PROPOSED LEGISLATIVE FRAMEWORK FOR THE CONTROL OF E-MAIL SPAM

(Joint IDA-AGC Consultation Paper)

25 May 2004

PROPOSED LEGISLATIVE FRAMEWORK FOR THE CONTROL OF E-MAIL SPAM

CONTENTS

JOINT IDA–AGC CONSULTATION PAPER

PROPOSED LEGISLATIVE FRAMEWORK FOR THE CONTROL OF E-MAIL SPAM

EXECUTIVE SUMMARY

Spam is a complex, multi-faceted issue and there is no single solution against spam. To reduce spam in Singapore, the Infocomm Development Authority of Singapore (IDA) is adopting a multi-pronged approach which combines use of technology, public education, self-regulation, spam control legislation and international cooperation.

2 IDA and the Attorney-General's Chambers of Singapore (AGC) have conducted a joint study to review Singapore's legislative options against spam as part of the multi-pronged approach. This Consultation Paper seeks guidance and feedback on the proposed legislative framework for the control of spam.

3 The proposed legislative framework seeks to balance the legitimate interests and concerns of different groups such as e-mail users and Internet Service Providers (ISPs) on the one hand, and marketers on the other. The proposal to introduce spam control legislation is consistent with many developed IT savvy jurisdictions such as Australia, the United Kingdom, the United States, Japan and South Korea. These countries have enacted anti-spam legislation.

4 This Consultation Paper highlights the main features of the proposed legislative framework, as follows:

(a) Definition of spam;

(b) Application of the proposed legislation;

(c) Requirements for the sending of unsolicited commercial e-mail;

(d) Legal action for breach of the requirements;

(e) Civil action for dictionary attacks and use of automated spamming tools; and

(f) Codes of practice.

Definition of spam

5 It is proposed that spam be defined as unsolicited commercial e-mail messages.

6 Commercial communications would exclude communications such as those between private individuals, Government to citizen communications, appeals for donations by charities and religious organizations, and messages which are of a purely factual nature.

Application of the proposed legislation

7 It is proposed that the legislation apply to spam transmitted in bulk. The definition of "in bulk" is important. It may be determined by a subjective test or by reference to a minimum numerical threshold.

8 It is further proposed that the legislation apply to spam originating from or received in Singapore. This would serve to minimize the risk that Singapore may be used as a base for which spamming activities against addressees in other countries can be carried out.

9 Apart from the spammer, it is proposed that the merchant or business commissioning or procuring spam should also be made liable for unlawful spam under the proposed legislation.

Requirements for the sending of unsolicited commercial e-mail

10 Not all unsolicited commercial e-mail communications would be disallowed. Unsolicited commercial e-mail communications which comply with the minimum standards for an opt-out regime, labelling requirements and other prescribed requirements will be regarded as legitimate communications under the proposed legislation. They will not be subject to any legal action as long as all opt-out requests are complied with.

11 The proposed legislation will establish an opt-out regime, requiring senders of unsolicited commercial e-mail to provide an opt-out mechanism which complies with the following minimum standards:

(a) Each unsolicited commercial e-mail should contain a valid return e-mail address to which an opt-out request can be sent

by a recipient, or an Internet location address at which a recipient can access the opt-out mechanism.

(b) Instructions for opting out of future unsolicited commercial e-mails can be in other languages but there should be one version in English.

(c) The opt-out mechanism should be functional.

(d) Where an opt-out request has been received, the sender should not transfer the e-mail address of the recipient in a manner contrary to his request, for example, where the recipient has requested to opt-out of future unsolicited commercial e-mails from the sender as well as his partners, the recipient's e-mail address should not be transferred to business partners for the purposes of enabling them to send unsolicited commercial e-mail.

(e) Senders of unsolicited commercial e-mails must comply with opt-out requests within a specified time frame.

12 To encourage self-help, it is proposed to establish minimum labelling standards to identify unsolicited commercial e-mails. The following requirements are proposed:

(a) The subject title of e-mail messages should not be labelled in a manner that misleads the recipient as to their content;

(b) The subject title should contain the characters '[ADV]' to identify unsolicited commercial e-mail messages as such;

(c) The e-mail messages should not contain a false header;

(d) The e-mail messages should have a genuine e-mail address; and

(e) The e-mail messages should have a valid postal address.

