expects to deliver her message without interruption; and a radio or TV producer transmits his program into the void, with no assurance anyone has a receiver switched on. Another example of asymmetric communication is an advertising poster: its message is available to anyone who looks in the right place, but there is no direct channel for replying. In symmetric communication, we generally know whom we are communicating with: we talk to the shop assistant, or with our group of friends.

Thus we can divide communications into broadcast media, which are asymmetric, and addressed media, which are largely symmetric. There are grey areas, particularly in direct, person–to–person communication: if a group of friends has a conversation at a larger party, is that addressed: just to the group, or broadcast: to anyone within earshot – non-verbal messages and social etiquette provide an answer.

However, when we consider electronic communication, the division between broadcast and addressed becomes clearer. TV and radio are clearly broadcast. Telephone, fax and email are clearly addressed (so–called “broadcast fax” is not broadcast in this classification: technically, the equipment makes a series of calls to different numbers, and delivers the message to each one – every fax is addressed).

The division of communications into broadcast and addressed is highly significant. It

is justification for the exclusion, in paragraph 3 of the Proposals, of “transmissions of sound or video material on broadcasting channels” from the scope of the proposed legislation. Addressed also implies that *we know who the recipient is* (for some value of “know” – when we call ‘999’, we intend to communicate with an Emergency Dispatcher, but we do not know their name, the context defines which aspect of identity is relevant). Therefore, it is misuse to use an addressed medium of communication when the intent of the sender is to reach a broadcast audience.

On the Internet, the World Wide Web is the obvious example of a broadcast medium. Technologies such as phone, fax and SMS do not provide a broadcast medium in this classification.

3.1 Trespass

All forms of electronic communication are not free: at a minimum, users must invest in appropriate equipment to transform the electronic signals to something that can be perceived by people. In addition, for an addressed medium, recipients pay for their address. This payment takes different forms: mobile phone users pay a service provider to get a number and the matching SIM card; an individual Internet user pays an ISP for access to a mailbox on the ISP’s servers; organisations pay a registration company for their domain name, and then buy servers and pay staff to administer individual email accounts within that domain. Addresses are therefore private property: people and organisations are spending time and money to acquire and maintain them.

Another cost of addressed media is the cost of receiving each message. There is a technical cost, which is usually small (vanishingly small for email); and a human cost: each addressed message demands an individual decision, even of that decision is just to delete it. Individually, the costs are small, but they become significant when the volume of messages grows. In catastrophic cases, the volume of messages causes problems: the recipient’s systems become overloaded and fail – storage space is filled up, and messages are rejected, or, worse, just disappear. There are numerous examples of this happening for email, the usual response is to expand the capacity of the system, i.e. to pay more.

One definition of trepass is, “encroachment: an intrusion into someone’s privacy or time”; another is “the act or an instance of going onto somebody else's land or entering somebody else's property without permission”. UEMs are therefore a type of trespass: they encroach on the recipient’s time, and they occupy the recipient’s

property: space in the mailbox or airtime on the phone etc.

But does the mere act of establishing an address imply an open invitation to communicate? Why do people use electronic communications? There are a myriad of answers, including:

- "To keep in contact with my friends and family."
- "For customer enquiries: sales and complaints."
- "To contact our support staff during an emergency."
- "So my wife can call when the baby comes."

Often, the volume of UEMs can interfere with the intended purpose of the recipient (it is annoying and wastes time to look at and delete unwanted messages to find the latest family news); and in some cases UEMs can seriously interfere with the intended purpose of the recipient (if unsolicited automated voice calls continue to grow, staff on call may be continually woken by unwanted calls). Therefore, it is a fundamental question whether users should have the right to decide what their address (their property) is used for.

3.2 Freedom of Speech and Expression

Does regulation of UEMs have an impact upon freedom of speech? Guiding principle 4 states, "Freedom of speech and expression must not be impaired". Paragraph 20 of the Proposals reflects the argument that the freedoms would not be affected because the regulations would only be recognising the right not to listen, but still concludes that the legislation should only regulate commercial messages.

The thrust of the argument in Paragraph 20 is unclear, is the Government suggesting that newspaper automated telephone surveys are an important aspect of freedom of speech and expression? Every one of the people surveyed has the right to write a letter to the newspaper, so it is not freedom of speech and expression for the survey respondents. The newspaper also has alternate means of contacting potential respondents (they can print a notice), they could even ask for volunteers to receive regular automated calls, so that the calls would no longer be unsolicited.

