For Discussion
On 11 July 2005

Legislative Council Panel On Information Technology and Broadcasting

Draft Framework of Proposed Anti-spam Legislation

PURPOSE

This paper seeks Members' views on the draft framework of the proposed anti-spam legislation in Hong Kong.

BACKGROUND

2. On 25 June 2004, the Office of the Telecommunications Authority (OFTA) issued a consultation paper on "Proposals to contain the problem of Unsolicited Electronic Messages (UEMs)" (the Consultation Paper). The Consultation Paper examined the problem caused by various forms of UEMs (so-called "spam"), the effectiveness of the current measures and sought views on a range of possible ways to combat the problem, including the need for enactment of an anti-spam legislation.

3. Drawing on the views and ideas in the submissions and the latest developments, the Secretary for Commerce, Industry and Technology 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. Specifically, he intended to introduce a new anti-spam legislation.

4. Hong Kong has sophisticated telecommunications facilities, enormous capacity for external communications, high penetration rates for personal computers, Internet, and mobile services, and is an externally

oriented economy. All these factors have made Hong Kong vulnerable to spam. The proposed anti-spam legislation should help regulate the use of electronic messages as the means for promotion and/or sale of products and/or services, prevent Hong Kong from becoming a spam haven sheltering illicit spammers, and facilitate cooperation with law enforcement agencies of economies with similar legislation.

5. Between March and June 2005, we have engaged representative stakeholders to seek their views on the guiding principles and the key aspects of the framework for the proposed anti-spam legislation.

EXISTING LEGISLATIVE PROVISIONS ON SPAMMING-RELATED ACTIVITIES

6. At present, while there is no specific legislation dealing with UEMs, certain aspects of the spamming problem can be addressed by existing provisions in the legislation of Hong Kong. These are set out at **Annex A**. Nevertheless, those ordinances do not regulate the act of sending UEMs *per se*.

7. Some major overseas jurisdictions, such as Australia, the United Kingdom (UK), the United States of America (US), South Korea, and Japan, have introduced specific anti-spam legislation. A table comparing the key aspects of these anti-spam legislation is at **Annex B**.

GUIDING PRINCIPLES

8. After discussion with stakeholders, we consider that the proposed legislation should be guided by the following principles –

(a) recipients should have the right to decide whether to receive and refuse UEMs;

(b) the legislation should provide room for the development of e-marketing as a legitimate promotion channel;

(c) the legislation should prevent Hong Kong from becoming a safe haven for illicit spamming activities;

(d) freedom of speech and expression must not be impeded;

(e) penalties and remedies against spammers should be proportionate to the severity of the offences; and

(f) statutory provisions should be enforceable with reasonable efforts.

DRAFT FRAMEWORK

Scope

Nature of UEMs

9. The anti-spam legislation of all five economies cited in Annex B cover commercial communications only. For example, the Spam Act 2003 of Australia is applicable to "commercial electronic messages" unless they are exempted. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR 2003) of the UK is applicable to e-mail for direct marketing purposes. The US CAN-SPAM Act defines "commercial electronic mail message" as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)".

10. Since most UEMs in Hong Kong are of a commercial nature, we propose that we should align with other jurisdictions by regulating only UEMs of a commercial nature. This is a pragmatic approach that would bring the majority of UEMs under the legislation. Non-commercial messages, such as Government-to-citizen communications, appeals for donations by charities and religious organisations, and communications from political parties, will not be covered in the proposed legislation.

Form of UEMs

11. Anti-spam laws of different economies differ in which forms of UEMs their laws cover. In Australia, its anti-spam law regulates electronic messages, which are defined as including e-mails, instant messages and telephone calls. UK's legislation covers the use of automated calling systems, fax and e-mails. The laws of US and Japan focus on e-mails only. South Korea's law embraces e-mail, telephone, fax, and "other media prescribed by the Presidential Decree".

