File Ref: CTB(CR) 7/5/18(06)

LEGISLATIVE COUNCIL BRIEF

UNSOLICITED ELECTRONIC MESSAGES BILL

INTRODUCTION

A

At the meeting of the Executive Council on 4 July 2006, the Council ADVISED and the Chief Executive ORDERED that the Unsolicited Electronic Messages Bill (the Bill), at **Annex A**, should be introduced into the Legislative Council.

JUSTIFICATIONS

Problems Caused by UEMs

2. Hong Kong's externally-oriented economy as supported by our sophisticated telecommunications facilities, enormous capacity for external communications and high penetration rates for personal computers, internet and mobile services are all factors which make Hong Kong vulnerable to the problems caused by unsolicited electronic messages (UEMs). UEMs cause significant concerns to the community. Recipients of UEMs not only suffer inconvenience, but may incur extra expenses, such as wasted fax paper or roaming phone charges. Businesses suffer lost productivity with employees spending time to find genuine business correspondence from spam e-mails. They incur expenditure to increase the capacity of their e-mail servers and purchase anti-spamming software. Telecommunications service providers need to increase the bandwidth of their systems to cope with the increased traffic caused by UEMs. For e-mail, the industry estimated that over 60% of all e-mails received in Hong Kong are UEMs. They also need to handle complaints from their customers about UEMs.

Lack of Statutory Provision

3. There are existing provisions in the Telecommunications Ordinance (Cap. 106), Crimes Ordinance (Cap. 200), Theft Ordinance (Cap. 210) and Personal Data (Privacy) Ordinance (Cap. 486) prohibiting certain acts that may facilitate or lead to spamming, or certain criminal acts supported by spamming activities. However, there is no statutory provision for regulating the conducts of, and responsibilities for, sending UEMs and related activities. In line with many advanced economies such as the US, the EU and Australia, we consider that Hong Kong should introduce a dedicated piece of

anti-spamming legislation. Without such legislation, Hong Kong can easily become a safe haven for illicit spammers driven here from economies with such legislation.

PROPOSAL

Balance Between Allowing e-Marketing and Respecting the Right of Recipients

4. The need to strike a balance between respecting the right of a recipient to refuse further UEMs and allowing electronic marketing to develop in Hong Kong as a legitimate promotion channel was well recognised in the submissions received during the public consultation exercise which was launched in January 2006. Nevertheless, views were diverse on where that right balance should be. In sum, business interests, including small and medium enterprises (SMEs), preferred more room and flexibility for e-commerce and e-marketing development. On the other hand, consumer groups and many individuals preferred a higher level of protection and less disturbance for recipients against UEMs.

5. We consider that the right balance should be set having regard to the circumstances in Hong Kong. Ninety-eight percent of Hong Kong's business enterprises are SMEs which provide employment to some 50% of the workforce in the private sector. These SMEs generally do not have a strong customer base and may not have the resources to undertake costly promotion activities. Electronic communications are a low cost means for them to develop their businesses. We consider it inappropriate to tilt the balance overly towards maximising protection for recipients which may result in stifling the survival and growth of SMEs. Instead, the emphasis of the Bill should be on prescribing clear responsibilities and obligations for e-marketing activities so that the wishes of individual recipients would be respected.

Coverage of UEMs

a) <u>UEMs originating from or sent to Hong Kong</u>

6. UEMs can come from all over the world. According to industry statistics, over 99% of spam e-mails come from outside Hong Kong. For spam telephone calls, fax and Short Messaging Service (SMS) messages, most of them are currently initiated locally. However, with increasing adoption of Internet Protocol based communications under which there is no charging hurdle for cross-boundary communications, it is possible that UEMs could increasingly be coming from outside Hong Kong.

7. Due to the cross-boundary nature of UEMs, our anti-spam legislation should tackle UEMs originating from Hong Kong, as well as those sent from overseas to a Hong Kong electronic address. Such provisions will lay the ground for our law enforcement agencies to co-operate with their overseas counterparts in exchanging information and intelligence, tracking down major overseas spammers and collecting evidence that may support prosecution of spammers in Hong Kong or overseas jurisdictions. These provisions can also demonstrate to the international community Hong Kong's resolve to and contribution towards tackling this essentially global problem.

b) UEMs of a commercial nature

8. UEMs in Hong Kong are pre-dominantly of a commercial nature. Overseas anti-spam legislation invariably covers such messages only. Accordingly, we propose that the Bill should adopt a targetted approach by regulating the sending of electronic messages of a commercial nature, ie, the content of the message is about offering or promoting goods or services for furtherance of business. Communications not offering or promoting goods or services for the furtherance of business, eg, communications from the Government, calls for donation from charitable organizations and bills or invoices from a business entity, would fall outside the scope of the Bill.

c) Person-to-person messages excluded

9. We consider that a technology neutral stance should be adopted so that any forms of electronic messages, including e-mail, fax, SMS, voice or video calls, should be regulated. But we propose to exclude person-to-person voice or video messages without pre-recorded or synthesised elements (ie, machine generated or simulated), and broadcasting materials already regulated under the Broadcasting Ordinance or the Telecommunications Ordinance.

10. Some submissions to the consultation suggested that person-to-person telemarketing calls cause as much nuisance to a recipient as pre-recorded telemarketing calls and should similarly be regulated. Our view is that such calls require substantial manpower resources and time from the telemarketers. The extent to which they can cause nuisance to recipients, and lead to abuse of the telecommunications networks is much more limited than voice or video messages with pre-recorded or synthesised elements. In view of this, to leave room for such normal and legitimate marketing activities, we consider that the Bill should not regulate person-to-person telemarketing calls. Nevertheless, we have structured the Bill so that if it is decided in future to bring person-to-person telemarketing calls into the ambit of the Bill, such decision could be effected expeditiously by way of a notice published in the Gazette.

Opt-out Regime

11. We propose to adopt an "opt-out" regime, whereby a sender may send electronic messages to recipients, but must provide a functional unsubscribe facility through which a recipient can send a request to stop receiving further electronic messages at his electronic address. To support the "opt-out" regime, we propose to empower the Telecommunications Authority (TA) to set up "do-not-call registers" for suitable types of electronic addresses that the purpose of which would be to facilitate recipients to opt out from receiving further commercial electronic messages from all electronic marketers and for senders of commercial electronic messages to ascertain the electronic addresses to which they should not send further commercial electronic messages unless they have specific consents. There was community concern about potential abuse of the information on the do-not-call registers. We propose to make it an offence for an electronic marketer using those information from the TA for any purpose other than for ascertaining whether a registered user of an electronic address does not wish to receive unsolicited commercial electronic messages at that electronic address, punishable by fine and imprisonment terms similar to the offence of abusing harvested electronic addresses lists described in paragraph 14 below.

12. We propose to require senders of commercial electronic messages to include accurate sender information in the messages to enable the recipients to contact them as necessary. We also propose to prohibit misleading subject headings in commercial e-mail messages.

Enforcement and Penalties

13. We propose to adopt an enforcement notice regime for the above rules. If the TA forms an opinion that a contravention has taken place and will likely continue or be repeated, he will issue an enforcement notice to the organization in breach specifying the steps to remedy the contravention. Failure to comply with an enforcement notice will be an offence punishable by fine up to $100,000 for the first conviction, and to $500,000 for the second or subsequent conviction. We propose to set up an appeal board whereby the recipient of an enforcement notice could appeal against the decision of the TA. Because non-compliance with an enforcement notice will be a criminal offence, the Department of Justice considered that an administrative appeal mechanism is necessary to afford a recipient of an enforcement notice an opportunity to challenge the merits of the administrative decision of the TA in relation to issuing the enforcement notice. To prevent possible abuse of the appeal mechanism, for example, for the purpose of delaying the implementation of an enforcement notice, we propose to make clear

that, unless it is ordered by the appeal board, the lodging of an appeal will not suspend the operation of the enforcement notice, and that the appeal board will be empowered to make an award on costs against an appellant if it is satisfied that the appeal is conducted in a frivolous or vexatious manner.

14. We propose to prohibit the supply, acquisition or use of electronic address-harvesting software or harvested lists of electronic addresses for sending commercial electronic messages without the consent of registered users of electronic addresses. We also propose to prohibit other techniques commonly used by spammers, including the so-called "dictionary attacks" that send commercial electronic messages to automatically generated electronic address, use of "open relays" or "open proxies" for sending commercial electronic messages that can hide the true sources of the messages, and the use of automated means to register for e-mail accounts that could be used for spamming and discarded after they are traced or blocked. These contraventions should not be subject to the enforcement notice regime, but would be prosecuted in court and subject to a fine of up to $1,000,000 and imprisonment for up to 5 years. These techniques should not be adopted by businesses engaged in legitimate electronic marketing activities. The relatively heavy penalty should not be a concern to them.

15. For fraud and related activities in connection with spamming, we propose to impose even heavier penalty of a fine of any amount to be determined by the court and imprisonment of up to 10 years. These offences are adapted from the national anti-spam law of the United States. We propose that the Hong Kong Police Force will be responsible for enforcing these fraud and related offences.

16. We also propose to empower the victims of UEMs to make civil claims for loss or damage against the party who sent the UEMs in contravention of the Bill, irrespective of whether the party had been convicted. Since some victims may only suffer relatively small amounts of monetary losses, e.g. mobile phone roaming charges, we propose that the Small Claims Tribunal should have the jurisdiction to hear and determine such claims for monetary losses up to the amount within the jurisdiction of the Tribunal (i.e. $50,000). For higher losses or damages, the claims should be pursued in the District Court.

THE BILL

17. The main provisions are –

(a) Clauses 2 to 5 define, among other terms, the meaning of "commercial electronic messages", "Hong Kong link", "send"

and "consent";

(b) Clause 6 and Schedule 1 set out the types of electronic messages excluded from the application of the Bill;

(c) Clause 7 imposes a requirement on a sender of a message to include in the message accurate sender information and empowers Secretary for Commerce, Industry and Technology (SCIT) to specify in Regulation the exact types of sender information to be included in different types of electronic messages;

(d) Clause 8 imposes a requirement on a sender of a message to provide in the message a functional unsubscribe facility;

(e) Clauses 9 and 10 mandate that a sender shall cease to send further messages to an electronic address within 10 working days after an unsubscribe request in respect of that electronic address is sent or that electronic address is listed in a do-not-call register;

(f) Clause 11 prohibits misleading subject headings in commercial e-mail messages;

(g) Clause 12 prohibits the senders to withhold or to conceal the calling line identification information of the telephone or facsimile number from which the commercial electronic message is sent;

(h) Clauses 14 to 16 prohibit the supply, acquisition and use of address-harvesting software and harvested-address lists for sending commercial electronic messages without the consent of the registered users of the electronic addresses and prescribe the penalty for the offences;

(i) Clause 17 prohibits sending commercial electronic messages to electronic addresses obtained by automated means, such as the so-called "dictionary attacks", and prescribes the penalty for the offence;

(j) Clause 18 prohibits the use of scripts or other automated means to register for five or more electronic addresses to send multiple commercial electronic messages and prescribes the penalty for the offence;

(k) Clause 19 prohibits relay or retransmission of multiple commercial electronic messages through open relays or open proxies and prescribes the penalty for the offence;

(l) Clauses 21 to 25 prohibit fraud and related activities in connection with sending multiple commercial electronic messages and prescribe the penalty for the offences;

(m) Clauses 28 and 29 respectively empowers the TA to approve codes of practice and prescribes that while failure to observe codes of practice are not contraventions, codes of practice are admissible in evidence in legal proceedings if the court decides they are relevant to determining a matter;

(n) Clauses 30 to 32 empower the TA to establish, maintain and operate do-not-call registers of different types of electronic addresses and prescribe conditions for making available information in the registers, and prescribe an offence for abusing the use of those information;

(o) Clauses 34, 37 and 38 prescribe the powers of the TA to obtain information and, subject to search warrants from a magistrate, enter and search premises;

(p) Clauses 35 and 36 respectively empowers the TA to issue enforcement notices for contravention of rules of sending commercial electronic messages and prescribes the offence for contravening an enforcement notice;

(q) Clause 40 empowers the TA to recover the costs of investigation from a party convicted by the court of an offence;

(r) Clauses 43 to 51 establish the Unsolicited Electronic Messages (Enforcement Notices) Appeal Board and prescribe the power of the Chief Executive to appoint the Chairman, Deputy Chairmen and Members of the Appeal Board, the power of the Appeal Board, the right of a person to appeal, the procedure on appeal, the power of the Court of Appeal to determine questions of law, offences relating to appeals and the power of the SCIT to make relevant rules;

(s) Clause 52 empowers a person suffering loss by another person contravening the Bill to bring civil proceedings in the District Court, or in the Small Claims Tribunal where the amount claimed is within its jurisdiction;

(t) Clauses 53 and 54 clarify the liability of employers, principals, employees, directors and partners in acts done or practices engaged in contravention of the Bill; and

(u) Clause 56 empowers SCIT to make regulations for carrying out the purposes and provisions of the Bill.

LEGISLATIVE TIMETABLE

18. The legislative timetable is as follows: –

Publication in the Gazette	7 July 2006
First Reading and commencement of Second Reading debate	12 July 2006
Resumption of Second Reading debate, committee stage and Third Reading	to be notified

IMPLICATIONS OF THE PROPOSAL

Economic Implications

19. The proposed legislation is expected to bring about net economic benefits to the community. Though the proposal will incur compliance costs to those business enterprises which use electronic messages for legitimate marketing purposes, the statutory requirements are not unduly onerous and most responsible electronic marketers should be able to comply with them at acceptable extra costs. Moreover, for the responsible electronic marketers, the cost of compliance is likely to be outweighed by the potential gain through better trust of customers on electronic communications channels, facilitating the further development of electronic commerce in Hong Kong. For businesses and individuals in general, the potential reduction of spam would help to reduce the expenses and productivity losses they incur for processing, filtering and handling spam. They would also benefit from improved telecommunication network efficiency in Hong Kong as a result of reduced spam.

Financial and Civil Service Implications

20. The Office of the Telecommunications Authority (OFTA) will be the enforcement agency of the regulatory measures mentioned in paragraphs 11-14 above. The resources required for the implementation of these measures will be absorbed by OFTA Trading Fund. In addition, the Hong Kong Police Force will enforce the provisions relating to fraud and related activities mentioned in paragraph 15 above with its existing resources.

21. The Communications and Technology Branch of the Commerce, Industry and Technology Bureau (CITB) will provide secretariat support for the proposed UEMs (Enforcement Notices) Appeal Board within its existing resources. It is estimated that the

operating cost of the Board would be about $2 million per annum, mainly for the annual retainer fees for the Chairman and Deputy Chairman, honorarium for panel members, and other miscellaneous costs for hearing. No additional civil service post will be created.

Other Implications

22. The proposal is in conformity with the Basic Law, including the provisions concerning human rights. It has no environmental or sustainability implications.

PUBLIC CONSULTATION

23. We launched a 2-month public consultation exercise on 20 January 2006 on the detailed legislative proposals for the Bill, attended many forums and seminars on the subject, and consulted the Information Technology and Broadcasting Panel of the Legislative Council on 17 March 2006. A total of 71 submissions have been received. There was strong support for the Government to introduce a piece of anti-spam legislation. Specific comments on the detailed legislative proposal have been considered and incorporated in the Bill where appropriate.