An argument can be made that an opt-out regime would leave dangerous potential for attacking freedom of speech and expression. One possible attack would be to collect the addresses of political opponents, and then to provide the list (or even sell it – damaging the ability of opponents to communicate and making a profit at the same

time!) to as many marketing companies as possible. Collecting the addresses would not be a crime, and, having obtained the addresses, the marketing companies would be free to use them until they were told to stop (under an opt-out regime), but the result would be that the targeted politicians would loose a channel of communications.

Politicians need to publish contact addresses widely, so this scenario is possible even without a deliberately abusive opponent.

3.3 Commerce, Fraud and Religion

Paragraph 20 claims, "[Commercial UEMs] form a distinct category of messages that can be easily defined, identified and targeted", but many UEMs that are a problem might not fit into the narrow category of trade in goods and services:

1. Advanced fee fraud: While a great many of these are false invitations to participate in money laundering (arguably trade in services), some start, "You have won the lottery", so there is no suggestion of a commercial relationship, or illegal intent of the recipient.
2. Disguised advertisement: One example said (in part):

   > Subject: Re: your web site is interesting...
   > this is your non-profit/charity contact email address right?
   > If so... we will email your web site to 2,500,000 opt-in emails for free
   > http://
   > …
   > this non-commercial, non-transactional, non-relationship, courtesy emailing

   It seems unlikely that this message is entirely honest about its intentions: at best, it is a loss-leader for a spammer, but criminal fraud also seems likely.

3. Attack on Freedom of Religion: Some messages just contain a religious chant. According to the precepts of the religion, if the recipient merely reads the chant it has a mystical effect, and the sender derives some religious benefit. Therefore, the intent of the sender is to force someone to participate in the sender's religion, without consent, for the sender's personal (but non-commercial) gain.
4. Stock Market Alert: Some UEMs provide "news" about share price movements, with the obvious intent of causing particular buying behaviour in the recipients. Presumably, the sender intends to profit, not from any commercial interaction with the recipient, but by manipulating the share price. Of course, some people

subscribe and even pay for stock market news; those are clearly solicited messages. One possibility is that the unsolicited messages are intentionally imitating the subscription services, to deceive the recipients.

These examples illustrate that “commercial UEMs” are not an easily defined, distinct category, and also that there are classes of UEM that should be controlled, but are non-commercial. Only controlling commercial messages complicates things for the recipients: they must check whether an unsolicited message can be classed as commercial before reporting it. What is the justification for putting this burden on the recipient?

4 SME Marketing

The Proposals rightly emphasise the importance of SMEs to Hong Kong (Executive Summary paragraphs 5 and 9, paragraphs 14) and use this to justify the opt-out regime (Executive Summary paragraph 5, paragraphs 32 and 33). The Hong Kong Computer Society is not an SME society, but many of its members are employed by or are involved in SMEs. In many cases, these SMEs were “early adopters” of Internet technology, and therefore they can offer advice from their own experience:

1. Receiving UEMs costs you money, even deleting messages without reading wastes time. Worse, occasionally you will delete important messages by mistake. The more UEMs you receive, the more likely you will mistake an important message for a UEM.
2. You will receive more UEMs in future than you do now. It takes time for an address to be passed onto many spammers lists, a new address usually receives little spam but that will change sooner or later.
3. Electronic communications is a low cost method of communicating with your customers, but your customers expect and deserve respect:
    i. Maintain your address lists carefully, your existing customers may want to hear from you regularly, but if they do not, adding them to your list without permission will annoy them and they will go elsewhere.
    ii. Unsolicited messages have a very low response rate, they are most suitable for businesses that do not need a large number of customers: like fraudulent scams.
    iii. Your website is your primary electronic method of reaching new customers. Search engines are the easiest way for people to find your site.
4. Some (misguided) administrators are blocking messages from large blocks of

addresses, such as whole ISPs, or even whole countries that they consider to be likely spam sources. It is difficult to check whether your messages are being blocked – you might be loosing business today because your replies are not arriving. The only way to reduce this is to make sure your community is not regarded as a spam source: do not send UEMs yourself, and support strong legislation for Hong Kong.

The freedom to send UEMs is the freedom to contaminate your drinking water supply.

5 The Registered User of an Electronic Address

The first guiding principle states,

> The registered user of an electronic address should have the right to decide whether to receive or refuse further electronic messages at that electronic address.