Legal action

13 Where spam is transmitted in breach of the minimum standards for the opt-out regime, labelling or other prescribed requirements, it is proposed that ISPs which have suffered loss or damage as a result of the

spamming activity be given a statutory right to commence a civil action in court. The remedies available are:

(a) damages for pure economic loss suffered because of the unlawful spam; or

(b) statutory damages for notional loss; and

(c) costs and expenses of the action.

14. ISPs may also apply to the court for an injunction to stop the unlawful spamming activity.

Civil action for dictionary attacks and use of automated spamming tools

15 Where spam is sent through the use of a dictionary attack or any automated spamming tool, it is proposed that ISPs be allowed to commence legal action against the spammer without having to prove that the e-mail messages fail to comply with the requirements for the sending of unsolicited commercial e-mail.

Co-regulation - codes of practice

16 It is proposed that the spam control legislation impose a duty on industry players, such as ISPs, to issue and adopt a self-regulatory code of practice, which will, for example, set minimum standards of technical spam control measures and provide for best practices, and which will be self-enforcing. It is proposed that the code of practice be drawn up by the industry.

JOINT IDA–AGC CONSULTATION PAPER

PROPOSED LEGISLATIVE FRAMEWORK FOR THE CONTROL OF E-MAIL SPAM

PART I
INTRODUCTION

1.1 Spam or unsolicited commercial e-mail is a problem for everyone. In recent years, spam has moved from being a minor nuisance to a social and economic problem. Spam impedes the efficient use of e-mail for personal and business communications, and threatens the growth and acceptance of legitimate e-commerce.[1]

1.2 To reduce spam in Singapore, the Infocomm Development Authority of Singapore (IDA) is adopting a multi-pronged approach which combines the use of technology, public education, self-regulation, spam control legislation and international cooperation. IDA together with the Attorney-General's Chambers of Singapore (AGC) embarked on a study to review Singapore's legislative options against spam. This Joint Consultation Paper is a result of the study.

1.3 Part 2 of this Paper discusses the problems caused by spam and the need to balance the legitimate interests of different groups when seeking to address the problems. Part 3 discusses IDA's multi-pronged approach to control spam and the introduction of spam control legislation as part of the multi-pronged approach. The current laws are also discussed. Annex A contains extracts of the current legislative provisions. At Part 4, it is recognized that the enactment of spam control legislation is in line with the recent trend in developed IT savvy jurisdictions. A table comparing the legislative and regulatory framework in selected jurisdictions, namely Australia, the United Kingdom, the United States, Japan and South Korea, is at Annex B. Part 5 discusses the legislative issues and the proposed legislative framework for the control of spam.

1.4 We invite comments and feedback on the proposed legislative framework. A list of questions is at Annex C.

[1] *An Anti-Spam Action Plan for Canada*, Industry Canada, May 2004.

- Please send your feedback to the Policy and Competition Development Group of IDA, marked "**Re: Anti-spam law public consultation**":
  - Via e-mail, at **antispam_submissions@ida.gov.sg**;
  - By post (a diskette containing a soft copy would be appreciated) to "**Policy and Competition Development Group, Infocomm Development Authority of Singapore, 8 Temasek Boulevard, #14-00 Suntec Tower Three, Singapore 038988**"; or
  - Via fax at **6211 2207**.

  Please include your personal / company particulars as well as your correspondence address, contact number and e-mail address in your response.

  IDA reserves the right to make public all or parts of any responses to this consultation (including your name and your personal / company particulars). Your response may also be quoted or referred to in subsequent publications or made available to third parties. Any part of the response which is considered confidential must be clearly marked and placed as an annex to the comments raised.

- The closing date for this consultation is **26 July 2004**.