12. We propose to cover all forms of electronic messages including e-mails, faxes, SMS/MMS and voice/multi-media messages generated by automated means (e.g. pre-recorded voice messages sent through Interactive Voice Response System (IVRS)). This is suitable to the rapid development of the information and communications technology industry, where new forms of electronic communications may be created to meet demand and where the costs of sending electronic messages in potentially less spam-prone areas (e.g. SMS/MMS currently) could fall, making them economically viable for spamming. It was reported that in Japan, where the anti-spam legislation covers e-mails only, some spammers have shifted their activity over to the SMS/MMS platform. We consider that the compliance burden on businesses should not be too onerous if the requirements in the proposed legislation are reasonable and are indeed good practices to be promoted within the industry.

13. Unlike telephone calls generated by automated means, which could be generated in large numbers within a short period of time and at low costs, the costs for manually making the calls are higher which may limit the extent to which such calls would become a spam problem. We also need to balance the right of recipients with the right of businesses to use such means for legitimate commercial purposes. We therefore propose to exclude voice calls / multi-media calls which are not generated by automated means from the proposed legislation.

Origin of UEMs

14. Guided by the principle of enforceability with reasonable efforts, we propose to stipulate that the proposed anti-spam legislation will be

applicable to the act of sending the UEM, if the initiator of the UEM, or an agent of the initiator of the UEM commissioned to send the UEM, is physically in Hong Kong, irrespective of where the sending server is located, or at which geographic location the spammer targets. This approach has the following advantages:

(a) since most forms of spam in Hong Kong actually originate locally, the legislation could tackle them effectively. For e-mails spam the majority of which originate from overseas, we would seek international cooperation in curbing the problem;
(b) it would prevent Hong Kong from becoming a haven for spammers;
(c) it is enforceable with reasonable efforts; and
(d) it is in line with the international best practice.

Right of Recipients

"Opt-in" vs. "Opt-out"

15. There are generally two regimes for safeguarding recipients from spam. An "opt-out" regime requires the sender to stop sending further unsolicited commercial communications to a recipient if the recipient so requests. Until the request is made, the sender may send such messages. In comparison, under an "opt-in" regime, the sender cannot send any unsolicited commercial communications unless the sender has some pre-existing business relationship with the recipient, or until such time the potential recipient indicates to the sender that he wishes to receive such communications. Approximately two-thirds of the World's anti-spam laws (including the many state spam laws in the US) are considered "opt-out" while approximately one-third are "opt-in"[1].

16. The "opt-in" regime provides a higher standard for protection for recipients. However, since electronic communication is a low cost means for Small and Medium Enterprises (SMEs) to promote their products and services, the "opt-in" regime is potentially a barrier to SMEs and start-ups. It should be noted that for serious UEM cases with criminal intent, the

[1] Source: a Discussion Paper issued by the International Telecommunication Union on "Countering Spam: How to Craft an Effective Anti-Spam Law"

existing or the proposed legislation would try to tackle them irrespective of whether an "opt-in" or an "opt-out" regime is adopted.

17. On the other hand, the "opt-out" regime would provide companies with more room to promote their products or services, and in turn, facilitate development of SMEs. Bearing in mind that 98% of Hong Kong's business establishments are SMEs providing employment to 60% of the workforce, and that SMEs, particularly start-ups, generally do not have a strong customer base, and may not have the resources to undertake costly promotional activities, the "opt-out" regime appears more appropriate for Hong Kong. It is also consistent with the approach in regulating direct marketing activities using personal data under the Personal Data (Privacy) Ordinance (Cap. 486). In day-to-day activities, the "opt-out" approach is generally accepted by the community. It provides recipients with the choice to browse through promotion information before deciding whether to receive further messages. But there are also shortcomings of the "opt-out" regime. It could send a negative signal to the spammers that UEMs could be sent without consent. The act of opting out could enable spammers to confirm the recipients' existence that may encourage further spamming and sharing of e-mail addresses. Recipients also need to unsubscribe from a large number of messages initially. These shortcomings can however be addressed through wider education on tackling spam, and effective enforcement of the proposed anti-spam legislation in future. On balance, therefore, the "opt-out" regime would be more appropriate for the circumstances of Hong Kong.

Unsubscribe Request

18. As an UEM from a company may promote different products and/or services in the same message, the legislation needs to specify exactly what a recipient is opting out or unsubscribing from – whether from all future messages from the sending party of the UEM, or only from future messages promoting similar products or services. We propose the former approach which is clearer to recipients. That is, once a recipient chooses to unsubscribe a message from a sending party, the unsubscription will be applicable to all messages sent from the same sending party (who can either be a person/company sending the message or having authorised the sending of the message, as the case may be) in relation to all types of

products and/or services. However, if the sender provides recipients with a choice of messages by products/services to be unsubscribed, the unsubscription should only be confined to messages for such products and/or services specified by the recipients.

