Consultation Paper on
Legislative Proposals to Contain the Problem of Unsolicited Electronic Messages

Commerce, Industry and Technology Bureau
January 2006

Contents

Foreword

This document sets out the Government's detailed legislative proposals to regulate activities related to the sending of unsolicited electronic messages.

Please send your comments on the proposals to the Communications and Technology Branch of the Commerce, Industry and Technology Bureau by 20 March 2006 by any of the following means:

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

Fax (852) 2511 1458
(852) 2827 0119

E-mail uem@citb.gov.hk

We assume that all submissions to this consultation are not made in confidence unless specified otherwise. We may reproduce and publish the submissions in whole or in part in any form and to use, adapt, or develop any proposals put forward without seeking permission or providing acknowledgement of the party making the proposal.

All personal data submitted will only be used for purposes which are directly related to the Government's consideration, preparation and processing of the Unsolicited Electronic Messages Bill. They may be transferred to other departments/agencies for the same purpose. For access to or correction of personal data contained in your written materials, please contact us.

Executive Summary

Unsolicited electronic messages (UEMs) are causing serious concern in the community. We need a piece of anti-spam legislation as part of a multi-faceted strategy to tackle the problem. This consultation paper seeks the views of the public on the detailed legislative proposals for the Unsolicited Electronic Messages Bill (UEM Bill).

2. The following six guiding principles, aiming at striking a balance among the interests of different stakeholders, are proposed for the UEM Bill -

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

2) There should be room for the development of e-marketing in Hong Kong as a legitimate promotion channel.

3) Hong Kong should avoid becoming a haven for illicit spamming activities.

4) Freedom of speech and expression must not be impaired.

5) Penalties and remedies should be proportionate to the severity of the offences.

6) The legislative provisions should be enforceable with reasonable effort.

3. We propose that only commercial electronic messages should be regulated. All non-commercial communications from governments, political parties, religious groups, charities, companies or other persons should not be affected. In view of the rapid development of information and communications technology, we propose that the UEM Bill should cover generally all forms of electronic communications, unless it is specifically excluded, so as to cater for future developments in technologies and services. In line with the generally accepted practice in Hong Kong and to leave room for normal and legitimate marketing activities, we propose that person-to-person voice or video telephone calls

without any pre-recorded elements should be excluded from the application of the UEM Bill. We also propose that transmissions of sound or video material on broadcasting channels that are already regulated under the Telecommunications Ordinance (Cap. 106) and the Broadcasting Ordinance (Cap. 562) should similarly be excluded from the regulatory framework of the UEM Bill.

4. Due to the distinct cross-boundary nature of some of the UEMs, we propose that even if the spamming act may occur outside Hong Kong, as long as the unsolicited commercial electronic message has a "Hong Kong link", then any related contraventions of the UEM Bill should fall within the jurisdiction of Hong Kong. Extra-territorial application is necessary for giving Hong Kong's law enforcement agencies a formal basis on which to seek co-operation with overseas law enforcement agencies in tackling the problem of UEMs. It would also send the right signal to overseas spammers that their actions towards Hong Kong recipients will not be tolerated.

Rules about sending commercial electronic messages

5. Overseas experience has been inconclusive as to whether an "opt-in" regime[1] or an "opt-out" regime[2] is more effective in curbing spam. Electronic communications are a low cost means for small and medium enterprises (SMEs) to promote their products or services. SMEs play an important role in the Hong Kong economy. Having regard to the need to provide SMEs and start-up enterprises in Hong Kong with room to promote their products or services using low cost means, we propose to adopt an opt-out regime.

6. To implement the opt-out regime, we propose to require a sender of commercial electronic message to provide a functional unsubscribe facility to enable a registered user of an electronic address to notify the sender that he does not wish to receive further commercial electronic messages from that sender. The unsubscribe message should take the form of an instruction to the sender of the commercial electronic

[1] An "opt-in" regime requires the sender of commercial electronic messages to have pre-existing business relationship with the recipient, or have obtained a consent from the recipient before he could send commercial electronic messages to that recipient.

[2] An "opt-out" regime requires the sender of commercial electronic messages to stop sending further commercial electronic messages to a recipient if the recipient so requests. But before receiving such a request, the sender may continue to send such messages to the recipient.

message, unless the registered user of the electronic address specifies in the unsubscribe message certain categories of products or services in the instruction which he is willing to continue to receive, in which case the sender may continue to send messages about the specified categories of products or services.

7. The functional unsubscribe facility should be operational for at least 30 days to enable the registered user of an electronic address to take a decision within a reasonable period on whether to send an unsubscribe request to that sender. The unsubscribe request should take effect within 10 working days and should last for an indefinite period, unless cancelled by the registered user of the electronic address. To facilitate investigation and enforcement, copies of such unsubscribe requests should be retained by the sender of commercial electronic messages for at least 7 years after they are received.

8. We propose to empower the Telecommunications Authority (TA) to set up "do-not-call registers" of appropriate types of electronic messages, to supplement the functional unsubscribe facility requirement for the opt-out regime. Electronic addresses that are placed in these registers will have the same effect as sending an unsubscribe message to all e-marketers. The TA will consider the appropriate types of electronic addresses suitable for setting up such registers. Initially, three registers may be set up – one for telephone numbers for pre-recorded voice, sound, video or image messages, one for telephone numbers for Short Messaging Service (SMS) / Multimedia Messaging Service (MMS) messages, and one for telephone numbers for fax messages.

9. We propose that all commercial electronic messages should contain accurate sender information, including the name, physical address and electronic address of the sender. If the sending party is an organisation, the organisation's name should also be included. Such sender information should be accurate for 30 days after the commercial electronic message is sent. We also propose to prohibit misleading subject headings in commercial e-mail messages.

10. We propose to adopt an enforcement notice regime for enforcing the above rules. If the TA is of the opinion that an e-marketer has contravened the rules and it is likely that the contravention will continue or be repeated, the TA will issue an enforcement notice

specifying the contravention and the steps to remedy the contravention. Contravention of an enforcement notice should be punishable by fine up to $100,000. Continuing offences should be punishable by a further fine of $1,000 a day. We propose to allow a person charged to prove as a defence that he has exercised all due diligence to comply with the enforcement notice concerned.

Rules about address harvesting

11. Address-harvesting is a prevalent technique among spammers to maximise the reach of their UEMs. We propose to prohibit the supply, acquisition or use of address-harvesting software or harvested-address lists in contravention of the rules about sending commercial electronic messages. We propose that on summary conviction, offenders should be punished by a fine up to $100,000 and by imprisonment for up to 2 years. On conviction on indictment, we consider that the fine should rise to a maximum of $1,000,000 and by imprisonment for up to 5 years.

Offences relating to the sending of commercial electronic messages

12. We propose to prohibit sending commercial electronic messages to electronic addresses obtained using automated means, such as the so-called "dictionary attacks". We also propose to prohibit any person from knowingly sending a commercial email message through open relays or open proxies designed to hide the true identity of the original sender.

13. We propose to prohibit the use of scripts or other automated means to register for multiple e-mail addresses, such as the so-called "automatic throwaway accounts". However, system administrators of an internal information system may use automated means to create multiple e-mail addresses in the course of their functions. Such circumstances will be exempted.

14. For the above three offences, we propose that the penalty on summary conviction should be a fine up to $100,000 and imprisonment for up to 2 years. On conviction on indictment, we propose that the penalty should increase to a fine of up to $1,000,000 and imprisonment for up to 5 years.

15. We propose to impose the heaviest penalties for offences related to fraud and related activities in connection with sending multiple commercial electronic messages. These offences are –

(a) accessing a computer or telecommunications device without authorisation (e.g. hacking) and intentionally initiating the transmission of multiple commercial electronic messages;

(b) sending multiple commercial electronic messages from a computer or telecommunications device without authorisation with the intent to deceive or mislead recipients as to the origin of such messages (e.g. spamming through zombie computers[3]);

(c) falsifying or altering the part of header information which is machine-generated automatically in multiple commercial electronic messages and intentionally initiating the transmission of such messages;

(d) registering for 5 or more electronic addresses or 2 or more domain names using information that falsifies the identity of the actual registrant and intentionally initiating the transmission of multiple commercial electronic messages from such electronic addresses or domain names;

(e) falsely representing himself to be the registrant of 5 or more electronic address or 2 or more domain names and intentionally initiating the transmission of multiple commercial electronic messages from such electronic addresses or domain names.

16. We propose to impose a penalty on conviction on indictment to a fine of any amount as determined by the Court and to imprisonment for up to 10 years. These offences will be enforced by the Hong Kong Police Force.

---

[3] A computer attached to the Internet that has been compromised by a hacker, a computer virus, or a Trojan program and used to perform malicious tasks such as spamming under remote direction, with the owner normally unaware of such tasks.

Compensation

17. We propose that a person who contravenes any provisions in the UEM Bill should be liable to pay compensation to the affected parties for the pecuniary loss sustained as a result of the contravention. In addition, we propose that the Court may also order a respondent not to repeat or continue the conduct or act, perform reasonable act or course of conduct to redress any loss or damage suffered by a claimant, grant an injunction or order other appropriate measures. In such civil claims, we propose to make clear that the respondent may prove as a defence that he had taken all reasonable care to avoid the contravention concerned. Such civil claims should be subject to the limitation period of 6 years.

Other Provisions

18. We propose to give the investigation powers to the TA, including the power to obtain information or documents relevant to an investigation and the power to enter and to seize, remove or detain any things upon obtaining a warrant from a magistrate. Failure, when ordered by a magistrate, to provide the information or documents requested by the TA, should be subject on conviction to a fine up to $50,000 and imprisonment for 2 years.

19. We propose that the Court may order a person convicted under the UEM Bill as a result of investigation by the TA to pay to the TA the whole or a part of the costs and expenses of the investigation.

20. We propose to make clear that for contraventions under the UEM Bill, employers and principals are responsible for the acts done or practices engaged by their employees and agents respectively. However, this is subject to a due diligence defence.

21. We propose to make clear that if a company, other body corporate or a partnership has committed an offence, a director of a company or a body corporate, or a partner of the partnership shall also be presumed to have committed the offence. However, we propose that there should be a defence that the director or partner did not authorise the act.

22. Other provisions proposed for the UEM Bill include clarification of liability of telecommunications service providers and owners of computers or telecommunications devices, services or networks involved in contraventions, powers for making regulations and codes of practices, and offences in relation to obstruction of TA in discharging his duties.

23. We also propose that different parts of the UEM Bill may commence on different dates to provide flexibility for e-marketers to gear up their equipment.

Part I Introduction

Background

On 25 June 2004, the Office of the Telecommunications Authority (OFTA) issued a public consultation paper on "Proposals to contain the problem of unsolicited electronic messages"[1]. That paper examined the problem caused by various forms of unsolicited electronic messages (UEMs), sometimes called "spam", the effectiveness of existing anti-spam measures and sought views on a range of possible ways to combat the problem, including the need for anti-spam legislation.

2. Drawing on the views and ideas expressed in the submissions to that consultation[2] and on the latest developments, the Secretary for Commerce, Industry and Technology (SCIT) announced on 24 February 2005 a package of measures under the "STEPS" campaign[3] to tackle the problem of UEMs. A new piece of anti-spam legislation is one of the measures proposed under this campaign. At **Annex A** is a detailed description of the measures under the "STEPS" campaign.

3. Between March and June 2005, the Commerce, Industry and Technology Bureau (CITB) engaged representative stakeholders to seek their views on the guiding principles and the key aspects of the framework for the proposed anti-spam legislation. Following those informal consultations, CITB presented the draft framework of the proposed anti-spam legislation to the Legislative Council Panel on Information Technology and Broadcasting[4] in July 2005. Taking into account the views expressed at that Panel as well as the latest developments in anti-spam legislation in other jurisdictions, CITB has prepared the detailed legislative proposals contained in this paper for the purpose of soliciting the views of the public.

The Case for Anti-Spam Legislation

4. Hong Kong is an externally-oriented economy and was the 11th largest trading entity in the world in 2004. It serves as a global centre for trade, finance, business and communications. Electronic communications are of vital importance in supporting such roles. Our sophisticated telecommunications facilities, enormous capacity for external communications and high penetration rates for personal

---

[1] http://www.ofta.gov.hk/en/report-paper-guide/paper/consultation/20040625.pdf
[2] http://www.ofta.gov.hk/en/report-paper-guide/paper/consultation/20041102/table.html
[3] "STEPS" stands for strengthening existing regulatory measures, technical solutions, education, partnerships and statutory measures.
[4] http://www.legco.gov.hk/yr04-05/english/panels/itb/papers/itb0711cb1-1985-1e.pdf

computers, Internet, and mobile services are all factors which make Hong Kong vulnerable to damages caused by UEMs.

5. UEMs are causing serious concern in the community. Recipients suffer inconvenience and potential financial loss. Recipients of junk faxes incur extra expenses in consumables. Recipients of pre-recorded telephone messages incur additional phone charges. Spam e-mails sent with malicious intent may compromise personal privacy by deceiving recipients to provide personal information that may then be disclosed to strangers, leading to possible financial loss. For businesses, spam e-mails add to their running costs. They suffer from lost productivity as employees must take the time to sort the spam e-mails from genuine business correspondence, and they face additional costs for screening tools to block spam. The rising trend of crime-related spam activities has an adverse impact on public confidence in the adoption of e-commerce. For telecommunications service providers, they have to increase their system bandwidth and/or capacity to cope with the increased traffic load arising from UEMs. Spam e-mails consume their computer capacities.

6. In Hong Kong, provisions in existing legislation cover some of the more serious aspects of the UEM problem. For example, if the sending of UEMs involves unauthorised access to programs or data held in a computer (commonly known as hacking), it may be punishable as an offence under section 27A of the Telecommunications Ordinance (TO) (Cap. 106). If a spammer sends an e-mail to a computer causing it to cease functioning, or in a manner which amounts to "misuse of a computer" as defined in section 59 of the Crimes Ordinance (Cap. 200), he could be liable for an offence under section 60 of the same ordinance. If e-mails are used as vehicles to deceive recipients (e.g. "419" letters[5] and phishing e-mails[6]), an element of "fraud" may be involved. If proved, this could constitute an offence under section 16A of the Theft Ordinance (Cap. 210). If e-mails contain malware (e.g., Trojan programs[7], virus, hacking tools) which facilitate the sender of the e-mails to gain access to a computer system without authority, then depending on the intent of the person gaining access to the computer system, he could have committed an offence under section 27A of the Telecommunications

---

[5] Also known as the Nigerian Advance Fee Scam, "419" letters are named after the section of the Nigerian penal code which addresses fraud schemes. The letters generally purport to come from a high-ranking official who needs to remove a huge sum of cash from his country. The recipients are asked for the use of their bank accounts to transfer the total amount into the banking system, for a percentage of the money in return. The recipients are also asked to deposit money into a specified bank account to help cover expenses for completing the deal, which may include paying bribes to other parties.

[6] The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

[7] Trojan programs - Destructive computer programs that pretend to be useful, harmless applications.

