PROPOSALS TO CONTAIN THE PROBLEM OF UNSOLICITED ELECTRONIC MESSAGES

Consultation Paper

INTRODUCTION

1. The telecommunications network, in particular the Internet, has become a borderless communications medium widely adopted by the business sector and the community at large. The information and communications technology (ICT) available nowadays offers enormous potential to expand business opportunities, reduce costs, increase efficiency, improve the quality and facilitate the greater participation of small business in global commerce. While the telecommunications network offers exciting new opportunities for reaching the world, it has at the same time facilitated the collection of contact information such as electronic mail (email) addresses, fax numbers and mobile phone numbers etc. of large numbers of individuals and corporations, and the distribution of information to them through the electronic medium, quickly and, in the case of email or fax, at almost no marginal costs when compared to the traditional paper-based direct marketing mails.

2. The developments in technology have led to an increase in the use of email as a very convenient mode of transmission of messages. Currently, the most prevalent form of unsolicited electronic messages takes the form of emails in general, and the use of public networks to transmit bulk unsolicited electronic mail is often referred to as “spamming” and the mail as “spam”. Most of the bulk unsolicited electronic mail is of a commercial nature, promoting products or services, and could be likened to an extension of traditional unsolicited mail and other direct marketing practices. Nevertheless, in a broader context, unsolicited electronic messages may take other forms. For example, the more traditional way of sending unsolicited electronic messages by fax remains to be a nuisance to some recipients. Moreover, the trend of sending unsolicited promotion messages via the use of short messaging service (SMS) and multi-media messaging service (MMS) on mobile phones is on the rise.

3. This consultation is to review the problem caused by various forms of unsolicited electronic messages, the effectiveness of the current measures which deal with the problem of unsolicited electronic messages and will discuss a range of possible measures to combat the problem, including the need for enactment of legislation and the strengthening of current guidelines/codes of practice.

4. The Government is mindful that the introduction of additional regulations on unsolicited electronic messages will invariably lead to compliance costs on those engaging in direct marketing or telemarketing practices. The extent of the costs will depend on, among other things, the type of regulation. That said, in considering whether to introduce additional regulation, the impact on these marketers, the costs/nuisance to recipients of unsolicited electronic messages, Internet service providers (ISPs) and mobile service providers etc, and the costs and effectiveness of enforcement will need to be considered. The Government is aware that a proper balance needs to be struck between the social and economic impact of unsolicited electronic messages and the effectiveness and efficiency of our telecommunications network as a communications medium for the general community and the business sector.

DEFINITION OF "UNSOLICITED ELECTRONIC MESSAGES"

5. Before embarking on the proper regulatory measures to combat unsolicited messages sent through the electronic medium, it is necessary to first define the problem at which these regulatory measures are targeting.

Electronic messages

6. Apart from email spams, unsolicited "electronic" messages can be sent via SMS, MMS, fax, and voice mails. With the increasing popularity of mobile phones in Hong Kong, unsolicited electronic messages taking the form of SMS and MMS on mobile phones, sometimes also referred to as "spam", are also getting more popular. Today, SMS and MMS spam is generally perceived as a less serious problem than email spam. However, with the growth in the use of mobile phones and the advancement of ICT, it may be beneficial if our regulatory framework, if any, will take an accommodating

approach and will be technology neutral. It will then encompass unsolicited electronic messages taking the form of emails and other forms of messages transmitted through the electronic medium, such as SMS and MMS etc., and will be able to keep pace with the technological advancement.

7. While there has been a shift of focus to email, SMS and MMS spam, the more traditional way of sending unsolicited messages by fax should not be overlooked. In 2003, the complaints received by all the local Fixed Telecommunications Network Service (FTNS) operators totalled a number of 24 232. For the purposes of formulating the appropriate regulatory measures, the term "unsolicited electronic messages" should include those received via fax.

Unsolicited

8. The key aspect of "unsolicited electronic messages" is that the electronic messages must be "unsolicited". In general, a message is considered to be unsolicited if there is no prior relationship between the parties, and the recipient has not explicitly consented to receive the message. It can also mean that the recipient has previously sought to terminate the relationship, usually by instructing the other party not to send any more communications in the future.

9. It should be noted that "unwanted" messages may not amount to "unsolicited" messages, because the recipient may have previously consented to the receipt of these messages. While some people consider all advertisements or even all unwanted email or mobile phone messages to be spam, the anti-spam community has generally accepted that spam refers only to those messages the receipt of which has not been consented to.

10. It is a common debate whether the sending of commercial messages should be permission-based, i.e. with the prior consent of the recipient. "Permission" itself may also vary in different degrees. On the one hand, a recipient may have given his express prior consent (this is sometimes referred to as "opt-in") to the receipt of commercial messages. On the other hand, there may simply be a pre-existing business relationship between the sender and the recipient from which consent can be inferred. In this case, the sender will be at liberty to send out commercial messages unless the recipient has

actively informed the sender that he does not wish to receive any such messages. Others argue that marketing companies should also have their rights to market their goods or services. The sending of commercial messages should not need a permission from the recipient beforehand so long as there is a way for the recipient to choose not to receive future messages. This is referred to as "opt-out".

11. In the *Position Paper of Asia Digital Marketing Association on legislation to fight spam* (http://www.asiadma.com/downloads/guidelines/pdf/100040/Position_of_the_ADMA_on_legislation_to_fight_spam.pdf), the Asia Digital Marketing Association (ADMA) advocates the permission-based email marketing in order to help fight spam and help assure that consumers only receive information that is relevant or of interest to them. The ADMA issued a set of *Guidelines for Responsible Email Marketing* to promote the implementation of permission-based campaigns with respect to email marketing.

Commercial

12. "Commercial" is generally defined in terms of message content regardless of the actual or presumed intention of the sender. It should cover both "direct" and "indirect" marketing. A typical definition includes any message that promotes the sale of goods or services. It is difficult, if not impossible, to provide an exhaustive definition. The preferred approach is to adopt a simple definition to the term "commercial", while setting out exceptions to list out which will not be considered "commercial".

13. In Australia, the Spam Act 2003 stipulates that a key attribute of the type of message covered by the legislation is that it is "commercial" in nature – it either offers a commercial transaction, or directs the recipient to a location where a commercial transaction takes place. The definition for "commercial" has also enabled the legislation to catch spam which is of a fraudulent nature. On the other hand, the US CAN-SPAM Act 2003 defines "commercial" electronic message to mean "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service".

Bulk

14. One of the real problems with spamming often lies in the volume of email messages sent to the recipients. For that reason, spam sometimes refers to unsolicited electronic mail sent in large quantities – i.e. in bulk. A single message sent to a very large number of recipients clearly qualifies as bulk. By the same token, separate but identical copies of a message that are sent to a large number of recipients are also considered to be sent in bulk. Substantially similar messages, as well as identical copies of a single message, probably also qualify as "bulk". There is no generally agreed threshold – it varies on a case by case basis.