19. Drawing reference to the anti-spam law in US, we propose that the sending party would need to effect the requests for un-subscription within 10 working days from the day when the requests are submitted by the recipients.

Activities to be Prohibited

20. There are different kinds of spamming activities. Drawing on the provisions in anti-spam legislation in other jurisdictions, we propose that there could be three groups of activities to be prohibited, categorised according to their degree of seriousness –

Group 1	Group 2	Group 3
(a) Continue to send commercial electronic messages to a recipient after his/her unsubscription request should have taken effect. (b) Failure to provide a functional unsubscribe facility. (c) Failure to provide accurate sender information. (d) Commercial electronic messages having misleading subject headings.	(e) Harvesting electronic addresses from websites or web services that have published a notice prohibiting the transfer of electronic addresses for the purpose of spamming. (f) Supply or offer to supply electronic address-harvesting software and harvested-electronic address lists for the purpose of spamming. (g) Acquisition of electronic address-harvesting	(l) Use a computer or communications device without authorisation, and intentionally initiate the transmission of multiple commercial electronic messages from or through such computer/device. (m) Use a computer or communications device to relay or retransmit multiple commercial electronic messages, with the intent to deceive or mislead recipients, or any Internet access service or communications

Group 1	Group 2	Group 3
	software and harvested-electronic address lists for the purpose of spamming. (h) Use of electronic address-harvesting software and harvested-electronic address lists for the purpose of spamming. (i) Sending commercial electronic messages to non-existent electronic addresses (e.g. using a "dictionary attack"). (j) Using scripts or other automated ways to register for multiple electronic communication or user accounts for the purpose of spamming. (k) Relaying electronic messages through a computer or network without permission – for example, by taking advantage of open relays or open proxies without authorisation.	services, as to the origin of such messages. (n) Materially falsify header information in multiple commercial electronic messages and intentionally initiate the transmission of such messages. (o) Register, using information that materially falsifies the identity of the actual registrant, for [five] or more electronic communications accounts or [two] or more domain names, and intentionally initiate the transmission of multiple commercial electronic messages from any combination of such accounts or domain names. (p) Falsely represent oneself to be the registrant or the legitimate successor in interest to the registrant of [five] or more Internet Protocol addresses or domain names, and intentionally

Group 1	Group 2	Group 3
		initiate the transmission of multiple commercial electronic messages from such addresses.

21. Group 1 activities are those that could be committed, possibly inadvertently, by legitimate e-marketers, and undermine the proposed "opt-out" regime and the ability of the recipients of UEMs to exercise their rights. Group 2 activities are common techniques used by spammers to maximise their reach of potential recipients. Group 3 activities are activities with serious criminal intent.

Proposed Penalty Framework

Group 1 Activities

22. For Group 1 activities, our policy objective should be to put right malpractices. We are hence of the view that we may adopt a mechanism similar to the Enforcement Notice regime under the Personal Data (Privacy) Ordinance (Cap. 486). The enforcement agency should be given the power under the proposed legislation to issue an enforcement notice to parties considered by the enforcement agency to have failed to comply with the requirements of the proposed legislation in relation to Group 1 activities. If a party fails to comply with the enforcement notice, the enforcement agency may initiate proceedings to seek the court to impose a fine. Drawing on the penalties applied in Australia for similar offences, we propose that the appropriate level of fine is towards the upper end of the levels prescribed in schedule 8 of the Criminal Procedure Ordinance (Cap. 221) (i.e. up to $100,000).

23. We propose that OFTA should be the enforcement agency for Group 1 activities. As it operates on a trading fund basis, OFTA should be entitled under the proposed legislation to recover the whole or the part (as the case may be) of the costs and expenses as a civil debt due to it on a conviction before a court, similar to the arrangements under section 184 of

the Securities and Futures Ordinance (Cap. 571).