Ordinance (Cap. 106) and/or the offence of "access to computer with criminal or dishonest intent" under section 161 of the Crimes Ordinance (Cap. 200). The above statutory provisions are reproduced at **Annex B**.

7. However, there is no general legislation in Hong Kong to regulate the sending of UEMs and related activities. We need such legislation to address concerns about the impact of UEMs on the effectiveness of electronic communications and the costs to end-users. Such legislation can also send a clear message to spammers that these activities will not be tolerated.

8. Some types of UEMs (e.g., e-mail) have a distinct cross-boundary nature. They originate from outside Hong Kong and may have been routed through a number of other territories before they reach the recipients in Hong Kong, which may or may not be the final destination for the UEMs. We need to work closely with overseas jurisdictions to ameliorate the problem. However, such international co-operation can be made more effective if it is supported by local legislation on UEMs in each of the respective jurisdictions. Partly for this reason, a number of overseas jurisdictions have enacted, or are about to enact, anti-spam legislation, although the scope, application and features of their regimes may differ. **Annex C** gives an overview of the key features of the anti-spam legislation in selected jurisdictions. If Hong Kong is to avoid becoming a safe haven for illicit spammers who are driven here from jurisdictions which have anti-UEM legislation in place, then we must enact anti-spam legislation on our own. Such legislation will facilitate co-operation with law enforcement agencies in jurisdictions which have similar legislation.

9. A significant portion of the UEMs which originate locally concern marketing for products and services. Ninety-eight percent of Hong Kong's business establishments are small and medium size enterprises (SMEs) and they provide employment to 60% of the workforce. These SMEs, particularly start-up enterprises, generally do not have a strong customer base and may not have the resources to undertake costly promotion activities. Many SMEs therefore rely on electronic communications to promote their products. It is important that, on the one hand, legitimate e-marketers should not suffer from the increasing marginalisation or reduction in efficacy due to the proliferation of UEMs. On the other hand, consumers should be protected from marketing messages which they do not wish to receive. We therefore need legislation to regulate the use of UEMs as a means of promotion and/or sale of products and services.

Legislation as Part of a Basket of Measures

10. It is widely recognised that anti-spam legislation alone is not a panacea to the problems of UEM. It should form part of a multi-faceted strategy to address the issue. Legislation by itself, without any corresponding technical solutions to be installed by recipients to protect themselves from spam, or without public education programs to teach consumers how to deal with spam, would only be partially effective in addressing the problem. The STEPS campaign referred to in paragraph 2 above has made a useful start and needs to be reinforced by a piece of carefully crafted legislation which addresses the unique situation in Hong Kong.

Part II Objectives and Guiding Principles

Objectives

11. The proposed legislation should introduce a statutory framework for regulating activities related to the sending of commercial UEMs. We propose that this framework should achieve the following broad objectives –

(a) implement a statutory scheme to give recipients of UEMs the option of whether to receive or refuse further messages from e-marketers and introduce appropriate penalties for those disrupting the operation of the scheme;

(b) prohibit spamming-related activities that abuse electronic communications channels, including attempts by spammers to hide their identity or the origin of their UEMs, in order to avoid being traced or having their messages blocked;

(c) prevent Hong Kong from becoming a safe haven and base of operation for illicit spammers; and

(d) make the e-commerce environment in Hong Kong more secure, thereby helping to improve the efficiency of the economy and maintaining Hong Kong's position as an international business centre.

Guiding Principles

12. The regulation of activities related to the sending of UEMs could impact on many stakeholders in the community, with potentially conflicting interests, including businesses with products or services to promote, e-marketers, Internet service providers and consumers. It is important that our legislative proposals should strike a balance among the interests of different stakeholders, with a view to the overall good of the community. With this in mind, we propose the following six guiding principles for the proposed anti-spam legislation, tentatively referred to as "Unsolicited Electronic Messages Bill" (UEM Bill) –

Guiding Principle 1

The registered user of an electronic address[8] should have the right to decide whether to receive or refuse further electronic messages at that electronic address.

13. An electronic communication involves two parties – the senders of the message and the recipients of the message. For the recipient of the message, it is quite often that the message needs to be received and read before the recipient can decide whether the message is an abuse of the communication channel by the sender of the message. As such, we consider that the legislative proposals should contain arrangements which recognise the right of the recipient to read a message before deciding whether to refuse to receive further electronic messages they do not desire. Unsolicited electronic messages should refer to those sent to a recipient in circumstances where the recipient has exercised his right to refuse to receive further such messages.

Guiding Principle 2

There should be room for the development of e-marketing in Hong Kong as a legitimate promotion channel.

14. In view of the important role played by SMEs in our economy and SMEs' reliance on electronic communications as a low cost marketing tool (paragraph 9 above), we consider that the legislative proposals should ensure that there would be room for the development of e-marketing in Hong Kong as a legitimate promotion channel.

Guiding Principle 3

Hong Kong should avoid becoming a haven for illicit spamming activities.

15. The industry has estimated that the percentage of e-mail spam originating from Hong Kong contributed less than 5% of all e-mail spam received by Hong Kong e-mail services. Recent studies suggest that this percentage has declined further over the past year to less than 1%[9]. It is encouraging to note that Hong Kong does not produce spam in any substantial way to plague its own, or overseas e-mail users. However, our legislative proposals should have regard to the aim of

---

[8] "Electronic address" is defined in paragraph 29(a).

[9] See spam statistics from MailProve at http://www.mailprove.com/main_site/news/ne_spamstatistics_hk.htm

preventing Hong Kong from becoming a safe haven for illicit spamming activities, whether such activities originate locally or are driven here from overseas economies. We must preserve the level of trust that overseas e-mail receivers and servers have for e-mails sent from Hong Kong. Indeed, the experience in Australia is that the enactment of anti-spam legislation has been effective in halting major e-mail spamming operations in Australia, or driving them out of Australia[10].

Guiding Principle 4

Freedom of speech and expression must not be impaired.

16. Any measures implemented to tackle the problem of UEMs should not impair, or be seen to impair, freedom of speech and expression. In Hong Kong, freedom of speech is protected under Article 27 of the Basic Law and Article 16 of the Hong Kong Bill of Rights Ordinance (Cap. 383). This fundamental right of Hong Kong residents should not be affected in any way by our legislative proposals to contain the UEM problem.

Guiding Principle 5

Penalties and remedies should be proportionate to the severity of the offences.

17. The penalties and remedies in the legislative proposals should be proportionate to the severity of the offences in terms of their criminal intent and their impact on victims, drawing reference to the legislation and arrangements made in overseas jurisdictions.

Guiding Principle 6

The legislative provisions should be enforceable with reasonable effort.

18. In drafting any legislation, it would not be meaningful to propose provisions which cannot in practice be properly enforced. Accordingly, we propose that only provisions which can be enforced with reasonable effort should be included in the UEM Bill.

We wish to seek comments on the proposed broad objectives and guiding principles for the UEM Bill.

[10] http://www.itu.int/osg/spu/cybersecurity/contributions/Australia_spamregime_review.pdf

Part III Scope of Application

Nature of electronic messages

19. Since most UEMs attempt to promote or offer products or services, we consider that the UEM Bill should only regulate commercial UEMs. It should cover messages the primary purpose of which is the commercial advertisement or promotion of a commercial product or service. We also note that the anti-spam legislation in overseas jurisdictions set out in Annex C only regulate commercial UEMs. In other words, non-commercial communications from governments, political parties, religious groups, charities, companies or other persons should not be affected in any way by the Bill.

20. Some stakeholders commented that UEMs of a non-commercial nature may equally cause nuisance to recipients and should be brought within the ambit of the Bill. Automated telephone surveys by newspapers has been cited as one example. They argued that freedom of speech and expression would not be affected since the Bill would only be recognising the right of a recipient to choose whether to listen to the sender or not. Our view is that since messages of a commercial nature form the bulk of the problem of UEMs, the legislation should deal with commercial UEMs first and foremost. They form a distinct category of messages that can be easily defined, identified and targeted.

Form of electronic messages

21. The problem of UEMs spans across different forms of electronic communication, although the severity of the problem differs for each mode of communication. In Hong Kong's context, it is generally recognised that e-mail, voice telephony and facsimile are the forms of electronic communication which suffer the most from UEMs. This may be due to the cost structures of sending messages through these forms of electronic communication. In the case of e-mail, the incremental cost of sending additional messages is close to nil. For pre-recorded voice messages and facsimile messages, if the sender is making local calls over the fixed-line telecommunications network, the incremental cost of sending additional messages is also close to nil, with the fixed-tariff charge structure prevailing in Hong Kong.

22. But with the rapid development of information and communications technology, new forms of electronic communication may emerge which could also become susceptible to UEMs. Spammers

may also shift their channel of sending UEMs to other modes of electronic communications in response to changes in the cost structure for particular forms of electronic communications[11]. Thus, unlike the anti-spam legislation in some other jurisdictions, we propose that the UEM Bill should cover generally all forms of electronic communications, unless it is specifically excluded, so as to cater for future developments in technologies and services. We consider that the compliance burden on businesses should not be too onerous if the regulatory requirements in the UEM Bill are reasonable, and reflect sound practices for fostering good customer relationships.

Specific forms of electronic communications to be excluded

23. On the other hand, we recognise that casting too wide a net for the regulatory regime could have an adverse impact on normal business activities. For instance, it is a generally accepted practice in Hong Kong for sales persons to make personal telephone calls to promote certain products or services to existing or potential clients. Such promotion calls require the business entity undertaking the promotion to devote substantial manpower resources and time to the promotion. To leave room for such normal and legitimate marketing activities, we are of the view that we should be light handed in regulating this mode of e-marketing. We further believe that making person-to-person calls of this nature should not be considered as an abuse of the communications channel. We therefore propose to exclude the normal voice, or video, telephone calls that do not contain any pre-recorded elements from the application of the Bill. We suggest the use of "pre-recorded elements" in the electronic message as the demarcation line for the applicability of the Bill. This is to plug a potential loophole arising from the possibility of some unscrupulous e-marketers using short person-to-person greetings as a preamble to pre-recorded messages with a view to avoiding the regulatory burden under the Bill.

24. Transmissions of sound or video materials on broadcasting channels may also be considered as messages transmitted through electronic means. However, to what extent the concept of "unsolicited messages" can be applied to broadcast content is highly debatable, and in any case such content is already regulated under the Telecommunications Ordinance (Cap. 106) and the Broadcasting Ordinance (Cap. 562). For this reason, we do not consider it necessary to subject such transmissions to the regulatory framework of the UEM Bill.

---

[11] It was reported that in Japan, where the anti-spam legislation initially covered e-mails only, some spammers have shifted their activity to the Short Messaging Service (SMS) / Multi-media Messaging Service (MMS) platform after the enactment of the legislation.

Electronic messages with a Hong Kong nexus

25. It was suggested in the draft framework for the UEM Bill presented to the Legislative Council Information Technology and Broadcasting Panel on 11 July 2005 that the Bill should be applicable to the act of sending, or causing the sending of, commercial electronic messages if the person involved is physically present in Hong Kong, irrespective of where the commercial electronic messages are sent to.

26. We have carefully reviewed this approach and propose to revise it to provide a more general coverage. Provided the electronic message has a Hong Kong "nexus" or connection, for example –

(a) the message originates from Hong Kong (Hong Kong source); and/or

(b) the message is sent through Hong Kong to another destination (Hong Kong pathway); and/or

(c) the message is sent to an electronic address in Hong Kong (Hong Kong victim); and/or

(d) the marketing of the message, or, promotion or advertising of the service by means of a UEM is in Hong Kong,

then any contraventions of the UEM Bill should fall within the jurisdiction of Hong Kong, irrespective of whether there are or may be any acts done outside Hong Kong. The "nexus" or connection with Hong Kong is the proper and commonly used basis for conferring jurisdiction on the Hong Kong courts.

27. The revised proposal could bring within the ambit of the UEM Bill persons who send UEMs from an overseas jurisdiction to Hong Kong in circumstances where there is a Hong Kong pathway, and/or a Hong Kong victim and/or marketing etc. of the message or service by means of the UEM in Hong Kong. In this sense the legislation may be considered extra-territorial. This is broader than our original proposal of focusing on UEMs sent from Hong Kong only. We have come to the view that the UEM Bill should not be so restricted in its application. This extra-territorial application of the UEM Bill, but only in circumstances where there is a Hong Kong "nexus", could enable the tracking and identification of overseas spammers spamming into or through Hong Kong as well as the collection of evidence against them to

be done more effectively with a view to bringing them to justice. It will also extend the scope of the **civil** action that an aggrieved person may wish to pursue. We are however aware that despite the extra-territorial application of the UEM Bill, it may be difficult in practice to prosecute and sue offenders due to the complex cross-boundary nature of the activities involved, which very often involve multiple parties utilizing different equipment and techniques to hide their identity and location. There will be a need on occasions to work with overseas service providers and law enforcement agencies with uncertain or at least variable results.

28. In spite of the fact that there may be difficulties in enforcement, we consider it desirable to cast a wider net so that overseas spammers will know that that their actions towards Hong Kong recipients will not be tolerated by the civil and criminal law of Hong Kong. Australia's Spam Act 2003 has a similar extra-territorial application. As we understand it, the extra-territorial application of Australia's Spam Act 2003 was designed to pave the way for future international co-operation, possibly under some kind of anti-spam treaty. Singapore's proposed Spam Control Bill has also adopted the Australian approach. All communications sent from or received on a public network within the European Union member states are covered by Anti-spam legislation under Article 3(1) of the Directive 2002/58/EC of the European Parliament and of the Council. Italy and France have introduced anti-spam law to impose on spammers a term of maximum imprisonment of 3 years and 5 years respectively. We consider that a similar forward-looking approach should be adopted in Hong Kong. Those outside Hong Kong who send or cause to be sent UEMs should still be governed by local (Hong Kong) legislation in circumstances where the Hong Kong "nexus" or connection exists. To the extent that those responsible have a business or assets to protect in Hong Kong they would be well advised to heed the local legislation.

Legislative Proposals

29. For the purposes of the Bill, we propose to –

(a) define "electronic address" to mean a "string" (i.e. any sequence of letters, characters, numbers and/or symbols) specifying the source or destination of an electronic message, including but not limited to telephone numbers, fax numbers, e-mail addresses, Internet Protocol addresses, and instant message screen names or instant messaging names. The

definition should be technologically neutral and should cover all forms of current and future electronic messages as far as possible;

(b) define "electronic message" to include any form of electronic communication, including but not limited to text, voice, sound, image or video message, transmitted over a public telecommunications service. In other words, electronic communications over private telecommunications services, such as e-mail communications of an organisation, within an internal network, would not be subject to the application of the Bill;

(c) define "commercial electronic message" to mean any electronic message at least one of the purposes of which is to offer, advertise, promote, or sponsor the provision of goods, facilities, services, land or a business or investment opportunity, etc., in the course of or in the furtherance of any business;

(d) establish a schedule listing certain forms of electronic messages that are to be excluded from the application of the Bill. The schedule should initially contain three types of electronic messages:

(i) voice, sound, image or video images involving person-to-person interactive communications between a caller and a recipient without any pre-recorded element;

(ii) television program services regulated under the Broadcasting Ordinance (Cap. 562); and

(iii) sound broadcasting services regulated under the Telecommunications Ordinance (Cap. 106);

(e) empower SCIT to amend the schedule described in (d) by regulation, in order to enable the Bill to cater for future technological or service developments, as necessary; and

(f) define a "Hong Kong link" for a commercial electronic message to mean a message that has a Hong Kong nexus, including but not limited to the following circumstances –

(i) the message originates from Hong Kong;

(ii) the message is sent through Hong Kong to another destination;

(iii) the message is sent to an electronic address in Hong Kong; and

(iv) the marketing of the message, or, promotion or advertising of the service by means of a UEM is in Hong Kong.

