



**Proposals to Contain the Problem of Unsolicited Electronic Messages
Consultation Response**

25 October, 2004

CONTENTS

INTRODUCTION	3
DEFINITION OF “UNSOLICITED ELECTRONIC MESSAGES”	4
ELECTRONIC MESSAGE.....	4
UNSOLICITED.....	5
UNSOLICITED BULK TRANSMISSIONS & COMMERCIAL COMMUNICATIONS	6
NATURE OF THE PROBLEM	7
PERSONAL PRIVACY CONCERNS.....	7
BUSINESS IMPAIRMENT	7
INAPPROPRIATE CONTENT	7
WASTE OF RESOURCES.....	7
SIZE OF THE PROBLEM	9
EXISTING MEASURES AND THEIR EFFECTIVENESS	11
LEGISLATION.....	11
VOLUNTARY CODES OF PRACTICE.....	12
TECHNICAL TOOLS	13
POSSIBLE SOLUTIONS	15
INDUSTRY CO-OPERATION	15
USERS’ EDUCATION	17
TECHNICAL SOLUTIONS.....	18
LEGISLATION.....	19
OTHER CONTROLS INTRODUCED BY PCCW-HKT.....	25
CONCLUSION	26

Introduction

1. PCCW-HKT Telephone Limited (“**PCCW-HKT**”) welcomes the opportunity to provide its comments on OFTA’s consultation paper regarding the *Proposals to Contain the Problem of Unsolicited Electronic Messages* (“**Consultation Paper**”).
2. The transmission of unsolicited electronic messages has been a problem affecting service providers and users for a number of years. It is only the format of these messages which has evolved as technology develops. For instance, in the early days of simple voice telephony and fax, the problem of unsolicited electronic messages was merely confined to “cold calls” and junk faxes. Nowadays, however, with the increasing use of mobile services and the internet, the problem has been extended to unsolicited messages being sent to mobile handsets and being received over the internet into email accounts.
3. This paper provides PCCW-HKT’s comments on each of the questions put forward by OFTA in the Consultation Paper.

Definition of “Unsolicited Electronic Messages”

4. Before discussing the nature and extent of the problem, it is important to be clear on what constitutes an *unsolicited electronic message*. PCCW-HKT considers the following definition to be appropriate.

Electronic Message

5. PCCW-HKT regards the following types of communication as falling within the ambit of *electronic messages*:

- Telephone calls or voicemail;
- Electronic mail (“**email**”);
- Text messages (“**SMS**”) or multi-media messages (“**MMS**”); and
- Facsimile transmissions (“**fax**”).

On this basis, PCCW-HKT submits that the consultation should cover unsolicited communications transmitted by all of the above media.

6. Amongst the types of media noted, email “spam” and junk faxes are generally perceived to cause by far the most serious problems worldwide today (in terms of volume of messages), and hence most of the comments provided by PCCW-HKT in its submission are made in relation to these two specific areas. In fact, spam and its associated hazards (e.g. the spreading of computer viruses through email) has become such a problem that, according to a survey conducted by MessageLabs (a major email filtering service provider), 62% of companies would be prepared to give up email if the threat posed by spam, viruses and other email-related problems is not contained. The size of the problem associated with spam and junk faxes in Hong Kong is discussed later on in this submission. That is not to say, however, that the other types of electronic messages should be ignored.

7. Junk SMS and MMS delivered to mobile phones, for instance, is on the increase and, if this problem is not recognised, the risk is that junk SMS and MMS could one day flood mobile phones much to the same extent as email spam does on computers today. In fact, in Japan, where text messaging is more popular than email, there are already signs that junk SMS is already as big a problem as spam. NTT DoCoMo Inc., Japan’s largest mobile operator, is reported to stop an average of 960 millions pieces of junk SMS each day (more than 80% of messages) delivered to its subscribers.

8. On a similar basis, junk phonecalls or promotional recorded messages are a growing source of consumers’ complaints in Hong Kong. Recent press reported that OFTA had logged 172 complaints concerning pre-recorded promotional calls and calls from sales staff in the first half of this year, compared to 207 for the whole of last year.

9. With the increasing use of Voice over Internet Protocol (“VoIP”) services, the problem of junk phonecalls is expected to grow. Such calls will be easier to make compared to calls made using the traditional Public Switched Telephone Network, since telemarketers will now be able to use IP technology to send recorded messages to thousands of addresses (telephone numbers) at a time, much in the same way that junk email is transmitted over the internet today.

10. For “VoIP spam”, voicemail boxes will likely be hit the most, as they will record every promotional message received. This could potentially have a serious and costly impact on storage.

11. The issues raised in the Consultation Paper are universal in nature and, to a greater or lesser extent, apply to all the types of unsolicited communications specified above. The specific comments made by PCCW-HKT in this submission on spam and junk faxes therefore could be universally applied to all forms of unsolicited electronic communications.

12. It would be better for the regulatory framework to take a technology neutral approach and cover unsolicited electronic messages generated using all media, since the resulting framework will then have the advantage of being technology neutral and be able to keep pace with technological advancement.

Unsolicited

13. A message should be treated as “unsolicited” if the recipient has not granted his or her prior consent to receive the communication from the sender. This permission, however, can be expressed or implied. Messages could therefore be treated as legitimate if the recipient has established a “prior relationship” with the sender. For instance, having had previous contact with the sender could be regarded as authorising the sender to send messages to the recipient, unless the recipient expressly informs the other party that it does not wish to receive any further communications. The definition proposed by PCCW-HKT is in line with the “opt-in” approach adopted in the European Union and Australia.