Group 2 Activities

24. Group 2 activities would unlikely be undertaken by legitimate business. They are activities whereby spammers use tools and means to abuse the electronic communications channels to gain financial benefits. As such, we do not consider that the offenders should be given an opportunity to make amend by way of an enforcement notice. The enforcement agency should start court proceedings as soon as it has sufficient evidence to press charges. On the level of penalty, we consider that the levels of fine prescribed in schedule 8 of the Criminal Procedure Ordinance (Cap. 221) may not be sufficient as a deterrent and propose to prescribe higher levels of fines in the proposed legislation. We consider that rising fines for each subsequent breach may be called for as deterrents. It is for consideration whether imprisonment should also be a possible penalty for Group 2 activities.

25. We propose that OFTA could be the enforcement agency for Group 2 activities. OFTA should similarly be entitled to recover the whole or the part (as the case may be) of the costs and expenses as a civil debt due to it on a conviction before a court.

Group 3 Activities

26. For Group 3 activities which are deliberately undertaken by spammers with clear criminal intent, imprisonment would be necessary as a penalty. We can make reference to the existing offence of "access to computer with criminal or dishonest intent" under Section 161 of the Crimes Ordinance (Cap. 200)[2], which attracts a penalty of up to 5 years imprisonment on conviction upon indictment. Under section 60 of the Crimes Ordinance (Cap. 200), a person who without lawful excuse destroys or damages any property can be liable for imprisonment for up to 10 years.

---

[2] Under this section, any person who obtains access to a computer-
(a) with intent to commit an offence;
(b) with a dishonest intent to deceive;
(c) with a view to dishonest gain for himself or another; or
(d) with a dishonest intent to cause loss to another
commits an offence and is liable on conviction upon indictment to imprisonment for 5 years.

It is for consideration whether apart from imprisonment, financial penalties should be imposed for Group 3 activities.

27. In view of the nature of Group 3 activities, enforcement would be undertaken by the Police.

Rights to Commence Legal Actions

28. For the anti-spam legislation, we consider it necessary for the government to take up the primary responsibility to carry out investigations, take enforcement actions, and commence legal actions.

29. As regards the rights of victims, some overseas legislation give the victims of spam the right to bring actions against spammers while other jurisdictions recognise that the victims generally do not have the necessary resources to carry out investigations and bring actions to court.

30. For the proposed legislation in Hong Kong, our preliminary view is to follow the arrangement in the Personal Data (Privacy) Ordinance (Cap. 486) whereby victims should be empowered by the proposed legislation to seek damages from the convicted spammers, but separate from the proceedings undertaken by the enforcement agency against the spammers. Internet service providers, the intermediary parties (e.g. those whose computers were hacked and damaged because of spammers' actions), and the recipients of UEMs would have the statutory right to make civil claims against convicted spammers.

WAY FORWARD

31. Subject to Members' views, we shall proceed to formulate the details of the legislation which would form the basis for public consultation around end 2005 or early 2006. Our target is to introduce the bill into the Legislative Council within 2006.

32. Before the proposed legislation commences operation, the Government would mount a public information programme on the detailed provisions of the legislation so that the public, SMEs and e-marketers

would understand their rights and responsibilities under the legislation. Companies and e-marketers would be allowed time to set up their systems to enable them to operate effectively under the "opt-out" regime.

Communications and Technology Branch
Commerce, Industry and Technology Bureau
July 2005

Existing Legislative Provisions on Spamming-related Activities

(a) If the sending of spam involves unauthorised access to computer by telecommunications (commonly known as hacking), it may be punishable under Section 27A of the Telecommunications Ordinance. (Relevant provision is at **Annex A1**.)

(b) If a spammer sends e-mails to a computer causing it to cease functioning, or in a manner which amounts to "misuse of a computer" as defined in Section 59 of the Crimes Ordinance, he could be liable for an offence under Section 59 of the Crimes Ordinance. Alternatively, he could have committed an offence of criminal damage under Section 60 of the Crimes Ordinance. (Relevant provisions are at **Annex A2**.)

(c) If e-mails are used as vehicles to deceive inadvertent victims (e.g. "419" letters and phishing e-mails), an element of "fraud" may be involved. If proved, this will constitute an offence under Section 16A of the Theft Ordinance. (Relevant provision is at **Annex A3**.)