NATURE OF THE PROBLEM

Objectionable content

15. Spam is problematic for a number of reasons. Many of the objections to spam relate to its content. There are obvious concerns with the illicit content of a considerable amount of spam – including those which promote pornography, illegal gambling services, pyramid selling, get rich quick schemes or misleading and deceptive business practices.

Invasion of personal privacy and nuisance to consumers

16. Spam is an intrusive nuisance to consumers. There are significant privacy issues surrounding the manner by which email addresses and personal information are collected and handled. For example, some common address collection methods condemned by consumers include address collectors covertly harvest email addresses off the Internet, collect them as users visit certain Internet sites, and buy and sell them in bulk without the knowledge or consent of the owner. Many spammers do not provide unsubscribe facility to users. Others complain that even if there is an unsubscribe option, it is simply not functioning or even serves as a confirmation that the email address in question is valid and active, which in turn would invite more spam.

17. There are complaints that spam has caused overloading of e-mail storage and hence the resulting extra payment of fees. Among the complaints

on extra charges for email storage, some complainants reported an accrual storage charges of up to HK$2,000 for extra storage of undeleted spams in the email account.

18. There are also complaints from mobile phone users that SMS are received without their consent.

19. In the case of home fax, there are complaints that fax users receive marketing faxes throughout the night with huge consumption of papers. Certain junk fax senders operate on automatically generated numbers and have the tendency of directing the fax messages to these automatically generated numbers regardless of whether they are fax, household or mobile phone users. Recipients of "fax tones" at their mobile phones are irritated by the nuisance and the airtime wastage incurred. Recipients of "fax tones" at household phones are also disturbed.

Problems for businesses

20. Unsolicited electronic messages cost businesses money in the form of lost worker productivity, the need to upgrade network capacity (in the case of email spam) and other wastage of resources. When hit with certain kinds of spam attacks, businesses have to invest resources in a security investigation.

21. Senders of unsolicited electronic messages occasionally put the name of legitimate company in the "From" header or elsewhere in the message, to give the impression that the message is from the well-known company or is sent with their approval. The reputation of these legitimate businesses suffers.

22. Unsolicited electronic messages often affect how legitimate businesses can market their products. In the case of email, for instance, many consumers subscribe to email lists from well-known companies in order to receive special discount offers and notices of sales or new products. However, these emails are sometimes confused with spam messages, either by filtering products or by the recipients.

Network issues

23. Regardless of the content, spam causes harm to ISPs because it uses large amount of bandwidth and storage space. It also upsets their customers and adds costs to technical support. To combat bulk emails, ISPs need to build enormous capacity into their systems. The increased volume of emails can also significantly slow down the speed of Internet, overload servers and threaten network integrity.

24. Rather than collecting real addresses, some spammers try multiple combinations of common names, or even all combinations of letters, at a popular domain name. This puts a huge drain on the ISP's servers as tens of thousands of emails are sent and bounce messages returned for addresses that have never existed.

25. Spammers sometimes use open relays to disguise the origin of their messages, to deflect complaints, to circumvent "spamblocking" by other sites, and to increase the volume of messages they can send. Third-party relaying usually represents theft of service because it is an unauthorised appropriation of computing resources. Third-party relaying consumes bandwidth and storage capacity and can result in performance degradation and even system crashes. The highest costs usually are the staff time needed to deal with bounced messages, complaints and system reconfiguration.

Other methods used by spammers

26. Forgery of message headers is another tactic commonly used by spammers. Spam tends to generate a lot of complaints from irate recipients. Therefore spammers usually try to deflect those complaints by, for example, using a false return email address in the message header, often combined with a false "remove" address in the body of the message.

SIZE OF THE PROBLEM

27. As discussed above, there are different forms of spam depending on the different mode of technology deployed in sending the spam. While at present, the problem of junk fax and spam in relation to email is more serious a

problem than that in relation to SMS and MMS, the latter is of a growing concern as the development in new technology leads to a reduction in costs of sending SMS and MMS.

Email

28. In December 2003, the Hong Kong Internet Service Providers Association (HKISPA) conducted a survey on the issue of spam, gathering data from eleven ISPs, which offer services to over 90% of Internet users in Hong Kong. On the assumption that spam covers both unsolicited commercial and bulk emails, the survey revealed that 50% of all emails handled by ISPs in Hong Kong is spam, with a significant 5% of it originating from Hong Kong, and a further 20-40% from other Asian sources. It also estimated that the total loss to the economy is in the order of HK$ 10 billion per year to the society (nearly 70% of which was the cost of lost productivity of employees in identifying and deleting spam).

29. One may compare the spamming problem in Hong Kong with other places. According to Brightmail, an anti-spam software company, spam volumes in May 2004 accounted for 64% of all email traffic on the Internet, up from just 8% of traffic in mid-2001. Another anti-spam solution company, MessageLabs, found that 76% of the emails it scanned in May 2004 was spam. It is likely that this proportion is increasing if spam volumes are indeed rapidly growing as is widely believed.

SMS and MMS

30. Although junk SMS and MMS have not reached the same volume as inbox-clogging junk emails, the increase in SMS traffic during the past couple of years has no doubt led to an increase in unsolicited SMS and MMS. At present, it is possible to send SMS from both an Internet email account or from a fixed line network. The recent technological and market development have significantly reduced the costs of sending spam SMS/MMS, which may lead to a further increase in spam volume. Although SMS/MMS spamming is currently less problematic than email spam, it could become a greater problem as it is currently in Japan, should the costs of sending SMS/MMS be reduced or pricing policies changed.

Fax

31. There are two main groups of fax senders. Some are small shop-owners who make use of a single faxline to advertise their own products or services. The nature of their business will necessitate them to publish their telephone numbers and other contact details in order that interested customers may easily contact them. The rest of the fax senders provide direct marketing services for their customers on a much larger scale. Many of them would deploy a large number of faxlines and send fax advertisements 24 hours a day non-stop. Depending on the requirement of their clients, the fax senders may send the advertisements indiscriminately, or they may send them to a focused group of faxlines.

32. The charge structure of a particular telecommunications service will determine whether the direct marketing community would make use of that service to deliver their business. In Hong Kong, the business faxline is provided on a flat-rate basis at less than $130 a month. The marginal cost for using a faxline for direct marketing purpose is negligible and Hong Kong therefore sees a thriving direct marketing business using faxline as the delivery means.

33. According to the returns from the local FTNS operators, there were 24 232 complaints in 2003. These complaints contained sufficient information for the FTNS operators to take follow-up actions. Of these complaint cases, 15 491 were filed by customers who have already registered their telephone numbers in the "not-to-call" list. Obviously many fax senders still send commercial messages to those who have chosen not to receive such messages.

34. **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**.

EXISTING MEASURES AND THEIR EFFECTIVENESS

Legislation

35. Under the existing legal framework, there are certain provisions which deal with offences in connection with voice calls. There are also provisions which may arguably cover certain aspects of spam but, as we set out below, none of the provisions tackle spams on its own.