14. An opt-in approach is preferable to an “opt-out” approach, which assumes, right from the very start, that the sender is permitted to transmit electronic messages to the recipient until the latter expressly informs the sender that he/ she does not wish to continue receiving such messages. The opt-out approach is less effective than the opt-in approach in combating spam as the messages will continue to be sent to the recipient until the latter takes action to stop the transmissions. On this basis, the opt-out approach may not result in a significant reduction in the volume of spam.

15. The opt-out approach also provides little assurance to the recipient of the message that he/ she will cease to receive any further communications from the sender, even after the recipient has given the sender explicit instructions not to dispatch any further messages. Email security provider MessageLabs recently

revealed that spammers are now using the opt-out link contained in unsolicited emails to turn computers into open proxies for distributing more spam. On this basis, it advised email users not to click on such opt-out links provided in spam emails.

16. Unsolicited messages must be distinguished from “unwanted” communications. Unwanted communications merely refer to messages which cause inconvenience to the recipient but which the recipient has expressly or impliedly consented to receive.

17. PCCW-HKT recognises that there may be concerns from the marketing community in taking measures to legislate against unsolicited messages, especially if an opt-in approach is adopted, since, quite often, marketers are required to send communications to parties with whom they have never had any contact. This approach might therefore be seen as limiting the marketing opportunities that are available. PCCW-HKT would, however, argue that the adoption of an opt-in approach, whereby the recipient has granted his or her prior permission to receive the communication, would in fact ensure a more targeted audience and hence better results.

Unsolicited Bulk Transmissions & Commercial Communications

18. Spam is defined by the Hong Kong Anti-Spam Coalition in its White Paper on *Legislation: One of the key pillars in the fight against spam* (January 2004) (“**White Paper**”) as “unsolicited bulk email and unsolicited commercial email”. For messages to qualify as spam, however, PCCW-HKT considers that it is irrelevant whether the message has been sent out in bulk or whether the message has a commercial (i.e. promotes the sales of goods or services) nature.

19. Though usually dispatched in bulk, it is not necessary for the same communication to have been sent out to a large number of people before it can be classified as spam. The unsolicited nature of the message should be sufficient to qualify it as spam. Equally, it is not necessary to restrict the definition of spam to commercial messages, since non-commercial messages cause just as much nuisance to the recipient.

Nature of the Problem

20. Unsolicited electronic messages are generally considered to be undesirable. The Consultation Paper has already outlined the problems caused by the sending of such messages. These can be broadly summarised into the following categories:

Personal Privacy Concerns

21. Spammers harvest email addresses off the internet and direct marketers obtain telephone numbers through a variety of sources without the knowledge of the owner, which may amount to an abuse of personal information. Contacting a party without his or her prior permission is an intrusive nuisance and raises substantial personal privacy concerns. In some cases, message headers are forged by the spammer such that the recipient is misled as to the real sender, in which case, an innocent party unjustly becomes the victim of complaints from the recipients of the message. Worse still is the use of non-functioning return email addresses or email addresses which purport to allow you to stop receiving future communications when, in reality, they only serve to confirm the validity of the recipient's email address.

Business Impairment

22. As mentioned above, in some cases, the spammer is able to forge the sending address of the message such that an innocent party (which may be a commercial organisation) could be perceived to be the sender of the message. If anti-spam organisations decide to take action against the "spammer", there could be wide-spread blocking of the organisation's IP address, resulting in potentially significant impairment to the business.

Inappropriate Content

23. The non-discriminatory manner in which telephone numbers, fax numbers and email addresses are selected by the message sender means that very often the content of the message is inappropriate for, or irrelevant to, the recipient. Sometimes, faxes are unknowingly transmitted to telephone numbers, producing an annoying fax transmission tone when the phone is answered by the called party. In a lot of cases, the content is offensive or of a nature not suitable for the receiving party.

Waste of Resources

24. The sending of unsolicited electronic messages wastes human and material resources. A substantial amount of time, effort and cost are expended by recipients in having to filter their email before deleting the messages. In the case of junk faxes, paper is wasted when these transmissions are received, whilst substantial storage capacity and bandwidth are used up by unsolicited electronic messages in delivering voicemail, bulk email and SMS/ MMS. Service providers are forced to build in large amounts of storage capacity and bandwidth unnecessarily just to accommodate the large volume of messages. This costs money and slows down the performance of the networks.

25. The sending of unsolicited electronic messages clearly causes serious problems. It is therefore imperative that OFTA take immediate regulatory action to curb the growth of such electronic transmissions.

Size of the Problem

26. As OFTA describes in the Consultation Paper, several organizations have already conducted studies to determine the extent of the problem surrounding the transmission of unsolicited electronic messages. Whilst the studies were mainly focussed on email and fax, the results of the studies indicate the issue to be fairly serious:

- 50% of all emails handled by Internet Service Providers (“ISPs”) in Hong Kong is spam, with 5% originating from Hong Kong and 20-40% from other Asian countries¹. On an international basis, figures in the region of 64% to 76% have been quoted as being the percentage of email traffic on the internet relating to spam;
- The total loss to the Hong Kong economy amounts to some HK\$10 billion per annum, of which 70% of this relates to lost productivity. In the USA, the cost of spam to recipient organizations is believed to exceed US\$9 billion annually²; and
- There were around 24,000 complaints made by customers to the local Fixed Telecommunications Network Services (“FTNS”) operators last year regarding junk faxes. Over 60% of these complaints were made by customers whose fax numbers were supposedly listed on a “not-to-call” list.

27. In paragraph 34 of the Consultation Paper, OFTA asks respondents to quantify the extent of the problem:

The Government welcomes interested parties to submit their comments, with relevant records, data and statistics on the extent of the unsolicited electronic messages problem and the loss in monetary terms caused by unsolicited electronic messages to them. Assumptions made and methodologies used in the submissions, such as how the survey samples were selected and whether the estimates or surveys are based on certain definitions e.g. unsolicited messages generally or unsolicited commercial e-mails only, should be clearly stated.