PUBLICITY

24. A press briefing on the Bill will be held on 6 July 2006. A press release will be issued and a spokesman will also be made available to answer media enquiries.

BACKGROUND

25. On 25 June 2004, OFTA issued a public consultation paper on "Proposals to contain the problem of unsolicited electronic messages". That paper examined the problem caused by various forms of UEMs, 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.

26. Drawing on the views and ideas expressed in the submissions to that consultation and on the latest developments, the then SCIT announced on 24 February 2005 a package of measures under the "STEPS" campaign to tackle the problem of UEMs. "STEPS" stands for Strengthening existing regulatory measures, Technical solutions, Education, Partnerships and Statutory measures. A new piece of anti-spam legislation was one of the measures proposed under that campaign.

27. Between March and June 2005, CITB engaged representative stakeholders to seek their views on the guiding principles and key aspects of the framework for the proposed anti-spam legislation. Following those informal consultations, a draft framework was presented to the Information Technology and Broadcasting Panel of the Legislative Council 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 developed detailed legislative proposals for the Bill and launched a 2-month public consultation exercise on 20 January 2006.

ENQUIRIES

28. For any enquiries relating to this Brief, please contact –

Mr Tony Li
Principal Assistant Secretary
Communications and Technology Branch
Commerce, Industry and Technology Bureau
Tel : 2189 2210
Fax : 2511 1458
E-mail : tyyli@citb.gov.hk

Communications and Technology Branch
Commerce, Industry and Technology Bureau
5 July 2006

Annex A

UNSOLICITED ELECTRONIC MESSAGES BILL

CONTENTS

PART 3

RULES ABOUT ADDRESS-HARVESTING AND RELATED ACTIVITIES

PART 4

FRAUD AND OTHER ILLICIT ACTIVITIES RELATED TO TRANSMISSION OF COMMERCIAL ELECTRONIC MESSAGES

PART 5

ADMINISTRATION AND ENFORCEMENT

PART 6

UNSOLICITED ELECTRONIC MESSAGES (ENFORCEMENT NOTICES) APPEAL BOARD

PART 7

MISCELLANEOUS

A BILL

To

Provide for the regulation of the sending of unsolicited electronic messages and for connected purposes.

Enacted by the Legislative Council.

PART 1

PRELIMINARY

1. Short title and commencement

(1) This Ordinance may be cited as the Unsolicited Electronic Messages Ordinance.

(2) This Ordinance shall come into operation on a day to be appointed by the Secretary for Commerce, Industry and Technology by notice published in the Gazette.

2. Interpretation

(1) In this Ordinance, unless the context otherwise requires –

"account" (帳戶) includes –

(a) a free account;

(b) a pre-paid account; and

(c) anything that may reasonably be regarded as the equivalent of an account;

"Authority" (電訊局長) means the Telecommunications Authority appointed under section 5 of the Telecommunications Ordinance (Cap. 106);

"business" (業務) includes a trade or profession;

"commercial electronic mail message" (商業電郵訊息) means a commercial electronic message sent to an electronic mail address;

"commercial electronic message" (商業電子訊息) means an electronic message the purpose, or one of the purposes, of which is –

(a) to offer to supply goods, services, facilities, land or an interest in land;

(b) to offer to provide a business opportunity or an investment opportunity;

(c) to advertise or promote goods, services, facilities, land or an interest in land;

(d) to advertise or promote a business opportunity or an investment opportunity;

(e) to advertise or promote a supplier, or a prospective supplier, of goods, services, facilities, land or an interest in land; or

(f) to advertise or promote a provider, or a prospective provider, of a business opportunity or an investment opportunity,

in the course of or in the furtherance of any business;

"consent" (同意) has the meaning assigned to it by section 5 (*meaning of "consent" and related matters*);

"court" (法院) includes a magistrate;

"domain name" (域名) means a string (any sequence or combination of letters, characters, numbers or symbols of any language) registered with or allocated or assigned by a domain name authority as part of an electronic address on the Internet;

"domain name authority" (域名當局) means a domain name registrar, domain name registry or other domain name registration body;

"do-not-call register" (拒收登記冊) means a register established under section 30 (*Authority may establish do-not-call registers*);

"electronic address" (電子地址) means a string (any sequence or combination of letters, characters, numbers or symbols of any language) used to specify a source or destination of an electronic message and includes, but is not limited to, an electronic mail address, Internet protocol address, instant messaging account name, telephone number and facsimile number;

"electronic mail address" (電郵地址) means an electronic address consisting of a user name or mailbox (commonly referred to as the "local part") and a reference to a domain name (commonly referred to as the "domain part"), whether or not displayed, to which an electronic message can be sent;

"electronic message" (電子訊息) includes a message in any form sent over a public telecommunications service to an electronic address and includes, but is not limited to –

(a) a text, voice, sound, image or video message; and

(b) a message combining text, voice, sound, images or video;

"enforcement notice" (執行通知) means a notice issued under section 35 (*Authority may issue enforcement notice*);

"function" (職能) includes a power and a duty;

"Hong Kong company" (香港公司) means –

(a) a company within the meaning assigned by section 2(1) of the Companies Ordinance (Cap. 32); or

(b) a body corporate that is incorporated or otherwise established by or under any other Ordinance;

"Hong Kong link" (香港聯繫) has the meaning assigned to it by section 3 (*meaning of "Hong Kong link"*);

"legal proceedings" (法律程序) means legal proceedings of any kind, whether civil or criminal and whether under this Ordinance or otherwise;

"mistake" (錯誤) means a reasonable mistake of fact;

"organization" (機構) includes –

(a) a Hong Kong company;

(b) any other company or body corporate, wherever incorporated or otherwise established; and

(c) a partnership, association, society or other body of persons, whether corporate or unincorporate and whether formed or established in Hong Kong or elsewhere;

"public telecommunications network" (公共電訊網絡) means a telecommunications network offered for use by the general public;

"public telecommunications service" (公共電訊服務) has the meaning assigned to it by section 2(1) of the Telecommunications Ordinance (Cap. 106);

"registered user" (登記使用者), in relation to the sending of a commercial electronic message to an electronic address, means –

(a) if the electronic address is an electronic mail address, the individual or organization who is responsible for the relevant electronic mail address account;

(b) if the message is sent to an electronic address in connection with an instant messaging service, the individual or organization who is responsible for the relevant instant messaging account;

(c) if the electronic address is a telephone number or facsimile number, the individual or organization who is responsible for the relevant telephone or facsimile account; or

(d) in any other case, the individual or organization who is responsible for the relevant electronic address account;

"regulations" (規例) means regulations made under section 56 (*regulations*);

"Secretary" (局長) means the Secretary for Commerce, Industry and Technology;

"send" (發送) has the meaning assigned to it by section 4 (*meaning of "send" and related matters*);

"software" (軟件) includes a combination of software and associated data;

"supply" (供應) means supply by way of sale, transfer, exchange, lease, hire or hire-purchase;

"telecommunications" (電訊) has the meaning assigned to it by section 2(1) of the Telecommunications Ordinance (Cap. 106);

"telecommunications device" (電訊裝置) includes any computer, instrument, apparatus or equipment used for the purpose of telecommunications;

"telecommunications network" (電訊網絡) has the meaning assigned to it by section 2(1) of the Telecommunications Ordinance (Cap. 106);

"telecommunications service" (電訊服務) has the meaning assigned to it by section 2(1) of the Telecommunications Ordinance (Cap. 106);

"telecommunications service provider" (電訊服務提供者) means a licensee as defined in section 2(1) of the Telecommunications Ordinance (Cap. 106);

"unsubscribe request" (取消接收要求) has the meaning assigned to it by section 8(4) (*commercial electronic messages must contain unsubscribe facility*);

"working day" (工作日) means any day other than a public holiday or a black rainstorm warning day or gale warning day within the meaning assigned by section 71(2) of the Interpretation and General Clauses Ordinance (Cap. 1).

(2) In this Ordinance, a reference to the performance of a function includes the exercise of a power and the discharge of a duty.

(3) For the avoidance of doubt, references in this Ordinance to organizations shall not be construed as implying that references to persons do not include companies, bodies corporate, partnerships, associations, societies or other bodies of persons.

3. Meaning of "Hong Kong link"

(1) For the purposes of this Ordinance, a commercial electronic message has a Hong Kong link if, and only if –

(a) the message originates in Hong Kong;

(b) the individual or organization who sent the message or authorized the sending of the message is –

(i) an individual who is physically present in Hong Kong when the message is sent;

(ii) an organization (other than a Hong Kong company) that is carrying on business or activities in Hong Kong when the message is sent; or

(iii) a Hong Kong company;

(c) the telecommunications device that is used to access the message is located in Hong Kong;

(d) the registered user of the electronic address to which the message is sent is –

(i) an individual who is physically present in Hong Kong when the message is accessed; or

(ii) an organization that is carrying on business or activities in Hong Kong when the message is accessed; or

(e) the message is sent to an electronic address that is allocated or assigned by the Authority.

(2) For the purposes of subsection (1)(b), (c), (d) and (e), it is immaterial whether the commercial electronic message originates in Hong Kong or elsewhere.

(3) For the purposes of subsection (1)(b)(iii), it is immaterial whether the commercial electronic message is sent, or is authorized to be sent, from Hong Kong or elsewhere.

4. Meaning of "send" and related matters

(1) For the purposes of this Ordinance, "send" (發送), in relation to an electronic message, includes cause to be sent and attempt to send.

(2) For the purposes of this Ordinance (including subsection (3)), if an individual authorizes the sending of a commercial electronic message and he does so on behalf of an organization, then –

(a) the organization shall be treated as authorizing the sending of the message; and

(b) the individual shall be treated as not authorizing the sending of the message.

(3) For the purposes of this Ordinance, if –

(a) a commercial electronic message is sent by an individual or organization; and

(b) the sending of the message is not authorized by any other individual or organization,

the first-mentioned individual or organization shall be treated as authorizing the sending of the message.

(4) For the purposes of any legal proceedings, a telecommunications service provider who merely provides a service that enables a commercial electronic message to be sent shall, unless the contrary is proved, be presumed not to have sent the message and not to have authorized the message to be sent.

(5) For the purposes of any legal proceedings, if a commercial electronic message is sent and at the relevant time the telecommunications device, service or network from which it was sent was controlled by a person without the knowledge of the owners or authorized users of the telecommunications device, service or network, the owners or authorized users shall, unless the contrary is proved, be presumed not to have sent the message and not to have authorized the message to be sent.

(6) In subsection (5), "control" (控制) means either physical control or control through the use of software or other means.

5. Meaning of "consent" and related matters

(1) In this Ordinance, unless the context otherwise requires –

"consent" (同意) means express consent, given either orally or in writing;

"withdraw" (撤回), in relation to consent, means to withdraw the consent either orally or in writing.

(2) For the purposes of this Ordinance, the registered user of an electronic address shall be treated as having given his consent to the sending of a commercial electronic message to that electronic address if the registered user or a person on his behalf –

(a) has, either in response to a clear and conspicuous request for consent or at his own initiative, given his consent to the sending of the message; and

(b) has not, within a reasonable period before the sending of the message, withdrawn the consent referred to in paragraph (a).

(3) For the purposes of this Ordinance (including subsection (2)), if a person other than the registered user of an electronic address uses the relevant account to send an electronic message about –

(a) consent; or

(b) withdrawal of consent,

that person shall be treated as having been authorized to send that message on behalf of the registered user.

(4) Subsection (3) shall not be construed as limiting the circumstances in which a person other than the registered user of an electronic address may –

(a) consent; or

(b) withdraw consent,

on behalf of the registered user.

(5) For the avoidance of doubt, the registered user of an electronic address may at any time withdraw any consent given by him to the sending of a commercial electronic message.

6. Exclusions

(1) This Ordinance does not apply to any matter falling within a description set out in Schedule 1.

(2) The Secretary may, by notice published in the Gazette, amend Schedule 1.

PART 2

RULES ABOUT SENDING COMMERCIAL ELECTRONIC MESSAGES

7. Commercial electronic messages must include accurate sender information

(1) A person shall not send a commercial electronic message that has a Hong Kong link unless –

(a) the message includes clear and accurate information identifying the individual or organization who authorized the sending of the message;

(b) the message includes clear and accurate information about how the recipient can readily contact that individual or organization;

(c) the message includes such information and complies with such conditions as is or are specified in the regulations, if any; and

(d) the information included in the message in compliance with this subsection is reasonably likely to be valid for at least 30 days after the message is sent.

(2) Subsection (1) does not apply if the person –

(a) sent the commercial electronic message by mistake; or

(b) did not know, and could not with reasonable diligence have ascertained, that the message had a Hong Kong link.

8. Commercial electronic messages must contain unsubscribe facility

(1) A person shall not send a commercial electronic message that has a Hong Kong link unless –

(a) the message includes –

(i) a statement to the effect that the recipient may use an electronic address or other electronic means specified in the message ("the unsubscribe facility") to send an unsubscribe request to the individual or organization who authorized the sending of the message; or

(ii) a statement to similar effect;

(b) the statement is presented in a clear and conspicuous manner;

(c) if the unsubscribe facility is a telephone number or facsimile number, it is a number allocated or assigned by the Authority;

(d) the unsubscribe facility is reasonably likely to be capable of receiving the recipient's unsubscribe request, if any, at all times during a period of at least 30 days after the message is sent; and

(e) the unsubscribe request may be sent by the recipient free of any charge to the recipient for the use of the unsubscribe facility.

(2) Subsection (1) does not apply if the person –

(a) sent the commercial electronic message by mistake; or

(b) did not know, and could not with reasonable diligence have ascertained, that the message had a Hong Kong link.

(3) A person to whom an unsubscribe request is sent under this section shall ensure that a record of the request is retained in the format in which it was originally received, or in a format that can be demonstrated to represent accurately the information originally received, for at least 7 years after its receipt.

(4) In this section, "unsubscribe request" (取消接收要求), in relation to a commercial electronic message the sending of which is authorized by an individual or organization, means –

(a) a message to the effect that the registered user of the electronic address to which the message is sent does not wish to receive, at that electronic address, any further commercial electronic messages from or authorized by that individual or organization; or

(b) a message to similar effect.

9. Commercial electronic messages must not be sent after unsubscribe request is sent

(1) This section applies if a person sends an unsubscribe request to an individual or organization using the unsubscribe facility provided under section 8 (*commercial electronic messages must contain unsubscribe facility*).

(2) The individual or organization shall, within 10 working days from the day on which the unsubscribe request is sent –

(a) cease sending any further commercial electronic messages to the electronic address in respect of which the unsubscribe request was sent; and

(b) cease authorizing the sending of any further commercial electronic messages to that electronic address.

(3) Subsection (2) does not apply in relation to a commercial electronic message if, subsequent to the sending of the unsubscribe request, the registered user of the relevant electronic address has given his consent to the sending of the message.

(4) Subsection (2) does not apply in relation to a commercial electronic message if the individual or organization concerned –

(a) sent the message, or authorized it to be sent, by mistake; or

(b) did not know, and could not with reasonable diligence have ascertained, that the message had a Hong Kong link.