(d) If the e-mails contain malware (e.g. Trojan programmes, virus, hacking tools etc.) facilitating the sender to gain access to a computer system without authority, then depending on the intent of the person gaining unauthorised access to the computer system, he could have committed an offence under Section 27A of the Telecommunications Ordinance and/or "access to computer with criminal or dishonest intent" under Section 161 of the Crimes Ordinance. (Relevant provision is at **Annex A4**.)

雙語法例資料系統
Bilingual Laws Information System

Individual Section Mode

Previous section of enactment | Next section of enactment | Switch language | Back to the List of Laws

Contents of Section

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

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

(a) the intent of the person need not be directed at-
(i) any particular program or data;
(ii) a program or data of a particular kind; or
(iii) a program or data held in a particular computer;
(b) access of any kind by a person to any program or data held in a computer is unauthorized if he is not entitled to control access of the kind in question to the program or data held in the computer and-
(i) he has not been authorized to obtain access of the kind in question to the program or data held in the computer by any person who is so entitled;
(ii) he does not believe that he has been so authorized; and
(iii) he does not believe that he would have been so authorized if he had applied for the appropriate authority.

(3) Subsection (1) has effect without prejudice to any law relating to powers of inspection, search or seizure.
(4) Notwithstanding section 26 of the Magistrates Ordinance (Cap 227), proceedings for an offence under this section may be brought at any time within 3 years of the commission of the offence or within 6 months of the discovery of the offence by the prosecutor, whichever period expires first.
(Added 23 of 1993 s. 2)

Previous section of enactment | Next section of enactment | Switch language | Back to the List of Laws

Individual Section Mode

Previous section of enactment | Next section of enactment | Switch language | Back to the List of Laws

Contents of Section

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

PART VIII

CRIMINAL DAMAGE TO PROPERTY

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

(a) property of a tangible nature, whether real or personal, including money and-
(i) including wild creatures which have been tamed or are ordinarily kept in captivity, and any other wild creatures or their carcasses if, but only if, they have been reduced into possession which has not been lost or abandoned or are in the course of being reduced into possession; but
(ii) not including mushrooms growing wild on any land or flowers, fruit or foliage of a plant growing wild on any land; or
(b) any program, or data, held in a computer or in a computer storage medium, whether or not the program or data is property of a tangible nature.

In this subsection, "mushroom" (菌類植物) includes any fungus and "plant" (植物) includes any shrub or tree. (Replaced 23 of 1993 s. 3)
(1A) In this Part, "to destroy or damage any property" (摧毀或損壞財產) in relation to a computer includes the misuse of a computer.
In this subsection, "misuse of a computer" (誤用電腦) means-

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

and any act which contributes towards causing the misuse of a kind referred to in paragraph (a), (b) or (c) shall be regarded as causing it. (Added 23 of 1993 s. 3)

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

(a) having the custody or control of it;
(b) having in it any proprietary right or interest (not being an equitable interest arising only from an agreement to transfer or grant an interest); or
(c) having a charge on it.

(3) Where property is subject to a trust, the persons to whom it belongs shall be so treated as including any person having a right to enforce the trust.
(4) Property of a corporation sole shall be so treated as belonging to the corporation notwithstanding a vacancy in the corporation.

(Added 48 of 1972 s. 3)
[cf. 1971 c. 48 s. 10 U.K.]

Previous section of enactment | Next section of enactment | Switch language | Back to the List of Laws

Individual Section Mode

Contents of Section

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

(1) A person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage any such property or being reckless as to whether any such property would be destroyed or damaged shall be guilty of an offence.
(2) A person who without lawful excuse destroys or damages any property, whether belonging to himself or another-

(a) intending to destroy or damage any property or being reckless as to whether any property would be destroyed or damaged; and
(b) intending by the destruction or damage to endanger the life of another or being reckless as to whether the life of another would be thereby endangered,

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

(Added 48 of 1972 s. 3)
[cf. 1971 c. 48 s. 1 U.K.]