28. PCCW-HKT is not able to offer any extensive figures quantifying the extent of problem concerning unsolicited electronic messages. It does, however, consider unsolicited bulk email to pose, by far, the most serious problems amongst the various types of electronic communications today. PCCW-HKT estimates that roughly 80% of the email traffic it handles each day relates to unsolicited bulk email and that around 15-20 man-days each month are expended dealing with spam.

¹ From a survey conducted by the Hong Kong Internet Service Providers Association (“HKISPA”) in December 2003

² Ferris Research 2003

29. As the amount of email messages increases, the time spent addressing problems associated with unsolicited electronic messages is also likely to increase, unless measures are promptly introduced to curb the growing volume of spam. Email traffic will continue to increase because it is a powerful, cheap and convenient means of communication. According to IDC, a market intelligence and advisory firm in the information technology and telecommunications industries, the number of emails sent daily is expected to exceed 60 billion worldwide, almost double the number of daily email messages in 2002.

30. In addition, on average, PCCW-HKT receives around 5,500 cases of complaint regarding junk faxes each month through a variety of channels, including telephone, fax and mail. PCCW-HKT requires 3 staff to handle these complaints, costing a total of HK\$45,000 per month.

31. It is clear that, if nothing else, from PCCW-HKT's perspective, the problems experienced with at least two forms of unsolicited electronic message (i.e. junk email and junk faxes) are already very serious. Any further figures provided by the respondents to quantify the extent of the problems associated with these types of messages are therefore likely to do no more than emphasise the gravity of the issue.

32. In fact, besides the survey conducted by the HKISPA referred to earlier, there was another survey conducted in December 2003 by the Office of Mr. Sin Chung Kai on *Unsolicited E-Messages*. This survey highlighted the following key points:

- Amongst email, fax, SMS and phone calls, junk email is the most prevalent form of unsolicited e-message, with over 95% of respondents receiving this type of message each day;
- Unsolicited e-messages are a nuisance to society, with more than 80% of respondents finding such messages annoying; and
- The problem of unsolicited e-messages has imposed additional costs on the consumer, requiring the message recipient to invest time and effort to delete the message (almost 90% of respondents) or adopt filtering tools (almost 50% of respondents).

33. It is clear that the problem associated with spam is already quite significant in Hong Kong. The industry must therefore now focus its attention on what needs to be done in order to combat the issue at hand.

Existing Measures and their Effectiveness

34. There are existing measures in place which deal with the issue of unsolicited electronic messages. In this section, PCCW-HKT comments on their effectiveness.

Legislation

35. Hong Kong does not currently have any form of anti-spam legislation to prevent the sending of unsolicited electronic mail to its millions of internet enabled citizens. Legislation does exist, however, to deal with certain aspects of unsolicited electronic communications.

36. *Summary Offences Ordinance (Cap. 228)*. This piece of legislation is primarily focussed on outlawing the sending of messages containing malicious content and nuisance telephone calls rather than the transmission of junk messages. It is therefore doubtful whether unsolicited electronic communications are covered by this Ordinance. Also, since the relevant provisions within the Ordinance dealing with the sending of messages were last updated a while ago back in 1991, they do not adequately take into account several new forms of electronic media which have become increasingly popular as a means of conveying unsolicited electronic messages i.e. fax, email and SMS.

37. *Personal Data (Privacy) Ordinance (Cap. 486)*. This Ordinance covers the use of personal information when conducting direct marketing activities. It is not entirely clear, however, whether junk email and faxes are outlawed under this piece of legislation given that:

- The Ordinance defines “direct marketing” as those activities where the information is addressed to a **specific person** or **specific persons by name**. Given that junk email and faxes rarely address the recipient by name, this form of unsolicited electronic communication could conceivably fall outside the provisions of the Ordinance; and
- The provisions of the Ordinance are limited to the use of “personal data”, which is any data from which it is practicable to ascertain the identity of the individual. It could be argued that, in the absence of other information, an email address or a fax number does not amount to personal data under the Personal Data (Privacy) Ordinance.

38. *Telecommunications Ordinance (Cap. 106)*. There are no provisions contained within the Telecommunications Ordinance which deal directly with the prevention of unsolicited electronic messages. Section 27A of the Telecommunications Ordinance, as mentioned by OFTA in the Consultation Paper, is more concerned with using telecommunications to access unauthorised information on a computer rather than the sending of unsolicited messages. There are, on the other hand, certain Sections within the Telecommunications Ordinance which appear to make it **unlawful** for a service provider to take action to prevent the transmission of spam. For instance, Section 24 and Section 25 of the Telecommunications

Ordinance make it **unlawful** for a party to interfere in the transmission of electronic messages. It is not clear, however, whether this action would be permitted if it has been carried out for the purposes of preventing spam. PCCW-HKT discusses these Sections in greater detail later on in this submission.

39. *Crimes Ordinance (Cap. 200)*. The particular Sections of the Crimes Ordinance (Sections 59, 60 and 161) quoted by OFTA in the Consultation Paper make it unlawful for a person to intentionally and, without permission, cause damage to another person's computer (or the contents of the computer) or to access a computer with the intention of committing an offence. However, in the context of spamming, unless the sender has the intention of causing the recipient's computer to malfunction or the email actually causes damage to the recipient's computer, it is doubtful whether the spammer can be caught under the provisions of the Crimes Ordinance. Rather, it is likely that the aforementioned Sections of the Crimes Ordinance are primarily intended to deal with parties who create and send out "computer viruses" with the intention of causing harm to computer systems.

40. It is therefore clear that there is a lack of legislation dealing directly with unsolicited electronic messages and an urgent need for specific legislation to be introduced in Hong Kong to tackle this growing problem.