(5) In this section, "unsubscribe facility" (取消接收選項) has the same meaning as in section 8 (*commercial electronic messages must contain unsubscribe facility*).

10. Commercial electronic messages must not be sent to electronic address listed in do-not-call register

(1) A person shall not send a commercial electronic message that has a Hong Kong link to an electronic address that, at the time the message is sent, is listed in a do-not-call register.

(2) Subsection (1) does not apply in relation to a commercial electronic message if, prior to or subsequent to the listing of the electronic address in the do-not-call register, and whether before or after the commencement of this section, the registered user of the electronic address has given his consent to the sending of the message.

(3) Subsection (1) does not apply if the electronic address has been listed in the do-not-call register for less than 10 working days at the time the commercial electronic message is sent.

(4) Subsection (1) does not apply if the person –

(a) sent the commercial electronic message by mistake; or

(b) did not know, and could not with reasonable diligence have ascertained, that the message had a Hong Kong link.

11. Commercial electronic mail messages must not use misleading subject headings

A person shall not send a commercial electronic mail message that has a Hong Kong link if the subject heading of the message, if any, would be likely to mislead the recipient about a material fact regarding the content or subject matter of the message.

12. Commercial electronic messages must not be sent with calling line identification information concealed

(1) A person who sends a commercial electronic message that has a Hong Kong link from an electronic address that is a telephone number or facsimile number ("the sending number") shall not –

(a) conceal or withhold from the called party the calling line identification information of the sending number; or

(b) perform any operation or issue any instruction in connection with the sending of the message for the purpose of, or that has the effect of, concealing or withholding from the called party the calling line identification information of the sending number.

(2) In this section, "calling line identification information" (來電線路識別資料) means telecommunications network information generated and transmitted by the calling party's telecommunications network for the purpose of enabling the called party's telecommunications network to identify the telephone number or facsimile number of the calling party.

PART 3

RULES ABOUT ADDRESS-HARVESTING AND RELATED ACTIVITIES

13. Interpretation of Part 3

(1) In this Part –

"address-harvesting software" (地址收集軟件) means software that is specifically designed or marketed for use for –

(a) searching the Internet or a public telecommunications network for electronic addresses; and

(b) collecting, compiling, capturing or otherwise obtaining those electronic addresses;

"harvested-address list" (地址收集清單) means –

(a) a list of electronic addresses;

(b) a collection of electronic addresses; or

(c) a compilation of electronic addresses,

where the production of the list, collection or compilation is, to any extent, directly or indirectly attributable to the use of address-harvesting software.

(2) For the purposes of this Part, a person sends multiple commercial electronic messages if he sends more than 100 commercial electronic messages during a 24-hour period or more than 1 000 commercial electronic messages during a 30-day period.

14. Supply of address-harvesting software or harvested-address list

(1) No person shall supply or offer to supply –

(a) address-harvesting software;

(b) a right to use address-harvesting software;

(c) a harvested-address list; or

(d) a right to use a harvested-address list,

to another person ("the customer") for use in connection with, or to facilitate, the sending of commercial electronic messages that have a Hong Kong link without the consent of the registered users of the electronic addresses to which they are sent.

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine at level 6.

(3) A person who knowingly or recklessly contravenes subsection (1) commits an offence and is liable on conviction on indictment to a fine of $1,000,000 and to imprisonment for 5 years.

(4) It is a defence to a charge for an offence under subsection (2) for the person charged to prove that he did not know and had no reason to suspect that the customer, or another person, intended to use the address-harvesting software or the harvested-address list, as the case may be, in connection with, or to facilitate, the sending of commercial electronic messages that have a Hong Kong link without the consent of the registered users of the electronic addresses to which they are sent.

(5) It is a defence to a charge for an offence under subsection (2) for the person charged to prove that he took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

15. Acquisition of address-harvesting software or harvested-address list

(1) No person shall acquire –

(a) address-harvesting software;

(b) a right to use address-harvesting software;

(c) a harvested-address list; or

(d) a right to use a harvested-address list,

for use in connection with, or to facilitate, the sending of commercial electronic messages that have a Hong Kong link without the consent of the registered users of the electronic addresses to which they are sent.

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine at level 6.

(3) A person who knowingly or recklessly contravenes subsection (1) commits an offence and is liable on conviction on indictment to a fine of $1,000,000 and to imprisonment for 5 years.

(4) It is a defence to a charge for an offence under subsection (2) for the person charged to prove that he took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

16. Use of address-harvesting software or harvested-address list

(1) No person shall use –

(a) address-harvesting software; or

(b) a harvested-address list,

in connection with, or to facilitate, the sending of commercial electronic messages that have a Hong Kong link without the consent of the registered users of the electronic addresses to which they are sent.

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine at level 6.

(3) A person who knowingly or recklessly contravenes subsection (1) commits an offence and is liable on conviction on indictment to a fine of $1,000,000 and to imprisonment for 5 years.

(4) It is a defence to a charge for an offence under subsection (2) for the person charged to prove that he took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

(5) In this section, "use" (用、使用) does not include the act of forwarding the address-harvesting software or harvested-address list to another person.

17. Sending of commercial electronic message to electronic address obtained using automated means

(1) No person shall send a commercial electronic message that has a Hong Kong link to an electronic address that was obtained using an automated means.

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine at level 6 and to imprisonment for 2 years.

(3) A person who knowingly or recklessly contravenes subsection (1) commits an offence and is liable on conviction on indictment to a fine of $1,000,000 and to imprisonment for 5 years.

(4) It is a defence to a charge for an offence under subsection (2) for the person charged to prove that he did not know and had no reason to suspect that the electronic address was obtained using an automated means.

(5) It is a defence to a charge for an offence under subsection (2) for the person charged to prove that he took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

(6) In this section –

"automated means" (自動化方法) means an automated process that generates possible electronic addresses by combining letters, characters, numbers or symbols into numerous permutations;

"obtained" (取得), in relation to an electronic address, means obtained, whether before or after the commencement of this section, by –

(a) the person charged; or

(b) any person from or through whom the person charged acquired the electronic address.

18. Use of scripts or other automated means to register for 5 or more electronic mail addresses

(1) No person shall use scripts or other automated means to register for 5 or more electronic mail addresses from which to send, or enable another person to send, multiple commercial electronic messages that have a Hong Kong link without the consent of the registered users of the electronic addresses to which they are sent.

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine at level 6 and to imprisonment for 2 years.

(3) A person who knowingly or recklessly contravenes subsection (1) commits an offence and is liable on conviction on indictment to a fine of $1,000,000 and to imprisonment for 5 years.

(4) Subsection (1) does not apply to –

(a) a person who performs functions in connection with the administration of the information systems of an organization, when performing such functions; or

(b) a telecommunications service provider, when acting in connection with the provision of a public telecommunications service.

(5) In this section –

"register" (登記), in relation to an electronic mail address, means –

(a) to register with an authority responsible for allocating or assigning the electronic mail address or approving its allocation or assignment; or

(b) to be allocated or assigned the electronic mail address with the approval of such an authority;

"scripts" (手稿程式) means a list of instructions or commands to an information system.

19. Relay or retransmission of multiple commercial electronic messages

(1) No person shall use a telecommunications device, service or network to relay or retransmit multiple commercial electronic messages that have a Hong Kong link, with the intent to deceive or mislead recipients, or any telecommunications service provider, as to the source of such messages.

(2) A person who contravenes subsection (1) commits an offence and is liable –

(a) on summary conviction, to a fine at level 6 and to imprisonment for 2 years; or

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

PART 4

FRAUD AND OTHER ILLICIT ACTIVITIES RELATED TO TRANSMISSION OF COMMERCIAL ELECTRONIC MESSAGES

20. Interpretation of Part 4

(1) In this Part –

"initiate" (啟動), in relation to a commercial electronic message, means –

(a) to originate or send such a message;

(b) to procure the origination or sending of such a message; or

(c) to attempt to originate or send, or procure the origination or sending of, such a message,

but does not include actions that constitute the routine conveyance of such a message;

"routine conveyance" (例行傳遞) means the transmission, routing, relaying, handling or storing, through an automatic technical process, of an electronic message in relation to which message another person has identified the recipient or provided the recipient's electronic address.

(2) For the purposes of this Part, a person initiates the transmission of multiple commercial electronic messages from a telecommunications device, service or network if he initiates the transmission of more than 100 commercial electronic messages during a 24-hour period, or more than 1 000 commercial electronic messages during a 30-day period, from that telecommunications device, service or network.

(3) For the purposes of this Part, more than one person may be considered to have initiated the transmission of a commercial electronic message or multiple commercial electronic messages.

21. Initiating transmission of multiple commercial electronic messages from telecommunications device, etc., accessed without authorization

(1) A person who knowingly or recklessly –

(a) accesses a telecommunications device, service or network without authorization; and

(b) initiates the transmission of multiple commercial electronic messages that have a Hong Kong link from that telecommunications device, service or network,

commits an offence and is liable on conviction on indictment to a fine and to imprisonment for 10 years.

(2) For the purposes of subsection (1), a person accesses a telecommunications device, service or network without authorization if –

(a) he accesses that telecommunications device, service or network by any means or in any manner;

(b) he is not entitled to obtain such access; and

(c) he has not been authorized to obtain such access by any person who is entitled to grant him such access.

22. Initiating transmission of multiple commercial electronic messages with intent

to deceive or mislead recipients as to source of messages

(1) A person who knowingly initiates the transmission of multiple commercial electronic messages that have a Hong Kong link from a telecommunications device, service or network without authorization, with the intent to deceive or mislead recipients as to the source of such messages, commits an offence and is liable on conviction on indictment to a fine and to imprisonment for 10 years.

(2) For the purposes of subsection (1), a person initiates the transmission of a commercial electronic message from a telecommunications device, service or network without authorization if –

(a) he initiates the transmission of the message from that telecommunications device, service or network by any means or in any manner;

(b) he is not entitled to initiate that transmission; and

(c) he has not been authorized to initiate that transmission by any person who is entitled to authorize him to initiate the transmission.

23. Falsifying header information in multiple commercial electronic messages

(1) A person who –

(a) materially falsifies header information in multiple commercial electronic messages that have a Hong Kong link; and

(b) knowingly or recklessly initiates the transmission of such messages from a telecommunications device, service or network,

commits an offence and is liable on conviction on indictment to a fine and to imprisonment for 10 years.

(2) For the purposes of subsection (1) but subject to subsection (3), a person materially falsifies header information in a commercial electronic message if he knowingly falsifies, alters, conceals, deletes or withholds any information 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 transmission of the message.

(3) For the purposes of subsection (1) and in relation to the sending of a commercial electronic message from an electronic address that is a telephone number or facsimile number ("the sending number"), the person initiating the transmission of such a message shall not be treated as having materially falsified header information by reason only that he has performed any operation or issued any instruction in connection with the sending of the message for the purpose of, or that has the effect of, concealing or withholding from the called party the calling line identification information of the sending number.

(4) In this section –

"calling line identification information" (來電線路識別資料) has the same meaning as in section 12(2) (*commercial electronic messages must not be sent with calling line identification information concealed*);

"header information" (標頭資料) means the information attached to a commercial electronic message by a telecommunications device, service or network for the purpose of identifying, or purporting to identify, the person sending the message or the source, routing or destination of the message, and –

(a) in relation to a commercial electronic mail message, includes, but is not limited to, the originating domain name, Internet protocol address and electronic mail address, but excludes the content in the SMTP data portion; and

(b) in relation to any other form of commercial electronic message, includes, but is not limited to, the electronic address from which the message originates;

"SMTP data portion" (《簡單郵遞傳送規約》數據部分) has the meaning assigned to it by the Simple Mail Transfer Protocol of Internet Official Protocol Standards, or any successor protocols, published by the Internet Engineering Task Force, or any of its successors, as amended from time to time.

24. Registering for electronic addresses or domain names using information that falsifies identity of actual registrant

(1) A person who –

(a) knowingly registers, using information that materially falsifies the identity of the actual registrant, for 5 or more electronic addresses or 2 or more domain names; and

(b) knowingly or recklessly initiates the transmission of multiple commercial electronic messages that have a Hong Kong link from any of such electronic addresses or domain names or from any combination of such electronic addresses or domain names,

commits an offence and is liable on conviction on indictment to a fine and to imprisonment for 10 years.

(2) For the purposes of subsection (1), a person uses information that materially falsifies the identity of the actual registrant if he knowingly falsifies, alters, conceals, deletes or withholds any information in such manner as to –

(a) impair the ability of the relevant authority responsible for allocating or assigning the electronic address or approving its allocation or assignment or the relevant domain name

authority, as the case may be, to identify or locate the actual registrant; or

(b) impair the ability of the recipient of any commercial electronic message transmitted from the electronic address or domain name, a telecommunications service provider processing the message or any other person to identify, locate or respond to the person who initiated the transmission of the message.

(3) In this section, "register" (登記、註冊) means –

(a) in relation to an electronic address –

(i) to register with an authority responsible for allocating or assigning the electronic address or approving its allocation or assignment; or

(ii) to procure the allocation or assignment of the electronic address, or the approval of its allocation or assignment, by such an authority; and

(b) in relation to a domain name, to register the domain name with, or to procure its allocation or assignment by, any domain name authority.

25. False representations regarding registrant or successor in interest to registrant of electronic address or domain name

(1) A person who –

(a) falsely represents 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

(b) knowingly or recklessly initiates the transmission of multiple commercial electronic messages that have a Hong Kong link from any of such electronic addresses or

domain names or from any combination of such electronic addresses or domain names,

commits an offence and is liable on conviction on indictment to a fine and to imprisonment for 10 years.

(2) In this section, "registrant" (登記人、註冊人) means a person who registers for an electronic address or domain name within the meaning assigned by section 24(3) (*registering for electronic addresses or domain names using information that falsifies identity of actual registrant*).

PART 5

ADMINISTRATION AND ENFORCEMENT

26. Interpretation of Part 5

In this Part –

"approved code of practice" (認可實務守則) has the meaning assigned to it by section 28(8) (*Authority may approve codes of practice*);

"authorized officer" (獲授權人員) means a public officer authorized by the Authority under section 27 (*Authority may appoint authorized officers*);

"specified offence" (指明罪行) means an offence under this Part or Part 3 (*rules about address-harvesting and related activities*).

27. Authority may appoint authorized officers

The Authority may authorize in writing any public officer to perform any of the functions conferred or imposed on authorized officers by this Ordinance as are specified in the authorization.

28. Authority may approve codes of practice

(1) Subject to subsection (3), for the purpose of providing practical guidance in respect of the application or operation of any provision of this Ordinance, the Authority may –

(a) approve and issue such codes of practice (whether prepared by him or not) as in his opinion are suitable for that purpose; and

(b) approve such codes of practice issued or proposed to be issued otherwise than by him as in his opinion are suitable for that purpose.

(2) A code of practice –

(a) may consist of a code, standard, rule, specification or any other documentary form of practical guidance prepared by the Authority or other body or authority; and

(b) may apply, incorporate or refer to any document that has been formulated or published by a body or authority either as in force at the time the document is approved by the Authority or as amended, formulated or published from time to time.