36. In relation to the content of the message, for instance, the Control of Obscene and Indecent Articles Ordinance (Cap. 390) prohibits the publication and public display of obscene and indecent articles (including printed matters, sound-recordings, films, video-tapes, discs and electronic publications). Likewise, the Prevention of Child Pornography Ordinance (Cap. 579) deals with the publication of child pornography.

37. However, there is currently no legislation which deals specifically with the act of sending out unsolicited electronic messages *per se*.

Summary Offences Ordinance (Cap. 228)

38. Section 20 of the Summary Offences Ordinance ("SOO") deals with offences in connection with telephone calls or messages or telegrams[1]. The provision was last amended in 1991 when Internet usage was largely confined to the academic community and the exponential growth of mobile phones had yet to take place. The statutory provision, as it now stands, targets mainly at nuisance telephone calls without reasonable cause, and is not intended to deal with the problem of junk fax or spam which uses other means of electronic communications.

---

[1] Any person who-
(a) sends any message by telegraph, telephone, wireless telegraphy or wireless telephony which is grossly offensive or of an indecent, obscene or menacing character; or
(b) sends by any such means any message, which he knows to be false, for the purpose of causing annoyance, inconvenience or needless anxiety to any other person; or
(c) persistently makes telephone calls without reasonable cause and for any such purpose as aforesaid,
shall be liable to a fine of $1,000 and to imprisonment for 2 months.
(Added 36 of 1935 S.2. Amended 90 of 1991 S.28.)

Personal Data (Privacy) Ordinance (Cap. 486)

39. Section 34 of the Personal Data (Privacy) Ordinance ("PDPO") deals with the use of personal data in direct marketing. Section 34(2) of PDPO defines "direct marketing" as

(a) The offering of goods, facilities or services;
(b) The advertising of the availability of goods, facilities or services; or
(c) The solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes,

by means of-

(i) information or goods sent to any person by mail, facsimile transmission, electronic mail, or other similar means of communication, where the information or goods are addressed to a **specific person or specific persons by name** (emphasis added); or

(ii) telephone calls made to specific persons.

40. Section 34(1) of PDPO stipulates that the direct marketer, in using personal data for direct marketing purposes, shall:

(1) The first time he so uses those data inform the data subject that the data user is required, without charge to the data subject, to cease to so use those data if the data subject so requests.

(2) If the data subject so requests, cease to so use those data without charge to the data subject.

A direct marketing company as the data user should provide an opportunity for an individual to "opt-out" from receiving marketing contacts the first time when the direct marketing company uses that individual's personal data for direct marketing. The Privacy Commissioner also issued the Guidelines on Cold-Calling[2].

[2] http://www.pco.org.hk/english/publications/fact3_coldcall.html

41. The purpose of PDPO is to protect the privacy interests of living individuals in relation to personal data. Accordingly, it covers any data relating directly or indirectly to a living individual (data subject) from which it is practicable to ascertain the identity of the individual. PDPO is not designed to deal with normal direct marketing messages delivered by fax or email which seldom address the recipients by names. An email address by itself, in the absence of any other identifying particulars of an individual, may not amount to personal data under PDPO.

Telecommunications Ordinance (Cap. 106)

42. If the sending of spam involves unauthorized access to computer by telecommunications (commonly known as hacking), it is punishable under section 27A of the Telecommunications Ordinance. However, the focus of this provision is on the unauthorised nature of the access to computer, rather than the act of sending email spam per se.

Crimes Ordinance (Cap. 200)

43. Section 60 of the Crimes Ordinance provides that "*a person who without* lawful *excuse destroys or damages any property belonging to another intending to destroy or damage any such property or being reckless as to whether any such property would be destroyed or damaged shall be guilty of an offence*". Section 59 of the Crimes Ordinance specifies that "*to destroy or damage any property*" in relation to a computer includes the "*misuse of a computer*", and "*misuse of computer*" means

> "(a) to cause a computer to function other than as it has been established to function by or on behalf of its owner; notwithstanding that the misuse may not impair the operation of the computer or a program held in the computer or the reliability of data held in the computer;
>
> (b) to alter or erase any program or data held in a computer or in a computer storage medium;

(c) to add any program or data to the contents of a computer or of a computer storage medium,

and any act which contributes towards causing the misuse of a kind referred to in paragraph (a), (b) or (c) shall be regarded as causing it."

44. If, for example, a person sends spams to a computer causing it to cease functioning, that person may be liable to an offence under Sections 59 and 60 of the Crimes Ordinance. However, it should be noted that these provisions aim to punish acts which have the result of destroying or damaging property by misusing a computer, and are not intended to criminalise the act of sending unsolicited electronic messages through a computer.

45. Section 161(1) of the Crimes Ordinance (Cap. 200) provides that any person who obtains access to a computer

(a) with an intent to commit an offence;
(b) with a dishonest intent to deceive;
(c) with a view to dishonest gain for himself or another; or
(d) with a dishonest intent to cause loss to another

commits an offence. A person accessing a computer with the intent to commit an offence will be punishable for his act of accessing the computer instead of the offence to be committed itself. Again this provision focuses on the criminal or dishonest intention when accessing the computer, as opposed to the act of sending unsolicited messages by the computer *per se*.

46. It can be seen that none of the existing legislative provisions outlined above tackle spam directly.

Voluntary Codes of Practice

Email

47. In February 2000, the HKISPA issued the Anti-Spam Code of Practice, which covers bulk unsolicited email messages or articles sent via email without the recipients' prior request or consent. The Code sets out the

sanctions, such as suspension of services, that should be imposed on subscribers that are found to engage in spamming. However the Code is voluntary and spammers are not members of the Association.

48. The Code also recommends the preventive measures that should be taken by ISPs to reduce the possibility of spamming. These measures include:

(1) prohibition of relay mail;
(2) restriction on the amount of outgoing mail provided for web email and pre-paid accounts;
(3) restriction of the use of port 25;
(4) ISP should publish its procedures for handling incidents of spam, either in print or on a web site. The procedures should include the setting up of an "abuse" account to receive and follow-up customer complaints about spamming.

49. The HKISPA conducted a survey on the effectiveness of the Code of Practice in June 2001. The HKISPA found that while the Code had helped reduce spam, it was not effective in the face of the growth of Internet, the availability of automated spam generating software and the rapid growth of Internet penetration in the mainland.

50. The HKISPA found that the Real-Time Blackhole List (RBL) operated by http://mail-abuse.org, has been employed by member ISPs and has helped reduce spam. However, the RBL is operated in the United States and it cannot help ISPs in Hong Kong to identify spam from Mainland China or Chinese Taipei. The HKISPA therefore recommended the drawing up of a local name list of email servers (M-List) that are reasonably suspected to have transmitted spam. ISPs may then configure their mail servers to look out for, and give special treatments to, emails delivered from the servers within the M-List. Special treatments may include virus scanning, labelling for indication to the email recipients, or return the mail to the sender. The HKISPA further recommended that the M-List should be operated and maintained by a neutral entity, such as the Hong Kong Computer Emergency Response Team (HKCERT).