PART 2
PREVALENCE OF SPAM AND CHALLENGES POSED

2.1 Spam is a term generally used to refer to unsolicited e-mail messages, usually transmitted to a large number of recipients. The marketers that send spam are called "spammers". The e-mail messages that spammers send usually have a commercial focus, promoting or selling products or services. They also share one or more of the following characteristics:[2]

(a) They are sent in an untargeted and indiscriminate manner, often by automated means;

(b) They include or promote illegal or offensive content;

(c) Their purpose is fraudulent or otherwise deceptive;

(d) They collect or use personal information;

(e) They are sent in a manner that disguises the originator; and

(f) They do not offer a valid and functional address to which recipients may send messages opting out of receiving further unsolicited messages.

2.2 There has been a dramatic growth of spam or unsolicited commercial e-mail in recent years[3]. According to a recent local survey by IDA[4], spam accounts for 35% of all e-mail received in Singapore.

2.3 Spam impedes the efficient use of e-mail for personal and business communications and commerce. It is eroding consumer confidence in the security and usability of the electronic medium. Left unchecked, it may even threaten the viability of the Internet as a tool for communication and commerce. A recent survey by the Trans-Atlantic Consumer Dialogue (TACD), an international consumer advocacy group, found that 52% of respondents were shopping less online or not at all because of concerns that any

[2] *Final Report of the NOIE Review of the Spam Problem and How It Can Be Countered*, The National Office for the Information Economy, Australia, at 6.
[3] According to Brightmail, an anti-spam software vendor, spam accounted for 64% of all e-mail traffic on the Internet in April 2004, up from just 8% of traffic in mid-2001. See: http://www.brightmail.com/spamstats.html.
[4] IDA Survey on Unsolicited E-mails (2003).

personal data they submitted would result in more spam[5]. In the IDA survey, 24% of respondents cited junk e-mail as the "most important concern when using the Internet"[6].

2.4 Spam has many victims. For individuals and businesses, spam consumes limited bandwidth and computer storage space, takes time to delete, delays the delivery of messages and causes legitimate messages to be mistakenly deleted. 81% of local e-mail users dislike receiving spam.

2.5 Spam is also a sap on productivity. The United Nations Conference on Trade and Development estimates that the global economic impact of spam could reach US$20 billion in lost time and productivity. Based on the findings of the IDA survey, the corresponding productivity loss for Singapore is estimated at about $1.9 million per month or approximately $23 million per year[7]. This works out to $16 per e-mail user per year on average. This amount excludes the loss suffered by Internet Service Providers (ISPs) and businesses.

2.6 For ISPs, spam puts a strain on services, forces expenditures on additional equipment and personnel and causes consumer complaints. The 3 major local ISPs[8] each receive thousands of spam-related complaints a month. Spam has occasionally caused congestion in their servers and delays in e-mail delivery.

2.7 Spam threatens the growth of legitimate e-commerce. It undermines consumer confidence in e-commerce including e-marketing. Spam also has a detrimental impact on legitimate direct marketers. As spam devalues the use of e-mail as a marketing channel, legitimate direct marketers may lose this important and cost-effective means of reaching out to targeted potential customers.

[5] TACD report on Consumer Attitudes Regarding Unsolicited Commercial E-mail (Spam) (Oct – Dec 2003)
[6] IDA Survey on Unsolicited E-mails (2003). In comparison, 60% of respondents cited computer viruses as their most important concern when using the Internet.
[7] Cost of spam = Time spent on handling spam x salary per hour.
[8] The 3 major local ISPs are Pacific Internet Pte Ltd, SingNet Pte Ltd and StarHub Pte Ltd.

Challenges posed by spam

2.8 There are a number of reasons for the proliferation of spam. Firstly, spamming is profitable. The very low marginal cost of sending bulk e-mail to individual addresses means that the marketing costs can be recovered even if the response rate is very low. According to one spammer, a return rate as low as 0.001% can be profitable[9] while a recent study contains anecdotal evidence that spammers can get started for under US$1,500 and earn back their initial investment within a few days[10]. This encourages the indiscriminate use of e-mail as an advertising medium i.e. spamming.