(3) Where a code of practice is approved under subsection (1), the Authority shall, by notice published in the Gazette –

(a) identify the code concerned and specify the date on which its approval is to take effect; and

(b) specify the provision or provisions of this Ordinance for which the code is so approved.

(4) The Authority may –

(a) from time to time revise the whole or any part of any code of practice prepared by him under this section; and

(b) approve any revision or proposed revision of the whole or any part of any code of practice for the time being approved under this section.

(5) The provisions of subsection (3) shall, with the necessary modifications, apply in relation to any revision or approval under subsection (4)

as they apply in relation to the approval of a code of practice under subsection (1).

(6) The Authority may at any time withdraw his approval from any code of practice approved under this section.

(7) Where under subsection (6) the Authority withdraws his approval from a code of practice approved under this section, he shall, by notice published in the Gazette, identify the code concerned and specify the date on which its approval is to cease to have effect.

(8) References in this Ordinance to an approved code of practice are references to that code as approved under this section and as it has effect for the time being, including by virtue of any revision of the whole or any part of it approved under this section.

(9) The power of the Authority under subsection (1)(b) to approve a code of practice issued or proposed to be issued otherwise than by him shall include the power to approve a part of such a code and, accordingly, in this Ordinance, "code of practice" may be read as including a part of such a code.

(10) For the avoidance of doubt, it is hereby declared that a code of practice approved under subsection (1) is not subsidiary legislation.

29. Use of approved codes of practice in legal proceedings

(1) 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.

(2) 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 –

(a) the code of practice is admissible in evidence in the proceedings; and

(b) 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.

(3) In any legal proceedings, a code of practice that appears to a court to be the subject of a notice under section 28(3) (*Authority may approve codes of practice*) shall, in the absence of evidence to the contrary, be presumed to be the subject of such notice.

(4) In any legal proceedings, a document that purports to be a copy of a code of practice that is the subject of a notice under section 28(3) (*Authority may approve codes of practice*) shall, in the absence of evidence to the contrary, be presumed to be a true copy of the code.

(5) In this section, "court" (法院) includes –

(a) a magistrate;

(b) the Unsolicited Electronic Messages (Enforcement Notices) Appeal Board established under section 43(1) (*Appeal Board established*); and

(c) any other tribunal.

30. Authority may establish do-not-call registers

(1) The Authority may for the purposes of this Ordinance establish and keep one or more registers containing a list of electronic addresses, each of which is to be known as a do-not-call register.

(2) The purposes of a do-not-call register are –

(a) to provide registered users of electronic addresses with a convenient means by which they may notify senders of commercial electronic messages that they do not wish to receive such messages at those electronic addresses; and

(b) to provide senders of commercial electronic messages with a convenient means by which they may ascertain whether

a registered user of an electronic address does not wish to receive unsolicited commercial electronic messages at that electronic address.

(3) Without limiting the generality of subsection (1), the Authority may establish and keep separate do-not-call registers for different kinds of electronic addresses.

(4) A do-not-call register may be kept in such form as the Authority considers appropriate including –

(a) in a documentary form; or

(b) in a form other than a documentary form.

(5) If a do-not-call register is kept in a form other than a documentary form, then the information contained in it pursuant to subsection (1) must be capable of being reproduced in a legible form.

(6) The Authority shall not list an electronic address in a do-not-call register unless the registered user of that electronic address has given his consent to its inclusion in the register and to it being made available under section 31 (*access to do-not-call registers*).

(7) A document purporting to be –

(a) a copy of an entry in or extract of a do-not-call register; and

(b) certified by the Authority or an authorized officer as a true copy of the entry or extract referred to in paragraph (a),

shall be admissible as evidence of its contents in any legal proceedings.

(8) The Authority may do all things necessary to be done to establish, maintain and operate do-not-call registers for the purposes of this Ordinance.

31. Access to do-not-call registers

(1) To achieve the purposes described in section 30(2) (*Authority may establish do-not-call registers*), the Authority shall cause a do-not-call register,

or the information contained in it, to be made available to senders of commercial electronic messages.

(2) Without limiting the generality of subsection (1), the Authority may cause a do-not-call register, or the information contained in it, to be made available to senders of commercial electronic messages in such form and manner, and subject to such conditions, as the Authority considers appropriate.

32. Offences relating to misuse of information

(1) No person to whom an unsubscribe request is sent under section 8 (*commercial electronic messages must contain unsubscribe facility*) shall use any information obtained thereby other than for the purpose of complying with the requirements of that section or section 9 (*commercial electronic messages must not be sent after unsubscribe request is sent*).

(2) No person to whom a do-not-call register, or any information contained in a do-not-call register, is made available under section 31 (*access to do-not-call registers*) shall use any information obtained thereby other than for the purpose described in section 30(2)(b) (*Authority may establish do-not-call registers*).

(3) A person who contravenes subsection (1) or (2) commits an offence and is liable on summary conviction to a fine at level 6.

(4) A person who knowingly or recklessly contravenes subsection (1) or (2) commits an offence and is liable on conviction on indictment to a fine of $1,000,000 and to imprisonment for 5 years.

(5) It is a defence to a charge for an offence under subsection (3) for the person charged to prove that he took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

33. Authority may issue directions to telecommunications service providers

(1) Subject to subsection (2), the Authority may issue directions in writing to a telecommunications service provider requiring it to take such action as the Authority considers necessary –

(a) to facilitate the telecommunications service provider's compliance with any provision of this Ordinance or the regulations; or

(b) to enable the Authority or an authorized officer to perform any function under this Ordinance or the regulations,

and the telecommunications service provider shall give effect to such directions.

(2) No direction shall be issued under subsection (1) unless the Authority is satisfied that the telecommunications service provider has been afforded a reasonable opportunity to make representations to the Authority.

34. Authority may obtain information or documents relevant to investigation

(1) If the Authority is satisfied that there are reasonable grounds for believing that a person is, or is likely to be, in possession of information (including but not limited to passwords) or a document that is relevant to the Authority's investigation of a contravention or suspected contravention of a provision of this Ordinance, the Authority may serve a notice in writing on the person, accompanied by a copy of this section in Chinese and English –

(a) requesting the person to –

(i) give the information in writing to the Authority; or

(ii) produce the document to the Authority,

as the case requires, before a date ("the relevant date") specified in the notice, being a date reasonable in all the circumstances of the case; and

(b) stating that if the person is of the view that he cannot, or does not wish to, comply with the request, then he may

make representations in writing to the Authority as to why he is of that view before the relevant date.

(2) Where the Authority receives representations referred to in subsection (1)(b) from a person, the Authority shall, after considering the representations, serve a notice in writing on the person –

(a) stating that the Authority has considered the representations; and

(b) stating either –

(i) that the notice served on the person under subsection (1) is withdrawn with effect from the date of service of the notice under this subsection; or

(ii) that the notice served on the person under subsection (1) remains in force and the Authority will on a date specified in the notice served under this subsection seek an order under subsection (3) unless the person has, before that date, complied with the notice served on the person under subsection (1).

(3) Where a notice served on a person under subsection (1) has not been withdrawn under subsection (2)(b)(i) and the person has not complied with the notice before the relevant date, or before the date specified in the notice served on the person under subsection (2), as the case may be, then a magistrate may –

(a) if satisfied by information on oath that there are reasonable grounds for believing that the person is, or is likely to be, in possession of the information or a document to which the first-mentioned notice relates and that the information or document is relevant to the Authority's investigation of

a contravention or suspected contravention of a provision of this Ordinance; and

(b) after considering the representations, if any, referred to in subsection (1)(b) received by the Authority in consequence of the service of the first-mentioned notice,

issue an order that the person shall, within the time specified in the order, give the information in writing to the Authority or produce the document to the Authority, as the case requires.

(4) Any information or document to be given or produced to the Authority by a person in compliance with a notice under subsection (1) or an order under subsection (3) shall be so given or produced by reference to the information or document at the time of service of that notice except that the information or document may take account of any processing that was done between the time of service and the time when the information or document is so given or produced if that processing would have been done irrespective of the service of that notice.

(5) The Authority shall not disclose any information or document given or produced to him under this section unless he is satisfied that –

(a) it is necessary to disclose the information or document for the purposes of a proceeding under subsection (3);

(b) it is necessary to disclose the information or document for the purposes of –

(i) the prevention or detection of crime;

(ii) the apprehension, prosecution or detention of offenders; or

(iii) the fulfilment of any obligation under an international agreement applicable to Hong Kong and relating to unsolicited electronic messages; or

(c) it is otherwise in the public interest to disclose the information or document.

(6) The Authority shall, before he discloses any information or document under this section, give the person who gave or produced the information or document to the Authority a reasonable opportunity to make representations on the proposed disclosure, and the Authority shall consider all representations made to him before he makes a final decision to disclose the information or document, as the case may be.

(7) For the avoidance of doubt, it is hereby declared that where a person gives or produces any information or document under this section notwithstanding that the information or document is the subject of a confidentiality agreement with another person that prevents the first-mentioned person from releasing the information or document, the first-mentioned person shall not be liable for any civil liability or claim whatever in respect of the giving or production of that information or document, as the case may be, contrary to that agreement.

(8) Nothing in this section shall require a person to give any information, or to produce any document, that the person could not be compelled to give in evidence, or produce, in civil proceedings before the Court of First Instance.

(9) A person commits an offence if he, without reasonable excuse –

(a) fails to comply with an order under subsection (3);

(b) fails to comply with subsection (4); or

(c) in purported compliance with a notice under subsection (1) or an order under subsection (3), knowingly gives information that is false or misleading,

and shall be liable on summary conviction to a fine at level 5 and to imprisonment for 2 years.

(10) In this section, "processing" (處理), in relation to any information or document, includes amending, augmenting, deleting or rearranging all or any part of the information or document, whether by automated means or otherwise.

35. Authority may issue enforcement notice

(1) Where the Authority is of the opinion that any person –

(a) is contravening any provision of Part 2 (*rules about sending commercial electronic messages*); or

(b) has contravened any provision of Part 2 (*rules about sending commercial electronic messages*) in circumstances that make it likely that the contravention will continue or be repeated,

then the Authority may serve a notice in writing on the person, accompanied by a copy of this section in Chinese and English –

(c) stating that he is of that opinion;

(d) specifying the contravention as to which he is of that opinion and the reasons why he believes it is a contravention; and

(e) directing the person to take such steps as are specified in the notice to remedy the contravention or the matters occasioning the service of the notice, as the case may be, within such period as is specified in the notice.

(2) The steps specified in an enforcement notice to remedy any contravention or matter to which the notice relates may be framed –

(a) to any extent by reference to any approved code of practice; and

(b) so as to afford the relevant person a choice between different ways of remedying the contravention or matter, as the case may be.

(3) Subject to subsection (4), the period specified in an enforcement notice for taking the steps specified in it shall not expire before the end of the period specified in section 44 (*appeals to Appeal Board*) within which an appeal against the notice may be made.

(4) If the Authority is of the opinion that by reason of special circumstances the steps specified in an enforcement notice should be taken as a matter of urgency –

(a) he may include a statement to that effect in the notice together with the reasons why he is of that opinion; and

(b) where such a statement is so included, subsection (3) shall not apply but the notice shall not require those steps to be taken before the end of the period of 7 days beginning with the date on which the notice was served.

(5) The Authority may cancel an enforcement notice by notice in writing served on the relevant person.

36. Offence relating to enforcement notices

(1) A person who contravenes an enforcement notice served on him under section 35 (*Authority may issue enforcement notice*) commits an offence.

(2) A person who commits an offence under this section is liable –

(a) on a first conviction, to a fine at level 6; and

(b) on a second or subsequent conviction, to a fine of $500,000,

and, in the case of a continuing offence, to a further daily fine of $1,000 for each day during which the offence continues.

(3) It is a defence to a charge for an offence under this section for the person charged to prove that he exercised all due diligence to comply with the enforcement notice.

37. Powers of entry, search, arrest, etc.

(1) The Authority or an authorized officer may –

(a) without warrant, arrest any person whom he reasonably suspects of having committed a specified offence; and

(b) where a warrant has been issued under section 38 (*power of magistrate to issue search warrant*) in respect of any premises or place –

(i) enter and search the premises or place;

(ii) detain any person found in or on the premises or place, during such period as is reasonably required to permit the search to be carried out, where that person might prejudice the purpose of the search if he were not so detained; and

(iii) seize, remove or detain any telecommunications device or other thing found in or on the premises or place that is or that contains, or that appears to him to be or to contain, or to be likely to be or to contain, evidence of the commission of a specified offence.

(2) The Authority or an authorized officer may, in the performance of his functions under subsection (1) –

(a) break into and forcibly enter any premises or place that he is empowered to enter and search; and

(b) remove by force any person or thing obstructing him in the performance of such functions.

(3) The Authority or an authorized officer may, in carrying out a search of any premises or place entered under this section –

(a) inspect, operate and analyze any telecommunications device or other thing found in or on the premises or place;

(b) require any information that relates, or that appears to him to relate, or to be likely to relate, to the commission or suspected commission of a specified offence and that is –

(i) contained in a computer in, on or accessible from the premises or place; or

(ii) contained in any other telecommunications device or other thing found in or on the premises or place and that is capable of being retrieved on a computer,

to be produced on a computer in or on the premises or place in a visible and legible form, and examine the information;

(c) require any information described in paragraph (b) to be produced in a form in which it can be taken away and in which it is either visible and legible or capable of being retrieved on a computer; and

(d) take away the copy so produced under paragraph (c).

(4) Where the Authority or an authorized officer arrests a person under subsection (1)(a), he shall, without delay, take the person to a police station to be dealt with there in accordance with the Police Force Ordinance (Cap. 232) or deliver him into the custody of a police officer for that purpose.

(5) The Authority or an authorized officer may call upon police officers or other public officers to assist him in the performance of any function under this section.

(6) This section is without prejudice to any powers of arrest, entry and search conferred on police officers under any other law.

38. Power of magistrate to issue search warrant

Where a magistrate is satisfied by information on oath that there are reasonable grounds for suspecting that there is, or is likely to be, in or on any

premises or place any telecommunications device or other thing that is or that contains, or that is likely to be or to contain, evidence of the commission of a specified offence, the magistrate may issue a warrant authorizing the Authority or an authorized officer to enter and search the premises or place.

39. Obstruction of Authority, authorized officers, etc.

(1) Without prejudice to any other Ordinance, a person who –

(a) wilfully obstructs the Authority or an authorized officer in the performance of his functions under this Ordinance;

(b) wilfully fails to comply with any requirement properly made to him by the Authority or an authorized officer; or

(c) without reasonable excuse, fails to give the Authority or an authorized officer any other assistance that he may reasonably require to be given for the purpose of performing his functions under this Ordinance,

commits an offence and is liable on summary conviction to a fine at level 3 and to imprisonment for 6 months.

(2) Without prejudice to any other Ordinance, a person who makes a statement that he knows to be false or does not believe to be true, or otherwise knowingly misleads the Authority, an authorized officer or any other person in the performance of his functions under this Ordinance commits an offence and is liable on summary conviction to a fine at level 5 and to imprisonment for 2 years.