We propose to use the "Hong Kong link" concept in various sections of the Bill to specify the extra-territorial applicability of those sections.

We wish to seek comments on the above legislative proposals for defining the scope of application of the UEM Bill.

Part IV Rules About Sending Commercial Electronic Messages

30. This part sets out the basic regulatory regime for sending commercial electronic messages.

Opt-out regime

31. From the earlier public consultation exercise and informal discussions with representative stakeholders, we are aware that the community holds different views on whether the appropriate regulatory regime for Hong Kong should be an "opt-in" regime or an "opt-out" regime. In essence, an opt-out regime requires the sender of UEMs to stop sending further commercial electronic messages to a recipient if the recipient so requests. Until the request is made by a recipient, the sender may continue to send such commercial electronic messages to him. In comparison, under an opt-in regime, the sender cannot send any UEMs unless the sender has some pre-existing business relationship with the recipient, or until such time as the potential recipient indicates to the sender that he wishes to receive such communications.

32. The opt-in regime can be seen to provide a higher standard of protection for recipients. However, since electronic communications is a low cost means for small and medium enterprises (SMEs) to promote their products and services, an opt-in regime could create a substantial obstacle to the promotion activities of SMEs and start-up enterprises. It is questionable whether such a relatively heavy-handed approach is necessary. For an opt-in regime to be established and sustained, there must exist among the different stakeholders a recognition of the rights of the recipients. But it is unlikely that illicit spammers with malicious intent would respect such rights. Adopting an opt-in regime would therefore be unlikely to be effective in reducing the volume of UEMs sent by those spammers.

33. On the other hand, an opt-out regime would provide companies with room to promote their products or services, and in turn, facilitate development of SMEs. Bearing in mind the importance of SMEs to the economy of Hong Kong, an opt-out regime appears more appropriate for us. It is also consistent with the approach in regulating direct marketing activities using personal data under section 34 of the Personal Data (Privacy) Ordinance (Cap. 486) (reproduced at **Annex D**).

34. In day-to-day activities, the opt-out approach is generally accepted by the community. It provides recipients with the choice to browse through promotion information before deciding whether to

receive further messages. But we recognise that there could be shortcomings of an opt-out regime. It could send a negative signal to spammers that UEMs can be sent without consent. Some claim that the current spamming situation in the US, with its CAN-SPAM Act[12] imposing an opt-out regime, is an indication of the failure of such a regime in curbing spamming. There were criticisms that the Act in fact legalised spamming. However, the US Federal Trade Commission (FTC), on examining the data from an international e-mail filtering company on the volume of spam e-mails received in the UK, which imposes an opt-in regime, believes that the opt-in regime in the UK has not decreased the amount of spam e-mail UK citizens receive[13]. Thus, overseas experience is probably inconclusive as to whether an opt-in or an opt-out regime is more effective in curbing spam. Another possible shortcoming is that the act of opting out could enable a spammer to confirm a recipient's existence and thereby encourage further spamming and sharing of e-mail addresses. Recipients might also need to unsubscribe from a large number of messages initially. These shortcomings can however be addressed through the introduction of additional safeguards under an opt-out regime such as wider education on tackling spam, and effective enforcement of the UEM Bill. On balance, we propose an opt-out regime for Hong Kong.

35. According to the International Telecommunication Union[14], approximately two-thirds of the world's anti-spam laws (including the many state spam laws in the US) are considered to be opt-out regimes while approximately one-third are opt-in regimes. We also note that Singapore, where most spam e-mails also originate from outside the country, has recently proposed to adopt an opt-out regime in its proposed Spam Control Bill[15].

Implementing the opt-out regime

36. To implement an effective opt-out regime for UEMs, we propose the following elements –

(a) to require the sender of commercial electronic messages to

---

12 http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf

13 Page 28 of "National Do Not Email Registry: A Report to Congress" by FTC at http://www.ftc.gov/reports/dneregistry/report.pdf

14 "Countering Spam: How to Craft an Effective Anti-Spam Law" by the International Telecommunication Union at http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_How%20to%20craft%20and%20effective%20anti-spam%20law.pdf.

15 Spam Control Bill - http://www.ida.gov.sg/idaweb/doc/download/I2883/2nd_Joint_IDA-AGC_Consultation_Paper.pdf

include a functional unsubscribe facility to enable a registered user of an electronic address to indicate to the sender his wish not to receive further commercial electronic messages at his electronic address from that sender;

(b) the establishment of do-not-call registers for different types of electronic addresses, to enable a registered user of an electronic address to notify all e-marketers of his wish not to receive further commercial electronic messages at his electronic address;

(c) to require the sender of commercial electronic messages to include accurate sender information to enable a recipient to identify and contact the sender if necessary;

(d) to prohibit the sending of further commercial electronic messages to an electronic address after an unsubscribe message becomes effective or the electronic address is included in a do-not-call register, subject to affirmative consent given to the sender (criteria detailed in paragraph 44);

(e) to prohibit misleading subject headings in commercial e-mails; and

(f) the establishment of an "enforcement notice" regime with appropriate penalties for mandating a sender of commercial electronic messages to comply with the above elements.

Functional unsubscribe facility

37. This facility should enable a registered user of an electronic address to communicate with the sender of commercial electronic message, with minimal effort, and without cost hurdles, his wish not to receive –

(a) all further commercial electronic messages from the sender; or

(b) specific categories of commercial electronic messages (e.g. for different product/service categories) from the sender.

38. To remove any ambiguity, such unsubscribe message should take the form of an instruction to the sender of the commercial electronic

message. That is, it should instruct the sender of the commercial electronic message not to send any further messages to that electronic address. The only exception is when the unsubscribe message applies only to certain categories of products/services prescribed by the recipient, in which case the sender may continue to send messages offering or promoting other categories of products/services not prescribed by the recipient. The ability to unsubscribe from specific categories of commercial electronic messages is considered desirable in order to provide a recipient with more choice of the content of the messages he would like to receive.

39. The unsubscribe facility provided to the recipient should be functional for a reasonable period of time to enable the recipient to exercise his choice. It is unreasonable to require the unsubscribe facility prescribed in an UEM to be functional forever, since the e-marketer may change, for example, the e-mail address or Internet hyperlink for receiving unsubscribe messages due to normal business activities such as moving to a new domain name. However, the functional period of the unsubscribe facility should not be too short or else the recipient would be compelled to make a quick decision on whether to receive further messages from the e-marketer. We consider the 30-day period prescribed in the US CAN-SPAM Act[16] to be reasonable and we propose to adopt the same period in the UEM Bill.

40. Upon receipt of an unsubscribe message, the sender may need some time to process the unsubscribe message in order to remove the electronic address from the marketing database. While large companies may be able to automate this process, we are concerned that SMEs may not be quite so automated in their setups and would need a bit more time to give effect to an unsubscribe message. Drawing reference to the US CAN-SPAM Act[17], we propose that the effective date from which no further commercial electronic messages may be sent to the electronic address should be 10 working days after the unsubscribe message is sent.

41. We consider that an unsubscribe message which is sent to a sender of a commercial electronic message should generally last for an indefinite period. Nevertheless, it may be too onerous on the e-marketers to require them to retain a copy of each unsubscribe message received, or keep them in a format which represents accurately the information originally received, for an indefinite period. To strike a

---

[16] Section 5(a)(3)(A)(ii)
[17] Section 5(a)(4)

balance between the need to have access to such records for investigation and enforcement purposes and to avoid imposing too burdensome a requirement on e-marketers, we propose that the UEM Bill should require such information be retained for at least 7 years after they are received.

42. We recognise that a recipient might change his mind after he submits an unsubscribe message to a particular sender. We therefore propose that if that recipient sends an affirmative consent to the sender to receive commercial electronic messages, any previous unsubscribe message sent by him to that sender would be deemed to be cancelled.

43. We also recognise that the sender of the commercial electronic message and the recipient may have independently entered into contractual or other arrangements regarding the receipt of such messages. We consider that the statutory provisions for the provision of functional unsubscribe facility should not void such private arrangements between the two parties.

Do-not-call registers

44. It has been suggested that the Government should consider setting up "do-not-call registers" of telephone numbers so as to provide members of the public a means by which they may opt out from receiving UEMs from all e-marketers. We accept that this is a worthwhile mechanism to supplement the functional unsubscribe facility requirement for the opt-out regime. Electronic addresses that are placed in such registers should have the same effect as sending an unsubscribe message to all e-marketers. The e-marketers must not send commercial electronic messages to electronic addresses on the registers unless the e-marketers have received individual affirmative consents from the registered users of the electronic addresses (prior or subsequent to the inclusion of the electronic addresses on the registers). Similar to unsubscribe messages, subsequent to the addition of an electronic address on a do-not-call register, a recipient may send an affirmative consent to an e-marketer seeking to receive commercial electronic messages, and the e-marketer could do so in spite of the electronic address of the recipient appearing on the do-not-call register.

45. We propose not to prescribe the scope and form of the do-not-call registers in the UEM Bill, but to empower the Telecommunications Authority (TA) to set up such registers as he considers appropriate. This is necessary because for certain types of electronic addresses, a do-not-call register could be counterproductive. For instance, there is a "National Do Not Call Registry" of home

telephone numbers in the US for telemarketing calls[18]. The US FTC has studied the possibility of establishing a "National Do Not Email Registry" and concluded in its report to the US Congress[19] that "a National Do Not Email Registry, without a system in place to authenticate the origin of e-mail messages, would fail to reduce the burden of spam and may even increase the amount of spam received by consumers". With an empowering provision in the UEM Bill, the TA would be able to take into account technological standards and developments and new types of electronic messages in deciding whether to establish do-not-call registers for different types of electronic addresses. The detailed functioning of such registers should be prescribed by the TA through codes of practices. Our present thinking is to establish a register of telephone numbers for opting out of pre-recorded voice, sound, video or image promotion messages, a register of telephone numbers for opting out of SMS/MMS promotion messages, and a register of telephone numbers for opting out of promotion fax messages.

Accurate sender information

46. An important aspect of a successful opt-out regime is the ability to identify, locate and contact the sender of a UEM, so that a recipient may follow up with the sender as necessary and enforcement action may be taken against a sender who does not implement the opt-out regime, for example, by not implementing the unsubscribe requests. We propose that all commercial electronic messages should contain clear and accurate information identifying the person or organisation who sent, or in the case of a party contracting another party to send the message on its behalf, both the contracting and contracted parties. Such information should include the name, physical address and electronic address of the person sending the message. If an organisation is the sending party, the name of the organisation and the name, physical address and electronic address of the person sending the message on behalf of this organisation should be included. Drawing on the requirements in other anti-spam legislation[20], and in line with the period required for the functional unsubscribe facility, we consider that the sender information should be valid for at least 30 days after the message is sent. This period is considered reasonable, balancing the possibility of the sender legitimately migrating to say, a new domain name with a new set of e-mail addresses, and the period for aggrieved recipients to identify the appropriate person to contact and follow up on messages sent by the recipient.

---

[18] https://www.donotcall.gov

[19] "National Do Not Email Registry: A Report to Congress" by FTC at http://www.ftc.gov/reports/dneregistry/report.pdf

[20] For example, section 17(1)(d) of Spam Act 2003 of Australia at http://scaleplus.law.gov.au/html/pasteact/3/3628/pdf/Spam2003.pdf

47. It has been suggested that a physical address should be required as part of the sender information to facilitate a recipient or law enforcement agency to contact and locate the sender as necessary. However, it has been reported that some illicit spammers use physical addresses in remote locations, such as some African countries, thereby *prima facie* satisfying the statutory requirement but in reality making it difficult for law enforcement agencies to verify whether those physical addresses are real and are actually used by the sender. We consider that it would be more useful to enforcement agencies if a sender of commercial electronic messages is required to provide not only physical addresses, but also other contact addresses one of which must be the same type as the message itself (e.g. a contact e-mail address for commercial electronic messages sent by e-mail, a contact fax number for commercial electronic messages sent by fax).

Misleading subject headings

48. The prohibition of misleading subject headings in an e-mail message is a requirement under the US CAN-SPAM Act[21], but it is not found in other overseas anti-spam legislation. It is targeted at e-mail messages which have a data structure with a "subject heading" entry. The content in such an entry is displayed first before the recipient of the e-mail message chooses whether to open the particular e-mail message to read.

49. An accurate subject heading is an important identifier for an e-mail commercial message concerning the content of the message itself. A misleading subject heading in an e-mail message, on the other hand, can trick a recipient into opening a message he would otherwise not be interested in. Such an action could potentially expose the recipient's computer or telephone to infection by a computer virus or malware such as spyware. To enhance transparency of the message, we therefore propose to prohibit the sending of commercial e-mail messages with subject headings that could mislead a recipient about the content or subject matter of the message. It is for consideration whether this prohibition should be subject to the malicious intent of the sender e.g. by infecting a recipient's computer. Our inclination is that a misleading subject header in itself should be prohibited.

[21] Section 5(a)(2)

Enforcement notice

50. The above rules about sending commercial electronic messages aim to put in place a regulatory regime whereby e-marketing companies could respect and implement the wishes of recipients of commercial electronic messages. We consider that our enforcement objective should be to put right malpractices and to develop appropriate systems. We recognise however that even legitimate e-marketers may inadvertently commit non-compliance. We consider that they should initially be advised of such non-compliance and be given the opportunity to rectify the arrangements within a reasonable period of time.

51. Accordingly, we propose to adopt an enforcement notice regime for those rules. If, following the completion of an investigation, the TA is of the opinion that an e-marketer has contravened the rules and it is likely that the contravention will continue or be repeated, then the TA will issue an enforcement notice to that e-marketer specifying the contravention and the steps required to remedy the contravention within a prescribed period of time. Such required steps may draw reference to any codes of practice that the TA has published or contain a choice between different ways of remedying the contravention.

52. Anyone aggrieved by an administrative decision by the Government may seek judicial review. If necessary, we would consider providing a separate administrative appeals channel for enforcement notices under the UEM Bill.

Offence in relation to enforcement notice

53. To ensure that enforcement notices would be complied with, we propose that the contravention of an enforcement notice should be made an offence, punishable by fine at level 6 prescribed in schedule 8 of the Criminal Procedure Ordinance (Cap. 221) (i.e. $100,000). Continueing offences should be punishable by a further fine of $1,000 a day.