51. The OFTA has received complaints that spammers identified themselves as the webmaster of the ISPs when they sent unsolicited

advertisements to the customers of these ISPs. Misled by the header which gave the impression that the email was sent by the webmaster of their service provider, customers would be induced to read the emails only to find that they are unsolicited advertisements. Often the aggrieved customers would file complaint emails against the ISPs blaming the service providers for originating the junk email. The ISPs are of the opinion that not only would this disrupt the network operations, their reputation would also be severely damaged.

52. Based on its review, the HKISPA takes the view that existing voluntary framework is not sufficiently comprehensive nor adequate in dealing with all the problems associated with unsolicited emails, and recommends that legislative means with punitive provisions be introduced.

SMS and MMS

53. In December 2001, the six mobile operators in Hong Kong agreed on a set of Code of Practice on "Handling of Unsolicited Promotional IOSMS under the Code of Practice for Inter-Operator Short Message Service (IOSMS)" which sets out the guidelines for facilitating the sending of promotional SMS vis-à-vis operators. However, this code is voluntary, does not cover intra-operator unsolicited messages and does not prevent an operator from sending unsolicited messages to its own customers.

Fax

54. Under the existing administrative framework, faxline users who do not wish to receive unsolicited fax advertisements may put their fax numbers on a "not-to-call" list to be observed by all senders of fax advertisements. Recipients of unsolicited fax advertisements may file a complaint with their FTNS operators. Legitimate cases of complaints will lead to sanctions against the sender, including the suspension or termination of their faxlines.

55. Senders of fax advertisements have to observe a set of voluntary guidelines issued by the OFTA defining acceptable arrangements for sending advertisements through fax. These arrangements include:

(1) unsolicited advertisements should not be sent to numbers on the "not-to-call" list; and

(2) the advertisement should contain the necessary identifying information and contact details of the sender so that the parties receiving the fax messages may readily contact the sender to exercise their right not to receive any more such fax advertisements.

56. The local wire-line FTNS network operators have agreed to a Code of Practice setting out the standard procedures for handling complaints against unsolicited fax advertisements. On 2 January 2004, the OFTA revised this set of voluntary Code of Practice. Paragraph 6 of the Code makes it clear that while the Code is voluntary in nature, the FTNS operators have the responsibility to protect the interest of users of telecommunications services and to inform them of the proper and acceptable way to use fax transmission for advertising purposes. The Telecommunications Authority (TA) considers this as good customer service which is expected of the FTNS operators. The new Code also puts a heavier penalty by allowing the FTNS operators to disconnect all the lines instead of the line in question of the registered subscriber at a given address if three (3) substantiated complaints are received.

Technical Tools

57. Currently, some technical tools are available in the market to reduce the number of unsolicited electronic messages. In the case of emails, for instance, software tools can partially stop the spam problem at several levels. There are many tools available for end users to control spam, often provided free of charge. Other blocking techniques can be used by ISPs. Below are some examples of the commonly used technical tools.

58. It should however be noted that filtering messages costs ISPs time and money and slows network performance without reducing the number of spam messages being sent at the origin. Another problem is that filtering products are not always easy to design, configure or install in a way which would block most spam but without blocking wanted messages.

Users' arrangements

59. Technical tools and consumer awareness options may help alleviate spam, in the short and medium term.

60. Fax users (in the case of junk fax), Internet users (in the case of email spam) and mobile phone users (in the case of SMS/MMS spam) can ignore spam and delete it. Users are encouraged to follow the users' tips published by their respective network operators. Internet users are also advised to avoid going to places where spammers generate mailing lists, such as newsgroups, chat rooms and public directories.

61. Internet users who regularly post their address online are advised to set up another email account for these postings and save the personal email account for family and friends. Alternatively, they could alter the email address by adding words or additional characters and add a note to explain to their friends about how the proper address could be extracted. This would ensure that the email address being harvested by automatic email scanners would not work.

Blocking devices

62. These tools attempt to block spam based on the content of the e-mail messages and headers. They can learn to recognise spam based on the users' classification of e-mails that are received.

63. A whitelist is a list of email addresses that are certified as legitimate senders. In a challenge-response system, the server holds all email from unrecognised addresses while it sends an automated message to the sender of the email. The automated message will verify that the sender is a real person, not an automated bulk email programme, by asking him or her to reply to the message or enter some information at a web site.

64. These tools would allow businesses and individuals to either allow only emails from approved sources or to be used in conjunction with filtering. While this method may be reasonable for some home users, it may be inefficient for businesses, government offices, and individuals who often receive emails from people they have never previously contacted.

65. Several organisations provide spam blacklists, which collect the IP address information of known spammers. These lists can then be included in filters to block all incoming emails from the blacklisted addresses. This method may however have the downside of blocking non-spam since IP addresses are not always specific to a particular computer or account. In this case blocking email from a particular IP address may block emails from everyone belonging to a certain ISP.

66. In the case of fax, junk fax senders sometimes hide their line numbers by activating the caller number display (CND) blocking function (i.e. the sender's telephone number will not be displayed at the receiving end's CND unit) when they send junk fax. Other than doing something at the sending side, some preventive measures could be implemented at the receiving side. Some FTNS operators offer a screening service called "block-the-blocker" for customers who do not wish to receive junk faxes from those lines the number of which has been "blocked". However, this measure will not be able to block junk fax sent out through Private Automatic Branch Exchange systems where the CND is usually denoted as "O" or "Out-of-area".

Efforts by ISPs

67. At the Internet servers and networks, ISPs have been implementing technical measures such as blocking all packets throughout their networks with destination of TCP port 25 (SMTP) and also switch off the relaying function of the email server. This will ensure that spammers cannot use the dial-up service to access open email servers on their ISPs. It also prevents customers from accidentally running an open email server, which could be used, without customer's knowledge, as a source of spam from somewhere else. ISPs are also advising customers tips and appropriate measures to be adopted to combat spam such as by providing them with suitable filtering software at their computers.

POSSIBLE SOLUTIONS

Industry co-operation

68. At present, there are voluntary codes of practice on the conduct of sending unsolicited messages in the area of fax, email and SMS. While these codes are voluntary in nature, strict adherence to these codes by the industry players – FTNS operators, ISPs and mobile operators is important to help combat the problems created by spam.

69. Industry bodies, such as the HKISPA and their members may be encouraged to:

- 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 their subscribers for dealing with spam.

70. Industry players may also get together for the compilation of a common blacklist of spammers. This could be a significant improvement on unregulated blacklists that currently operate, which have been a blunt tool that in effect often victimised innocent Internet users, many of whom had already been spoofed by the offending spammer.