40. Recovery of costs and expenses of investigation by Authority

(1) Where a person is convicted by a court of a specified offence on a prosecution instituted as a result of an investigation by the Authority, the court may order the person to pay to the Authority the whole or a part of the costs and expenses of that investigation.

(2) Any costs and expenses awarded to the Authority by an order made under this section shall constitute a debt due to the Authority from the person ordered to pay them and are recoverable as a civil debt.

(3) For the avoidance of doubt, this section is without prejudice to any power conferred on the court under the Costs in Criminal Cases Ordinance (Cap. 492).

41. Immunity of Authority, authorized officers, etc.

(1) No person to whom this subsection applies, acting in good faith, shall be personally liable for any civil liability or claim whatever in respect of any act done or default made in the performance or purported performance of any function under this Ordinance.

(2) The persons to whom subsection (1) applies are –

(a) the Authority;

(b) any authorized officer; and

(c) any police officer or other public officer assisting the Authority or authorized officer in the performance or purported performance of any function under this Ordinance.

PART 6

UNSOLICITED ELECTRONIC MESSAGES (ENFORCEMENT NOTICES) APPEAL BOARD

42. Interpretation of Part 6

In this Part –

"appeal" (上訴) means an appeal under section 44 (*appeals to Appeal Board*);

"Appeal Board" (上訴委員會) means the Unsolicited Electronic Messages (Enforcement Notices) Appeal Board established under section 43(1) (*Appeal Board established*);

"appellant" (上訴人) means a person lodging an appeal;

"Chairman" (主席) means the Chairman of the Appeal Board appointed under section 43(2) (*Appeal Board established*);

"Deputy Chairman" (副主席) means a Deputy Chairman of the Appeal Board appointed under section 43(2) (*Appeal Board established*);

"panel member" (備選委員) means a member of the panel of persons appointed under section 43(5) (*Appeal Board established*);

"presiding officer" (審裁官), in relation to an appeal, means the presiding officer referred to in section 45(1)(a) (*procedure on appeal*).

43. Appeal Board established

(1) A board to be known as the "Unsolicited Electronic Messages (Enforcement Notices) Appeal Board" is established.

(2) Subject to subsections (3) and (4), the Chief Executive shall appoint a person to be the Chairman of the Appeal Board and such other persons as he thinks fit to be Deputy Chairmen of the Appeal Board.

(3) A person shall not be appointed under subsection (2) unless the person is eligible to be appointed a District Judge under section 5 of the District Court Ordinance (Cap. 336).

(4) Subject to subsections (7) and (8), the Chairman and a Deputy Chairman shall each be appointed for a term of not more than 3 years but may be reappointed.

(5) The Chief Executive shall appoint a panel of persons not being public officers whom he considers suitable for appointment under section 45(1)(b) (*procedure on appeal*) as members of the Appeal Board.

(6) An appointment under subsection (2) or (5) shall be notified in the Gazette.

(7) The Chairman, a Deputy Chairman or a panel member may at any time resign by notice in writing to the Chief Executive.

(8) The Chief Executive may revoke the appointment of the Chairman, a Deputy Chairman or a panel member on the ground of incapacity, bankruptcy, neglect of duty or misconduct proved to the satisfaction of the Chief Executive.

(9) The remuneration, if any, of the Chairman, a Deputy Chairman and a panel member shall be paid at a rate that the Financial Secretary determines.

44. Appeals to Appeal Board

(1) A person on whom an enforcement notice is served under section 35 (*Authority may issue enforcement notice*) may appeal to the Appeal Board against the enforcement notice or any part of the enforcement notice.

(2) A person who wishes to appeal under this section must lodge a notice of appeal with the Appeal Board not later than 14 days after the enforcement notice is served on him under section 35 (*Authority may issue enforcement notice*).

(3) Unless ordered by the Appeal Board under section 46(1)(*i*) (*powers of Appeal Board*), the lodging of a notice of appeal shall not have the effect of suspending the operation of the enforcement notice or any part of the enforcement notice under appeal.

45. Procedure on appeal

(1) For the purposes of an appeal, the Appeal Board shall consist of –

(a) the Chairman or a Deputy Chairman, as determined by the Chairman, who shall preside at the hearing (the "presiding officer"); and

(b) 2 panel members appointed by the presiding officer.

(2) If the term of appointment of the presiding officer or a panel member appointed under subsection (1) expires during the hearing of an appeal, the presiding officer or panel member may continue to hear the appeal until the appeal is determined.

(3) In the hearing of an appeal, every question before the Appeal Board shall be determined by the opinion of the majority of the members hearing the appeal except a question of law which shall be determined by the presiding officer, and in the case of an equality of votes the presiding officer shall have a casting vote.

(4) A party to an appeal shall be entitled to be heard either in person or through a counsel or solicitor, and if any party is a company, through any of its directors or other officers, or if a partnership, through any of its partners.

(5) The Appeal Board may, if it sees fit, permit a party to an appeal to submit written representations to the Appeal Board in lieu of appearing in person or through a counsel or solicitor at a sitting of the Appeal Board.

(6) Every sitting of the Appeal Board shall be held in public unless the Appeal Board considers that in the interests of justice a sitting or part of a sitting should not be held in public, in which case it may hold the sitting or part of the sitting in private.

(7) After hearing an appeal, the Appeal Board shall determine the appeal by upholding, varying or quashing the enforcement notice and may make such consequential orders as it considers necessary.

(8) Every decision of the Appeal Board under subsection (7) shall be in writing and contain a statement of the reasons for the decision.

46. Powers of Appeal Board

(1) Subject to section 47 (*privilege against disclosure*) and section 50 (*privileges and immunities of Appeal Board members and witnesses*), in the hearing of an appeal, the Appeal Board may –

(a) subject to subsection (2), receive and consider any material, whether by way of oral evidence, written statements, documents or otherwise, and whether or not it would be admissible in a court;

(b) by notice in writing signed by the presiding officer, summon any person –

(i) to produce to the Appeal Board any information or document that is relevant to the appeal and is in his custody or under his control; or

(ii) to appear before the Appeal Board and to give evidence relevant to the appeal;

(c) administer oaths and affirmations;

(d) require evidence to be given on oath or affirmation;

(e) make an award as to costs –

(i) against an appellant, if the Appeal Board is satisfied that he has conducted his case in a frivolous or vexatious manner; and

(ii) against any other party to the appeal, if the Appeal Board is satisfied that in all the circumstances of the case it would be unjust and inequitable not to do so;

(f) where the Appeal Board is satisfied that it is just and equitable to do so, require a party to the appeal to pay the costs of the Appeal Board in hearing the appeal;

(g) make an order prohibiting a person from publishing or otherwise disclosing any material the Appeal Board receives;

(h) make an order prohibiting the publication or other disclosure of any material the Appeal Board receives at a sitting, or part of a sitting, that is held in private; and

(i) make an order suspending the operation of an enforcement notice.

(2) Subsection (1)(a) shall not entitle a person to require the Appeal Board to receive and consider any material that had not been submitted to or made available to the Authority at any time before the enforcement notice under appeal was served.

(3) Costs referred to in subsection (1)(e) and (f) are recoverable as a civil debt.

(4) The Chairman may determine any matter of practice or procedure relating to the hearing of appeals where no provision governing such matter is made in this Ordinance or in the rules made under section 51 (*rules*).

47. Privilege against disclosure

For the purposes of an appeal, the appellant, the Authority and any other person summoned under section 46(1)(b) (*powers of Appeal Board*) shall each have the same privileges in respect of the disclosure of any material as if the proceedings before the Appeal Board were proceedings before a court.

48. Case may be stated for Court of Appeal

(1) The Appeal Board may refer any question of law arising in an appeal to the Court of Appeal for determination by way of case stated.

(2) On the hearing of the case, the Court of Appeal may –

(a) determine the question stated; or

(b) remit the case to the Appeal Board, in whole or in part, for reconsideration in the light of the Court's determination.

(3) Where a case is stated under subsection (1), the Appeal Board shall not determine the relevant appeal before the Court of Appeal determines the relevant point of law.

49. Offences relating to appeals

(1) In relation to an appeal, a person who, without reasonable excuse, refuses or fails –

(a) to attend and give evidence when required to do so by the Appeal Board;

(b) to answer truthfully and completely questions put to him by the Appeal Board; or

(c) to produce any document that he is required by the Appeal Board to produce,

commits an offence and is liable on summary conviction to a fine at level 3 and to imprisonment for 6 months.

(2) A person who publishes or otherwise discloses any material in contravention of –

(a) an order under section 46(1)(g) (*powers of Appeal Board*); or

(b) an order under section 46(1)(h) (*powers of Appeal Board*),

commits an offence and is liable on summary conviction to a fine at level 5 and to imprisonment for 2 years.

(3) It is a defence to a charge for an offence under subsection (2)(b) for the person charged to prove that he did not know and had no reason for knowing that the Appeal Board had made an order under section 46(1)(h) (*powers of Appeal Board*) prohibiting the publication or other disclosure of the material concerned.

50. Privileges and immunities of Appeal Board members and witnesses

(1) The Chairman, a Deputy Chairman and a panel member have, in the performance of their functions under this Part, the same privileges and immunities as a judge of the Court of First Instance in civil proceedings in that Court.

(2) A witness before the Appeal Board shall be entitled to the same privileges and immunities as if he were a witness in civil proceedings in the Court of First Instance.

51. Rules

The Secretary may make rules –

(a) to provide for the lodging of appeals; and

(b) relating to the practice and procedure of the Appeal Board.

PART 7

MISCELLANEOUS

52. Claims for loss or damage

(1) A person who suffers loss or damage by reason of a contravention of any provision of this Ordinance ("the claimant") shall be entitled to bring proceedings against the person who committed the contravention (whether or not he has been convicted of an offence in relation to the contravention).

(2) Subject to subsection (5), proceedings under subsection (1) shall be brought in the District Court but all such remedies shall be obtainable in such proceedings as, apart from this subsection, would be obtainable in the Court of First Instance.

(3) Without limiting the generality of subsection (2), the District Court may, if it considers it fair, just and reasonable in the circumstances to do so –

(a) make a declaration that the respondent has committed an act, or engaged in conduct, in contravention of this Ordinance;

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

(c) order that the respondent shall pay to the claimant compensation by way of damages for any loss or damage suffered by the claimant by reason of the respondent's act or conduct; and

(d) grant an injunction or any other appropriate remedy, order or relief against the respondent.

(4) By virtue of this subsection and notwithstanding any other law, the District Court shall have jurisdiction to hear and determine any proceedings under subsection (1) and shall have all such powers as are necessary or expedient for it to have in order to provide, grant or make any remedy, injunction, order or relief mentioned in subsection (3).

(5) Where an amount claimed for loss or damage under subsection (1) does not exceed the amount mentioned in paragraph 1 of the Schedule to the Small Claims Tribunal Ordinance (Cap. 338), the proceedings shall be brought in the Small Claims Tribunal, and that Ordinance shall apply to the claim in the same manner as if it were a monetary claim founded in tort as referred to in that paragraph.

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

(7) For the avoidance of doubt, nothing in this section affects, limits or diminishes any rights, privileges, obligations or liabilities conferred or imposed on a person under any other enactment or rule of law.

53. Liability of principals, agents, employers and employees

(1) Any act done or conduct engaged in by a person in the course of his employment (the "employee") shall be treated for the purposes of this Ordinance 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.

(2) Any act done or conduct 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 this Ordinance as done or engaged in by that other person as well as by him.

(3) In any proceedings for an offence under this Ordinance brought against any person in respect of an act or conduct alleged to have been done or engaged in, as the case may be, by an employee or agent of that person, it is a defence for that person to prove that he took such steps as were practicable to prevent the employee or agent from doing the act or engaging in the conduct, or from doing or engaging in, in the course of his employment or authority, acts or conduct, as the case may be, of that description.

(4) In any proceedings for an offence under this Ordinance brought against any employee in respect of an act or conduct alleged to have been done or engaged in, as the case may be, by the employee, it is a defence for the employee to prove that he did the act or engaged in the conduct in good faith –

(a) in the course of his employment; or

(b) in accordance with instructions given to him by or on behalf of his employer in the course of his employment.

(5) Subsection (4) does not apply to an employee who, at the time the act was done or the conduct was engaged in, was in a position to make or influence a decision regarding that act or conduct.

54. Liability of directors, partners, etc.

(1) Where a company or a partnership has done any act or engaged in any conduct constituting an offence under this Ordinance, the following person shall, unless he proves that he did not authorize the act to be done or the conduct to be engaged in, be presumed also to have done the act or to have engaged in the conduct –

(a) in the case of the company –

(i) any director of the company who, at the time the act was done or the conduct was engaged in, was responsible for the internal management of the company; or

(ii) if there was no such director, any person who, at the time the act was done or the conduct was engaged in, was responsible under the immediate authority of the directors of the company for the internal management of the company;

(b) in the case of the partnership –

(i) any partner in the partnership who, at the time the act was done or the conduct was engaged in, was responsible for the internal management of the partnership; or

(ii) if there was no such partner, any person who, at the time the act was done or the conduct was engaged in, was responsible under the immediate authority of the partners in the partnership for the internal management of the partnership.

(2) Where an unincorporated body of persons has done any act or engaged in any conduct constituting an offence under this Ordinance, any officer or other person who, at the time the act was done or the conduct was engaged in, was responsible for the internal management of the body shall, unless he proves that he did not authorize the act to be done or the conduct to be engaged in, be presumed also to have done the act or to have engaged in the conduct.

(3) A person charged with an offence under this Ordinance by virtue of subsection (1) or (2) is taken to have proved that he did not authorize the act in question to be done or the conduct in question to be engaged in if –

(a) sufficient evidence is adduced to raise an issue with respect to that fact; and

(b) the contrary is not proved by the prosecution beyond reasonable doubt.

55. Transactions relating to contravention not void or voidable

A transaction is not void or voidable by reason only that a contravention of any of the provisions of this Ordinance has taken place in relation to or as a result of the transaction.

56. Regulations

The Secretary may make regulations –

(a) for the purposes of any provision of this Ordinance that contemplates or authorizes the making of regulations with respect to any matter;

(b) providing for such matters as are necessary for giving full effect to the provisions of this Ordinance; and

(c) generally for carrying out the purposes and provisions of this Ordinance.

57. Consequential amendments

The enactments referred to in Schedule 2 are amended in the manner set out in that Schedule.

SCHEDULE 1 [s. 6]

MATTERS EXCLUDED FROM APPLICATION OF ORDINANCE

Item	Description
1.	Voice, sound, image or video messages, or messages combining text, voice, sound, images or video, that involve person-to-person interactive communications between a caller and a recipient without any pre-recorded or synthesized (machine-generated or simulated) element.
2.	Voice, sound, image or video messages, or messages combining text,

voice, sound, images or video, that involve –

(a) person-to-person interactive communications between a caller and a recipient; and

(b) a pre-recorded or synthesized (machine-generated or simulated) element,

whereby the pre-recorded or synthesized element is activated in response to information communicated by the caller.