Legislative Proposals

54. With regard to the proposed requirement for accurate sender information, we propose to specify in the UEM Bill that a commercial electronic message with a Hong Kong link shall not be sent, or caused to be sent, unless –

(a) the message includes clear and accurate information identifying the sender of the message, that is –

(i) where the sender is a person, his full name;

(ii) where the sender is an organisation, the full name of the organisation and the full name and title of the person who sent the message on behalf of the organisation;

(b) the message includes clear and accurate information about how the recipient of the message can readily contact the sender, which information should identify a physical address and at least one electronic address that is compatible with the form in which the message was sent; and

(c) the information referred to in (b) is reasonably likely to be valid for at least 30 days after the message is sent.

55. With regard to the proposed requirement for a functional unsubscribe facility, we propose to specify in the UEM Bill that a person shall not send, or cause to be sent, a commercial electronic message that has a Hong Kong link to an electronic address unless –

(a) the message includes a clear and conspicuous statement to the effect that the registered user of the electronic address may use an electronic address identified in the message to send an unsubscribe message to the sender. The unsubscribe message may provide a list from which the recipient may choose the specific types of commercial electronic messages he does not want to receive;

(b) the electronic address identified in the message is reasonably likely to be capable of receiving an unsubscribe message during a period of at least 30 days after the message is sent; and

(c) the use of the electronic address identified in the message is provided free of charge to the registered user of the electronic address;

except where –

(d) the person who sends the message does not know or could not with reasonable diligence have ascertained that the

message has a Hong Kong link;

(e) the person who sent the message or caused the message to be sent, by mistake; or

(f) the requirement above is inconsistent with the terms of a contract or other agreement between the sender and the recipient.

56. We also propose to specify in the UEM Bill that –

(a) a person who receives an unsubscribe message shall ensure that a record of the unsubscribe messages is retained in a format which it was originally received, or in a format which can be demonstrated to represent accurately the information originally received, for at least 7 years after the receipt of the unsubscribe message; and

(b) a person who receives an unsubscribe message shall not disclose any information contained in the unsubscribe message to any other person, except with the affirmative consent of the person whose particulars are contained in the unsubscribe message.

57. To give effect to the unsubscribe message, we propose that the UEM Bill should specify that after an unsubscribe message has been sent, the sender of the commercial electronic message should cease to send further commercial electronic messages to the electronic address specified in the unsubscribe message within 10 working days from the day on which the unsubscribe message is sent, except where subsequent to the sending of the subscribe message, the registered user of an electronic address has given his affirmative consent to receive all or specified types of commercial electronic messages from the sender concerned.

58. With regard to the proposed do-not-call registers, we propose to specify in the UEM Bill that –

(a) the TA may establish and maintain registers of electronic addresses to be known as do-not-call registers;

(b) the TA shall make available the do-not-call registers for public inspection in the form of an online record;

(c) do-not-call registers shall be admissible as evidence of its contents in legal proceedings;

(d) the TA may do all things necessary to be done to establish, maintain and operate do-not-call registers for the purpose of the UEM Bill; and

(e) a person shall not send, or cause to be sent, a commercial electronic message that has a Hong Kong link to an electronic address no later than 10 working days after it has been included in a do-not-call register, except where the registered user of an electronic address has given his affirmative consent to receive all or specified types of commercial electronic messages from the sender concerned.

59. With regard to subject headings in commercial e-mails, we propose that the UEM Bill should specify that a person shall not send, or cause to be sent, a commercial electronic message that has a Hong Kong link by e-mail if the subject heading of the e-mail would likely mislead the recipient about a material fact regarding the content or subject matter of the message.

60. With regard to enforcement notices, we propose to specify in the UEM Bill that –

(a) where, following the completion of an investigation, the TA is of the opinion that any person –

(i) is contravening the rules about sending commercial electronic messages (paragraphs 54 to 59 above), or has contravened and it is likely that the contravention will continue or be repeated, the TA may serve on the person an enforcement notice in writing –

- stating that he is of that opinion;

- specifying the contravention and the reasons why he believes it is a contravention; and

- directing the person to take such steps as are specified in the notice to remedy the contravention within a specified period (ending no earlier than the time allowed for making an appeal). Such remedy may be framed by reference to any code of practice

which the TA may prescribe in support of the UEM Bill or afford the person a choice between different ways of remedying the contravention or matter;

(b) in special circumstances, the TA may specify in an enforcement notice remedial steps to be taken as a matter of urgency within 14 days, but no shorter than 7 days after the notice was served. The TA will give his reason in the enforcement notice why he is of the opinion that urgent steps should be taken;

(c) in special circumstances, the TA may also serve an enforcement notice notwithstanding that an investigation has not completed. He shall explain in the enforcement notice the reason of special circumstances justifying the urgent serving of enforcement notice before the completion of an investigation;

(d) any person who contravenes an enforcement notice served on him commits an offence and is liable on conviction to a fine at level 6 prescribed in schedule 8 of the Criminal Procedure Ordinance (Cap. 221) and, in the case of a continuing offence, to a further fine of $1,000 for every day during which the offence continues;

(e) it shall be a defence for the person charged to prove that he exercised all due diligence to comply with the enforcement notice concerned.

We wish to seek comments on the above legislative proposals for prescribing the rules about sending commercial electronic messages.

Part V Rules About Address-Harvesting

61. Address-harvesting, in the context of spamming, means the acts done by spammers to search for and collect new electronic addresses (mostly e-mail addresses) from telecommunications networks, particularly the Internet, for sending spam. They use software to scan web pages, newsgroups, chat rooms, message boards and e-mail service directories etc. for obvious signs of e-mail addresses like those containing "@" followed by ".com" and then "harvest" them into lists for sending spam. According to a study by the FTC[22], chat rooms, newsgroups and web pages are the most harvested forum for e-mail addresses.

62. Because this technique is prevalent among spammers to maximise the reach of their spam e-mails, some overseas anti-spam legislation prohibits the supply, acquisition and/or use of address-harvesting software and harvested-address lists in connection with sending commercial electronic messages[23]. Since spammers can easily collect large numbers of e-mail addresses through the use of this technique and then send spam to those addresses, it can be considered as an abuse of the electronic communications system with the price for such abuse being paid for by communications service providers (e.g. Internet service providers) and recipients. We are therefore of the view that the UEM Bill should also contain similar provisions to prohibit such activities, tackling the issue from three sides – supply, acquisition and use.

63. Although address-harvesting activities are probably confined to e-mail addresses on the Internet, we consider it desirable to maintain a technology neutral approach so that the statutory provisions would be able to cover harvesting activities for other types of electronic addresses that may become more common in the future.

64. As pointed out by some stakeholders, address-harvesting software does have some legitimate uses, e.g., for corporate-wide system administration purposes. For the UEM Bill, we propose to link the offence to using address-harvesting software or harvested-address lists in connection with sending commercial electronic messages when it is done

---

[22] http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.pdf

[23] Australia's Spam Act 2003 prohibits the supply, acquisition and use of address-harvesting software and harvested-address lists in connection with sending commercial electronic messages. US's CAN-SPAM Act stipulates a prohibition to transmit unlawful commercial e-mail messages using, or to provide list of addresses obtained through, address harvesting. The anti-spam law in South Korea has similar prohibitions on the act of harvesting e-mail addresses from websites that expressly prohibit automated harvesting with software, the sale and circulation of e-mail addresses harvested and the knowing use of e-mail address harvested. Singapore's proposed Spam Control Bill prohibits the sending of an electronic message to electronic addresses through the use of address harvesting software.

in contravention of the requirements under opt-out regime. This linkage is considered necessary because under an opt-out regime, it is acceptable for an e-marketer to send the first and subsequent commercial electronic message to a recipient until and unless the recipient has expressed his wish not to receive such messages. Thus, using address-harvesting software or a harvested-address list for the purpose of sending commercial electronic messages before an unsubscribe message is sent is, strictly speaking, not aiding in any wrongful act. However, if an e-marketer does not comply with the opt-out regime and at the same time uses address harvesting techniques indiscriminately, then he should be punished not only for non-compliance with the opt-out regime, but also for using address-harvesting software and/or harvested-address lists in an abusive way.

65. Given the implication of address harvesting to the problem of UEMs and the potential gain that a spammer may obtain through the use of such techniques, we consider that a relatively heavy penalty, with the possibility of imprisonment, should be introduced. For the supply, acquisition and use of address-harvesting software or harvested-address list, we consider that on summary conviction, offenders should be punished by a fine up to level 6 as prescribed in Schedule 8 of the Criminal Procedure Ordinance (Cap. 221) (i.e. $100,000) and by imprisonment for up to 2 years. On conviction on indictment, we consider that the fine should rise to a maximum of $1,000,000 and by imprisonment for up to 5 years.

Legislative Proposals

66. In the UEM Bill, we propose to specify that –

(a) no person shall supply or offer to supply address-harvesting software, a harvested-address list, or a right to use them to another person, subject to a defence that he has no reason to suspect that the acquirer of the address-harvesting software, harvested-address list or the right intended to use them in connection with the sending of commercial electronic messages in contravention of the requirements of the opt-out regime;

(b) no person shall acquire address-harvesting software, a harvested-address list, or a right to use them for use in connection with, or to facilitate, the sending of commercial electronic messages in contravention of the requirements of

the opt-out regime;

(c) no person shall use address-harvesting software or a harvested-address list in connection with the sending of commercial electronic messages in contravention of the requirements of the opt-out regime. The act of forwarding address-harvesting software or a harvested-address list to another person or organisation should be caught by (a) above and should not constitute a "use" of such software or address list;

(d) a contravention of the above requirements is an offence and a person who commits such an offence is liable –

(i) on summary conviction, to a fine at level 6 as prescribed in Schedule 8 of the Criminal Procedure Ordinance (Cap. 221) (i.e. $100,000) and to imprisonment for 2 years; or

(ii) on conviction on indictment, to a fine of $1,000,000 and to imprisonment for 5 years.

We wish to seek comments on the above legislative proposals for prescribing the rules about address harvesting.

Part VI Offences Relating to the Sending of Commercial Electronic Messages

67. Apart from harvesting e-mail addresses, spammers may use other techniques to maximise the reach of their messages, e.g., through blasting such messages indiscriminately with a view to identifying the genuine addresses, using different, multiple electronic addresses for sending messages with a view to getting as many messages through as possible before spam filters kick in to block the sources, and seeking open facilities from which electronic messages can be sent to avoid identification and possibly blocking. Illicit spammers may even use fraud or related means with clear malicious intent. We have drawn reference to the anti-spam legislation of different overseas jurisdictions in putting forward the following proposals.

68. Where the offences in this part are linked to the transmission of "multiple" commercial electronic messages, we propose to adopt a benchmark for defining "multiple" similar to that prescribed in the US CAN-SPAM Act[24] and Singapore's proposed Spam Control Bill[25] at –

(a) more than 100 commercial electronic messages during a 24-hour period; or

(b) more than 1,000 commercial electronic messages during a 30-day period.

<u>Sending commercial electronic messages to electronic addresses obtained by automated means</u>

69. Apart from harvested address lists, spammers can also generate electronic address lists automatically by combining names, letters, characters, numbers or symbols and then sending out commercial electronic messages to those address lists (so-called "dictionary attacks"). The purpose of spammers in launching dictionary attacks is not only to get as many commercial electronic messages through to recipients as possible, but also to identify genuine electronic addresses which can then be made targets for subsequent spamming activities. We are thus of the view that sending a commercial electronic message to an electronic address obtained through dictionary attacks should be prescribed as an offence. Penalties should be of the same magnitude as that for supplying, acquiring or using address-harvesting software or harvested-address lists, at a fine at level 6 (i.e. $100,000) and

[24] Section 4(a)
[25] Section 6(1)

imprisonment for 2 years on summary conviction, and at a fine of $1,000,000 and imprisonment of 5 years on conviction on indictment.

Use of scripts or other automated means to register for multiple e-mail addresses

70. In order to bypass spam filters before spamming activities are detected, some spammers use scripts or other automated means to register for multiple e-mail addresses which can then be used for spamming activities (so-called "automatic throwaway accounts"). There is a specific provision in the US CAN-SPAM Act[26] prohibiting the use of scripts or other automated means to register for multiple e-mail accounts or online user accounts from which to transmit a commercial electronic message that is unlawful under that Act. We propose to introduce a similar provision in the UEM Bill. We propose that the penalty should be the same as for dictionary attacks above.

71. We note that there may be circumstances where system administrators of an internal information system of an organisation, or providers of public telecommunications services, may use automated means to create multiple e-mail addresses in the course of performing their functions for their clients. These circumstances should be exempted from the above prohibition.

Relay or re-transmission of commercial electronic message without authorisation

72. Another common technique used by spammers is to send spam e-mails through open relays[27] or open proxies[28] on the Internet, thereby enabling them to hide behind those facilities and to disguise the real origin of the messages. Although most system administrators recognise the threat and secure their relays and proxies accordingly, unprotected open relays and open proxies are still common. For example, in some places with very limited Internet infrastructure, open relays may be set up for the entire local community to use e-mail services. Just because these facilities exist should not mean that spammers should be allowed to abuse them.

73. In the US CAN-SPAM Act[29], there is a specific provision prohibiting any person from knowingly relaying or retransmitting a

---

[26] Section 5(b)(2)
[27] E-mail servers configured in such as way that allow anyone on the Internet to send e-mail through it.
[28] Proxy servers which are accessible by anyone outside the authorised group, i.e. virtually any Internet users.
[29] Section 5(b)(3)

commercial electronic e-mail message that is unlawful under the Act from a computer or network that the person has accessed without authorisation. We propose to adopt a similar provision in the UEM Bill. With regard to the penalty for a contravention, we propose the same treatment as for dictionary attacks mentioned in paragraph 69 above.

Fraud and related activities in connection with sending electronic messages

74. The US CAN-SPAM Act prohibits 5 types of fraud and related activities that occur in connection with e-mails[30]. We propose to introduce similar provisions in the UEM Bill with the effect of prohibiting –

(a) hacking into a computer or telecommunications device, service or network, or obtaining similar unauthorised access, and subsequently transmitting multiple commercial electronic messages from those facilities;

(b) sending multiple commercial electronic messages from a computer or telecommunications device, service or network without authorisation (e.g., through zombie computers) in order to mislead recipients as to the origin of such messages and prevent blocking by spam filters;

(c) falsifying or withholding header information (e.g., e-mail spoofing[31]) and transmitting multiple commercial electronic messages, again to mislead the recipient as the origin of the message and to prevent blocking by spam filters. However, it is generally accepted by the community that Internet e-mail users may not always use real names in identifying themselves. Although such identification entered by the sender of an e-mail is part of an e-mail header, we consider that not using one's real name should not constitute an offence. Thus, we propose that the offence in respect of the header information of e-mail messages should be confined to acts of falsifying the part of e-mail header associated with the originating domain name, IP address and e-mail address inserted by e-mail servers automatically as routing information, but should exclude the content in the Simple Mail Transfer Protocol[32] data portion that is normally

[30] Section 4(a)
[31] Disguising that the e-mail comes from someone else.
[32] Also known by the acronym of SMTP

entered by e-mail users themselves;

(d) registering for 5 or more electronic addresses or 2 or more domain names, using a false identity or withholding the identity, and intentionally transmitting multiple commercial electronic messages using such electronic addresses or domain names;

(e) falsely representing himself to be the registrant of 5 or more electronic addresses or 2 or more domain names, and intentionally transmitting multiple commercial electronic messages.