But this implies there is an individual (the “registered user”) associated with each address. This is not always the case, many organisations use general-purpose addresses, such as info@company.com or postmaster@company.com, which may be serviced by a group of staff. In this situation, it is the legal person, the organisation that should have control. However, many organisations assign addresses derived from people’s names (e.g. james@company.com, j.wong@company.com), and people use such addresses for both personal and professional communication. In this situation, should the employee or the organisation have control? If the organisation decides to filter messages to employees, are they liable for the personal messages they block?

Some organisations have already considered this issue. They may assign addresses related to the job function (e.g. cip-iss-a-is@organisation.hk) or they may have an explicit policy that defines their rules on the use of communication systems, or even both.

This issue should be clarified, not just in the scope of control of UEMs, but also for personal data privacy. We recommend that “registered user” should be the “owner”, where owner is defined as the (legal or natural) person that pays for the address, with the exception that, if the address includes or is derived from the name of the person who uses the address and the owner of the address has no policy otherwise, the user is the registered user. Thus, an organisation could define a policy that prohibits the use of company addresses for personal communication, and still define addresses derived

from employees' names without loosing control of its communications. This still leaves a grey area of what happens when an employee ceases to be an employee, which should be considered further.

6 Do-Not-Call Registers

The issue of Do-Not-Call Registers is an area where an opt-in regime has a clear advantage. With an opt-in regime, a do-not-call register is unnecessary. Effectively, all addresses are automatically on the register. However, the discussion of do-not-call lists in the Proposals does not consider the advantages of cryptographic technology.

Section 45 of the Proposals reports,

> The US FTC has studied the possibility of establishing a "National Do Not Email Registry" and concluded in its report to the US Congress that "a National Do Not Email Registry, without a system in place to authenticate the origin of e-mail messages, would fail to reduce the burden of spam and may even increase the amount of spam received by consumers".

This report is recognizing that a do-not-email register that simply lists the addresses will be an enormous list of valid email addresses. Spammers could send messages to the list with no penalty, if they are careful to make their messages untraceable. The Proposals therefore do not recommend establishing a do-not-call list for email:

> Our present thinking is to establish a register of telephone numbers for opting out of pre-recorded voice, sound, video or image promotion messages, a register of telephone numbers for opting out of SMS/MMS promotion messages, and a register of telephone numbers for opting out of promotion fax messages.

As we have previously pointed out, the fact that the strongest measure to limit UEMs proposed is inapplicable in email, where the problem is greatest, clearly indicates that the opt-out regime is the wrong approach.

However, technology can be used to obviate this problem, to some extent. We need to make it possible for marketers to check whether an address is on the do-not-call register, without providing the addresses to the marketers. A cryptographic hash function is useful here. Instead of publishing the addresses, a list of cryptographic hashes of the addresses is published. The marketers can then apply the same hash

function to the addresses on their mailing lists, and remove the addresses when the hashes match. Because of the mathematical nature of a cryptographic hash, it is infeasible to derive the address from its hash, so the list can be freely published without providing spammers with a resource to misuse.

This sounds very technical, how do you calculate a cryptographic hash of an address? Would this create an unreasonable burden on SMEs trying to reach the market? Fortunately, the software to do this is freely available, and pre-installed on many systems. Calculating a cryptographic hash of an address is possible in a single command line:

```
echo "user@company.com.hk"|md5sum
```

Checking whether an address is on a hashed do-not-call register is a little more complicated, but still easily achieved in a single line:

```
echo "user@company.com.hk"|grep `md5sum` donotcall
```

Of course, it can also be achieved in many other ways, and it should, ideally, be integrated with the mailing list software.

It should also be noted that it is not only email that has a problem with sender authentication. Although telecommunications companies do have records of calls and messages for phone calls, faxes, SMS and MMS; they are not generally accessible to the recipients. Caller Number Display is still, usually, a charged extra service, and the caller can withhold their number (as it is not possible to distinguish between local calls with the number withheld, and overseas calls, where the number is unavailable, people who communicate overseas cannot simply reject such calls). The sender's number on SMS and MMS messages can be omitted or falsified by telecommunications service providers (and there are clear examples of service providers doing this).

Therefore, if an opt-out regime is chosen, the do–not–call register will be the only preventative measure that recipients can use. It should not be restricted to mediums where the problem of UEMs is less and the register contents should be protected using a cryptographic hash. It is not an unreasonable burden to require marketers to use freely available software to check their lists against the published hashes.