3. Television programme services regulated under the Broadcasting Ordinance (Cap. 562).

4. Sound broadcasting services regulated under the Telecommunications Ordinance (Cap. 106).

SCHEDULE 2 [s. 57]

CONSEQUENTIAL AMENDMENTS

Telecommunications Ordinance

1. **Offences by telecommunications officer, etc.**

(1) Section 24 of the Telecommunications Ordinance (Cap. 106) is amended by renumbering it as section 24(1).

(2) Section 24 is amended by adding –

"(2) This section does not apply to any act done by a telecommunications officer, or any person who, though not a telecommunications officer, has official duties in connection with a telecommunications service, for the purpose of –

(a) facilitating compliance with this Ordinance or any other law;

(b) implementing the terms or conditions of a licence of a licensee or any contract made

between a licensee and a customer of the licensee; or

(c) facilitating compliance with a lawful request of a customer of a licensee in connection with a service supplied by the licensee to the customer.".

Resolution establishing Office of the Telecommunications Authority Trading Fund

2. **Services to be provided under the trading fund**

Schedule 1 to the resolution of the Legislative Council establishing the Office of the Telecommunications Authority Trading Fund (Cap. 430 sub. leg. D) is amended, in item 1, by repealing "and the Telephone Ordinance (Cap. 269)" and substituting ", the Telephone Ordinance (Cap. 269) and the Unsolicited Electronic Messages Ordinance (of 2006)".

Electronic Transactions Ordinance

3. **Proceedings in relation to which sections 5, 5A, 6, 7 and 8 of this Ordinance do not apply under section 13(1) of this Ordinance**

Schedule 2 to the Electronic Transactions Ordinance (Cap. 553) is amended –

(a) in paragraph (zq), in the Chinese text, by repealing "；或" and substituting a semicolon;

(b) in paragraph (zr), by repealing the full stop at the end and substituting a semicolon;

(c) by adding –

"(zs) the Unsolicited Electronic Messages (Enforcement Notices) Appeal Board established

under the Unsolicited Electronic Messages Ordinance (of 2006).".

Explanatory Memorandum

The object of this Bill is to set up a scheme for regulating the sending of unsolicited electronic messages that have a commercial purpose, including e-mail messages and other forms of electronic messaging.

2. The Bill comprises 7 Parts and 2 Schedules. The main features of the Bill are –

(a) the establishment of rules about the sending of unsolicited commercial electronic messages including rules requiring such messages to include accurate sender information and an unsubscribe facility (*see Part 2 of the Bill*);

(b) the creation of offences relating to the supply, acquisition and use of software the main purpose of which is electronic address collection (otherwise known as "address-harvesting software"), and the supply, acquisition and use of lists of electronic addresses generated by such software (*see Part 3 of the Bill*);

(c) the creation of offences to prevent fraud and other illicit activities related to the transmission of commercial electronic messages (*see Part 4 of the Bill*);

(d) the establishment by the Telecommunications Authority ("the Authority") of codes of practice and "do-not-call" registers (*see Part 5 of the Bill*);

(e) an administrative enforcement regime that provides for the issue of enforcement notices (*see Part 5 of the Bill*) and an appeal mechanism (*see Part 6 of the Bill*); and

(f) a civil enforcement mechanism that provides for the awarding of damages and other relief to persons who suffer loss or damage by reason of a contravention of any of the provisions of the Bill (*see clause 52—claims for loss or damage*).

3. The Bill applies mainly to commercial electronic messages that have a "Hong Kong link". Essentially, a message has a Hong Kong link if the sender or recipient of the message has a connection to Hong Kong (*see discussion below at paragraph 6 for the meaning of "Hong Kong link"*).

Part 1—Preliminary

4. Clause 1 provides for the short title and the commencement of the Bill (when enacted). The Bill will commence on a day to be appointed by the Secretary for Commerce, Industry and Technology ("the Secretary") by notice published in the Gazette. By virtue of section 20 of the Interpretation and General Clauses Ordinance (Cap. 1), the notice may fix different days for different provisions of the Bill to commence.

5. Clause 2 sets out the main definitions for the purposes of the Bill. The following are the key definitions –

(a) "electronic message"—The term "electronic message" is a key concept in the definition of "commercial electronic message", which is broadly an electronic message that has a particular "commercial purpose" (*see paragraph (b) below*). The definition of "electronic message" has 2 parts. The first part describes the types of messages covered. Essentially, messages may take any form including text, voice, sound, image or video or any combination. The second part requires the message to be sent over a "public telecommunications service" to an

"electronic address". The term "public telecommunications service" is defined as having the same meaning as in the Telecommunications Ordinance (Cap. 106), where it is defined to mean "a telecommunications service which is offered for use to the general public". This includes telephone and facsimile services, broadband services, Internet services and other electronic means of communication. The term "electronic address" is defined to include, among other matters, e-mail addresses, Internet protocol addresses, instant messaging account names, telephone numbers and facsimile numbers. The most common examples of electronic messages are e-mail messages and SMS messages.

(b) "commercial electronic message"—This term is a key concept of the Bill. The definition is broadly based on whether or not the electronic message has a commercial purpose and is in the furtherance of any business. It is sufficient if one of the purposes of the message is a commercial purpose; it need not be the primary or sole purpose of the message. The definition sets out the various purposes that would bring a message within the meaning of the definition, including the following –

(i) offering to supply goods, services, facilities or land or to provide a business or investment opportunity (the term "supply" is defined to mean supply by way of sale, transfer, exchange, lease, hire or hire-purchase);

(ii) advertising or promoting goods, services, facilities or land or a business or investment opportunity; and

(iii) advertising or promoting a supplier of goods, services, facilities or land or a provider of a business or investment opportunity.

If an electronic message does not have such a commercial purpose, it will not be covered by the Bill. For example, a virus that is sent to many electronic addresses, which does not have any commercial purpose, would not be a commercial electronic message for the purposes of the Bill. Similarly, an electronic message about an amateur sporting event that does not have a commercial purpose in the sense described above would not be covered by the Bill.

(c) "organization"—This term is defined to include Hong Kong companies and other companies, bodies corporate, partnerships, associations, societies and other bodies of persons. The term is used in various provisions in the Bill, including clause 3 (*meaning of "Hong Kong link"*), clause 4 (*meaning of "send" and related matters*), clause 7 (*commercial electronic messages must include accurate sender information*), clause 8 (*commercial electronic messages must contain unsubscribe facility*) and clause 9 (*commercial electronic messages must not be sent after unsubscribe request is sent*).

(d) "registered user"—In essence, this term refers to the account holder of an electronic address account, whether it is an e-mail account, an instant messaging account, a

telephone account, a facsimile account or other type of electronic address account. The term is used in various provisions in the Bill, including clause 3 (*meaning of "Hong Kong link"*), clause 5 (*meaning of "consent" and related matters*), clause 8 (*commercial electronic messages must contain unsubscribe facility*), clause 9 (*commercial electronic messages must not be sent after unsubscribe request is sent*), clause 10 (*commercial electronic messages must not be sent to electronic address listed in do-not-call register*) and the clauses relating to address-harvesting (*see Part 3 of the Bill*).

Clause 2(3) provides that references in the Bill to "organizations" shall not be construed as implying that references to "persons" do not include companies, bodies corporate, partnerships, associations, societies or other bodies of persons. Section 3 of the Interpretation and General Clauses Ordinance (Cap. 1) provides that unless the contrary intention appears the word "person" includes "any body of persons, corporate or unincorporate". Clause 2(3) has been included in the Bill to avoid the possibility of a court finding a contrary intention in the Bill, in particular, to avoid the possibility of a court finding that a reference to "person" in the Bill does not include a company, body corporate, partnership, association, society or other body of persons.

6. Clause 3 sets out when a commercial electronic message has a "Hong Kong link" for the purposes of the Bill. The concept of a "Hong Kong link" is a key element of the provisions of Parts 2, 3 and 4 of the Bill, which set out rules about commercial electronic messages that have a "Hong Kong link". In broad terms, a commercial electronic message has a Hong Kong link if –

(a) the message originates in Hong Kong;

(b) the message is sent or is authorized to be sent by an individual who is physically present in Hong Kong, an

organization carrying on business or activities in Hong Kong or a Hong Kong incorporated company;

(c) the telecommunications device used to access the message is located in Hong Kong;

(d) the registered user of the electronic address to which the message is sent is physically present in Hong Kong (in the case of an individual) or is carrying on business or activities in Hong Kong (in the case of an organization); or

(e) the message is sent to an electronic address allocated or assigned by the Authority.

7. Clause 4 defines the meaning of "send" and provides for other related matters. The term "send" is defined in clause 4(1) to include cause to be sent and attempt to send. The purpose of this provision is to make clear that, when the term "send" is used in the context of the sending of commercial electronic messages, it does not require a person to have personally sent the message or for a person to have actually received the message. A message is to be treated as sent by a person if it has been sent by another person on his behalf or if he otherwise causes it to be sent, and it is to be treated as sent regardless of its successful receipt or otherwise.

Clause 4(2) to (6) provides for the circumstances in which the sending of a commercial electronic message will be treated as being authorized for the purposes of the Bill. The term "authorize", in relation to the sending of commercial electronic message, is used in clause 3 (*meaning of "Hong Kong link"*), clause 5 (*meaning of "consent" and related matters*), clause 7 (*commercial electronic messages must include accurate sender information*), clause 8 (*commercial electronic messages must contain unsubscribe facility*) and clause 9 (*commercial electronic messages must not be sent after unsubscribe request is sent*).

Clause 4(2) provides that if an individual authorizes the sending of a commercial electronic message and does so on behalf of an organization then the organization rather than the individual shall be treated as having authorized the sending of the message. This attribution of authorization to the organization rather than the individual is necessary to ensure that the information identifying the sender of the message refers to the organization rather than the individual (*see clause 7—commercial electronic messages must include accurate sender information*) and that an unsubscribe request may be sent to that organization rather than the individual (*see clause 8—commercial electronic messages must contain unsubscribe facility*). This ensures that if the individual is employed by an organization and subsequently leaves his employment, then the sender information or unsubscribe request will not be affected.

Clause 4(3) provides that if a commercial electronic message is sent by an individual or organization without being authorized by any other individual or organization, then the first-mentioned individual or organization shall be treated as having authorized the sending of the message. This provision has been included in the Bill to avoid any argument that an individual or organization cannot authorize something on his or its own behalf.

Clause 4(4) provides that for the purposes of any legal proceedings, a telecommunications service provider who merely provides a service that enables a commercial electronic message to be sent shall, unless the contrary is proved, be presumed not to have sent the message and not to have authorized the message to be sent. The term "telecommunications service provider" is defined in clause 2 of the Bill to mean a licensee as defined in section 2(1) of the Telecommunications Ordinance (Cap. 106). This provision has been included in the Bill to avoid any argument that a telecommunications service provider (for example, an Internet service provider) could be in breach of the prohibitions relating to the sending of commercial electronic messages simply because it has supplied the carriage service by which the message has been sent.

Clause 4(5) provides that for the purposes of any legal proceedings, if a commercial electronic message is sent and at the relevant time the telecommunications device, service or network from which it was sent was controlled by a person without the knowledge of the owners or authorized users of the telecommunications device, service or network, then the owners or authorized users shall, unless the contrary is proved, be presumed not to have sent the message and not to have authorized it to be sent. The term "control" is defined in clause 4(6) to mean either physical control or control through the use of software or other means. This provision has been included in the Bill to avoid any argument that an owner or authorized user of a computer which is, for example, infected by a virus could be in breach of the prohibitions as a result of the transmission of messages caused by that virus.

8. Clause 5 defines the meaning of "consent" for the purposes of the Bill and provides for other related matters, including withdrawal of consent. The concept of "consent" is a key element in the application provisions of the Bill relating to the sending of commercial electronic messages. Generally, the rules relating to the sending of commercial electronic messages set out in clause 9 (*commercial electronic messages must not be sent after unsubscribe request is sent*) and clause 10 (*commercial electronic messages must not be sent to electronic address listed in do-not-call register*) do not apply where the registered user of the relevant electronic address has consented to the sending of the message. Essentially, "consent" means express consent that is given either orally or in writing. Express consent covers the situation where a person specifically requests the sending of the relevant commercial electronic message from the sender. Clause 5(3) provides that if a person other than the registered user of the electronic address uses the relevant electronic address account to send an electronic message about consent or withdrawal of consent, then that person is to be treated as having been authorized to send that message on behalf of the registered user.

9. Clause 6 excludes the matters listed in Schedule 1 from the application of the Bill. Essentially, the exclusions cover the following matters –

(a) Person-to-person interactive communications without any pre-recorded or synthesized element. A normal telephone call between 2 individuals is an example of such communications.

(b) Person-to-person interactive communications that contain a pre-recorded or synthesized element but where the pre-recorded or synthesized element is activated in response to information communicated by the caller. For example, an individual may make a telephone call to a bank to enquire about a mortgage and a pre-recorded or synthesized element of the bank's answering machine may ask the caller to select certain options on the telephone in order to be directed to the appropriate bank officer responsible for answering enquiries about mortgages. While the caller is waiting, a pre-recorded message might announce the availability of new banking services. Such communications, where the pre-recorded or synthesized element is activated only in response to information communicated by the caller, are not intended to be covered by the Bill, even if they may have a commercial aspect.

(c) Television programme services.

(d) Sound broadcasting services.

Under clause 6(2) of the Bill, the Secretary is authorized to amend Schedule 1. The main purpose of this clause is to allow the Secretary to add to the list of exclusions in response to technological changes and other new developments.

Part 2—Rules about sending commercial electronic messages

10. Part 2 of the Bill sets out the main rules applying to the sending of commercial electronic messages that have a Hong Kong link (*see discussion above at paragraph 6 for the meaning of "Hong Kong link"*).

11. Clause 7(1) prohibits the sending of a commercial electronic message that has a Hong Kong link unless it contains certain information, including information that identifies the individual or organization who authorized the sending of the message (*see discussion above at paragraph 7 for the meaning of "authorized"*). The purpose of this provision is to support the opt-out regime such that the recipient of the commercial electronic message may follow up with the sender as necessary and enforcement action may be taken against a sender who does not comply with the opt-out regime. Under clause 7(1)(c), the message is required to include information and comply with conditions specified in the regulations made under the Bill. Clause 56 empowers the Secretary to make regulations for the purposes of the Bill and this provision will allow the Secretary to make regulations setting out the information requirements in greater detail and to set different requirements for the different technologies used to send commercial electronic messages. To ensure that senders do not circumvent the requirement by using information that was usable at the time of sending but is soon invalid or outdated, a safeguard is provided in clause 7(1)(d) that the information must be reasonably likely to be valid for at least 30 days after the messages are sent.

Clause 7(2) provides an exception to the prohibition in clause 7(1). In broad terms, the prohibition does not apply in cases where the relevant commercial electronic message was sent by mistake or the sender did not know, and could not with reasonable diligence have ascertained, that the message had a Hong Kong link.

12. Clause 8 prohibits the sending of a commercial electronic message that has a Hong Kong link unless the message includes an unsubscribe facility. The

prohibition does not apply if the person sent the message by mistake or did not know, and could not with reasonable diligence have ascertained, that it had a Hong Kong link. This requirement is included to ensure that recipients can unsubscribe from future communications. While many senders of commercial electronic messages already provide such an unsubscribe mechanism, a relatively common practice is that senders provide no real functional mechanism to allow a recipient to opt out of receiving future messages, for example, by providing as the unsubscribe mechanism a telephone number that is busy all the time.