75. Given the dishonest intent underlying such offences and the adverse implications of acts involved, we consider that the penalty should be comparable to the penalty for the existing offences under the Crimes Ordinance (Cap. 200) relating to obtaining access to a computer with criminal or dishonest intent[33] and the destruction or damage of property without lawful excuse[34]. We propose that offenders should be liable on conviction on indictment to a fine of an amount to be determined by the Court[35] and to imprisonment for 10 years.

Legislative Proposals

76. In the UEM Bill, we propose to specify that –

(a) no person shall send, or cause to be sent, a commercial electronic message that has a Hong Kong link to an electronic address if he believes that the electronic address was obtained or provided or made available using an automated means that generates possible electronic addresses by combining names, letters, characters, numbers or symbols into numerous permutations;

(b) no person shall use scripts (meaning a list of instructions to an information system that can be executed without user interaction) or other automated means to register for 5 or more electronic addresses from which to send, or enable

---

[33] Section 161
[34] Section 60
[35] Section 101F of the Criminal Procedure Ordinance (Cap. 221) provides that where an Ordinance prescribes a "penalty" for an offence and the amount of the fine is unspecified, that such offence shall, without prejudice to any law against excessive or unreasonable fines or assessments, be punishable by a fine of any amount.

another person to send, multiple commercial electronic addresses (meaning more than 100 commercial electronic messages during a 24-hour period or more than 1,000 commercial electronic messages during a 30-day period), but this requirement does not apply to a system administrator responsible for the administration of internal information systems of an organisation when performing his duties or a telecommunications service provider responsible for the provision of a public telecommunications service;

(c) no person shall knowingly send, or cause to be sent, a commercial email message that has a Hong Kong link from a computer or a telecommunication device, service or network through open relays or open proxies designed to hide the true identity of the original sender;;

(d) no person shall, for the purpose of sending commercial electronic messages that has a Hong Kong link to another person, knowingly –

(i) access a computer or telecommunications device, service or network without authorisation and intentionally initiate the transmission of multiple commercial electronic messages from or through such computer or telecommunications device, service or network;

(ii) send, or cause to be sent, multiple commercial electronic messages from or through a computer or telecommunications device, service or network without authorisation, with the intent to deceive or mislead recipients as to the origin of such messages;

(iii) materially falsify or alter the part of header information which is machine-generated automatically (meaning to alter or conceal header information in a commercial electronic message in such manner as to impair the ability of the recipient of the message, a telecommunications service provider processing the message or any other person to identify, locate or respond to the person who initiated the message) in multiple commercial electronic messages and intentionally initiate the transmission of such messages;

(iv) register, using information that materially falsifies the identity of the actual registrant, for 5 or more electronic addresses or 2 or more domain names, and intentionally initiate the transmission of multiple commercial electronic messages from any combination of such electronic addresses or domain names;

(v) falsely represent himself to be the registrant or the legitimate successor in interest to the registrant of 5 or more electronic addresses or 2 or more domain names, and intentionally initiate the transmission of multiple commercial electronic messages from any combination of such electronic addresses or domain names.

77. We propose to specify in the UEM Bill that any person who contravenes –

- paragraphs 76(a), (b) or (c) above commits an offence and is liable, on summary conviction, to a fine at level 6 (i.e. $100,000) and to imprisonment for 2 years, or on conviction on indictment, to a fine of $1,000,000 and to imprisonment for 5 years;

- paragraphs 76(d)(i), (ii), (iii), (iv) or (v) above commits an offence and is liable on conviction on indictment to a fine of any amount as determined by the Court and to imprisonment for 10 years.

We wish to seek comments on the above legislative proposals for prescribing offences relating to the sending of commercial electronic messages.

Part VII Compensation

78. Although the Government will take up the primary responsibility for carrying out investigations, taking enforcement actions, and commencing legal actions for contraventions of the UEM Bill, some persons may suffer losses as a result of another person's acts that are in contravention of the UEM Bill. We propose to set out in the UEM Bill the right of a victim to seek in the court compensation or other remedies from a person who has contravened the UEM Bill. We propose that the range of possible remedies include –

(a) an order that the person who contravened the UEM Bill shall not repeat or continue such conduct or act;

(b) an order that the person who contravened that UEM Bill shall perform any reasonable act or course of conduct to redress any loss or damage suffered by the victim;

(c) an order that the person who contravened the UEM Bill pay to the victim compensation by way of damages for the pecuniary loss suffered by reason of the contravention; and

(d) an injunction or any other appropriate remedy, order or relief against the person who contravened the UEM Bill.

79. We recognise that certain contraventions might have occurred despite the best efforts expended to prevent their occurrence. We therefore propose to make clear that, for the purpose of a person seeking compensation or any other remedy from another person by virtue of this part, it shall be a defence for the second-mentioned person to prove that he had taken such care as in all the circumstances was reasonably required to avoid the contravention concerned.

80. We also propose to make clear that nothing in this part shall affect, limit or diminish any rights or privileges, obligations or liabilities conferred or imposed on a person under any enactment or rule of law. If, for example, a person has a right under the common law to seek compensation for loss or damage caused by another person, it is our intention that he should still be entitled to take such civil action irrespective of the provisions in the UEM Bill.

81. For civil claims under this part, we propose that the Limitation Ordinance (Cap. 347) shall apply, with necessary modifications, to a claim under this part in the same manner as it applies

to an action founded on tort. Specifically, a limitation period of 6 years will apply to civil claims under this UEM Bill.

Legislative Proposal

82. We propose to specify in the UEM Bill that –

(a) a person ("the respondent") who contravenes any of the provisions in the UEM Bill shall be liable to compensation by way of damages to any other person ("the claimant") for the pecuniary loss sustained by the other person as a result of the contravention in circumstances where it would be fair, just and reasonable to do so;

(b) proceedings in (a) shall be brought in the District Court but all such remedies shall be obtainable in such proceedings as would be obtainable in the Court of First Instance;

(c) in proceedings in (a), the District Court may –

(i) make a declaration that the respondent has engaged in conduct, or committed an act, that is a contravention of the UEM Bill, and order that the respondent shall not repeat or continue such conduct or act;

(ii) order that the respondent shall perform any reasonable act or course of conduct to redress any loss or damage suffered by the claimant;

(iii) order that the respondent pay to the claimant compensation by way of damages for the pecuniary loss suffered by reason of the respondent's conduct or act;

(iv) grant an injunction or any other appropriate remedy, order or relief against the person who committed the contravention;

(d) the District Court shall have jurisdiction to hear and determine any proceedings under (c) above and shall have all the powers as are necessary or expedient for it to have in order to provide, grant or make any remedy, injunction or order mentioned in this UEM Bill;

(e) nothing in this part affects, limits or diminishes any rights or privileges, obligations or liabilities conferred or imposed on a person under any enactment or rule of law;

(f) in any proceedings brought against any person by virtue of this part, it shall be a defence for that person to prove that he had taken such care as in all the circumstances was reasonably required to avoid the contravention concerned; and

(g) the Limitation Ordinance (Cap. 347) shall apply, with necessary modifications, to a claim under this part in the same manner as it applies to an action founded on tort.

We wish to seek comments on the above legislative proposals for prescribing compensation.

Part VIII Powers for Investigation

83. We propose that the TA would be responsible for enforcing the UEM Bill, except for fraud and related activities in connection with sending commercial electronic activities (i.e., para. 76(d) in Part VI) which will be enforced by the Hong Kong Police Force alongside with their action in respect of other computer crimes. The TA would require specific powers to enable him to undertake investigations. We therefore propose that the UEM Bill confer the following powers on the TA –

(a) the power to obtain from any person information or documents relevant to the TA's investigation of a contravention or suspected contravention of a provision in the UEM Bill; and

(b) the power to enter premises and to seize, remove or detain any computers, telecommunications device, documents or any other things upon obtaining a warrant from a magistrate.

84. Other proposed provisions related to the above powers are –

(a) the power of the TA to call upon other public officers to assist him to exercise his powers for investigation;

(b) the obligation of the TA not to disclose any information or document provided to him for investigation unless it is in the public interest to do so or the person providing any information or document has been given the opportunity to make representation on the proposed disclosure of the information or document;

(c) failure to provide the information or document to the TA shall be an offence liable on conviction to a fine at level 5 (i.e. $50,000) and to imprisonment for 2 years; and

(d) the power of the Court to order a convicted person to pay to the TA the whole or a part of the costs and expenses of the investigation and the power of the TA to recover such costs and expenses as a civil debt.

Legislative Proposals

85. We propose to specify in the UEM Bill that –

(a) if the TA is satisfied that there are reasonable grounds for believing that a person is, or is likely to be, in possession of information or a document that is relevant to the TA's investigation of a contravention or suspected contravention of a provision of the Bill, the TA may serve a notice in writing on that person requesting the person to give the information in writing to the TA or produce the document to the TA as the case requires, before a specified date. But the notice should also give the person an opportunity to make representations, which will be duly considered by the TA, as to the reason why he cannot or does not wish to comply with the request;

(b) if the TA maintains his request in (a) after considering the representation, and the person still has not complied with the notice, a magistrate may issue an order that the person shall give the information or document to the TA within a specified timeframe;

(c) the TA shall not disclose any information or document given or produced to him under this section except subject to the requirement in (d) and if the TA considers that it is in the public interest to disclose that information or document;

(d) the TA shall give a person giving or producing any information or document a reasonable opportunity to make representations on a proposed disclosure of the information or document and shall consider all representations made to him before he makes a final decision to disclose the information or document;

(e) for the avoidance of doubt, where a person gives or produces any information or document notwithstanding that the information or document is the subject of a confidentiality agreement with another person, the first-mentioned person shall not be liable for any civil liability or claim in respect of the giving or production of that information contrary to that agreement;

(f) a person shall not be required to give any information or document, or produce any document, which the person could not be compelled to give in evidence, or produce, in civil proceedings before the Court of First Instance;

(g) a person commits an offence if he, without reasonable excuse –

(i) fails to comply with an order issued by a magistrate under (b) above; or
(ii) claims to have complied with a notice issued by the TA under (a) or an order issued by a magistrate under (b), knowingly gives information that is false or misleading;

and he shall be liable on conviction to a fine at level 5 (i.e. $50,000) and to imprisonment for 2 years;

(h) if a magistrate is satisfied by information on oath that there are reasonable grounds for suspecting that there is in any place any device or thing which may be seized, removed or detailed, he may issue a warrant authorising the TA or an authorised officer to enter and search the place;

(i) with the warrant in (h), the TA or an authorised officer may enter and search the premises in which he reasonably suspects there is any thing which appears to him to be or to contain evidence of a contravention under the UEM Bill, and seize, remove or detain that thing. The TA or an authorised officer may call upon other public officers to assist him in the exercise of his powers;

(j) where any person is convicted by a court on a prosecution instituted as a result of an investigation by the TA, the court may order the person to pay to the TA the whole or a part of the costs and expenses of the investigation and the TA may recover the whole or the part of the costs and expenses as a civil debt due to him.

We wish to seek comments on the above legislative proposals for prescribing powers for investigation.

Part IX Other Provisions

86. Supplementary provisions will be needed to support the functioning of the various rules, requirements and offences set out in earlier parts of this paper. The proposed supplementary provisions are described below.

Obstruction, etc., of the TA, authorised officers and other persons

87. The UEM Bill should afford protection to the TA, his authorised officers or any other persons called in to help them discharge their duties. We therefore propose to make it an offence for anyone who obstructs, hinders or resists such persons, fails to comply with their lawful requirements, knowingly makes a statement that misleads them or fails to give them any assistance which they reasonably require for the purpose of exercising their powers and performing their duties under the UEM Bill. Drawing on similar provisions in the Personal Data (Privacy) Ordinance (Cap. 486)[36], we consider that the appropriate penalty for such offences should be a fine at level 3 ($10,000) and imprisonment of 6 months.

Immunity for the TA, authorised officers and other persons

88. We propose to make clear that the TA, authorised officers and other persons called upon to assist them should not be held personally liable for their actions when they are performing their functions under the UEM Bill and are acting in good faith. Similar provisions are found in the Telecommunications Ordinance (Cap. 106)[37]. Of course, if any party is aggrieved by the act of the TA, authorised officers and other persons while they are performing their official duties, they could also make civil claims against the Government.

Liability of employers and principals

89. As contraventions may be committed by employees or agents on the instructions of their employers or principals respectively, similar to the Personal Data (Privacy) Ordinance (Cap. 486)[38], we consider it necessary to make clear that acts done or practices engaged in by a person in the course of employment (in the case of an employee) or with the authority of his principal (in the case of an agent), the acts done or practices engaged in should be considered as being done or engaged in

---

[36] Section 64(9)
[37] Section 39B
[38] Section 65

by the employer or principal as well as by the employee or agent. However, a defence should be provided to the employers and principals if they can prove that they have taken such steps as were practicable to prevent the employee or agent from doing that act or engaging in that practice in the course of their employment or authority. For example, if an employer has promulgated a clear company policy, and has regularly circulated such policy to all employees as a reminder, that commercial electronic messages must not be sent to telephone numbers on a do-not-call register, and has never requested any employees to do so, then it might be a justifiable defence for the employer should an employee ignore this policy and commit an offence under the UEM Bill.

Liability of persons other than principal offender

90. We also consider it necessary to clarify the liability of persons other than the principal offender. Modeling on the requirements in the Broadcasting Ordinance (Cap. 562)[39], we suggest that the UEM Bill should make clear that if a company, other body corporate or a partnership has committed an offence, a director of the company or a body corporate, or a partner of the partnership at the time when the offence was committed shall also be presumed to have done the act that committed the offence. But it should be a defence for such a director of company or body corporate or a partnership of a partnership to provide evidence that he did not authorise the act to be done.

Liability of telecommunications service provider

91. If a telecommunications service provider provides a service to a person who uses the service to send a commercial electronic message in contravention of the UEM Bill, we consider that the telecommunications service provider, who is merely providing a service and exercise no control over the content or use of such service, should not be treated as if it has sent, or has caused to be sent, the message. There is a similar provision in the Spam Act 2003 of Australia[40].

Liability of owners of computers or telecommunications device, service or networks

92. There may be circumstances when spammers take control (physical control or remote control through software or other means) of a computer or telecommunications device, service or network and commit an offence under the UEM Bill. For example, a spammer may install a

[39] Section 6(4)
[40] Section 9

Trojan program in a person's home computer thereby enabling the spammer to send a large number of commercial electronic messages from that computer (i.e., a zombie computer), with the owner of the computer totally unaware of such acts. We do not consider that such owners should be held liable for such acts and suggest that the UEM Bill should make clear that those messages should not be considered to be sent, or caused to be sent, by such owners.