Voluntary Codes of Practice

41. Whilst no specific legislation exists to combat unsolicited electronic messages, there are certain codes of practice which have been developed by the industry in an attempt to address the problem.

42. *Email*. The Anti-Spam Code of Practice issued by the HKISPA outlines certain technical conditions to which industry members are required to adhere in order to prevent spamming activities. Unfortunately, compliance with the Code of Practice is not obligatory and, in any case, the spammer is often not a member of the HKISPA. In the absence of legislation outlawing the sending of unsolicited electronic messages, therefore, it is hardly surprising that this Code of Practice is not considered effective.

43. Whilst the drawing up and maintenance of a local name list of email servers that are reasonably suspected to have transmitted spam (M-List) will help ISPs identify potential spam and take corrective action, this does not solve the problem of certain parties disguising themselves as another ISP when sending out spam. Under these circumstances, an innocent ISP may be put onto the M-List through no reason of its own and its reputation will be damaged.

44. *SMS and MMS*. On a similar basis to the Code of Practice issued by the HKISPA, a Code of Practice was agreed on by the mobile operators in Hong Kong setting out guidelines for sending promotional SMS. Again, this Code of Practice will never carry much weight unless it is supported by underlying legislation. In fact,

Hong Kong may need to consider legislating against the sending of unsolicited messages to mobile phones along the same lines as spam.

45. It is interesting to note that some countries have already taken action against unsolicited SMS and MMS. In August of this year, the Federal Communications Commission in the USA, with the support of marketers and the mobile industry, issued rules prohibiting companies from sending commercial messages to mobile phones without the user's permission.

46. *Fax.* There has been greater success in the prevention of junk faxes through the use of a "not-to-call" list which is required to be observed by senders of fax advertisements. As the sender risks having its faxlines cut off by the FTNS operator if the recipient of the junk faxes raises a legitimate complaint against the sender, there is more of an incentive for the sender to observe the guidelines on fax advertisements issued by OFTA, even if this is purely voluntary in nature.

47. On the whole, however, clearly it is not sufficient to simply rely on voluntary Codes of Practice to prevent the sending of unsolicited electronic messages. There must be stronger underlying legislation if this problem is to be properly resolved.

Technical Tools

48. Another measure that is currently adopted to combat the problem of unsolicited electronic messages (particularly spam and junk faxes), is the use of technical devices to prevent receipt of these messages.

49. *Users' Arrangements.* OFTA has suggested that recipients of unsolicited messages, either via fax, email or mobile phone, simply ignore the spam and delete it. This is hardly an effective means of combating spam since it does not stop the sender from sending the message in the first place. From the user's perspective, it would be better to minimise the opportunities for the sender to get hold of the user's fax number, email address or mobile phone number. This would include taking precautions when visiting websites and providing such personal information over the internet.

50. *Blocking Devices.* Such devices include tools that block spam based on the content of the email or the subject heading or systems that do not release emails from unrecognised senders to the recipient until the identity of the sender has been verified. Whilst the latter method could be used to ensure that only email is received from those senders from whom the customer has opted to receive email, this causes a problem for certain parties who are required to get in touch with individuals whom they have never contacted before e.g. Government offices and is therefore not entirely effective.

51. Another method used is to compile a blacklist of spammers and their IP addresses. All email from these addresses are then blocked so that they do not reach the customer. Whilst this seems a feasible way of stopping spammers, it has the

downside of potentially also stopping non-spam since IP addresses are not always specific to a particular computer or account.

52. *Efforts by ISPs.* The ISPs have achieved a reasonable degree of success in implementing measures to reduce the amount of spam. These include educating and advising its customers on how to minimise the risk of spammers getting hold of their personal information and also providing spam filtering services. Some ISPs also deliberately block packets destined for certain ports on their network in order ensure that potential offenders cannot access open email servers to send out spam.

53. Despite the existence of such tools, however, the bottom line is that these measures do not stop the sending of unsolicited messages. As a result, the root cause of the problem is not solved. Filtering email messages, whilst containing the spam, still cost time and money. Large volumes of spam on the internet continue to cause network performance and capacity issues. Junk faxes take up people's time and waste resources. Stronger measures must be adopted in order to discourage the sending of unsolicited messages.

Possible Solutions

54. The existing measures in place are clearly insufficient to combat the problem of unsolicited electronic messages. Additional, and more effective, measures need to be introduced. In this section, PCCW-HKT comments on the various solutions put forward by OFTA in the Consultation Paper to deal with the problem and suggests some additional measures.

Industry Co-Operation

55. There are already industry voluntary codes of practice in place governing the sending of fax, email and SMS messages by FTNS operators, ISPs and mobile operators. These were created in an effort to reduce the number of problems associated with unsolicited electronic communications. Unfortunately, by their very nature of being voluntary, these codes of practice cannot guarantee strict adherence by operators within the industry. More significantly, quite often the offender is not a service provider but an unscrupulous marketer.

56. In paragraph 71 of the Consultation Paper, OFTA asks respondents to put forward their views as to how the industry should cooperate to combat the sending of unsolicited messages and whether any of the measures proposed should be made mandatory:

The Government invites comments on whether the proposals as explained in paragraphs 68 to 70 above on industry co-operation should be introduced and whether such measures should be voluntary or any of them made mandatory.

57. Whilst it would be highly beneficial for the industry to follow codes of practice, to solely rely on this form of “soft” regulation would not be totally effective. Codes of practice must be accompanied by more stricter forms of regulation. If the only weapon available to combat unsolicited electronic messages were a voluntary set of guidelines, this would result in Hong Kong being continually isolated from overseas regimes in dealing with the problem, since there would be no legal basis in Hong Kong for an organization to take any action against offenders.