Clause 8(1)(a) to (e) sets out the conditions that the message must comply with. Clause 8(1)(a) provides that the message must include a statement to the effect that the recipient may use an electronic means specified in the message ("the unsubscribe facility") to send an unsubscribe request. The term "unsubscribe request" is defined in clause 8(4). Essentially, it is a message to the effect that the registered user of the electronic address to which the message is sent does not wish to receive any further commercial electronic messages from the sender. Clause 8(1)(b) requires the unsubscribe statement to be presented in a clear and conspicuous manner. Clause 8(1)(c) provides that if the unsubscribe facility is a telephone number or facsimile number, it must be a number allocated or assigned by the Authority. In effect, it must be a Hong Kong telephone number or facsimile number. Clause 8(1)(d) requires the unsubscribe facility to be reasonably likely to be capable of receiving unsubscribe requests for at least 30 days after the relevant commercial electronic message is sent. Finally, clause 8(1)(e) requires that the unsubscribe facility may be used by the recipient free of any charge.

Clause 8(2) provides an exception to the prohibition in clause 8(1) that is similar to the one contained in clause 7(2) (*see paragraph 11 above*).

Clause 8(3) requires a person to whom an unsubscribe request is sent to keep a record of the request for a period of at least 7 years.

13. Clause 9(1) and (2) in effect prohibits an individual or organization to whom an unsubscribe request is sent from sending, or authorizing the sending of, any further commercial electronic messages to the relevant electronic address after 10 working days from the day on which the unsubscribe request is sent.

Clause 9(3) provides that the requirements mentioned above do not apply if the registered user of the relevant electronic address has, subsequent to the sending of the unsubscribe request, given his consent to the sending of the commercial electronic message. Clause 9(4) provides a further exception that is similar to the one contained in clause 7(2) (*see paragraph 11 above*).

14. Clause 10(1) prohibits the sending of a commercial electronic message that has a Hong Kong link to an electronic address listed in a "do-not-call" register (*see discussion below at paragraph 37 for the meaning of "do-not-call register"*). Clause 10(2) provides that the prohibition does not apply if the registered user of the electronic address has given his consent to the sending of the commercial electronic message. Clause 10(3) provides that the prohibition does not apply if the electronic address has been listed in a "do-not-call" register for less than 10 working days. Clause 10(4) provides a further exception that is similar to the one contained in clause 7(2) (*see paragraph 11 above*).

15. Clause 11 prohibits the sending of commercial e-mail messages that have a Hong Kong link if the subject heading of the message would be likely to mislead the recipient about a material fact regarding the content or subject matter of the message.

16. Clause 12 prohibits a person who sends a commercial electronic message that has a Hong Kong link from an electronic address that is a telephone number or facsimile number ("the sending number") from concealing or withholding from the called party the calling line identification information of the sending number. It also prohibits the person from performing any operation or issuing any instruction for that purpose. The term "calling line identification information" refers to the information generated by the calling party's

telecommunications network for the purpose of enabling the called party's telecommunications network to identify the telephone number or facsimile number of the calling party.

Part 3—Rules about address-harvesting and related activities

17. Part 3 of the Bill is designed to prohibit what are commonly referred to as "address-harvesting", "dictionary attacks" and "brute force attacks" (*see discussions below at paragraphs 18 and 22 for the meaning of these terms*). Under this Part of the Bill the supply, acquisition and use of address-harvesting software is prohibited where it is used to send, or to facilitate the sending of, commercial electronic messages that have a Hong Kong link (*see discussion above at paragraph 6 for the meaning of "Hong Kong link"*) without the consent of the registered users of the electronic addresses to which they are sent. Part 3 also prohibits the supply, acquisition and use of lists produced using address-harvesting software.

18. Clause 13 defines the terms "address-harvesting software" and "harvested-address list". The term "address-harvesting software" means software that is specifically designed or marketed for use for searching the Internet or a public telecommunications network for electronic addresses (for example, e-mail addresses or telephone numbers) and collecting, compiling, capturing or otherwise obtaining those electronic addresses.

The term "harvested-address list" is defined to mean a list, collection or compilation of electronic addresses, where the production of the list, collection or compilation is, to any extent, directly or indirectly attributable to the use of address-harvesting software. Lists that consist primarily of addresses collected using address-harvesting software, but which include some addresses that have been obtained from other means, will be included in this definition. The definition does not cover lists that are compiled solely by means other than the

use of address-harvesting software. For example, it does not cover manually created lists.

Clause 13 also defines the meaning of "multiple" commercial electronic messages for the purposes of Part 3 of the Bill. In broad terms, "multiple" means more than 100 commercial electronic messages sent during a 24-hour period or more than 1 000 commercial electronic messages sent during a 30-day period.

19. Clause 14(1) prohibits any person from supplying or offering to supply address-harvesting software or a harvested-address list, or a right to use address-harvesting software or a harvested-address list, for use in connection with, or to facilitate, the sending of commercial electronic messages that have a Hong Kong link without the consent of the registered users of the electronic addresses to which they are sent. Under clause 14(2), a person who contravenes clause 14(1) is liable on summary conviction to a maximum fine at level 6 (currently $100,000). Under clause 14(3), a person who knowingly or recklessly contravenes clause 14(1) is liable on conviction on indictment to a maximum fine of $1,000,000 and imprisonment for a maximum term of 5 years.

Clause 14(4) and (5) provides a defence to a charge for an offence under clause 14(2). In broad terms, it is a defence for the person charged to prove –

(a) that he did not know and had no reason to suspect that the customer, or another person, intended to use the address-harvesting software or harvested-address list in connection with, or to facilitate, the sending of commercial electronic messages that have a Hong Kong link without the consent of the registered users of the electronic addresses to which they are sent; or

(b) that he took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

20. Clause 15(1) prohibits any person from acquiring address-harvesting software or a harvested-address list, or a right to use address-harvesting software or a harvested-address list, for use in connection with, or to facilitate, the sending of commercial electronic messages that have a Hong Kong link without the consent of the registered users of the electronic addresses to which they are sent. Under clause 15(2), a person who contravenes clause 15(1) is liable on summary conviction to a maximum fine at level 6 (currently $100,000). Under clause 15(3), a person who knowingly or recklessly contravenes clause 15(1) is liable on conviction on indictment to a maximum fine of $1,000,000 and imprisonment for a maximum term of 5 years.

Clause 15(4) provides that it is a defence to a charge for an offence under clause 15(2) for the person charged to prove that he took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

21. Clause 16(1) prohibits any person from using address-harvesting software or a harvested-address list in connection with, or to facilitate, the sending of commercial electronic messages that have a Hong Kong link without the consent of the registered users of the electronic addresses to which they are sent. The prohibition does not apply if the person uses the address-harvesting software or harvested-address list other than in connection with, or to facilitate, the sending of commercial electronic messages. For example, a non-commercial message from a government body may be sent where the electronic addresses have been collected via address-harvesting software or harvested-address lists.

Under clause 16(2), a person who contravenes clause 16(1) is liable on summary conviction to a maximum fine at level 6 (currently $100,000). Under clause 16(3), a person who knowingly or recklessly contravenes clause 16(1) is liable on conviction on indictment to a maximum fine of $1,000,000 and imprisonment for a maximum term of 5 years.

Clause 16(4) provides that it is a defence to a charge for an offence under clause 16(2) for the person charged to prove that he took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

22. Clause 17(1) prohibits any person from sending a commercial electronic message that has a Hong Kong link to an electronic address that was obtained using an automated means. The term "automated means" is defined to mean an automated process that generates possible electronic addresses by combining letters, characters, numbers or symbols into numerous permutations. The provision is intended to prohibit what are commonly referred to as "dictionary attacks" or "brute force attacks". The former describes the process of using combinations of common names or words to find the names of electronic address accounts while the latter describes the process of using all possible combinations of alphanumeric characters in various lengths, often in a sequential fashion, to find the names of such accounts.

Under clause 17(2), a person who contravenes clause 17(1) is liable on summary conviction to a maximum fine at level 6 (currently $100,000) and imprisonment for a maximum term of 2 years. Under clause 17(3), a person who knowingly or recklessly contravenes clause 17(1) is liable on conviction on indictment to a maximum fine of $1,000,000 and imprisonment for a maximum term of 5 years.

Clause 17(4) and (5) provides that it is a defence to a charge for an offence under clause 17(2) for the person charged to prove that he did not know and had no reason to suspect that the electronic address was obtained using an automated means or that he took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

23. Clause 18(1) prohibits any person from using scripts or other automated means to register for 5 or more e-mail addresses from which to send, or enable another person to send, multiple commercial electronic messages that have a

Hong Kong link without the consent of the registered users of the electronic addresses to which they are sent. Basically, "scripts" are instructions or commands to an information system (basically, a computer system).

Under clause 18(2), a person who contravenes clause 18(1) is liable on summary conviction to a maximum fine at level 6 (currently $100,000) and imprisonment for a maximum term of 2 years. Under clause 18(3), a person who knowingly or recklessly contravenes clause 18(1) is liable on conviction on indictment to a maximum fine of $1,000,000 and imprisonment for a maximum term of 5 years.

Clause 18(4) provides that the prohibition under clause 18(1) does not apply to –

(a) a person who performs functions in connection with the administration of an information system of an organization; or

(b) a telecommunications service provider acting in connection with the provision of a public telecommunications service.

24. Clause 19(1) prohibits any person from using a telecommunications device, service or network to relay or retransmit multiple commercial electronic messages that have a Hong Kong link, with the intent to deceive or mislead recipients, or any telecommunications service provider, as to the source of such messages. This provision is intended to prohibit the use of what is commonly referred to as "open relays" and "open proxies" to relay or retransmit commercial electronic messages. Under clause 19(2), a person who contravenes clause 19(1) is liable on summary conviction to a maximum fine at level 6 (currently $100,000) and imprisonment for a maximum term of 2 years, or on conviction on indictment to a maximum fine of $1,000,000 and imprisonment for a maximum term of 5 years.

Part 4—Fraud and other illicit activities related to transmission of commercial electronic messages

25. Part 4 of the Bill creates indictable offences relating to certain fraudulent and other illicit activities associated with the transmission of commercial electronic messages that have a Hong Kong link (*see discussion above at paragraph 6 for the meaning of "Hong Kong link"*). The proscribed activities relate to the more serious problems connected with the transmission of such messages. All of the offences in Part 4 of the Bill are punishable by imprisonment for a maximum term of 10 years and a fine. The offences do not specify the maximum amount of the fine and therefore, by virtue of section 101F of the Criminal Procedure Ordinance (Cap. 221), the court may levy a fine of any amount.

26. Clause 20 defines certain terms used in Part 4 of the Bill. It defines the meaning of "initiate" a commercial electronic message and the meaning of "multiple" commercial electronic messages, which are key concepts of the offences in Part 4. In broad terms, "multiple" means more than 100 commercial electronic messages sent during a 24-hour period or more than 1 000 commercial electronic messages sent during a 30-day period.

27. Clause 21 makes it an offence for any person to knowingly or recklessly initiate the transmission of multiple commercial electronic messages that have a Hong Kong link from a telecommunications device, service or network that the person has accessed without authorization.

28. Clause 22 makes it an offence for any person to knowingly initiate the transmission of multiple commercial electronic messages that have a Hong Kong link from a telecommunications device, service or network without authorization, with the intent to deceive or mislead recipients as to the source of such messages.

29. Clause 23 makes it an offence (subject to exceptions) for any person to materially falsify header information in multiple commercial electronic messages that have a Hong Kong link and to knowingly or recklessly initiate the

transmission of such messages from a telecommunications device, service or network.

30. Clause 24 makes it an offence for any person to knowingly register for 5 or more electronic addresses or 2 or more domain names, using information that materially falsifies the identity of the actual registrant, and to knowingly or recklessly initiate the transmission of multiple commercial electronic messages that have a Hong Kong link from such electronic addresses or domain names.

31. Clause 25 makes it an offence for any person to falsely represent himself to be the registrant or legitimate successor in interest to the registrant of 5 or more electronic addresses or 2 or more domain names and to knowingly or recklessly initiate the transmission of multiple commercial electronic messages that have a Hong Kong link from such electronic addresses or domain names.

Part 5—Administration and enforcement

32. Part 5 of the Bill confers the necessary powers on the Authority to enable him to establish codes of practice and "do-not-call" registers for the purposes of the Bill and to deal with other administrative matters. Part 5 also sets out various provisions relating to the enforcement of the Bill.

33. Clause 26 defines certain terms used in Part 5 of the Bill including "approved code of practice", "authorized officer" and "specified offence". The latter term is used in clause 37 (*powers of entry, search, arrest, etc.*), clause 38 (*power of magistrate to issue search warrant*) and clause 40 (*recovery of costs and expenses of investigation by Authority*). In essence, a specified offence includes all the offences under the Bill except for the offences under Part 4 (*fraud and other illicit activities related to transmission of commercial electronic messages*) and clause 49 (*offences relating to appeals*).

34. Clause 27 empowers the Authority to appoint "authorized officers". The Bill confers certain powers on authorized officers including the power to certify extracts from the "do-not-call" registers (*see clause 30(7)*), to arrest offenders

(*see clause 37(1)(a)*) and to search premises under the authority of a warrant (*see clause 37(1)(b)*). Clause 27 confers the necessary powers on the Authority to enable him to appoint such officers.

35. Clause 28 authorizes the Authority to establish codes of practice relating to any provision of the Bill. Codes of practice are intended to provide practical guidance in respect of the application or operation of the provisions of the Bill. They are required to be published in the Gazette but do not constitute subsidiary legislation.

36. Clause 29 provides for how a code of practice may be used in legal proceedings. In essence, clause 29 provides that –

(a) if the court (which is defined to include the Unsolicited Electronic Messages (Enforcement Notices) Appeal Board established under clause 43(1)) is satisfied that a provision of a code is relevant to determining a matter in issue in the proceedings before the court, the code is admissible in evidence in those proceedings; and

(b) if it is proven that a person either contravened or did not contravene a provision of a code, then that fact may be relied on by any party to the proceedings as tending to establish or negate a matter in issue in the proceedings.

37. Clause 30 authorizes the Authority to establish one or more "do-not-call" registers. The purposes of a "do-not-call" register are described in clause 30(2). In essence, there are 2 basic and complementary purposes. The primary purpose is to provide registered users of electronic addresses with a means by which they may notify senders of commercial electronic messages that they do not wish to receive such messages. The other purpose is to provide senders of commercial electronic messages with a convenient means by which they may ascertain whether a registered user of a particular electronic address does not wish to receive such messages. If an electronic address is listed in a "do-not-call"

register, then commercial electronic messages are prohibited from being sent to that electronic address unless the registered user of that electronic address has consented (*see clause 10—commercial electronic messages must not be sent to electronic address listed in do-not-call register*). The Authority will be responsible for managing and operating any "do-not-call" registers established for the purposes of the Bill. The Authority may only list an electronic address in a "do-not-call" register if the registered user of that electronic address has consented to its inclusion in the register and to it being made available to senders of commercial electronic messages under clause 31 (*access to do-not-call registers*).

