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

**Commerce, Industry and Technology Bureau**
**January 2006**

**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.