71. **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.**

Users' education

72. In the "*Anti-Spam Recommendations: Appropriate Legislation*" paper **(**http://www.hkcs.org.hk/en_hk/doc_general/as-recommend-final.pdf**)** submitted by the Information Security Specialist Group of Hong Kong Computer Society, it acknowledges that a single approach alone cannot combat

spam effectively. Rather, legislation, education and technical controls should be used in combination for maximum effectiveness. In Australia, the Australian Internet Industry Association has made education an important part of their anti-spam campaign with the slogan "Don't try – Don't buy – Don't reply".

73. In the Background Paper for the Organisation for Economic Co-operation and Development (OECD) Workshop on Spam, the OECD acknowledges that legislation is limited in its ability to protect a user from a foreign spammer, but steps taken by an informed user will help regardless of where the spammer is located. In the Spam Review Report prepared by the National Office for the Information Economy (NOIE) of Australia, it is recommended that consumer education is a key factor in any strategy to counter spam. In particular, consumers need to be educated and empowered so that they:

- can make informed choices in relation to spam reduction strategies and technologies;

- better understand the pitfalls of purchasing products promoted by spam both in terms of the risks they face given the dubious nature of many of these products and how the purchase would boost the commercial viability of spam;

- better understand how to protect their private information, such as email addresses, in the online environment thereby making spamming more difficult; and

- better understand their rights in relation to all aspects of spam and possible remedies where available.

74. The relevant industry bodies such as the HKISPA, the Hong Kong Anti-Spam Coalition, the Hong Kong Computer Society and the Asia Digital Marketing Association may work together to develop and implement an information campaign on spam that creates awareness and provides accurate information and useful resources to consumers.

75. **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.**

Technical solutions

76. In the case of email spam, there are anti-spam solutions available in the market to protect and help businesses, ISPs and individual users by filtering out unsolicited emails such as filters using "blacklists", "whitelists" ("approved sender lists") and digital signature schemes. Most anti-spam solutions include a combination of several technical components. Efforts to find technical solutions to spam prevention/reduction have been made at the individual company level and by many companies in a collective and co-operative way. For example, in April 2003, Microsoft, AOL, Earthlink and Yahoo announced that they were working together to block unidentified messages and to stop spammers from creating fraudulent email accounts. Recently, Microsoft predicted that its Anti-Spam Technology and Strategy Group which brings together specialists from across the company and integrates all of its anti-spam strategy and R&D efforts will be able to come up with technical solutions to solve the spamming problem within two years. In addition, some ISPs also gathered together to find technical solutions for spam.

77. For fax, customers may subscribe to the block-the-blocker services offered by some FTNS operators in order not to receive any anonymous calls including junk fax calls without the CND.

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

Legislation

79. Some jurisdictions, such as US, UK and Australia, have introduced anti-spam legislation while others have not. The **Annex** provides details of the anti-spam approach in some major overseas jurisdictions. They are extracted from the *Background Paper for the OECD Workshop on Spam* (Ref.: DSTI/ICCP(2003)10/FINAL).

80. There have been calls from various industry groups for an omnibus legislation to deal with all forms of unsolicited messages delivered by electronic means. In the White Paper on "*Legislation: One of the key pillars in the fight against spam*" (http://www.hkispa.org.hk/spam/20040113-coalition-paper.pdf) developed by the Hong Kong Anti-Spam Coalition, the Hong Kong Anti-Spam Coalition acknowledges that a legislation specifically targeted on spam would be a critical component of a comprehensive and effective solution to the spamming problem, and urges the Government to initiate public consultation on the drafting of specific legislation to combat spam. The Information Security Specialist Group of the Hong Kong Computer Society also recommends that new legislation dealing specifically with spam should be enacted.

81. However, others argue that a legislative approach will introduce additional compliance costs and burden for various parties. Many genuine businesses undertake marketing activities via email, telemarketing or fax. Majority of these businesses are currently behaving responsibly. Some argue that the enactment of a new legislation will place additional compliance burden and add cost on these businesses. Further, it should be noted that the sending of unsolicited messages, in particular emails and faxes, is an efficient and low costs marketing tool widely adopted by small and medium enterprises (SME). Some are of the opinion that the imposition of additional regulations on unsolicited electronic messages may impede such use by SMEs. Some consider that the enactment of a new legislation on unsolicited electronic messages will also have an impact on direct marketing businesses. The direct marketing businesses will need to review and possibly configure their direct marketing strategies to conform with the relevant legislation. They may choose to either cleanse or recreate their lists to only include those who meet the criteria or revisit their business mode, which will lead to additional compliance costs. Other people may be concerned that the new powers which an anti-spam legislation would give to the enforcement agency will erode the privacy of individuals in respect of their personal communications such as e-mails, fax, SMS and MMS.

82. The effectiveness of a new anti-spam legislation depends heavily on how vigorously it is enforced and the nature of the penalties to be imposed (i.e. civil and/or criminal). Enforcement of anti-spam legislation is likely to be fraught with difficulties:

(1) Spammers are difficult to trace. A number of methods are used by spammers to hide their identities. Source addresses are often arranged at random so that they are not easily identified. Spamware programmes automatically generate false headers and return address information. False headers allow spammers to ignore recipient requests to be removed from email lists and to obscure their identities by making themselves untraceable. Other spammers scan the Internet for open relays in foreign countries so that their messages cannot be easily traced. Some spammers register free email accounts and abandon them before they are caught. Spammers also use programmes that load in multiple accounts so that when one account is terminated, another automatically kicks in. "Spoofing" addresses are also used by spammers – this involves using false information as to the name of the sender. This can be either false information or in some cases using names of other commercial entities that are not involved with the spam operation.

(2) The extra-territorial nature of spam also makes enforcement of anti-spam legislation difficult. Spam travels across state and national boundaries. According to the survey conducted by the HKISPA on the issue of spam in December 2003, only 5% of spam originates from Hong Kong, which means that the remaining 95% of spam originates from overseas. It would not be easy to extend jurisdiction conferred by legislation to overseas countries. Even if this is done, enforcement agencies would likely encounter problems in enforcing the legislation overseas, such as in collecting evidence across the borders.

(3) Resources for enforcement and enforcement priority can also be matters of concern. By nature, enforcement of anti-spam legislation is resource-intensive. In many overseas jurisdictions spam prosecutions have not been a priority for prosecutors due to possibly lack of resources or existence of other more urgent tasks. From the largely private spam

litigation so far in the United States, one may infer that enforcement will continue to be a serious problem under even a new federal law. Even the most well-funded and vigorous plaintiffs have encountered increasing spam loads in spite of having brought multiple successful lawsuits. Quite often the problem of spam persists, not primarily because of a lack of laws, but because of a relative lack of resources for enforcement.