58. PCCW-HKT supports the continued development of codes of practice within the industry as this can only be beneficial to the operators and the consumers at large. However, considering the potential cost involved in complying with codes of practice, PCCW-HKT finds it preferable for adherence to such guidelines to remain on a voluntary, rather than mandatory, basis so as to allow the service provider a certain degree of flexibility. As long as there is more rigorous legislation introduced to deal with unsolicited electronic messages, there is no reason why observing the existing codes of practice should be made mandatory.

59. PCCW-HKT does not object to the list of initiatives put forward by OFTA in the Consultation Paper as long as compliance with the resulting guidelines is purely

on a “best efforts” basis. In paragraph 69 of the Paper, OFTA recommends that the HKISPA and its members:

- Build on the existing work done by the HKISPA and implement the Code of Practice to deal with spam;
- Develop better practice guidelines for ISPs (and their customers) to tackle spam;
- Further develop strategies to have internet users shut down open relay mail servers; and
- Publish tips for subscribers for dealing with spam.

From PCCW-HKT’s perspective, these initiatives are certainly worth pursuing within the industry and should assist in reducing the volume of spam.

60. OFTA’s suggestion, in paragraph 70, that industry players should jointly compile and make use of a common blacklist of spammers is also acceptable. The sharing of information amongst the operators will greatly enhance their ability to prevent spammers from repeating an offence.

61. The difficulty with implementing anti-spam measures, particularly if an opt-in approach is to be adopted by the industry, is that marketers would likely view this as imposing unnecessary restrictions on those parties to whom they may promote their goods and services. One possible solution worth considering (which would require cooperation amongst all the ISPs within the industry) is to require all promotional email messages to be sent via the ISP to its customers rather than directly from the marketing company. In this case, the marketing company will engage an ISP to send its promotional message to those of its subscribers who have previously consented to receiving messages of this nature. Any promotional messages dispatched directly from the marketing company will be treated as spam by the ISP and stopped.

62. This proposal has the advantage of:

- Giving the marketing company instant access to a large number of potential customers via the ISP;
- Ensuring that the marketing company’s promotional message is targeted at the right customer segment, since these customers will have expressed an interest in the type of product or service offered by the marketing company and will have agreed to receive such promotional messages when it subscribed for service from the ISP. Of course, the customer is permitted to discontinue receiving promotional messages delivered via the ISP at any time; and
- The proposal creates a valuable revenue stream to ISPs which they could use to finance the development of spam detection software.

63. This approach would seem to balance the interests of the marketing community whilst, at the same time, ensuring that the customer is not the recipient of irrelevant and unsolicited email communications.

Users' Education

64. To combat the problem of unsolicited electronic messages, it is not sufficient to rely on industry self-regulation in the form of codes of practice. In addition, users need to take action to minimize the chances of potential offenders being able to access their (fixed and mobile) phone number, fax number or email address.

65. In this section of the Consultation Paper, OFTA discusses user education in the specific context of email spamming. In paragraph 75 of the Consultation Paper, OFTA asks for comments on the proposal to initiate an anti-spam campaign and the form it should take:

The Government invites comments on whether such an anti-spam campaign should be mounted by the industry, and if so the form the campaign should take and the messages to be promoted in it.

66. Whilst unsolicited electronic messages are not confined to email alone, it is probably more beneficial for any user awareness campaign to focus on this mode of communication. There is relatively little that can be done by the public to stop an offender from accessing fixed line phone and fax numbers since these are readily available from printed and on-line directories.

67. Most internet users are already aware of spam since few users would have been able to avoid receiving at least some junk email. An awareness campaign would be effective if handled correctly, targeting the right messages to the public. These messages should, as a minimum, include the following:

- Explanation of how spammers are able to get hold of a user's email address;
- Advice to users on how to protect their personal information, including email addresses, so as to make it more difficult for spammers to operate; and
- What action to take if a user finds that he has been subject to a spam attack. Besides the installation of spam filtering software, users should be advised to inform their ISP and authorize the ISP to take action to prevent the spammer from sending further junk email.

Such a campaign would target internet users and ideally be conducted by one or more of the relevant industry bodies in Hong Kong such as the HKISPA, the Hong Kong Anti-Spam Coalition or the Hong Kong Computer Society.

68. User education is an important step in combating spam as there is little point in introducing preventative measures if the user is not aware that the actions he is taking may actually be encouraging the sending of such electronic messages.

Technical Solutions

69. Technical solutions are often adopted to identify and eliminate unsolicited electronic transmissions. In the case of spam, a filtering program is commonly used to spot transmissions which carry the characteristics of junk email or the ISP makes reference to “blacklists” of spammers, and these transmissions are either prevented from being delivered or segregated from the recipient’s bona fide email to facilitate dealing with as the recipient sees fit.

70. The solution usually adopted for fax transmissions is the same as that used for voice calls. Users normally subscribe to “block-the-blocker” services which prevent delivery of messages from senders who do not display their calling number.

71. For junk SMS and MMS, the problem is comparatively easier to contain since mobile networks (unlike the internet) are closed systems over which each operator exerts almost absolute control. It is therefore much simpler to prevent unsolicited SMS from reaching the subscriber. For instance, by imposing message volume limits on SMS senders, operators are able to stop the automated bulk transmissions that are normally associated with spamming activities.

72. In paragraph 78 of the Consultation Paper, OFTA seeks input on the technical solutions available and how effective they are:

The Government invites views and comments on the available technical solutions and their effectiveness.

73. The use of filters which make reference to blacklisted domains do not always achieve accurate results. In some cases, emails from certain innocent senders are unintentionally barred because the spammer has hoaxed the email address of the sender. Also, blacklists are only effective if they are kept up-to-date. Spammers can easily change domains and email addresses in order to avoid detection.