2.9 Secondly, the availability of sophisticated automated spamming tools makes it very easy for spammers to harvest or produce e-mail address lists and engage in indiscriminate mass mailing. For example, automated spamming tools exist that automatically navigate websites using a list of URLs that might be recursively retrieved from web pages in a search-engine fashion – collecting all the e-mail addresses found along the way. More insidiously, spammers may use random e-mail address generators to engage in "brute force" or "dictionary attacks". Dictionary attacks build address lists through computer-generated alphabetic permutations combined with address suffixes (for example, "@hotmail.com" or "@yahoo.com").

2.10 Thirdly, it is difficult to identify and hold spammers accountable for their practices. Spammers use spamware tools to automatically generate false headers and return address information to obscure their identities. They hide their tracks by sending spam through "open relays" located around the world. When their account with one ISP is terminated for spamming, they simply move on to another ISP. Varying regulations between countries places further obstacles in the way of implementing effective legal solutions to stop cross-border spam traffic. According to the IDA survey[11], 77% of spam received in Singapore originates from overseas-based companies.

[9] Wall Street Journal, 13 November 2002.
[10] Vircom, *Why Spammers Spam*, May 2004.
[11] IDA Survey on Unsolicited E-mails (2003).

Balancing the different interests

2.11 In seeking to address the spam problem, we need to balance the legitimate interests and concerns of different groups. On the one hand, we need to protect e-mail users and ISPs from the scourge of spam. Neither should we allow Singapore to become a safe haven for spammers.

2.12 On the other hand, we should not discourage the responsible use of e-mails for legitimate e-commerce and marketing purposes. Moreover, we have to be mindful that most spam received in Singapore originates from overseas-based spammers who are beyond the reach of our domestic laws. We should also be careful not to impede the use of e-mail as an efficient means of business communication including business to consumer (B2C) communication.

2.13 It is clear that there is no silver bullet to eradicate spamming. A judicious combination of appropriate legislation, public education, industry self-regulation, technical measures and international co-operation is likely to be the best way forward. While spam – like viruses – may well become a permanent feature of the Internet, a multi-pronged approach increases the odds that we will contain the problem.

PART 3
LEGISLATION IN THE CONTEXT OF A MULTI-PRONGED APPROACH

Multi-pronged approach

3.1 Spam is a multi-faceted problem which requires co-ordinated action by the Government as well as businesses and consumers. Accordingly, IDA is adopting a multi-pronged approach to fight spam and working with key stakeholders on a number of initiatives to curb the problem. Such a multi-pronged strategy has received wide acceptance internationally.

3.2 In Australia, the Government is adopting a series of measures to counter spam. Senator Richard Alston, Australia's Minister for Communications, Information Technology and the Arts, said that legislation is part of a "multi-layered" approach and is meant to complement the use of e-mail filtering software. Senator Alston acknowledged that the vast majority of spam originates overseas. He said, "But in the meantime, we can only do what's possible within Australia – but, of course, in combination with users helping themselves."[12]

3.3 An Anti-Spam Action Plan for Canada[13] was recently launched[14] on 11 May 2004 and includes a series of initiatives by the government, industry, marketers and consumers, focused on identifying measures to reduce and control spam. To oversee and coordinate the implementation of the action plan, a ministerial Spam Task Force was specially created.

3.4 On 17 May 2004, the New Zealand Government announced its proposal to tackle the spam problem through legislation as part of a multi-pronged approach alongside industry self-regulation, awareness and education campaigns, and international initiatives.[15]

---

[12] "Australian anti-spam legislation tabled in Parliament", James Pearce, *ZDNet Australia*, 18 September 2003, URL: http://www.zdnet.com.au/newstech/ebusiness/story/0,2000048590,20278732,00.htm.

[13] *An Anti-Spam Action Plan for Canada*, Industry Canada, May 2004, URL: http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00246e.html.

[14] The action plan was launched by the Honourable Lucienne Robillard, Minister of Industry and Minister responsible for the Economic Development Agency of Canada for the Regions of Quebec.

[15] Minister's Foreward, New Zealand Discussion Paper, *Legislating Against Spam*, Ministry of Economic Development, May 2004.