Regulations

93. While the UEM Bill provides a broad framework for the regulation of sending commercial electronic messages and prescribes the offences, some details of the regulatory framework may need to be prescribed. We propose that the Secretary for Commerce, Industry and Technology (SCIT) should be empowered to make regulations to give full effect to the UEM Bill and for its due administration. While we do not envisage such power to be used frequently, the availability of such power would enable SCIT to respond quickly to technology changes in order to ensure that the objectives of the UEM Bill would not be compromised.

Codes of practice

94. Similarly, for effective implementation of the regulatory regime under the UEM Bill, practical guidance on operational details may need to be provided to e-marketers by the regulator, having regard to the prevailing technologies and other considerations. Such guidance should best be promulgated by way of codes of practice. We intend to empower the TA to promulgate such codes and require the TA to publish them in the Gazette for public information.

95. Failure to comply with the codes should not of itself be an offence or lead to civil or criminal proceedings. However, we propose that during court proceedings, if the court considers that a provision of a code is relevant to the determination of a matter, then such code should be admissible in evidence. In addition, we propose that proof that a person has contravened, or did not contravene, a relevant provision of a code, may be relied on in the proceedings to assist the court to decide on the matter in question.

Commencement date

96. We propose to specify that the commencement date of the UEM Bill should be prescribed by SCIT by a notice in the Gazette so as to allow time for SMEs and e-marketers to prepare themselves for

compliance with the legislation. They would need to set up a system to operate the opt-out regime by gearing up their equipment and training up their staff. To provide flexibility, we suggest that different parts of the UEM Bill may be commenced on different dates.

Consequential amendments to other enactments

97. The TA is currently responsible only for the administration of the Telecommunications Ordinance (Cap. 106). His powers to regulate telecommunications licensees is also be related to the administration of that ordinance. There is a need to revise the Telecommunications Ordinance (Cap. 106) to prescribe that the TA's powers under this Ordinance may also be exercised to support the implementation of the UEM Bill, including the power to require the licensees under the Telecommunications Ordinance (Cap. 106) to implement measures or take steps in support of the TA's functions under the UEM Bill.

98. Section 24 of the Telecommunications Ordinance provides that a person performing a telecommunications service shall be guilty of an offence if he wilfully destroys, alters, intercepts, or abstains from transmitting any message. We consider it opportune to clarify beyond doubt that this section does not apply to acts done for the purpose of facilitating compliance with the UEM Bill or any other law (e.g. for implementing a spam filter to block electronic messages contravening the UEM Bill) or implement the terms of contract made between a telecommunications service provider and its customer (e.g. to provide service for blocking telephone calls from callers not revealing their originating telephone numbers).

99. The Resolution for the establishment of the OFTA Trading Fund prescribes the services which the TA needs to perform as provided currently under the various legislation. The Resolution would need to be revised to expand the scope of the services to be provided under the OFTA Trading Fund to encompass the TA's work under the UEM Bill.

Legislative Proposals

100. In the UEM Bill, we propose to specify that –

(a) any person who -

(i) without lawful excuse, obstructs, hinders or resists the

TA, an authorised officer or any other person in the performance of his functions or the exercise of his powers during investigation;

(ii) without lawful excuse, fails to comply with any lawful requirement of the TA, an authorised officer or any other person during investigation;

(iii) makes a statement which he knows to be false or does not believe to be true, or otherwise knowingly misleads the TA, an authorised officer or any other person in the performance of his functions or the exercise of his powers during investigation;

(iv) without reasonable excuse, fails to give the TA or an authorised officer or any other person any assistance which he may reasonably require to be given for the purpose of exercising his powers or performing his duties under the UEM Bill

commits an offence and is liable on conviction to a fine at level 3 (i.e. $10,000) and to imprisonment for 6 months;

(b) the TA, his authorised officer, or any other public officers assisting the TA or his authorised officer, acting in good faith, shall not be personally liable for any civil liability or claim whatever in respect of any act done or default made in the performance of any function, or the exercise of any power under the UEM Bill;

(c) any act done or practice engaged in by a person in the course of his employment shall be treated for the purposes of the UEM Bill as done or engaged in by his employer as well as by him, whether or not it was done or engaged in with the employer's knowledge or approval;

(d) any act done or practice engaged in by a person as agent for another person with the authority (whether express or implied, and whether precedent or subsequent) of that other person shall be treated for the purposes of the UEM Bill as done or engaged in by that other person as well as by him;

(e) in proceedings brought under the UEM Bill against any person in respect of an act or practice alleged to have been

done or been engaged in, as the case may be, by an employee of his, it shall be a defence for that person to prove that he took such steps as were practicable to prevent the employee or contractor of his from doing that act or engaging in that practice, or from doing or engaging in, in the course of his employment or authority, acts or practices, as the case may be, of that description;

(f) where a company, other body corporate or a partnership has committed an offence under the UEM Bill, any person who was a director of the company or body corporate, or a partner of the partnership at the time when the offence was committed shall, unless there is evidence to the contrary that he did not authorise the act to be done, be presumed also to have done the act;

(g) a telecommunications service provider who merely provides a service that enables a commercial electronic message to be sent shall not be taken to have sent or caused to have sent the message;

(h) if a computer or telecommunications device, service or network is controlled by a third party whether by physical possession or by possession of control through software or other means unknowing to the owners of such computer or telecommunications device, service or network, the owners of such computer or telecommunications device, service or network that enables a commercial electronic message to be sent shall not be taken to have sent or caused to be sent the message;

(i) a transaction is not void or voidable by reason only that a contravention of any of the provisions of the UEM Bill has take place in relation to or as a result of it;

(j) the Secretary for Commerce, Industry and Technology may make regulations providing for such matters as are contemplated by, or necessary for giving full effect to, the provisions of the UEM Bill and for their due administration;

(k) for the purpose of providing practical guidance in respect of any section of the UEM Bill, the TA may approve and issue such codes of practice as in his opinion are suitable for that purpose and by notice in the Gazette, identify the code

concerned, specify the date on which its approval is to take effect and specify for which of the sections of the UEM Bill the code is so approved. A code of practice is not subsidiary legislation for the purpose of Part V of the Interpretation and General Clauses Ordinance (Cap. 1);

(l) a failure on the part of any person to observe any provision of an approved code of practice shall not of itself render that person liable to legal proceedings of any kind, whether civil or criminal. However, if in any legal proceedings, the court is satisfied that a provision of an approved code of practice is relevant to determining a matter that is in issue in the proceedings, the code of practice is admissible in evidence in the proceedings and proof that the person contravened or did not contravene a relevant provision of the code of practice may be relied on by any party to the proceedings as tending to establish or negate that matter;

(m) the UEM Bill shall come into operation on a date to be appointed by the Secretary for Commerce, Industry and Technology by notice in the Gazette. The Secretary may appoint different dates for different sections of the UEM Bill to come into effect; and

(n) the enactments referred to below are to be amended –

(i) Section 6A(1) of the Telecommunications Ordinance (Cap. 106) is amended by adding "or any other Ordinance" after "this Ordinance";

(ii) Section 6A(3) of the Telecommunications Ordinance (Cap. 106) is amended by adding "or any other Ordinance" after "this Ordinance" whenever it appears;

(iii) Section 24 of the Telecommunications Ordinance (Cap. 106) is renumbered as section 24(1) and a new section 24(2) added as follows –

"(2) This section does not apply to any act done for the purpose of (a) facilitating compliance with the Unsolicited Electronic Messages Ordinance or any other law; or (b) implementing the terms of any contract made between a telecommunications service provider and a customer of the telecommunications service

provider."

(iv) Schedule 1 to the Office of the Telecommunications Authority Trading Fund Resolution (Cap. 430 sub. leg. D) is amended by repealing "and the Telephone Ordinance (Cap. 269)" and substituting ", the Telephone Ordinance (Cap. 269) and the Unsolicited Electronic Messages Ordinance."

We wish to seek comments on the above legislative proposals for prescribing other provisions supporting the implementation of the Bill.

Communications and Technology Branch
Commerce, Industry and Technology Bureau
January 2006

Annex A

Measures under the STEPS Campaign

"S" – Strengthening Existing Regulatory Measures

(1) Junk fax

The Government has worked with the fixed telecommunications network service (FTNS) providers to revise the Code of Practice on Procedures for Handling Complaints against Senders of Unsolicited Fax Advertisements in July 2005. Under the revised voluntary code, FTNS operators will disconnect all the fax lines provided to a subscriber at the same registered address if there are two established complaints (for not respecting the "not-to-call" list of fax numbers). In the past, fax lines would be terminated if there were three established complaints.

(2) Short Messaging Service (SMS)/Multi-media Messaging Service (MMS)

Apart from the six mobile operators, all seven mobile virtual network operators (MVNOs) and PCCW-HKT Telephone Ltd, the only FTNS operator currently providing fixed line SMS, have agreed to follow the existing voluntary code of practice on Handling of Unsolicited Promotional Inter-Operators Short Message Service (IOSMS).

(3) Pre-recorded voice messages

With a view to tackling the problem of spam phone calls arising from the use of automated machines such as the Interactive Voice Response System (IVRS), the Government is discussing with telecommunications operators on the establishment of an industry code of practice for their voluntary compliance. The draft has been prepared for comments by the telecommunications operators. Subject to the support of telecommunications operators, the Government would finalise the details of the code in the near future.

"T" – Technical Solutions

(1) Anti-spam website

The Government launched a dedicated anti-spam website (www.antispam.gov.hk) in May 2005. The website is regularly updated with latest anti-spam information, including user tips, best practices, technical solutions and relevant publications/press releases.

(2) Information security seminars/conferences

In 2005, Government representatives attended and contributed in various information security seminars/conferences to promote the use of technical solutions to contain the spam problem. Below were the industry events that the Government has participated in:-

- "Hong Kong Clean PC Day" Seminar;
- Information Security Summit 2005;
- Anti-spam Seminar "Key Challenges in Combating Spam";
- Anti-spam Talks for Tung Wah Group of Hospitals' Cyber World;
- Information Security Forum 2005;
- The 6th Info-Security Conference 2005;
- The 4th IT Directors' Meeting; and
- Hong Kong IBM User Group's Special Interest Group seminar "Sharpening Security Strategy: Case Studies in Spamming, Spyware and Wireless Threats"

The Government will continue to collaborate with the industry to organise seminars, conferences and exhibitions to promote the latest anti-spam technical solutions to all users. Specifically, a technical conference will be arranged in March 2006.

"E" – Education

(1) Anti-spam radio episodes

With a view to enhancing public awareness of the spam problem, two

series of 1-minute radio episodes, targeting at different sectors of the community, have been produced and started broadcast since April 2005.

(2) Roving exhibitions

Two rounds of roving exhibitions have been organised at popular shopping malls in Hong Kong, Kowloon and the New Territories. The exhibitions have featured nine display panels on the following subjects:-

(a) What is spam;
(b) How does spam affect the community;
(c) STEPS campaign;
(d) Anti-spam legislation;
(e) User tips: e-mail spam;
(f) User tips: fax spam;
(g) User tips: SMS and promotional calls;
(h) Guidelines for e-marketers; and
(i) Three smart tips to clean your PC.

(3) Anti-spam leaflets

An information leaflet setting out the anti-spam user tips has been produced and distributed to the public through various channels since August 2005. The leaflets have also been distributed to primary and secondary schools as supplementary teaching materials.

(4) Teaching materials for students and youngsters

A CD-ROM containing teaching materials to youngsters and students has been produced and was distributed to youth centres, and all primary and secondary schools in Hong Kong in August and September 2005 respectively. The same information has also been uploaded to the anti-spam website for reference by the general public.

(5) Seminars and workshops for business organisations

Since December 2005, the Government has started to collaborate

with different business associations to organise anti-spam briefing sessions for their members. Our aims are to explain to businesses the importance of information security and spam prevention, introduce relevant tools to them, and remind them on how they could avoid becoming spammers themselves.

"P" – Partnerships

(1) International partnerships

The Commerce, Industry and Technology Bureau has become one of the Founding Signatories of the Seoul-Melbourne Multilateral Memorandum of Understanding on Co-operation in Countering Spam (MoU). The MoU, established in April 2005, is geared towards cooperation and information sharing on technological, policy and educational solutions to spam and provides a platform for working level cooperation and information exchange among anti-spam agencies of Asia-Pacific signatories. Three MoU meetings were held in 2005. Below are the two key initiatives under discussion.

(a) The Internet Security Initiative (ISI) proposed by Australia – The Australian Communications and Media Authority (ACMA) has developed and is trialing a program that finds zombie computers on the Australian Internet. Under the trial program, ACMA will supply the Internet Service Providers (ISPs) involved in the trial with a list of infected Internet addresses on their networks periodically such that the ISPs may then contact and advise customers with infected computers on what they may need to do to fix the problem. The Government has informed HKISPA of this initiative, and HKISPA has been encouraging its members to take part in the trial and is considering if a similar protocol with local ISPs should be established.

(b) The Real-Time Blocking List (RBL) Project initiated by Korea – This involves a system to gather spam blocking information from the major webmail services, international spam block list, and spam information detected by anti-virus companies. Equipped with the capabilities for data analysis and categorisation, the

system is able to general real-time blocking lists for use by parties which subscribe to such. While the system is currently only available in Korea, the Korea Information Security Agency intends to expand the provision of the RBL available to other member economies under the MoU.

The Government attended the 6th APEC Ministerial Meeting on Telecommunications and Information Industry (TELMIN 6) in June 2005 when a set of anti-spam guidelines was endorsed.

(2) Local partnerships

The Government is working with the Hong Kong Internet Service Providers Association (HKISPA) to introduce various anti-spam measures. For example, HKISPA has revised its Anti-spam – Code of Practice in June 2005 for compliance by its members. In this revised code, HKISPA specifically encouraged its members to participate in cooperation with the Internet community of Hong Kong, support the initiatives of the Government, and share information with concerned parties in fighting spam.

HKISPA is also studying the feasibility of developing a common blacklist to filter spam at the local ISP level.

"S" – Statutory Measures

Drawing on the views and ideas received during the public consultation in 2004 and the latest developments, the Government decided to introduce a new anti-spam legislation to contain the problem of unsolicited electronic messages (UEMs). The proposed anti-spam legislation should help regulate the use of electronic messages as the means for promotion and/or sale of products and/or services, prevent Hong Kong from becoming a spam haven sheltering illicit spammers, and facilitate co-operation with law enforcement agencies of economies with similar legislation.

Taking into account the views received during this public consultation, the Government will draw up the Unsolicited Electronic Messages Bill and aim to introduce the Bill into the Legislative Council within 2006.

Annex B

Existing Legislative Provisions on Spamming-Related Activities

(a) If the sending of spam involves unauthorised access to computer by telecommunications (commonly known as hacking), it may be punishable under section 27A of the Telecommunications Ordinance (Cap. 106). (Relevant provision is at **Annex B1**.)