74. “Block-the-blocker” services, whilst successfully intercepting junk voice calls and fax transmissions before they reach the recipient, suffer from the shortcoming that they also block those genuine calls and faxes from senders who, for privacy reasons, have elected not to display their number. In addition, “block-the-blocker” services cannot stop junk calls and faxes if the sender does display its telephone or fax number.

75. PCCW-HKT maintains technical solutions designed to try and identify spam and block it from entering the PCCW-HKT network. Additional technical controls have been deployed in accordance with the anti-spam policy specified in the HKISPA guidelines and with the full support of OFTA and the HKISPA. These controls involve the SMTP port 25 being blocked to protect Netvigator customers from the receipt of spam email.

76. Further measures adopted by PCCW-HKT include:

- Proactively identifying domains from where spam originates; and
- Looking at the characteristics of transmissions to determine whether they are likely to be spam and then taking corrective action e.g. identifying a batch of a million electronic mail messages which all arrive at the same time from the same originating address.

77. Technical measures which involve the service provider examining the content of electronic messages and blocking those messages which are suspected of being unsolicited transmissions are an effective solution to combating the problem of spam. There is, however, a fundamental issue concerning the authority of the service provider to carry out such actions, which may require the express consent of the end user. This issue of legality is examined in the next section.

Legislation

78. The problem of unsolicited electronic messages must be addressed from more than one angle. Whilst industry cooperation, user education and technical solutions collectively provide a secure safeguard against junk calls, faxes and email transmissions, legislation is still an essential part in the suite of armour to provide legal recourse against offenders. Indeed, in the Hong Kong Anti-Spam Coalition's White Paper, it acknowledges that legislation specifically targeted on spam would be a critical component of a comprehensive and effective solution to the spamming problem, and it urges the Government to initiate public consultation on the drafting of specific legislation to combat spam. This viewpoint is also supported by the Hong Kong Computer Society.

79. In fact, throughout the world, different countries (including the USA and the EU) have enacted legislation to prohibit the sending of spam that contains misleading information in its subject line, uses a third party's domain name without permission, or misrepresents the message's point of origin. Hong Kong currently has no such legislative controls.

80. In paragraph 83 of the Consultation Paper, OFTA asks respondents to put forward their views on whether legislation should be introduced to combat spam and what can be done to existing measures to tackle the problem:

The Government would therefore like to invite views on the pros and cons of a legislative approach to combat spam, and whether and if so how existing measures to tackle the spamming problem should be strengthened.

81. As no legislative relief or protection operates within Hong Kong to prevent the occurrence of spam, PCCW-HKT can only rely on the good faith of its customers in refraining from activities that constitute spamming. The bottom line, however, is that spam is not illegal in Hong Kong. PCCW-HKT is therefore concerned that there is no legal basis to support its efforts in blocking spam.

82. PCCW-HKT believes that the issue of spam has now reached a point whereby the Hong Kong SAR Government needs to apply and enforce more legislative controls against the cause of the problem i.e. the spammers, rather than relying on existing contractual arrangements between ISPs and their customers to reduce the occurrence of spam. In the case of PCCW-HKT, there is often no contractual relationship between the end spammer and PCCW-HKT as the spammer is often found to be residing outside of Hong Kong. That is precisely why it is important to seek cooperation amongst the international community if spam is to be successfully contained.

83. In the public domain, there is general support amongst internet users to introduce some form of legislation against spam, indicating that users do not consider existing measures to be adequate in combating the problem. In a survey conducted in December 2003 by the Office of Mr. Sin Chung Kai³, it was found that over 80% of respondents agreed that Government intervention was necessary, particularly in the form of anti-spam legislation.

84. Those who do oppose legislation mainly do so on the grounds that this would limit freedom of speech and the free flow of information. Marketers are also likely to object to legislation if it places an additional (and costly) compliance burden on the business. PCCW-HKT, however, considers that, whilst freedom of speech and communication of information are important, the recipient should equally have the right not to receive the information. Legislating against unsolicited electronic messages ensures that communications sent by those wishing to exercise their freedom of speech are only received by those who have given their consent to receiving such messages. By restricting the recipients to those who have elected to receive such communications also ensures that any marketing messages are targeted at the right audience and renders the exercise more cost effective.

85. PCCW-HKT considers that the focus of any legislation should address three primary areas where the consumer and the ISP is harmed by spam:

- (i) Recipients are the victims of a deceptive consumer practice because they pay for the internet time and services that deliver the unsolicited email. Consumers waste their time downloading such emails, and false subject lines prevent them from properly deciding whether or not to delete the message. Recipients are also unable to ascertain the correct return email address in order to respond.
- (ii) Where an innocent party's email address has been misappropriated for use by a spammer as the sender of the spam message, the party will receive a flood of emails from victims of the spam message who decide to respond to the message. Misappropriated email return addresses may also cause a legitimate

³ See Annex 1 of the Hong Kong Anti-Spam Coalition's White Paper

website to shut down as a result of a large number of persons responding to the spam message.

- (iii) The ISP is harmed because mass electronic mailings clog systems and cause network overloading, down time, and costs associated with filtering potentially deceptive emails.

86. PCCW-HKT believes that the Hong Kong SAR Government should ensure new legislation is adopted to protect the public against spamming. Such legislation should aim to ensure there is a requirement for all email messages to be truthful in a manner designed not to burden commerce, and better facilitate commerce by legally eliminating a growing channel in which fraudulent and deceptive practices can be harboured.

87. To achieve this goal, PCCW-HKT considers that legislation should be introduced as soon as possible in Hong Kong to:

- (i) Define the following terms more clearly:
- Spam;
 - Unsolicited Advertising Information; and
 - Unsolicited Promotional Material.
- (ii) Treat material as being deceptive (and therefore unlawful) if it:
- misrepresents the sender (in the source or routing information); or
 - misrepresents the subject or content of the email; or
 - fails to provide reliable contact information for the real party in interest; or
 - fails to provide a reliable system whereby the recipient can choose to stop receiving future communications; or
 - is sent to an individual who has not opted to received the communication, or has already requested to be removed from the sender's list, or to whom the sending of unsolicited email is otherwise prohibited by law.