38. Clause 31 requires the Authority to make a "do-not-call" register, or the information contained in it, available to senders of commercial electronic messages. The Authority is given the power to decide the form and manner in which the information will be made available.

39. Clause 32(1) makes it an offence for any person to whom an unsubscribe request is sent under clause 8 (*commercial electronic messages must contain unsubscribe facility*) to use the information obtained thereby other than for the purpose of complying with the requirements of clause 8 or clause 9 (*commercial electronic messages must not be sent after unsubscribe request is sent*). The offence is intended to ensure that individuals or organizations to whom unsubscribe requests are sent do not use the information for a purpose unrelated to the requirements of clauses 8 and 9.

Clause 32(2) makes it an offence for any person to whom a "do-not-call" register, or the information contained in it, is made available under clause 31 (*access to do-not-call registers*) to use the information obtained thereby other than for the purpose described in clause 30(2)(b) (*Authority may establish do-not-call registers*). The offence is intended to ensure that persons to whom information contained in a "do-not-call" register is made available do not use the information other than for the purpose of ascertaining whether a registered user

of an electronic address does not wish to receive commercial electronic messages at that electronic address, which is the purpose described in clause 30(2)(b).

Under clause 32(3), a person who contravenes clause 32(1) or (2) is liable on summary conviction to a maximum fine at level 6 (currently $100,000). Under clause 32(4), a person who knowingly or recklessly contravenes clause 32(1) or (2) is liable on conviction on indictment to a maximum fine of $1,000,000 and imprisonment for a maximum term of 5 years.

Clause 32(5) provides that it is a defence to a charge for an offence under clause 32(3) for the person charged to prove that he took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

40. Clause 33 empowers the Authority to issue directions to a telecommunications service provider for the purpose of –

(a) facilitating the telecommunications service provider's compliance with the Bill or the regulations made under the Bill; or

(b) enabling the Authority or an authorized officer to perform any function under the Bill or the regulations.

41. Clause 34 provides that if the Authority 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 Authority's investigation of a contravention or suspected contravention of a provision of the Bill, he may serve a notice on the person requiring him to give the information or produce the document to the Authority. If the person is of the view that he cannot, or does not wish to, comply with the notice, then he may make representations to the Authority. If the Authority, after considering those representations, decides that the notice should remain in force, then the person must comply with the notice within a specified period, and if he fails to do so, the Authority may then seek an

order of a magistrate under clause 34(3) requiring the person to give the information or produce the document to the Authority.

Clause 34(8) provides that a person is not required to give any information or produce any document that may incriminate him.

Under clause 34(9), a person commits an offence if he, without reasonable excuse, fails to comply with an order made by a magistrate under clause 34(3). It is also an offence if he, without reasonable excuse, knowingly gives information that is false or misleading or fails to comply with clause 34(4), which in essence requires him to give the information or produce the document as it existed as at the time of service of the notice. The offences are punishable by a maximum fine at level 5 (currently $50,000) and imprisonment for a maximum term of 2 years. By virtue of section 94A of the Criminal Procedure Ordinance (Cap. 221), the burden of proving "reasonable excuse" mentioned in clause 34(9) lies on the person seeking to avail himself of the exception.

42. Clause 35 empowers the Authority to issue an enforcement notice to a person if he is of the opinion that that person is contravening any provision of Part 2 (*rules about sending commercial electronic messages*) or has contravened one of those provisions in circumstances that make it likely that the contravention will continue or be repeated. Under the enforcement notice, the Authority may direct the person to take corrective steps within a specified period, including steps recommended in a code of practice (*see clause 28—Authority may approve codes of practice*). The enforcement notice may be appealed to the Unsolicited Electronic Messages (Enforcement Notices) Appeal Board (*see Part 6 of the Bill*).

43. Clause 36 makes it an offence for any person to contravene an enforcement notice. The offence is punishable on a first conviction by a maximum fine at level 6 (currently $100,000) and on a second or subsequent conviction by a maximum fine of $500,000. In addition, in the case of a continuing offence, the court may impose a further maximum daily fine of $1,000 for each day during

which the offence continues. Clause 36(3) provides that it is a defence for the person charged to prove that he exercised all due diligence to comply with the enforcement notice.

44. Clause 37 empowers the Authority or any authorized officer to arrest without warrant any person whom he reasonably suspects of having committed a specified offence (*see discussion above at paragraph 33 for the meaning of "specified offence"*) and, where authorized by a warrant, enter and search the premises or place in respect of which the warrant is issued (*see clause 38—power of magistrate to issue search warrant*).

45. Clause 38 empowers a magistrate to issue a search warrant authorizing the Authority or an authorized officer to enter and search any premises or place if the magistrate is satisfied by information on oath that there are reasonable grounds for suspecting that there is, or is likely to be, in or on the premises or place any telecommunications device or other thing that is or that contains, or that is likely to be or to contain, evidence of the commission of a specified offence (*see discussion above at paragraph 33 for the meaning of "specified offence"*).

46. Clause 39(1) makes it an offence for any person to –

(a) wilfully obstruct the Authority or an authorized officer in the performance of his functions under the Bill;

(b) wilfully fail to comply with any requirement properly made to him by the Authority or an authorized officer; or

(c) without reasonable excuse, fail to give the Authority or an authorized officer any other assistance that he may reasonably require.

The offence is punishable by a maximum fine at level 3 (currently $10,000) and imprisonment for a maximum term of 6 months. By virtue of section 94A of the Criminal Procedure Ordinance (Cap. 221), the burden of proving "reasonable

excuse" mentioned in clause 39(1)(c) lies on the person seeking to avail himself of the exception.

Clause 39(2) makes it an offence for any person to make a statement that he knows to be false or does not believe to be true, or otherwise knowingly mislead the Authority, an authorized officer or any other person in the performance of his functions under the Bill. The offence is punishable by a maximum fine at level 5 (currently $50,000) and imprisonment for a maximum term of 2 years.

47. Clause 40 empowers the court to order a person who has been convicted of a specified offence to pay to the Authority the whole or a part of the costs and expenses of the investigation of that offence (*see discussion above at paragraph 33 for the meaning of "specified offence"*).

48. Clause 41 provides immunity from civil liability for the Authority, authorized officers and police officers in respect of any act done or default made by them in good faith in the performance of their functions under the Bill.

Part 6—Unsolicited Electronic Messages (Enforcement Notices) Appeal Board

49. Part 6 of the Bill establishes the Unsolicited Electronic Messages (Enforcement Notices) Appeal Board (the "Appeal Board") to which enforcement notices issued by the Authority may be appealed (*see clause 35—Authority may issue enforcement notice*). The basic procedure is as follows –

(a) The Appeal Board will have a Chairman and at least one Deputy Chairman, and a panel of members who are not public officers. Appointments to the Appeal Board will be made by the Chief Executive.

(b) The Chairman and Deputy Chairmen will be persons qualified for appointment as a District Judge under the District Court Ordinance (Cap. 336).

(c) The Appeal Board may uphold, vary or quash the enforcement notice and make consequential orders as may be necessary.

(d) Unless otherwise ordered by the Appeal Board, a decision appealed against is not suspended pending the appeal.

(e) Each hearing of the Appeal Board should comprise at least 3 members: the Chairman or a Deputy Chairman, who shall sit as the presiding officer, and 2 other members drawn from the appeal panel.

(f) Decisions by the Appeal Board are made by a simple majority, except where it involves a question of law which will be decided by the presiding officer.

(g) When hearing an appeal, the Appeal Board may administer oaths and affirmations, require evidence to be given on oath or affirmation, summon witnesses and order the recovery of costs incurred by the Appeal Board from any party to the appeal.

(h) The Appeal Board must state in writing the reasons for its decisions.

(i) Procedures relating to the hearing of appeals will be regulated by rules made by the Secretary. The Chairman may determine any matter of practice or procedure if the Bill or the rules do not contain provisions governing the matter.

50. Clause 42 defines certain terms used in Part 6 of the Bill including “appeal”, “Appeal Board”, “appellant”, “Chairman”, “Deputy Chairman”, “panel member” and “presiding officer”.

51. Clause 43 formally establishes the Appeal Board and provides for its composition, the terms of appointment for its members and their remuneration.

52. Clause 44 permits a person on whom an enforcement notice is served (*see clause 35—Authority may issue enforcement notice*) to appeal to the Appeal Board not later than 14 days after the enforcement notice is served on him.

53. Clause 45 provides for the procedure relating to an appeal including the following matters –

(a) For the purposes of an appeal, the Appeal Board shall consist of the Chairman or a Deputy Chairman ("the presiding officer") and 2 panel members appointed by the presiding officer.

(b) Every question before the Appeal Board shall be determined by the opinion of the majority of its members except a question of law which shall be determined by the presiding officer. In the case of an equality of votes, the presiding officer shall have a casting vote.

(c) Every sitting of the Appeal Board shall be held in public unless the Appeal Board considers that in the interests of justice the sitting should be held in private.

(d) A decision of the Appeal Board shall be in writing and include a statement of the reasons for the decision.

54. Clause 46 provides for the powers of the Appeal Board. Among other matters, the Appeal Board is given the power to –

(a) receive and consider any material;

(b) summon persons to appear before it or to produce to it any information or document that is relevant to the appeal;

(c) administer oaths and affirmations; and

(d) award costs against a party to an appeal.

55. Clause 47 provides that for the purposes of an appeal, the appellant, the Authority and any other person summoned to appear before the Appeal Board

shall each have the same privileges in respect of the disclosure of any material as if the proceedings before the Appeal Board were proceedings before a court.

56. Clause 48 allows the Appeal Board to refer any question of law arising in an appeal to the Court of Appeal for determination by way of case stated.

57. Clause 49 provides for offences in connection with appeals, including an offence relating to a person's failure without reasonable excuse to attend and give evidence when required to do so by the Appeal Board.

58. Clause 50 provides that members of the Appeal Board shall have the same privileges and immunities as a judge of the Court of First Instance in civil proceedings in that Court and that a witness shall be entitled to the same privileges and immunities as if he were a witness in civil proceedings in that Court.

59. Clause 51 empowers the Secretary to make rules regulating the practice and procedure of the Appeal Board.

Part 7—Miscellaneous

60. Part 7 of the Bill sets out miscellaneous and general provisions, including consequential amendments to other enactments.

61. Clause 52 creates a right of action that enables any person who suffers loss or damage by reason of a contravention of the Bill to bring proceedings against the person who committed the contravention. The right of action is not dependent on whether that person has been convicted of an offence. The proceedings must be brought in the District Court or, if the amount claimed does not exceed the amount mentioned in paragraph 1 of the Schedule to the Small Claims Tribunal Ordinance (Cap. 338) (currently $50,000), in the Small Claims Tribunal. If the proceedings are brought before the Small Claims Tribunal, the claim is to be treated by the Tribunal as a monetary claim founded in tort.

In essence, the remedies that the claimant may seek in the District Court include –

(a) a declaration that the respondent has committed an act in contravention of the Bill;

(b) an order that the respondent perform any reasonable act to redress any loss or damage suffered by the claimant;

(c) an order that the respondent pay compensation to the claimant for any loss or damage suffered by the claimant; and

(d) an injunction or any other appropriate remedy.

Under the Small Claims Tribunal Ordinance (Cap. 338), the jurisdiction of the Small Claims Tribunal for monetary claims founded in tort is currently limited to awarding damages of not more than $50,000. The Tribunal is not empowered to grant other remedies of the kind mentioned in paragraphs (a), (b) and (d) above.

62. Clause 53 sets out rules for determining the liability of principals and agents and employers and employees in cases where a principal or agent, or an employer or employee, has done any act or engaged in any conduct that contravenes the Bill. In essence, the rules provide that for the purposes of the Bill –

(a) an act done by an employee in the course of his employment shall be treated as having been done by both the employee and the employer;

(b) an act done by an agent for another person with the authority of that other person ("the principal") shall be treated as having been done by both the agent and the principal;

(c) in any criminal proceedings brought under the Bill in relation to an act done by an employee or agent of a person, it is a defence for that person to prove that he took

such steps as were practicable to prevent the employee or agent from doing the act; and

(d) in any criminal proceedings brought under the Bill against an employee, it shall be a defence for the employee to prove that he did the act in good faith in the course of his employment under the instructions of his employer.

63. Clause 54 sets out rules for determining the liability of persons who are responsible for the internal management of companies, partnerships or unincorporated bodies in cases where the company, partnership or unincorporated body has done any act or engaged in any conduct that constitutes an offence under the Bill. In essence, such persons are presumed also to have done the act or engaged in the conduct. A person charged with an offence under the Bill by virtue of clause 54(1) or (2) is taken to have proved that he did not authorize the act to be done or the conduct to be engaged in if sufficient evidence is adduced to raise an issue with respect to that fact and the contrary is not proved by the prosecution beyond reasonable doubt.

64. Clause 55 provides that a transaction is not void or voidable by reason only that a provision of the Bill has been contravened in relation to or as a result of the transaction. This provision has been included in the Bill to make clear that the Bill is not intended to interfere with the making of contracts or other transactions using electronic means of communications, notwithstanding that the communications may have been in breach of the requirements of the Bill.

65. Clause 56 empowers the Secretary to make regulations for the purposes of the Bill.

66. Clause 57 enacts Schedule 2 which makes consequential amendments to section 24 of the Telecommunications Ordinance (Cap. 106), Schedule 1 to the resolution of the Legislative Council establishing the Office of the Telecommunications Authority Trading Fund (Cap. 430D) made under the

Trading Funds Ordinance (Cap. 430), and Schedule 2 to the Electronic Transactions Ordinance (Cap. 553).

Section 24 of Cap. 106 makes it an offence for a telecommunications officer or any other person who has official duties in connection with a telecommunications service –

(a) to wilfully destroy, secrete or alter any message that he has received for transmission or delivery;

(b) to forge any message or utter any message that he knows to be forged or altered;

(c) to wilfully abstain from transmitting any message or wilfully intercept or detain or delay any message; or

(d) otherwise than in pursuance of his duty or as directed by a court, to copy any message or disclose any message to any person other than the person to whom it is addressed.

The amendment to section 24 of Cap. 106 makes clear that the offence does not apply to acts done by telecommunications officers or other persons who have official duties in connection with a telecommunications service for the purpose of –

(a) facilitating compliance with the Bill or any other law;

(b) implementing the terms or conditions of a licence of a licensee (a telecommunications service provider) or any contract made between a licensee and a customer of the licensee; or

(c) facilitating compliance with a lawful request of a customer of a licensee in connection with a service supplied by the licensee to the customer.

The amendment to Schedule 1 to Cap. 430D is technical and recognizes that the Authority will have responsibilities under the Bill in administering and enforcing its provisions.

The amendment to Schedule 2 to Cap. 553 has the effect of exempting from the application of sections 5, 5A, 6, 7 and 8 of Cap. 553 any information and documents used in proceedings before the Unsolicited Electronic Messages (Enforcement Notices) Appeal Board established under clause 43 of the Bill.