Individual Section Mode

Previous section of enactment | Next section of enactment | Switch language | Back to the List of Laws

Contents of Section

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

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

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

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

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

(3) For the purposes of this section-

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

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

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

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

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

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

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

(Added 45 of 1999 s. 3)

Previous section of enactment | Next section of enactment | Switch language | Back to the List of Laws

Individual Section Mode

Previous section of enactment | Next section of enactment | Switch language | Back to the List of Laws

Contents of Section

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

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

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

whether on the same occasion as he obtains such access or on any future occasion, commits an offence and is liable on conviction upon indictment to imprisonment for 5 years.
(2) For the purposes of subsection (1) "gain" (獲益) and "loss" (損失) are to be construed as extending not only to gain or loss in money or other property, but as extending to any such gain or loss whether temporary or permanent; and-

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

(Added 23 of 1993 s. 5)

Previous section of enactment | Next section of enactment | Switch language | Back to the List of Laws

Annex B

AN INTERNATIONAL COMPARISON OF SPAM CONTROL LEGISLATION[1]

	Australia	United Kingdom	United States	South Korea	Japan
Relevant legislation	Spam Act 2003 Spam (Consequential Amendments) Act 2003	Electronic Commerce (EC Directive) Regulations 2002 (ECR 2002) Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR 2003)	CAN-SPAM Act of 2003	Act on Promotion of Information and Communications Network Utilization and Information Protection of 2001	The Law on Regulation Transmission of Specified Electronic Mail (July 2002) Specific commercial transactions law (July 2002)
Definition of spam	The Act uses "commercial electronic messages". S 5(1) defines "electronic messages" to include e-mails, instant messages and telephone calls. S 6(1) defines "commercial electronic message".	ECR 2002 uses "unsolicited commercial communications sent by e-mail": reg 8 ECR 2002. PECR 2003 covers use of automated calling systems: reg 19(1), facsimile machines: reg 20(1), calls: reg 21(1) and electronic mails: reg 22 (1) NB. Some obligations applicable to commercial	The Act uses "commercial electronic mail messages": s 5(a)(4)(A). Definitions of - `electronic mail address': s 3(5); and -'electronic mail message': s 3(6).	Any commercial advertisement sent via e-mail, telephone, facsimile or other media prescribed by Presidential Decree transmitted to a consumer against consumer's expressed rejection and therefore in violation of the law.	The law uses "unsolicited commercial e-mail".

[1] Modified from information contained in the Joint IDA-AGC Consultation Paper on "Proposed Legislative Framework for the Control of E-mail Spam".

	Australia	United Kingdom	United States	South Korea	Japan
		communications generally			
Confined to "commercial" electronic messages	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Extra-territorial jurisdiction	Certain provisions of the Act apply to commercial electronic messages with an Australian link, which is defined in s 7.	-	-	-	-
Opt-in vs. opt-out	*Opt-in* Section 16(1): Unsolicited commercial electronic messages must not be sent: - unless recipient has consented: s 16(2). - consent can be express or inferred: para. 2 of Sch. 2.	*Opt-in* Person not to transmit unsolicited communications for the purposes of direct marketing by means of electronic mail unless recipient previously consented or sent at recipient's instigation: reg 22(2) PECR 2003. Reg 22(3) PECR 2003: Exceptions: - existing customer or contact details obtained from recipient in previous negotiations; - direct marketing of	*Opt-out* Prohibition of transmission of commercial electronic messages after objection: s 5(a)(4).	*Opt-out* Art 50 Restrictions on transmission of advertisement information: - any person shall be prohibited from transmitting advertisement information for the purpose of soliciting business against the addressee's explicit rejection of such information. In 2005, the Ministry of Information and	*Opt-out* Transmission of specified emails to person who has requested not to receive them prohibited.