(b) If a spammer sends e-mails to a computer causing it to cease functioning, or in a manner which amounts to "misuse of a computer" as defined in section 59 of the Crimes Ordinance (Cap. 200), he could be liable for an offence under section 59 of the Crimes Ordinance (Cap. 200). Alternatively, he could have committed an offence of criminal damage under section 60 of the Crimes Ordinance (Cap. 200). (Relevant provisions are at **Annex B2**.)

(c) If e-mails are used as vehicles to deceive inadvertent victims (e.g. "419" letters and phishing e-mails), an element of "fraud" may be involved. If proved, this will constitute an offence under section 16A of the Theft Ordinance (Cap. 210). (Relevant provision is at **Annex B3**.)

(d) If the e-mails contain malware (e.g. Trojan programmes, virus, hacking tools etc.) facilitating the sender to gain access to a computer system without authority, then depending on the intent of the person gaining unauthorised access to the computer system, he could have committed an offence under section 27A of the Telecommunications Ordinance (Cap. 106) and/or "access to computer with criminal or dishonest intent" under section 161 of the Crimes Ordinance (Cap. 200). (Relevant provision is at **Annex B4**.)

Chapter:	106	Title:	TELECOMMUNICATIONS ORDINANCE	Gazette Number:	36 of 2000
Section:	**27A**	Heading:	**Unauthorized access to computer by telecommunications**	Version Date:	16/06/2000

(1) Any person who, by telecommunications, knowingly causes a computer to perform any function to obtain unauthorized access to any program or data held in a computer commits an offence and is liable on conviction to a fine of $20000. (Amended 36 of 2000 s. 28)

(2) For the purposes of subsection (1)-

(a) the intent of the person need not be directed at-

(i) any particular program or data;

(ii) a program or data of a particular kind; or

(iii) a program or data held in a particular computer;

(b) access of any kind by a person to any program or data held in a computer is unauthorized if he is not entitled to control access of the kind in question to the program or data held in the computer and-

(i) he has not been authorized to obtain access of the kind in question to the program or data held in the computer by any person who is so entitled;

(ii) he does not believe that he has been so authorized; and

(iii) he does not believe that he would have been so authorized if he had applied for the appropriate authority.

(3) Subsection (1) has effect without prejudice to any law relating to powers of inspection, search or seizure.

(4) Notwithstanding section 26 of the Magistrates Ordinance (Cap 227), proceedings for an offence under this section may be brought at any time within 3 years of the commission of the offence or within 6 months of the discovery of the offence by the prosecutor, whichever period expires first.

(Added 23 of 1993 s. 2)

Annex B2

Chapter:	200	Title:	CRIMES ORDINANCE	Gazette Number:	
Section:	**59**	Heading:	**Interpretation**	Version Date:	30/06/1997

PART VIII

CRIMINAL DAMAGE TO PROPERTY

(1) In this Part, "property" (財產) means-

(a) property of a tangible nature, whether real or personal, including money and-

(i) including wild creatures which have been tamed or are ordinarily kept in captivity, and any other wild creatures or their carcasses if, but only if, they have been reduced into possession which has not been lost or abandoned or are in the course of being reduced into possession; but

(ii) not including mushrooms growing wild on any land or flowers, fruit or foliage of a plant growing wild on any land; or

(b) any program, or data, held in a computer or in a computer storage medium, whether or not the program or data is property of a tangible nature.

In this subsection, "mushroom" (菌類植物) includes any fungus and "plant" (植物) includes any shrub or tree. (Replaced 23 of 1993 s. 3)

(1A)In this Part, "to destroy or damage any property" (摧毀或損壞財產) in relation to a computer includes the misuse of a computer.

In this subsection, "misuse of a computer" (誤用電腦) 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. (Added 23 of 1993 s. 3)

(2) Property shall be treated for the purposes of this Part as belonging to any person-

(a) having the custody or control of it;

(b) having in it any proprietary right or interest (not being an equitable interest arising only from an agreement to transfer or grant an interest); or

(c) having a charge on it.

(3) Where property is subject to a trust, the persons to whom it belongs shall be so treated as including any person having a right to enforce the trust.

(4) Property of a corporation sole shall be so treated as belonging to the corporation notwithstanding a vacancy in the corporation.

(Added 48 of 1972 s. 3)

[cf. 1971 c. 48 s. 10 U.K.]

Chapter:	200	Title:	CRIMES ORDINANCE	Gazette Number:	
Section:	**60**	Heading:	**Destroying or damaging property**	Version Date:	30/06/1997

(1) 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.

(2) A person who without lawful excuse destroys or damages any property, whether belonging to himself or another-

(a) intending to destroy or damage any property or being reckless as to whether any property would be destroyed or damaged; and

(b) intending by the destruction or damage to endanger the life of another or being reckless as to whether the life of another would be thereby endangered,

shall be guilty of an offence.

(3) An offence committed under this section by destroying or damaging property by fire shall be charged as arson.

(Added 48 of 1972 s. 3)

[cf. 1971 c. 48 s. 1 U.K.]

Annex B3

Chapter:	210	Title:	THEFT ORDINANCE	Gazette Number:	45 of 1999
Section:	**16A**	Heading:	**Fraud**	Version Date:	16/07/1999

(1) If any person by any deceit (whether or not the deceit is the sole or main inducement) and with intent to defraud induces another person to commit an act or make an omission, which results either-

(a) in benefit to any person other than the second-mentioned person; or

(b) in prejudice or a substantial risk of prejudice to any person other than the first-mentioned person,

the first-mentioned person commits the offence of fraud and is liable on conviction upon indictment to imprisonment for 14 years.

(2) For the purposes of subsection (1), a person shall be treated as having an intent to defraud if, at the time when he practises the deceit, he intends that he will by the deceit (whether or not the deceit is the sole or main inducement) induce another person to commit an act or make an omission, which will result in either or both of the consequences referred to in paragraphs (a) and (b) of that subsection.

(3) For the purposes of this section-

"act" (作為) and "omission" (不作為) include respectively a series of acts and a series of omissions;

"benefit" (利益) means any financial or proprietary gain, whether temporary or permanent;

"deceit" (欺騙) means any deceit (whether deliberate or reckless) by words or conduct (whether by any act or omission) as to fact or as to law, including a deceit relating to the past, the present or the future and a deceit as to the intentions of the person practising the deceit or of any other person;

"gain" (獲益) includes a gain by keeping what one has, as well as a gain by getting what one has not;

"loss" (損失) includes a loss by not getting what one might get, as well as a loss by parting with what one has;

"prejudice" (不利) means any financial or proprietary loss, whether temporary or permanent.

(4) This section shall not affect or modify the offence at common law of conspiracy to defraud.

(Added 45 of 1999 s. 3)

Annex B4

Chapter:	200	Title:	CRIMES ORDINANCE	Gazette Number:	
Section:	**161**	Heading:	**Access to computer with criminal or dishonest intent**	Version Date:	30/06/1997

(1) Any person who obtains access to a computer-

(a) with 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,

whether on the same occasion as he obtains such access or on any future occasion, commits an offence and is liable on conviction upon indictment to imprisonment for 5 years.

(2) For the purposes of subsection (1) "gain" (獲益) and "loss" (損失) are to be construed as extending not only to gain or loss in money or other property, but as extending to any such gain or loss whether temporary or permanent; and-

(a) "gain" (獲益) includes a gain by keeping what one has, as well as a gain by getting what one has not; and

(b) "loss" (損失) includes a loss by not getting what one might get, as well as a loss by parting with what one has.

(Added 23 of 1993 s. 5)

Annex C

Comparison of Key Features of Spam Control Legislation in Other Jurisdictions

	Australia[1]	United Kingdom[1]	United States[1]	South Korea[1,2]	Japan[1]	Singapore[3]	New Zealand[4]
Relevant legislation	Spam Act 2003 Spam (Consequential Amendments) Act 2003 Spam Regulations 2004 Enforceable industry codes under the Telecommunication Act 1997	Electronic Commerce (EC Directive) Regulations 2002 (ECR 2002) Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR 2003)	CAN-SPAM Act of 2003	Act on Promotion of Information and Communications Network Utilization and Information Protection, etc	The Law on Regulation of Transmission of Specified Electronic Mail (July 2002) Specific commercial transactions law (July 2002)	Spam Control Bill (post consultation review)	Unsolicited Electronic Messages Bill
Definition of spam	The Act uses "commercial electronic messages". S 5(1) defines "electronic messages" to include e-mails, instant messages and messages sent to telephone account. S 6(1) defines "commercial	ECR 2002 uses "unsolicited commercial communications sent by e-mail": reg 8 ECR 2002. PECR 2003 covers use of automated calling systems: reg 19(1), facsimile machines: reg 20(1), calls: reg 21(1) and	The Act uses "commercial electronic mail messages": s 5(a)(4)(A). Definitions of - `electronic mail address': s 3(5); and -'electronic mail message': s 3(6).	Any advertisement information for profit transmitted via e-mail or other media prescribed by Presidential Decree transmitted to a recipient against the recipient's explicit rejection of such information. Any advertisement	The laws use "specified e-mail" or " commercial e-mail", which mean an electronic mail that is sent to people by a person or entity whose purpose is to send an advertisement for profit. The case the people consent to be sent is not included.	The Bill uses "unsolicited commercial electronic messages". Clause 4 defines "electronic message" as a message sent through electronic mail or to a mobile telephone. A message is not an electronic message if it is sent by	The Bill uses "commercial electronic messages" and "promotional electronic messages". The following messages are not electronic messages for the purpose of the Act: - voice calls made using (i) a standard

[1] Modified from information contained in the Joint IDA-AGC Consultation Paper on "Proposed Legislative Framework for the Control of E-mail Spam"
[2] Based on information contained in the revised Act on Promotion of Information and Communications Network Utilization and Information Protection, etc (Dec 2004)
[3] Based on information contained in the 2nd Joint IDA-AGC Consultation Paper on the Proposed Spam Control Bill at http://www.ida.gov.sg/idaweb/doc/download/I2883/2nd_Joint_IDA-AGC_Consultation_Paper.pdf
[4] Based on information contained in Unsolicited Electronic Messages Bill at http://www.brookers.co.nz/bills/new_bills/b052811.pdf

	Australia[1]	United Kingdom[1]	United States[1]	South Korea[1,2]	Japan[1]	Singapore[3]	New Zealand[4]
	electronic message".	electronic mails: reg 22 (1) NB. Some obligations applicable to commercial communications generally		information for profit transmitted via telephone or facsimile to a recipient without the recipient's prior consent.		way of voice call made using a telephone service Clause 3(1) defines "commercial electronic message" Clause 5(1) defines "unsolicited" Clause 6(1) defines "transmission in bulk" Clause 6(2) empowers the Minister to vary the number of electronic messages qualified for the definition of "transmission in bulk"	telephone service; or (ii) voice-over Internet protocol (IP) - fascimiles (See Schedule s5)
Confined to "commercial" electronic messages	Yes	Yes	Yes	Yes (advertisement information for profit)	Yes	Yes. Except Part III (Dictionary attack and address harvesting software), which shall apply to all electronic messages, whether or not they are unsolicited commercial electronic messages. (See Clause 11)	Include both commercial and promotional electronic messages Clause 6 defines the meaning of commercial electronic message. Clause 4(1) defines promotional electronic message
Extra-territorial	Certain provisions of the Act apply to	-	-	-	-	Certain provisions of the Act apply with	Certain provisions of the Act apply with

	Australia[1]	United Kingdom[1]	United States[1]	South Korea[1,2]	Japan[1]	Singapore[3]	New Zealand[4]
jurisdiction	commercial electronic messages with an Australian link, which is defined in s 7.					Singapore link, which is defined in Clause 7(2)	New Zealand link, which is defined in Clause 4(2)
Opt-in vs. opt-out	Opt-in Section 16(1): Unsolicited commercial electronic messages must not be sent: - unless recipient has consented: s 16(2). - consent can be express or inferred: para. 2 of Sch. 2.	Opt-in Person not to transmit unsolicited communications for the purposes of direct marketing by means of electronic mail unless recipient previously consented or sent at recipient's instigation: reg 22(2) PECR 2003. Reg 22(3) PECR 2003: Exceptions: - existing customer or contact details obtained from recipient in previous negotiations; - direct marketing of similar products and services; and - unsubscribe facility at time contact details collected and at each subsequent communication.	Opt-out Prohibition of transmission of commercial electronic messages after objection: s 5(a)(4).	Opt-out for email and other media prescribed by the Presidential Decree Opt-in for telephone and facsimile Art 50 Restrictions on transmission of advertisement information for profit: (1) - any person shall be prohibited from transmitting advertisement information for profit by means of email or other media prescribed by the Presidential Decree against the recipient's explicit rejection of such information. (2) - any person willing to transmit advertisement information for profit to recipient’s telephone or	Opt-out Transmission of specified e-mails or commercial e-mails to person who has requested not to receive them is prohibited.	Opt-Out Prohibition of transmission of commercial electronic messages within 10 business days from the day a recipient submits an unsubscribe request (See Clause 9(3))	Opt-in for unsolicited commercial electronic messages. (See Clause 9) Opt-out for promotional electronic messages (See Clause 10) Opting out of receiving promotional electronic messages takes effect at the end of a period of 5 working days. (See Clause 10(3))

	Australia[1]	United Kingdom[1]	United States[1]	South Korea[1,2]	Japan[1]	Singapore[3]	New Zealand[4]
				facsimile shall obtain the recipient's prior consent			
Valid return e-mail address	Commercial electronic message to include accurate information about how the recipient can readily contact sender: s 17(1)(b).	E-mail communications for the purposes of direct marketing not to be transmitted where valid return address has not been provided: reg 23(b) PECR 2003.	Unlawful to send commercial electronic mail message that contains header information that is materially false or misleading: s 5(a)(1) – - inclusion of return e-mail address: s 5(a)(3). - inclusion of physical address: s 5(a)(5)(iii). Secondary liability for businesses knowingly thus promoted: s 6.	Art 50(4) Restrictions on transmission of advertisement information for profit:- to explicitly indicate the name and contact information of the transmitter.	Unlawful to send specified e-mail or commercial e-mail that contains header information or an email address that is forged	Clause 10(1)d requires an accurate and functional electronic mail address or telephone number by which the sender can be readily contacted.	Commercial electronic messages and promotional electronic messages must include accurate sender information. The message must include accurate information about how the recipient can readily contact that person who sends, or cause to be sent, a commercial electronic message or a promotional electronic message. The information is reasonably likely to be valid for at least 30 days after the message is sent.. (See Clause 11(c), 11(d))
Functional unsubscribe facility	Commercial electronic messages must contain a functional unsubscribe facility: s 18(1).	Simple means of refusing use of contact details for the sending of electronic mail for the purposes of direct marketing to be provided at time contact details initially collected and at time of each	Functional internet-based opt-out mechanism: s 5(a)(3). Inclusion of clear and conspicuous notice of opportunity to opt out: s 5(a)(5)(ii).	Art 50(4) Restrictions on transmission of advertisement information for profit: - to explicitly indicate the matters concerning measures and methods by which receivers may easily express his	(see under Labelling requirements) Specified e-mail and commercial e-mail must include opt-out e-mail address. Labeling which states that the receivers	Clause 9(1) requires that unsolicited messages in bulk must include, for each message: - an electronic mail address, an Internet location address or a telephone number that a recipient may use to	Commercial electronic messages and promotional electronic messages must contain functional unsubscribe facility and the facility is reasonably likely to be functional and valid for at least 30 days after the principal