88. Legislation would demonstrate Hong Kong's seriousness and commitment in dealing with the problem of unsolicited electronic messages. At the very least, enacting legislation would act as an important deterrent to would-be senders of unsolicited messages. The EU, USA, Korea, Japan, Australia and other countries around the world have either already enacted laws or are well advanced in the process of deciding the best legislative route forward. Introducing legislation against unsolicited electronic messages in Hong Kong would be the only means to ensure that Hong Kong does not become a "safe haven" for would-be offenders.

89. It is important for any legislation to complement the laws in place at the moment. For this reason, it is essential to firstly clarify any existing legislation which

may have a bearing on the transmission of unsolicited electronic messages. In particular, it would be helpful if the Telecommunications Authority (“TA”) could clarify whether a service provider is authorised to stop emails or examine the contents of emails for the purpose of preventing spam since, at face value, these actions appear to contravene the provisions contained in the following Sections of the Telecommunications Ordinance:

- **Section 24.** *Offences by telecommunications officer, etc.* This Section deems a telecommunications officer to be guilty of an offence if he willfully abstains from transmitting any message or willfully intercepts or detains or delays any message.
- **Section 25.** *Secretion, etc., of messages by persons other than telecommunications officers.* This Section deems any other person to be guilty of an offence if he willfully secretes, detains or delays a message intended for delivery to some other person.

90. On the other hand, **Section 33** of the Telecommunications Ordinance on *Power of Governor to prohibit transmission of messages, etc.* permits a message not to be delivered to the intended recipient if, in the public’s interest, this has been authorized by the Governor (the TA ?).

91. Whilst PCCW-HKT recognises the privacy concerns regarding personal communications, it nevertheless considers that service providers should have the right to examine the contents of electronic messages and prevent the delivery of certain transmissions if it has genuine grounds to suspect that the message is unsolicited. In fact, PCCW-HKT would interpret Section 24 of the Telecommunications Ordinance as allowing operators to stop certain messages on the basis that, if Section 24 really were drafted with the intention of preventing operators from stopping *any* message then such parties would not be able to suspend a customer’s service even for non-payment of charges or downloading of illegal content or any unlicensed use. Yet, the present legislation does not make this particularly clear. Clearly, the service provider should be justified in blocking messages on the grounds of protecting its technical infrastructure from being inundated with spam (i.e. insufficient capacity to handle the flow of unnecessary messages) and to reduce the actual number of spam messages being delivered to its customers.

92. In paragraph 85 of the Consultation Paper, OFTA discusses the various areas to be considered if legislation against unsolicited electronic messages is to be introduced. PCCW-HKT provides its comments as follows:

- (1) *Scope of the legislation.* If legislation is enacted, it should be made as technology neutral as possible in order to cover all forms of unsolicited messages. This would avoid the necessity to introduce more legislation later on as new forms of technology are exploited to deliver unsolicited messages.
- (2) *Legislation restricted to messages of a commercial nature ?* Firstly, in a lot of instances, it is difficult to draw the distinction between “commercial” and

“non-commercial” messages. Secondly, one of the major objections to unsolicited messages is the fact that they were “unsolicited” rather than the content of the message itself. On this basis, PCCW-HKT considers there is no need to limit legislation to messages of a commercial nature.

- (3) *Only “bulk” messages to qualify as unsolicited electronic messages ?* It is not necessary for a message to be sent out in bulk before qualifying as an unsolicited electronic message. A message should be considered as spam by the very fact that the sender did not receive permission from the message recipient to send the message. In any case, it is difficult to define what level of quantity constitutes “bulk” messages. PCCW-HKT does, however, agree that the volume of unsolicited messages dispatched by the offender should be a consideration when determining the seriousness of the penalty.
- (4) *Cold calls, voice and video.* As stated earlier, PCCW-HKT considers that any legislation against unsolicited messages should be made as broad as possible in order to cover all forms of unsolicited messages. There is therefore no reason to specifically exclude cold calls, voice or video. It is not a question of how much resources the instigator needs to expend in order to reach the recipient (as OFTA has suggested), but the fact that the message/ call was not authorised by the recipient. Cold calls, voice and video are used by the instigator for the same purposes as other forms of unsolicited messages. They also have the same effect on the recipient and hence should be dealt with in the same manner as spam.
- (5) *Permission-based approach.* PCCW-HKT prefers that prior permission be granted by the recipient (either expressed or implied) before the sender is allowed to send messages to the recipient. Implied permission can be inferred from an existing business relationship. The recipient must, however, be allowed at any time to request that the sender discontinue from sending any further messages to the recipient.
- (6) *Opt-in or opt-out approach ?* An opt-in approach, whereby the sender is required to secure the express or implied consent from the message recipient before sending out the message, is the preferred option. This has the advantage of ensuring that message is targeted at the right audience. An opt-out approach does not really solve the problem of spam since spammers can still continue sending out messages indiscriminately until the recipient expressly requests the spammer to cease doing so. This approach would be in line with that adopted in the EU and Australia.
- (7) *Labeling of email headers.* PCCW-HKT agrees that senders should be prohibited from falsifying headers in email messages. However, since the problem may not simply be confined to message headers, PCCW-HKT suggests that any legislation to be introduced outlaw the falsification of any transmission data contained in unsolicited messages.