	Australia	United Kingdom	United States	South Korea	Japan
		similar products and services; and - unsubscribe facility at time contact details collected and at each subsequent communication.		Communication (MIC) in South Korea announced an opt-in policy from 31 March 2005 for UEMs send via phones or faxes, while for email spam, the opt-out policy will still be implemented.	
Valid return e-mail address	Commercial electronic message to include accurate information about how the recipient can readily contact sender: s 17(1)(b).	E-mail communications for the purposes of direct marketing not to be transmitted where valid return address has not been provided: reg 23(b) PECR 2003.	Unlawful to send commercial electronic mail message that contains header information that is materially false or misleading: s 5(a)(1) – - inclusion of return e-mail address: s 5(a)(3). - inclusion of physical address: s 5(a)(5)(iii). Secondary liability for businesses knowingly thus promoted: s 6.	Art 11 Ordinance of the Ministry of Information and Communication of the Act: - must have clear posting of addressor's name, telephone number and contact person.	(see under Labelling requirements) Unsolicited commercial e-mail must include sender's email address.
Functional unsubscribe facility	Commercial electronic messages must contain a functional unsubscribe facility: s 18(1).	Simple means of refusing use of contact details for the sending of electronic mail for the purposes of direct	Functional internet-based opt-out mechanism: s 5(a)(3). Inclusion of clear and	Art 11 Ordinance of the Ministry of Information and Communication of the Act:	(see under Labelling requirements) Unsolicited commercial e-mail must include

	Australia	United Kingdom	United States	South Korea	Japan
		marketing to be provided at time contact details initially collected and at time of each subsequent communication: reg 22(3)(c) PECR 2003. Valid return address to which opt-out request can be sent: reg 23(b) PECR 2003.	conspicuous notice of opportunity to opt out: s 5(a)(5)(ii).	- must have clear instructions on how to reject future e-mails; - commercial advertisement senders must install toll-free numbers so that recipients may express their intention not to receive any spam in the future. Art 50(2) Restrictions on transmission of advertisement information: - to indicate matters concerning easy methods to reject receipt of future advert. information.	opt-out e-mail address.
Identify sender	Commercial electronic message to clearly and Australia accurately identify sender: s 17(1)(a).	Commercial communications to clearly identify person on whose behalf it is made: reg 7(b) ECR 2002	Line identifying the person initiating the message to United States accurately not to be materially false or misleading: s 5(a)(1)(B) Secondary liability for businesses knowingly thus promoted: s 6.	Art 50(2) Restrictions on transmission of South Korea advertisement information: to indicate the following: - types of transmission and major contents in there; - name/contact means of	Unsolicited commercial e-mail must include Japan sender's name and address.

	Australia	United Kingdom	United States	South Korea	Japan
				addressor.	
Labelling requirements	-	Unsolicited commercial communications to be identifiable as such as soon as it is received: reg 8 ECR 2002. Commercial communications to be clearly identifiable as commercial communications: reg 7(a) ECR 2002. Promotional offers, competitions or games and conditions to be clearly identified: s 7(c) & (d) ECR 2002.	Prohibition of deceptive subject headings: s 5(a)(2). Inclusion of identifier that message is an advertisement or solicitation: s 5(a)(5)(i). Requirement to place warning labels on spam containing sexually oriented material: s 5(d).	Art 11 Ordinance of the Ministry of Information and Communication of the Act: - initials `ADV' must be included in mail header	Obligation of labelling for senders of specified email: 1. Identification as specified e-mail; 2. Sender's name/ address; 3. Sender's e-mail address; 4. Opt-out e-mail address.
Dictionary attacks	Person must not send commercial electronic message to a non-existent electronic address that he has no reason to believe that exists : s 16(6).	-	Prohibition to transmit unlawful commercial electronic mail messages using, or to provide list of addresses obtained through, dictionary attacks: s 5(b)(1)(A)(ii).	Art 50(6) Restrictions on transmission of advertisement information: prohibition on use of software or other technical equipment that generate contacts by collating with numbers, codes or characters.	Prohibition of mail transmission utilizing the program that generates random fictitious e-mail addresses Telecommunications carriers are permitted not to provide a volume of e-mail transmission services if the emails

	Australia	United Kingdom	United States	South Korea	Japan
					include random fictitious addresses.
Address harvesting	Address-harvesting software and harvested-address lists must not be: - Supplied: s 20(1); -Acquired: s 21(1); or - Used: s 22(1).	-	Prohibition to transmit unlawful commercial electronic mail messages using, or to provide list of addresses obtained through, address harvesting: s 5(b)(1)(A)(i).	2 of Art 50: Prohibition of harvesting e-mail addresses from websites, etc.: - no person shall harvest e-mail addresses from websites that expressly prohibit automatic harvesting with software or other equipment; - no sale or circulation of e-mail addresses in violation of (1); - no person shall knowingly use e-mail addresses that have been automatically harvested for purpose of sale/ exchange regarding transmission of advertisement information. Art 50(2) Restrictions on transmission of advertisement information: to indicate source of e-mail address harvested.	-