(4) The nature of penalty imposed by an anti-spam legislation would also have impact on its effectiveness. The CAN-SPAM Act of the United States creates civil and criminal penalties. It allows the Federal Trade Commission (FTC), state attorneys general and Internet service providers to sue companies which violate the law: a prosecution by the FTC can result in 3 years imprisonment for first time offenders and confiscation of proceeds from mailing as well as any computers, software, technology or equipment used during the offence. On the other hand, State Attorneys General can enforce the CAN-SPAM Act with a civil action and a fine of US$250/message for up to US$2 million is possible. ISPs can also enforce the CAN-SPAM Act with a civil action and claim damages of actual monetary loss. In Australia, the choice made under the Spam Act to go for civil rather than criminal penalties was a very deliberate one, the reasons being:

(a) the standard of proof in civil action is lower (i.e. balance of probabilities rather than beyond reasonable doubt);

(b) evidence handling restrictions are likely to be less stringent (both in-country and in transferring complaints between jurisdictions);

(c) the fines imposed through civil enforcement are generally heavier;

(d) from a legal policy point of view, civil penalty is more proportionate to the seriousness of the offence;

(e) civil penalty regime provides better flexibility and scalability (a range of penalties will be available including warnings, infringement notices and full court actions);

(f) it is cheaper to administer.

83. The anti-spam legislation which exists overseas has only been introduced in other jurisdictions recently and its effectiveness is yet to be seen and tested. Some therefore advocate that instead of resorting to legislation now, Hong Kong can consider strengthening existing measures to tackle spam first. After overseas countries have accumulated more experience with enforcing their anti-spam legislation, Hong Kong can assess if it wishes to consider enacting similar legislation in the light of the experience overseas. **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.**

84. In the event that a legislative approach is preferred, the Government will need to consult the public on the definitional issues discussed in paragraphs 5 to 14 above. The Government realises that unsolicited electronic messages is an efficient and low cost marketing tools adopted by businesses, in particular SMEs, and the introduction of additional regulations on unsolicited electronic messages will invariably lead to compliance costs on those who would like to send unsolicited electronic messages for marketing purpose. In considering whether new legislation should be introduced and the content of such legislation, the Government will need to balance the impact on senders of unsolicited electronic messages on the one hand, and the costs/nuisances to the recipients of unsolicited electronic messages and other concerned parties such as ISPs on the other.

85. The following issues need to be carefully considered should the legislative route be preferred:

(1) What should be the scope of the legislation? Should it be technologically neutral in covering all forms of unsolicited messages delivered by electronic means, or should it cover e-

mails and faxes only which account for the majority of complaints?

(2) Should the legislation cover only electronic messages of a "commercial" nature, or should it be wide enough to cover electronic messages of a "non-commercial nature"?

Typically spam has a commercial purpose: the promotion or sale of a product or service. However, some non-commercial messages may also be considered by some recipients as spam, for example unsolicited bulk messages with a political theme or religious purpose or that contains a virus. Covering non-commercial messages in the proposed legislation may lead to conflicts with principles such as freedom of speech and religion. It would also increase the challenge for enforcement and the corresponding expense.

(3) Whether the concept of "bulk" should be included in the legislative approach and if so, in what ways should it be included?

If the concept of "bulk" is to be embedded in any proposed legislation, the main issue would be how to define the volume of a message that must be sent within what time period for them to qualify as a bulk transmission. Another approach is not to employ the concept of "bulk", but to prescribe different penalties in accordance with the volume of messages that have been sent out.

(4) Whether cold calls, voice or video, should be excluded from the definition of electronic messages?

The resources that a marketer will need to put in by making cold-calls is significantly higher than other forms of electronic messages and hence cold-calling is generally less a problem. It is debatable whether it is necessary to include voice and video calls in any proposed legislation.

(5) In prohibiting unsolicited commercial electronic messages whether or not the permission-based approach is preferred and if so, the preferred form of permission, e.g. express or implied from pre-existing business relationship?

One approach is to stipulate in any proposed legislation that no person shall send unsolicited messages for commercial purposes unless prior consent (express or implied) has been obtained. Another approach is that no prior consent is needed, as in the case of ordinary paper mail.

(6) Whether an “opt-in”/“opt-out” approach should be adopted?

An “opt-in” scheme is where senders of unsolicited messages are required to secure express or implied prior consent from the intended recipients before sending out any message. An "opt-out scheme" is where senders of unsolicited electronic messages must provide the recipients with the means to inform the senders that they do not wish to receive unsolicited messages again. Among the economies which have legislated against unsolicited commercial electronic messages, EU countries and Australia have adopted the “opt-in” scheme. The US, Japan and South Korea, on the other hand, adopt the opt-out scheme.

(7) Whether the legislative approach should stipulate certain mandatory requirements on the labelling of email headers, and if so, what should the requirements be?

To tackle the problem of spammers putting in incorrect information in their message headers, any proposed legislation may require that commercial electronic messages be properly identified and labelled. The exact requirements to be put in would need to be carefully thought through.

(8) Whether restrictions on email address harvesting, automatic generation or list sharing should be included in the proposed legislative approach, and if so, the appropriate restrictions?

Many spammers use webcrawlers that search the Internet, collecting all the email addresses they find. Other spammers develop mailing lists from websites such as newsgroups, chat rooms and public directories. Some generate e-mail addresses by automatic means. Some people have therefore proposed prohibiting the harvesting of email addresses from websites and the generation of e-mail addresses by automatic means. Others suggest that any proposed legislation should also prohibit trade in email lists between ISPs.

(9) What is the scope of investigation and enforcement powers to be conferred on the relevant enforcement agency? What are the rights and obligations of the network/service providers to disclose information to the enforcement agency and to terminate or delete spam?

For any proposed legislation to be effective, the relevant enforcement agency should be vested with the necessary investigation and enforcement powers. For example, the enforcement agency should be vested with the necessary power to trace the origin of spam. In addition, under the current voluntary framework, the FTNS operators and the ISPs may be reluctant to disclose the identities of the spammers for fear of possible invasion of confidentiality and personal privacy. This raises the issue of whether network and service providers should be under a requirement to disclose the source of a call and/or other form of electronic communication which is suspected of sending spam. The FTNS operators and the ISPs sometimes have to terminate or delete spam. This also raises the issue of whether spam can be terminated or deleted by the FTNS operators or the ISPs while ensuring the free flow of communication.

(10) What will be the nature and extent of increase in compliance costs which will be brought about by the introduction of additional regulations on spamming?

The introduction of additional regulations on spamming will invariably lead to compliance costs on those who would like to send unsolicited electronic messages for marketing purpose. The extent of the costs will depend on, among other things, the type of regulation (e.g. opt-in or opt-out). There is therefore a question of what kind of compliance cost and its extent which may be brought by any proposed legislation when one designs the legislative elements.

INTERNATIONAL COOPERATION

86. Spam is a global problem. Establishing a domestic strategy for dealing with it can alleviate the problem only in terms of spam originated from Hong Kong. As revealed in the survey conducted by the HKISPA in December 2003, 5% of the spam in Hong Kong originates in Hong Kong, a further 20-40% from other Asian sources and the rest from other places. The spam originated in Hong Kong may also cause problem to users elsewhere. This being the case, having an anti-spam legislation in Hong Kong will only help to alleviate part of the problem of spam. We have to rely on international cooperative measures to deal with the majority of spam that originates outside Hong Kong.