	Australia[1]	United Kingdom[1]	United States[1]	South Korea[1,2]	Japan[1]	Singapore[3]	New Zealand[4]
		subsequent communication: reg 22(3)(c) PECR 2003. Valid return address to which opt-out request can be sent: reg 23(b) PECR 2003.		intention of rejecting the receipt of transmission.	could request the sender not to re-send the e-mail	submit an unsubscribe request; - a statement to the effect that a recipient may use the electronic mail address, Internet location address or telephone number provided in the unsolicited message to submit an unsubscribe request Clause 9(2) requires that the sender of the unsolicited message shall ensure that the electronic mail address, Internet location address or telephone number is valid and capable of receiving at all times during a period of at least 30 days after the unsolicited message is sent. Clause 9(3) requires that the sender and the person who authorised the sending of unsolicited message shall cease the sending of any further unsolicited messages within 10 business days from the day on which the	message is sent. (See Clause 12(1))

	Australia[1]	United Kingdom[1]	United States[1]	South Korea[1,2]	Japan[1]	Singapore[3]	New Zealand[4]
						unsubscribed request is submitted. Clause 9(4) requires that any person who receives an unsubscribe request shall not disclose any information contained in the unsubscribe request to any other person, except with the consent of the person whose particulars are contained in the unsubscribe request.	
Identify sender	Commercial electronic message to clearly and accurately identify sender: s 17(1)(a).	E-mail for the purposes of direct marketing not to United Kingdom be transmitted where identity of person on whose behalf communication is sent has been disguised or concealed: reg 23(a) PECR 2003. Commercial communications to clearly identify person on whose behalf it is made: reg 7(b) ECR 2002	Line identifying the person initiating the message to United States accurately not to be materially false or misleading: s 5(a)(1)(B) Secondary liability for businesses knowingly thus promoted: s 6.	Art 50(4) Restrictions on transmission of advertisement information for profit:- to indicate the following: - type and major contents of the information transmitted; - name/contact information of the transmitter.	Specified e-mail and commercial e-mail must include the sender's name and address.	Clause 10(1)d requires an accurate and functional electronic mail address or telephone number by which the sender can be readily contacted.	Commercial electronic messages and promotional electronic messages must include accurate sender information. The message must : - clearly and accurately identifies the person who authorised the sending of the message; and - include accurate information about how the recipient can readily contact that person. (See Clause 11(a), 11(b))
Labelling	-	Unsolicited	Prohibition of	Art 11 Ordinance of	Obligation of	Clause 10(1) requires	-

	Australia[1]	United Kingdom[1]	United States[1]	South Korea[1,2]	Japan[1]	Singapore[3]	New Zealand[4]
requirements		commercial communications to be identifiable as such as soon as it is received: reg 8 ECR 2002. Commercial communications to be clearly identifiable as commercial communications: reg 7(a) ECR 2002. Promotional offers, competitions or games and conditions to be clearly identified: s 7(c) & (d) ECR 2002.	deceptive subject headings: s 5(a)(2). Inclusion of identifier that message is an advertisement or solicitation: s 5(a)(5)(i). Requirement to place warning labels on spam containing sexually oriented material: s 5(d).	the Ministry of Information and Communication of the Act: - initials `ADV' must be included in mail header	labeling for senders of specified e-mail or commercial e-mail: 1. Identification as specified e-mail or commercial e-mail; 2. Sender's name/ address; 3. Opt-out e-mail address.	that each unsolicited message shall contain: - a subject title that does not mislead the recipient as to the content of the message; - the letters “<ADV>” with a space before the subject title to clearly identify that the message is an advertisement; and - header information that is not false or misleading.	
Dictionary attacks	Person must not send commercial electronic message to a non- existent electronic address that he has no reason to believe that exists: s 16(6).	-	Prohibition to transmit unlawful commercial electronic mail messages using, or to provide list of addresses obtained through, dictionary attacks: s 5(b)(1)(A)(ii).	Art 50(6) Restrictions on transmission of advertisement information for profit: prohibition on use of technical measures which automatically generate recipients’ contact information such as phone numbers, e-mail addresses, etc. through the combination of numbers, codes and letters.	Prohibition of mail transmission utilizing the program that generates random fictitious e-mail addresses	Clause 12(a) prohibits the use of dictionary attack to send electronic messages.	-

	Australia[1]	United Kingdom[1]	United States[1]	South Korea[1,2]	Japan[1]	Singapore[3]	New Zealand[4]
Address harvesting	Address-harvesting software and harvested-address lists must not be: - Supplied: s 20(1); -Acquired: s 21(1); or - Used: s 22(1).	-	Prohibition to transmit unlawful commercial electronic mail messages using, or to provide list of addresses obtained through, address harvesting: s 5(b)(1)(A)(i).	Art 50-2: Prohibition on collecting email addresses without permission, etc.: - (1) no person shall collect e-mail addresses from the Internet homepages without prior consent of the administrator or the manager by means of programs or other technical devices that make it possible to collect email addresses automatically; - (2) no person shall sell or distribute e-mail addresses that are collected in violation of (1); - (3) no person shall use the e-mail addresses for transmitting information with the knowledge that the prohibition is laid on collection, sale and distribution of such e-mail addresses under (1) and (2) Art 50(4) Restrictions on transmission of advertisement information for	-	Clause 12(b) prohibits the use of address harvesting software to send electronic messages.	Clauses 15, 16, 17 prohibit the supply, acquisition and use of address-harvesting software and harvested-address lists.

	Australia[1]	United Kingdom[1]	United States[1]	South Korea[1,2]	Japan[1]	Singapore[3]	New Zealand[4]
				profit: to indicate source of e-mail address obtained.			
Automated throwaway accounts	-	-	Unlawful to use automated means to register for multiple e-mail accounts from which to transmit unlawful commercial electronic mail messages: s 5(b)(2).	Art 50(6) - shall not take technical measures which automatically create email account with the aim of transmitting the advertisement information for profit	-	-	-
Right to commence legal action	"Victim" i.e. person who has suffered loss or damage, may apply to court for compensation if ACMA has initiated proceedings in the Federal Court, and a contravention of the Act has been found: s 28. Australian Communications and Media Authority (ACMA) may apply to court: ss 26, 28,29.	Person who suffers damage entitled to bring proceedings for compensation: reg 30 PECR 2003.	State Attorney-General may bring civil action: s 7(f). ISP adversely affected may bring civil action: s 7(g).	-	-	Person who has suffered loss or damage may commence an action in a court: Clause 14.	The following people can take legal actions: - any person affected by a civil liability event; - any person who suffers loss or damage as a result of the civil liability event; - service providers; and - the enforcement department (See Clause 23)
Exemptions on telecommuni-cations service providers	A person does not contravene the ancillary provisions (aiding, abetting, counselling, procuring) of the Act	-	-	Art 50-4(1) -every information and communications service provider may take steps to reject the provision of such	Telecommunication service providers could be exempted from providing service to the subscriber who sends	A person does not contravene the ancillary provisions (aiding, abetting, etc) of the Act merely because he provides,	A service provider does not send an electronic message, or cause an electronic message to be sent, or contravene the Bill,

	Australia[1]	United Kingdom[1]	United States[1]	South Korea[1,2]	Japan[1]	Singapore[3]	New Zealand[4]
	merely because the person supplies a carriage service that enables an electronic message to be sent. ss 16(10), 17(6), 18(7)			services, in the event that - transmission or receipt of the advertisement information causes or is feared to cause an impediment to the provision of services; - its user does not want to receive the relevant advertisement information; or - the service provided under contract is used for illegal transmission of the advertisement information	the amount of e-mails with fictitious address and may incur the damage of the facilities etc.	or operates facilities for, online services or network access, or provides services relating to, or provides connections for, the transmission or routing of data. Clause 13(2)	merely because the service provider provides a telecommunications service that enables an electronic message to be sent. (See Clause 20)
Obligation on telecommuni-cations service providers	The upcoming ISP Code will include ISP measures to address spam.	Service providers shall take appropriate technical and organisational measures to safeguard the security of that service, and inform the subscribers of the risk concerned. Reg 5 PECC		Art 50-4(2) and (3) When service provider intends to take steps to reject the provision of service, - include the matters concerning the rejection of the provision of services in the contents of the contract that is concluded with each of the users of such services; and - notify interested persons, etc., including users, who	It is necessary for the Minister to try to advise the Associations composed of telecommunications carriers. concerning the anti-spam solution business.	-	Clause 24 specifies that Service Providers must consider complaints. In considering a complaint, the service provider must have regard to any relevant, generally accepted industry code that applies to the service provider.

	Australia[1]	United Kingdom[1]	United States[1]	South Korea[1,2]	Japan[1]	Singapore[3]	New Zealand[4]
				are provided with the services of the fact.			
Remedies (Civil/Criminal)	The main remedies for breaches of the Act are: - civil penalties: Pt 4 - compensation to victim: s 28 - injunctions: Pt 5.	Compensation for person who suffers damage: reg 30 PECR 2003. Enforcement under Part V of the Data Protection Act 1998: reg 31 PECR 2003. - enforcement notice: reg 32 (failure to comply: offence (s 47))	Enforcement by Federal Trade Commission: - fines & imprisonment: s 4(a) amending s 1037(b) Chapter 47 of title 18, United States Code; and -forfeiture: s 4(a) amending s 1037(c) Chapter 47 of title 18, United States Code. Civil action by States: - injunction: s 7(f)(2); and - statutory damages: s 7(f)(3). Civil action by ISP: -injunction: s 7(g)(1)(A) - damages of actual monetary loss: s 7(g)(1)(B) - statutory damages: s 7(g)(3).	Art 67 Fine for Negligence: - not exceeding 30 million KRW. Art 64 Imprisonment or Fine: - imprisonment for not more than 2 years; or - fine not exceeding 10 million KRW. Art 65 Imprisonment or Fine: - imprisonment for not more than 1 year; or - fine not exceeding 10 million KRW.	Administrative Orders by Minster to keep law. Fines up to 1,000,000 yen or one year imprisonment assessed on failure to observe Administrative Order Fines of up to 1,000,000 yen or one year imprisonment assessed on the sender who disguised the sender's identity	The remedies for breaches of the Act are: - an injunction; - damages; and - statutory damages (See Clause 15)	Civil penalty regime The following people can take legal actions: - any person affected by the civil liability event; - any person who suffers loss or damage as a result of the civil liability event; - service providers; and - the enforcement department (See Clause 23)
Enforcement Agency	Australia Communications and Media Authority (ACMA)	OFCOM for matters under its existing functions as specified under Chapter 1 of the Communications Act 2003	Federal Trade Commission (FTC)	Korea Information Security Agency delegated by Ministry of information and Communication, Korea	Ministry of Internal Affairs and Communications (MIC) Ministry of Economy,	InfoComm Development Authority of Singapore (IDA)	Department of Internal Affairs

	Australia[1]	United Kingdom[1]	United States[1]	South Korea[1,2]	Japan[1]	Singapore[3]	New Zealand[4]
		The Information Commissioner for regulations relating to Data Protection Act 1998			Trade and Industry (METI) National Police Agency		
Persons who may be liable	Sender of commercial electronic messages. Any person who: - aids, abets, counsels or procures a contravention; - induces, whether by threats or promises or otherwise, a contravention; - in any way, directly or indirectly, is knowingly concerned in or party to, a contravention; or - conspires with others to effect a contravention.	Any person transmitting or instigating the transmission of a communication: PECR 2003	Sender of commercial electronic mail message. Any person who initiates/ procures transmission of commercial electronic mail message (s. 5)	Any person transmitting advertisement information for profit.	Sender (including corporation) or seller (including corporation) via commercial e-mail.	Any person who: - aids, abets, counsels or procures a contravention of the Bill; - induces, whether by threats, promises or otherwise, a contravention of the Bill; - is in any way, directly or indirectly, knowingly concerned in, or party to, a contravention; - conspires with others to effect a contravention. (See Clause 13(1))	A person must not: - aid, abet, counsel, or procure a breach; - induce, whether by threats or promises or otherwise, a breach; - be in any way, directly or indirectly, knowingly concerned in, or party to, a breach - conspire with others to effect a breach. (See Clause 19)
Multi-pronged approach	Australian Communications and Media Authority (ACMA) has the following additional functions: - education: s 42(a); - research: s 42(b); and - international co-operative	No formal regulatory framework mandated - but appropriate industry filtering initiatives encouraged.	Technical solution: - black lists - e-mail filters promoted. Self regulation.	Art 50-64 Dissemination of software for blocking advertisement information for profit (1) Minister of Information and Communication may develop and disseminate software	Publication about the state of introduction of anti-spam technology by mobile operators and ISPs.	The specific initiatives under each approach are: (a) Public Education - National Anti-spam Website - IDA Anti-spam Awareness Drive - SiTF Anti-spam	Multi-pronged approach including: - existing legislation; - self-regulation; - industry and user education; and - technical measures. Consumers and users are required to resolve spam problems with

	Australia[1]	United Kingdom[1]	United States[1]	South Korea[1,2]	Japan[1]	Singapore[3]	New Zealand[4]
	arrangements: s 42(c).			that recipients can conveniently block or report advertisement information for profit transmitted in violation of Art 50. (2) Minister may give support to relevant public institution, corporation or organization in order to promote development and dissemination of software for blocking or reporting pursuant to (1). (3) Necessary matters for concerning the method of development and dissemination pursuant to (1) and the support pursuant to (2) shall be prescribed by the Presidential Decree.		Initiative - Public Education Efforts by CASE and SBF; (b) Industry Self-Regulation - Efforts by ISPs - Efforts by DMAS; (c) Legislative Framework; and (d) International Cooperation.	the sender of the spam and their ISP. If an ISP considers that a complaint should be addressed by the government enforcement agency then the ISP can refer it on for action.

Communications and Technology Branch
Commerce, Industry and Technology Bureau
January 2006

Annex D

Chapter:	486	Title:	PERSONAL DATA (PRIVACY) ORDINANCE	Gazette Number:	
Section:	**34**	Heading:	**Use of personal data in direct marketing**	Version Date:	30/06/1997

(1) A data user who-

(a) has obtained personal data from any source (including the data subject); and

(b) uses the data for direct marketing purposes,

shall-

(i) the first time he so uses those data after this section comes into operation, 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;

(ii) if the data subject so requests, cease to so use those data without charge to the data subject.

(2) In this section-

"direct marketing" (直接促銷) means-

(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; or

(ii) telephone calls made to specific persons.

(Enacted 1995)