7 Accurate Sender Information

Paragraphs 46 and 47 of the Proposals discuss the importance of accurate sender

information to the opt-out regime. One problem that is overlooked is message length limits. SMS is probably the worst case. The maximum length of an SMS message is 160 Latin characters, or 80 Chinese characters. After deciding on the content of the unsolicited message, the sender will need to add: *name of the organisation* and the *name, physical address* and *electronic address* of the person sending the message on behalf of this organisation, plus, in the case of a party contracting another party to send the message on its behalf, the same information for both the contracting and contracted parties.

Of course, Hong Kong is a Region with two official written languages: English and Chinese. The recipient must be able to understand the sender information in order to use it, so it **must** be a requirement for the information to be included in the message in both languages.

Therefore, it is clear that an opt-out regime can only be considered viable for SMS when it is demonstrated that 160 characters is sufficient to express four English names, four Chinese names, two English physical addresses, two Chinese physical addresses and two electronic addresses, plus enough additional space for a reasonable marketing message.

Other messaging systems or content forms may also have limitations that raise similar problems. For example, if an advertisement is sent as a JPEG image, is it sufficient to include the sender information as part of the image? This information would be inaccessible to a blind person, utilising a screen reader to access her messages.

Paragraph 46 of the Proposals states, “An important aspect of a successful opt-out regime is the ability to identify, locate and contact the sender of a UEM”, but it is clear from these examples that limitations of the medium or characteristics of the recipient can prevent this vital information from being received. Therefore, an opt-out regime will fail.

8 Automation of Response

UEMs are an automated offence, so the response should also be automated, to some extent. UEMs have emerged as a problem because recipients are forced to expend resources to deal with them, it is therefore reasonable to make efforts to minimise the effort required to report and investigate incidents. Some suggestions follow:

8.1 Automation of Reporting

Anti-spam gateways are nowadays a common feature of email systems, depending on how the situation develops in future; they may also become a common feature of other messaging systems. Typically, the gateways evaluate a set of rules to determine whether each message is spam or not, and take action on the result. The action may be to refuse to accept the message, or to silently delete it, or to deliver it to a "quarantine" area for later decision by the recipient, or to deliver tagged with a warning. During this process, the gateway collects information that could be useful in an investigation: the last relay address, the apparent source, dates, times, and the message content. Currently, the information is discarded after the decision has been made in most cases.

Some mail system administrators have already configured reporting to the developer of the gateway system so that improvements can be made. Minor configuration changes could send that information to an investigation authority.

8.2 Automation of Investigation

The investigating authority would need to have systems to collate and categorise the automated reports. The processing of large numbers of reports would reveal useful information:

- Campaign Size: Larger campaigns cause more nuisance and therefore should be prioritised for further investigation and action.
- Enforcement Notice, Civil or Criminal: Campaigns that show features of fraud or hiding the sender's identity can be targeted for criminal investigation.
- Open Relays: By implementing an appropriate procedure with ISPs, unauthorised open relays in HK could be quickly shut down.

Thus, the enforcement authority can utilize the automated reports to maximise the effect it has on UEMs. The control of unauthorised open relays could be particularly important, because it would have immediate effect to reduce the spam passing through Hong Kong. Overseas service providers would be less likely to implement blanket blocking of messages from Hong Kong, improving the communications of Hong Kong businesses with the rest of the world.

8.3 Automation of Prosecution

Justice is a human activity that cannot be automated until the development not just of artificial intelligence, but artificial wisdom. However, some of the information from the automated investigation could be usefully permitted as evidence in court. This would probably be best used in sentencing – once the guilt of the offender has been determined "beyond reasonable doubt", the automated logs can demonstrate the extent of the offence. This can help keep the sentence proportional to the crime: prosecuting an instance of a $100 lottery advance fee fraud might seem a waste of court time, but when there are 100,000 other documented attempts to take into consideration, a stiffer sentence can be considered.

8.4 Automation of Compensation

When a court determines that the offender should pay compensation, the automated records can be used to determine how the compensation should be divided.

Concerning the size of the compensation, the paragraph 82.c. of the Proposals mentions "pecuniary loss". If this indicates that the claimant would need to demonstrate that they suffered monetary loss as a result of receiving the UEM, it would render prosecution of all but the most extreme cases uneconomic. The major consequential loss caused by a typical UEM is a few seconds of the recipient's time to identify that the message is unwanted, and a few more seconds to delete it. In a large organisation with thousands of staff that could amount to a few man-hours of lost time, but the burden of enumerating the lost time would outweigh the potential eventual compensation. If the organisation has installed an anti-spam gateway, the loss of the recipient's time is prevented, and only the even smaller loss of computer time to process the message could be claimed. Therefore, a specified nominal minimum loss per message, perhaps based on the value of the time taken by an average user to identify and delete a UEM, should be specified.