87. At the multilateral level, Hong Kong could work with Organisation for Economic Co-operation and Development (OECD), Asia-Pacific Economic Cooperation (APEC) or other relevant bodies to develop international co-operative mechanisms for dealing with spam.

Organisation for Economic Co-operation and Development (OECD)

88. The OECD issued the Guidelines for Consumer Protection in the Context of Electronic Commerce in 2000. The following principles are relevant to the spamming issue:

(1) Businesses should not exploit the special characteristics of electronic commerce to hide their true identity or location, or to avoid compliance with consumer protection standards and/or enforcement mechanisms.

(2) Advertising and marketing should be clearly identifiable as such.

(3) Businesses should develop and implement effective and easy-to-use procedures that allow consumers to choose whether or not they wish to receive unsolicited commercial email messages.

(4) Where consumers have indicated they do not want to receive unsolicited commercial email messages, such choice should be respected.

89. In June 2003, the OECD adopted new guidelines to foster international co-operation against cross-border fraud and deception – *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*. Spam messages that contain deceptive or fraudulent representations may fall within the scope of the guidelines, offering the prospect of putting into play the framework for enforcement co-operation outlined by the guidelines.

90. On 2-3 February 2004, the OECD organised a workshop on spam and one of the objectives is to consider the next steps with a view to increasing international cooperation to address the issue. The background paper for the OECD Workshop on Spam can be found at: http://www.olis.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/edfc2255d6a8a51ac1256e240030f5b6/$FILE/JT00157096.PDF

Asia-Pacific Economic Cooperation (APEC)

91. In the APEC Ministerial Meeting in 2003, Ministers endorsed conducting future work on "spam" in close collaboration with the OECD. The APEC E-commerce Steering Committee (ECSG) has endorsed a work programme on spam and identified several key issues for further exploration including, inter alia:

(1) identifying and reporting on the harm caused by various types of spam and spamming practices;

(2) identifying and encouraging means available for cross-border cooperation to combat fraudulent and deceptive spams;

(3) identifying and reporting on areas where domestic policies or laws, in combination with other solutions, might assist in preventing and responding to the harms caused by spam; and

(4) evaluating the effectiveness of measures to combat spam through use of quantifiable metrics.

92. The HKSAR is a member of the APEC and will continue to actively participate in the above endeavours.

World Summit on the Information Society (WSIS)

93. In the *Declaration of Principles* published at the WSIS on 12 December 2003, ITU member states expressly recognised that it is a key principle for building an inclusive Information Society to build confidence and security in the use of information and communication technologies. In paragraph 37 of the Declaration, member states expressly acknowledged that "*spam is a significant and growing problem for users, networks and the internet as a whole. Spam and cyber-security should be dealt with at appropriate national and international levels."* Member States further agreed in the *Plan of Action* adopted at the WSIS that appropriate action should be taken on spam at national and international levels.

INVITATION FOR COMMENTS

94. Comments are invited on paragraphs 34, 71, 75, 78 and 83. Any views and comments on this consultation paper should reach OFTA on or before 25 October 2004. Any person who submits his/her views and comments should be aware that the Government may publish all or any part of the views and comments received and disclose the identity of the source in such manner as the Government deems fit. Any part of the submission which is considered commercially confidential should be marked. The Government would take such markings into account in deciding whether or not to disclose such information. Depending on the responses the Government will

determine the next steps including possibly a second consultation on the relevant issues. Submission should be addressed to:

Office of the Telecommunications Authority
29/F Wu Chung House
213 Queen's Road East
Wanchai
Hong Kong
Attn: Public Affairs Manager (Consumer & Corporate Affairs)

An electronic copy of the submission should be sent by email to: uem-consultation@ofta.gov.hk. Comments can also be sent by fax to 2803 5112

Office of the Telecommunications Authority
25 June 2004

Annex. Anti-spam Approach in Some Overseas Jurisdictions

Australia

The SPAM Bill 2003 was passed by the Australian Parliament on 2 December 2003. The bill adopted an opt-in regime for commercial electronic messaging. Electronic messages include e-mails, instant messaging, text or video messaging to mobile phones and messages defined in the regulation. It also requires accuracy with regard to address of sender and a functioning unsubscribe facility; it prohibits the distribution and use of electronic address harvesting tools and harvested address lists; and encourages the development of appropriate industry codes. A flexible and dynamic civil sanctions regime such as warnings, infringement notices and court-awarded penalties is addressed in the bill as well. The spammers who contravene the legislation will be liable for up to a total of AUD 44,000 for contravention on a single day, while an organisation could be fined up to AUD 220,000 a day. Directory harvesting and dictionary attacks, when conducted for the purposes of engaging in spam or associated activities, are also banned under this legislation. The Australian Communications Authority (ACA) will have the power to investigate, issue infringement notices and institute proceedings. Where a person or company has suffered loss or damages due to a spammer's activity, the ACA may apply to the court on their behalf for compensation.

Canada

Before the Personal Information Protection and Electronic Documents Act was legislated, the Canadian government took the position that the distribution of unsolicited promotional and product information, in print form or electronically, was not illegal, nor was it regulated in Canada.[1] However, under the Act which came into force in January 2001, electronic mail addresses are considered personal information and thus subject to the provisions of the Act. The collection and use of personal information (such as e-mail addresses) without the consent of the data subject could run counter to the requirements of the Act. The Privacy Commissioner of Canada is entrusted with enforcing the Act.

The law also creates an obligation for firms and others who store electronic mail addresses to provide appropriate security for this personal information. In the first three years following the Act's adoption, the legislation applies to federally-regulated undertakings and to private sector firms who engage in inter-provincial and international trade in personal information. After this time, all organisations using personal information for the conduct of commercial activity will be covered. Thus, firms buying, selling, leasing or bartering electronic mailing lists, which are the basis for bulk unsolicited electronic mail, will be subject to the

---

[1] See Industry Canada (1999), "Internet and Bulk Unsolicited Electronic Mail (SPAM) Policy", July, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwGeneratedInterE/gv00188e.html, accessed 9 January 2004.

provisions of the legislation, if these transactions take place over provincial and national borders.[2] However, there is no specific regulation on spam to date.

Although there is no specific legislation dealing with spam in Canada, spam which conveys misleading representations or deceptive marketing practices could breach sections of the Competition Act and other statutes enforced by the Competition Bureau in Canada.

European Union

The new Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector was issued on 12 July 2002. The EU has adopted an "opt-in" approach for commercial communications by email (including SMS). Previously, the opt-in was applicable to faxes and automated calling machines.