-
- (8) *Restrictions on email harvesting etc.* PCCW-HKT concurs that activities spammers deploy to compile email address listing such as harvesting email addresses from websites, the generation of email addresses by automatic means and trading email lists between ISPs (without the email addressee's permission) should be prohibited.
- (9) *Scope of investigation and enforcement powers.* As mentioned earlier, there already exists legislation (in the Telecommunications Ordinance) which appears to bar telecommunications officers and other parties from stopping the transmission of messages. The exact rights of ISPs vis-à-vis examining the contents of messages and stopping the transmission of suspected spam needs to be clarified in any new legislation to be introduced.
- (10) *Increase in compliance costs.* There is no doubt that introducing any degree of legislation will result in an increase in compliance costs. This does not mean, however, that legislation should not be introduced simply in order to spare businesses from incurring such costs. Whilst it may be the case that the costs of compliance increase, it would equally be fair to say that marketing costs will decrease and promotions made more effective as communications are only sent to those parties who have consented to (and hence are interested in) receiving such messages.

93. In addition, PCCW-HKT suggests that any legislation to be introduced should clarify the following specific aspects:

- (i) Specify the extent of the ISP's powers to prevent its service from being used by another party to transmit spam, including the ability for the ISP to:
- block the receipt or transmission through its service of any spam that it reasonably believes is, or will be, sent in violation; and
 - protect itself from liability for any action voluntarily taken in good faith to block the receipt or transmission through its service of any spam which it reasonably believes is, or will be, sent in violation.
- (ii) Clarify the intentions of the Telecommunications Ordinance (Chapter 106) with respect to electronic mail and spam;
- (iii) Outlaw the falsification of transmission data in electronic mail;
- (iv) Making it unlawful for any person to knowingly sell, give, or otherwise distribute or possess with the intent to sell, give, or distribute software which:
- is primarily designed or produced for the purpose of facilitating or enabling the falsification of electronic mail transmission information or other routing information; or
 - has only a limited commercially significant purpose or use other than to facilitate or enable the falsification of electronic mail transmission information or other routing information; or

- is marketed by that person or another acting in concert with that person with that person's knowledge for use in facilitating or enabling the falsification of electronic mail transmission information or other routing information.
- (v) Clarify that the existing statutes do apply to “electronic mail”;
- (vi) Provide penalties and remedies for ISPs and customers against spammers who are sending unsolicited electronic communications. This is because, in order to effectively discourage the sending of spam, some kind of financial retribution from those parties causing the problems is necessary, and this is only possible through the introduction of legislation; and
- (vii) Give ISPs the ability to recover the costs of bringing legal actions against people to stop the sending of spam.

Other Controls introduced by PCCW-HKT

94. PCCW-HKT has introduced a number of business controls to deal with the problem of spam. These include the following measures:

- Deploying stringent anti-spam policies;
- Strictly prohibiting its customers from using their email accounts to send spam;
- Preventing the use of email accounts to harvest screen names to compile mailing addresses, or to do anything else that facilitates the transmission of spam;
- Not selling or distributing lists of its customers’ email addresses;
- Taking extensive precautions to maintain its customers’ privacy;
- Maintaining some of the most robust technological tools available to try and block spam before it even enters the PCCW-HKT network, and before it gets distributed to its customers; and
- Creating an extensive set of tools for its customers to give them control over the email they receive.

95. As a result of experiencing the various forms of attacks and in adopting the range of controls discussed, PCCW-HKT has found that:

- Feedback from other ISPs indicates that the extent of spam being sent by Netvigator has been significantly reduced;
- Complaints to the Netvigator postmaster have reduced to about 1,000 daily; and
- Complaints indicate that Netvigator spammers now generally originate from modem pools where the blocking of SMTP port 25 has not yet been enforced.

PCCW-HKT will continue to implement controls to safeguard its network and its customers from unsolicited electronic communications.

Conclusion

96. This is a timely consultation given the growing seriousness of the problem in Hong Kong. In fact, unsolicited electronic messages have become such a significant issue in other developed countries that legislation has been enacted in recent years to deal with the problem. There is clearly a need for the Hong Kong SAR Government to act promptly in order to ensure that the problem does not get out of hand.

97. To effectively resolve the problem of unsolicited electronic messages, the following overall approach should be adopted by the industry:

- An "opt-in" approach needs to be adopted to combat spam. This requires consent to have been granted by the email recipient to the sender before the sender is permitted to dispatch any electronic communications to the recipient. Consent can, however, be expressed or implied (i.e. via an existing business relationship). This approach is preferable to an "opt-out" scheme, which does not stop the initial volume of emails since spammers can continue to send out messages to the recipient until the recipient requests the offender to stop sending the messages;
- There needs to be a coordinated effort amongst organisations within Hong Kong to combat spam, including the maintenance of a spammers blacklist. On an international basis, regulators around the globe should cooperate with each other to implement anti-spam measures given that a large amount of spam originates from overseas. In fact, in the conclusion to the Background Paper for the OECD Workshop on Spam issued by the OECD on 22 January 2004, it suggested:

Spam is not the problem of any single country, or even limited to OECD member countries. It is a worldwide problem. With Internet access and use continuing to grow in developing countries, the global character of spam may yet expand further. It is increasingly clear that domestic efforts must be supplemented by internationally co-ordinated strategies to address the cross-border challenges posed by spam.

- Users should be educated as to how spam originates, how senders are able to get hold of contact details of users and how to avoid these details being accessed by spammers;
- Service providers should be encouraged to develop more effective anti-spam programs or filtering agents; and
- Strong legislation should be imposed against the sending of unsolicited electronic messages to act as an effective deterrent to potential spammers. At the same time, the TA needs to clarify the rights conferred on service providers by the existing legislation as regards the authority to prevent or alter electronic transmissions destined for its customers, since these represent the first steps that can be taken towards the prevention of unsolicited electronic messages.

The implementation of these measures should go a long way to ensure that the problem of unsolicited electronic messages does not grow out of control and is kept in check, if not completely eliminated.