	Australia	United Kingdom	United States	South Korea	Japan
Automated throwaway accounts	-	-	Unlawful to use automated means to register for multiple e-mail accounts from which to transmit unlawful commercial electronic mail messages: s 5(b)(2).	-	-
Right to commence legal action	"Victim" i.e. person who has suffered loss or damage, may apply to court for compensation: s 28. Australian Communications Authority (ACA) may apply to court: ss 26, 28,29.	Person who suffers damage entitled to bring proceedings for compensation: reg 30 PECR 2003.	State Attorney-General may bring civil action: s 7(f). ISP adversely affected may bring civil action: s 7(g).	-	-
Exemptions on telecommuni-cations service providers	A person does not contravene the ancillary provisions (aiding, abetting, counselling, procuring) of the Act merely because the person supplies a carriage service that enables an electronic message to be sent. ss 16(10), 17(6), 18(7)	-	-	-	-

	Australia	United Kingdom	United States	South Korea	Japan
Obligation on telecommuni-cations service providers	-	Service providers shall take appropriate technical and organisational measures to safeguard the security of that service, and inform the subscribers of the risk concerned. Reg 5 PECR			
Remedies (Civil/Criminal)	The main remedies for breaches of the Act are: - civil penalties: Pt 4 - compensation to victim: s 28 - injunctions: Pt 5.	Compensation for person who suffers damage: reg 30 PECR 2003. Enforcement under Part V of the Data Protection Act 1998: reg 31 PECR 2003. - enforcement notice: reg 32 (failure to comply: offence (s 47))	Enforcement by Federal Trade Commission: - fines & imprisonment: s 1037(b) Chapter 47 of title 18, United States Code; and -forfeiture: s 1037(c) Chapter 47 of title 18, United States Code. Civil action by States: - injunction: s 7(f)(2); and - statutory damages: s 7(f)(3). Civil action by ISP: -injunction: s 7(g)(1)(A) - damages of actual monetary loss: s 7(g)(a)(B) - statutory damages: s 7(g)(3).	Fines generally.	Administrative Orders by Minster to keep law Fines up to 500,000 yen assessed on failure to observe Administrative Order

	Australia	United Kingdom	United States	South Korea	Japan
Enforcement Agency	Australia Communications Authority (ACA)	Office of Communications (OFCOM) for matters under its existing functions as specified under Chapter 1 of the Communications Act 2003 The Information Commissioner for regulations relating to Data Protection Act 1998	Federal Trade Commission (FTC)	Korean Ministry of information and Communication	
Persons who may be liable	Sender of commercial electronic messages. Any person who: - aids, abets, counsels or procures a contravention; - induces, whether by threats or promises or otherwise, a contravention; - in any way, directly or indirectly, is knowingly concerned in or party to, a contravention; or - conspires with others to effect a contravention.	Any person transmitting or instigating the transmission of a communication: PECR 2003	Sender of commercial electronic mail message. Any person who initiates/procures transmission of commercial electronic mail message (s. 5)	Any person transmitting advertisement information.	Sender.

	Australia	United Kingdom	United States	South Korea	Japan
Multi-pronged approach	Australian Communications Authority (ACA) has the following additional functions: - education: s 42(a); - research: s 42(b); and - international co-operative arrangements: s 42(c).	No formal regulatory framework mandated - but appropriate industry filtering initiatives encouraged.	Technical solution: - black lists - e-mail filters promoted. Self regulation.	Art 50(4) Restrictions of service for transmitting advertisement: - ISP may deny certain services at their discretion where there is or will be obstruction caused by repetitive transmission spam, or if users don't wish to receive such information; - ISP shall indicate its right of denial in its contract ; - Where ISP intends to deny certain service, it shall give notice to user of that service or persons having an interest.	ISPs may take measures to suspend service usage for spammers. ISPs to provide email filtering services. Email marketing groups to make guidelines for email advertisements. Future plans to promote self-regulatory and technical solutions by ISPs and mobile operators. Awareness actions.

Communications and Technology Branch
Commerce, Industry and Technology Bureau
July 2005