Under the new directive, scope of "electronic mail" is broad and technology neutral. It includes any form of electronic communication for which the simultaneous participation of the sender and the recipient is not required. It covers not only traditional "email" but also SMS, MMS etc. The new directive contains three basic principles with regard to unsolicited commercial communications. First, according to Article 13(1), member states are required to prohibit the sending of unsolicited commercial communications by fax or email or other electronic messaging systems such as SMS and MMS unless prior consent of the person has been obtained (opt-in). This regime is applicable for commercial communications sent to individuals (natural persons) but member states can extend the scope to communications sent to businesses. There is a limited exception from the opt-in system for existing customers [Article 13(2)], for the use of contact detail obtained from customers in the context of a sale. But it may only be used by the same legal person for the marketing of "similar" products or services if an explicit opt-out is offered at the time of collection and with each subsequent message. Secondly, the disguise of identity of the sender is prohibited. Thirdly, direct marketing messages must include a valid return address where recipients may opt-out free of charge and in an easy manner.

The new directive specifies that Member States may introduce provisions on the retention of traffic and location data for law enforcement purposes. It further introduces controls on the use of cookies on websites. Cookies and similar tracking devices will be subject to a new transparency requirement – anyone that employs these kinds of devices must provide information on them and allow subscribers or users to refuse to accept them if they wish.

---

[2] See Industry Canada (1999), "Internet and Bulk Unsolicited Electronic Mail (SPAM) Policy", July, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwGeneratedInterE/gv00188e.html, accessed 9 January 2004.

Japan

In July 2002, two laws regulating spam came into effect. One is the Law on Regulation of Transmission of Specified Electronic Mail (Law No. 26 of 2002), which aims to regulate the transmission of unsolicited commercial e-mail. The law obligates senders of unsolicited e-mail to display the sender's name, contact information, and state at the beginning of the subject line if the e-mail is an advertisement that was neither consented to nor requested so that users have the option to automatically block all mail that contains unsolicited advertising. The law also prohibits the transmission of e-mails to randomly generated e-mail addresses. In addition, the law prevents senders from e-mailing recipients who have informed senders by phone or e-mail that they do not wish to receive e-mail from them. The Minister of Public Management, Home Affairs, Posts and Telecommunications issues administrative orders to compel illegal senders to comply with the law. If a sender violates the law after receiving the order, a JPN 500,000 (USD 4,180) fine for non-compliance may be imposed. The law allows telecommunication carriers to refuse e-mail from spammers if it creates system problems. The Minister has issued several administrative orders since the law came into force in July 2002.

The other is an amendment to update the 1976 Specified Commercial Transactions Law (Law No. 28 of 2002), which governs mail-order sales and was instituted in order to protect consumers from exploitive marketing techniques, such as direct marketing. It provides users with an opt-out option, requiring sellers of products or service providers which advertise through e-mail to display their name, contact information, and state at the beginning of the subject line if the e-mail is an advertisement that was neither consented to nor requested so that users have the option to automatically block all mail that contains unsolicited advertising. It also requires them to attach messages informing recipients how to reject future ads. Once the ads have been rejected by recipients, sellers of products or service providers are prohibited from sending the ads again. The Ministry of Economy, Trade and Industry sends warning messages to sellers of products or service providers who are likely to violate the law (3 700 messages were sent in 2002), and imposes governmental orders on them if they don't obey warning messages (two companies received such orders in October 2003). Violations of this new law will result in maximum prison terms of two years or fines up to JPN 3 million (USD 24,000).[3]

Korea

The Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection prohibits transmitting spam such as commercial advertisement against the addressee's express wishes. It also prohibits disregarding an opt-out request through technical

[3] See Cramer, Evan (2002), "The Future of Wireless Spam", *Duke Law and Technology Review*, Rev. 0021, www.law.duke.edu/journals/dltr/articles/2002dltr0021.html, accessed 9 January 2004.

manipulation. The Act prohibits transmitting adult advertisement via e-mail, telephone, facsimile, or others to juveniles. The Act also requires the sender to expressly indicate the objective of transmission and major contents thereof, the name and contact means of the sender, and an opt-out option. The Act requires labelling "ADV" or "ADLT" in headers and clear expression about a method for refusal of future messaging or advertisements for the recipient. Senders are not allowed to use irregular labels in headers.

Furthermore, spamming by using a programme or collecting e-mail addresses through technical means are prohibited. The act of sharing, selling, exchanging or providing others with a list of e-mail addresses harvested from Internet bulletin boards is also prohibited. In addition, the Act states that ISPs can deny services for transmitting information on condition that there is, or will be, intense concern about serious obstruction by large influxes of spam mail. Currently, the opt-out approach is adopted in Korea. However, on 19 October 2003, the Ministry of Information and Communication (MIC) announced that it will introduce an opt-in approach for mobile phone service. As amending the existing law will take time, opt-in will first be implemented via usage agreements between mobile service providers and information service providers. These agreements were to be put in place before the end of 2003. MIC also prohibits sending all advertisement messages during certain hours, for example from 21.00 to 8.00 hrs. MIC intends to amend the relevant law in early 2004.

New Zealand

Though New Zealand does not currently have spam legislation, they are actively considering legislative proposals.

Slovak Republic – No regulation

The Slovak Republic currently has no legislation with regard to spam.

Turkey

There is no regulation against spam at the moment. However, discussions are ongoing amongst computer systems administrators and ISP engineers and some experimental work is being carried out to explore technical solutions to reduce the negative effects of spam on Internet traffic.

United Kingdom

Where e-mail addresses constitute personal data because they contain an individual's name, any processing must be carried out in accordance with the requirements of the Data Protection Act of 1998. This means that any company that continues to process an e-mail address that contains personal data, in order to

send unsolicited marketing communications, after being instructed by the individual to stop, will be in breach of the Act's fair processing requirements.

In March 2003, the UK Department of Trade and Industry introduced new anti-spam regulations, including an opt-in requirement. The law was passed in September 2003 and came into force on 11 December 2003. Under the new law, companies must have explicit permission from e-mail recipients before sending out offers. The law allows individuals to sue companies sending unsolicited e-mail offers. It also requires Web sites to offer consumers the opportunity to reject cookies prior to placing them on users' computers and bans unsolicited text messages. The Information Commissioner will have greater power to follow up complaints. The opt-in rule under the new regulations does not apply to corporate e-mail addresses, which means the law excludes most work addresses from the opt-in requirement.

United States

On 16 December 2003, the United States passed legislation on spam ("CAN-SPAM Act") that, as of 1 January 2004, adopts an opt-out approach to spam. The legislation prohibits false or misleading subject header information and deceptive subject lines. It requires senders of unsolicited commercial e-mail to provide a mechanism to opt-out and requires senders to abide by recipients' requests to opt out. The legislation requires clear and conspicuous disclosure that the message is an advertisement. The senders must include a valid postal address in the e-mail and have a functioning e-mail address. The law also prohibits harvesting of e-mail addresses, dictionary attacks, and spoofing. The legislation also creates new criminal violations. For example, the law makes it a criminal violation to knowingly send unsolicited commercial e-mail with a materially falsified header. Finally, the law requires the FTC to develop a plan and timetable for implementation of a do-not-e-mail registry and report any concerns about such a registry to Congress within 6 months of the enactment of the Act.

* * *