9 Exemption of Non-Commercial Messages

The Proposals exclude non-commercial messages from control by the legislation, but many of the regulations are simply outlining the responsible use of the communications media. What is the justification for allowing, for example, a charity to:

1. hack into a computer or telecommunications device, service or network, or obtaining similar unauthorised access, and subsequently transmitting multiple non-commercial electronic messages from those facilities;
2. send multiple non-commercial electronic messages from a computer or telecommunications device, service or network without authorisation (e.g., through zombie computers) in order to mislead recipients as to the origin of such messages and prevent blocking by spam filters;
3. falsify or withhold header information (e.g., e-mail spoofing) and transmit multiple non-commercial electronic messages, again to mislead the recipient as the origin of the message and to prevent blocking by spam filters.
4. register for 5 or more electronic addresses or 2 or more domain names, using a false identity or withholding the identity, and intentionally transmitting multiple non-commercial electronic messages using such electronic addresses or domain names;
5. falsely representing himself to be the registrant of 5 or more electronic addresses or 2 or more domain names, and intentionally transmitting multiple non-commercial electronic messages;
6. not provide a functional unsubscribe facility;
7. continue sending non-commercial electronic messages after an unsubscribe message becomes effective.

Charities and political parties do not enjoy these sorts of exceptions for real-world activities. Indeed, some buildings prohibit entry for the purposes of distributing printed materials to residents, with no exceptions for charities and political parties, but there is no suggestion that this restricts free speech or the free flow of information.

It would be appropriate to allow more leeway to not-for-profit organisations, in particular, an organisation that relies on volunteers might require longer to comply with an unsubscribe message, but persistent abuse should not be tolerated.

10 Unreliability of Statistics

Paragraph 15 of the Proposals quotes statistics showing that only a small amount of spam received by Hong Kong addresses comes from Hong Kong. We caution that the statistics may not accurately reflect reality. It is not possible to be specific about the source quoted, because the methodology is not explained (but this, in itself, is a cause for concern), so the following issues are general possibilities that may or may not reflect problems with the quoted source:

1. Uncertain definition of spam. The working definition in most studies is, “whatever we detect”, but this takes no account of the effects of false positives and false negatives.
2. It is difficult to determine the original sender of a message; therefore most studies actually focus on the last known relay, and report that as the origin.
3. Statistics are usually produced by service providers, based on their customers’ messages, thus the statistics relate to “our customers in Hong Kong”, which may or may not reflect the situation in Hong Kong as a whole.
4. Comparisons over time are particularly suspect, because the customer base, the detection methods and the spam all change over time. There might be significant skew if a single, large customer joins or leaves, changing the overall pattern of communications.
5. Commercial concerns may influence how statistics are calculated and published.

Automated reporting to the investigation authority, as discussed in section 8.1 , could result in improved statistics and a better understanding of the UEM phenomena: The authority would receive a wider range of reports and it could develop an improved methodology, based on the public interest.

11 Replying to Spammers

An opt-out regime requires recipients to contact the senders when they want to stop receiving messages. The Government has published advice on this topic at http://www.antispam.gov.hk/english/email/email7.htm:

> **Should I complain or reply to the spammer in order to get my email address removed from the spam email list?**
>
> Do not reply or complain by simply clicking the reply button. Most likely, the reply address is forged. If you complain to that email address, or the ISP which provides such email address, you are more likely to be tricked by the spammer to waste your time (and the victim ISP and user's time) to complain the wrong party. Seek help from your ISP if you want to find out the real person sending you the spam email.
>
> Unless you are confident that the spam email organization is trustworthy, do not accept their offer to remove your email address from their spam email list and send them a request for such removal. Most likely, such a request is either ignored or worse, ends up as a confirmation that your email address is

valid, and subject it to promotion to a premier spam email list.

This advice is similar to the advice from many anti-spam companies and organisations, and the “Don’t Try, Don’t Buy, Don’t Reply” campaign run by the Australian Government (which has opt-in legislation).

However, it is clear that this advice is contrary to the requirements of a successful opt-out regime, as described in the Proposals. The Government should clarify whether and how it intends to change this advice, if its Proposals are passed into law, and why the changes make sense.

Hong Kong Computer Society
Unit 1801, Tai Tung Building, 8, Fleming Road, Wanchai, Hong Kong
Tel: +852 28342228 Fax: +852 28343003 Email: hkcs@hkcs.org.hk URL: www.hkcs.org.hk