3.5 In Singapore, IDA's multi-pronged approach calls for specific initiatives by both the Government and the industry at both domestic and international levels. It combines:

(a) Public education;

(b) Industry self-regulation;

(c) International Cooperation; and

(d) Legislation.

Each is elaborated upon in turn below.

Public education

3.6 In view of the global nature of the spam problem, public education and technical counter-measures remain Singapore's first line of defence against spam.

3.7 IDA and its strategic partners - the three major local ISPs, the Singapore IT Federation (SITF), the Consumer Association of Singapore (CASE), the Singapore Business Federation (SBF), and the Direct Marketing Association of Singapore (DMAS) – are stepping up their public education efforts. For a start, they have jointly set up a website, the "Singapore Anti-Spam Resource Centre"[16], to equip the public with the necessary knowledge and tools to fight spam. IDA has also started to integrate anti-spam into its existing public education efforts, for example, the National IT Literacy Programme.

3.8 IDA and its partners will also reach out to e-mail users through talks, seminars and workshops. In particular, SITF, supported by IDA and corporate sponsors, is holding a one-day public forum in June 2004 to raise public awareness of the e-mail spam problem. It will provide a forum for key stakeholders to explore ways and means of tackling the problem[17]. Key members of SITF have also come together to offer free downloads of popular anti-spam software on a trial basis to familiarise e-mail users with the plethora of technical solutions available against spam[18].

[16] http://www.antispam.org.sg/.
[17] Registration information is available at http://ssc.sitf.org.sg/antispam/.
[18] http://www.sitf.org.sg/ssc.

Industry self-regulation

3.9 On the self-regulatory front, the three major local ISPs – Pacific Internet, SingNet and StarHub – have taken the lead to implement a set of anti-spam guidelines. This is a significant step forward as ISPs are in the frontline in the fight against spam.

3.10 Meanwhile, the DMAS has issued a code of practice to guide members on the appropriate use of e-mail for marketing purposes. The code is mandatory for DMAS members and represents the efforts of the marketing community to safeguard e-mail as a channel of communication and commerce. DMAS is also setting up a Consumer Communications Preference Programme that will allow e-mail users to register their preference not to receive unsolicited commercial e-mail.

International co-operation

3.11 Given the international dimension of the spam problem, it is clear that individual countries cannot solve the spam problem alone. As a permanent solution to the spam problem will necessarily involve the entire international community, Singapore is committed to playing its part through participation in various global and regional anti-spam initiatives. Such fora will include International Telecommunication Union and ASEAN.

Legislation

3.12 Internationally, there is a recent trend towards legislating spam control measures. Legislation is important in that it signals that society regards spamming as a social mischief, deters would-be local spammers, reduces the risk that Singapore could become a safe haven for spammers and aligns Singapore with recent international trends.[19] However, legislation alone is not sufficient.

[19] In the New Zealand Discussion Paper, *Legislating Against Spam*, Ministry of Economic Development, May 2004, the benefits for New Zealand of legislating against spam are described as follows:

- It enables legal action to be taken against spammers based in New Zealand;
- It prevents New Zealand from being seen as a safe haven for spammers as legislative measures begin to be implemented in overseas jurisdictions;
- It assists New Zealand in efforts to obtain international co-operation to combat overseas sources of spam if we have our own house in order;
- It allows the New Zealand Government to effectively co-operate with overseas government anti-spam enforcement agencies, to help trace the sender and beneficiaries of spam sent to New Zealanders.

In order to effectively curb spam, legislation must be accompanied by technological measures, commitments by ISPs and legitimate marketers, and changes in consumer behaviour. Legislation should be seen as an important component which complements and reinforces the other elements of a collaborative and comprehensive approach.

3.13 Although legislation by itself will not be effective in combating spam, neither can technological solutions alone be adequate as they are defensive and not offensive measures against the originators of spam. Notwithstanding the practical difficulties of enforcement (for instance, the cross-border nature of spam), legislative spam control measures should be put in place to signal society's disapproval of spamming activities as anti-social conduct and the Government's serious view that spam threatens to undermine the growth of legitimate e-commerce and impedes the use of e-mail as an efficient business tool.

Current laws and need for spam control legislation

3.14 Certain aspects of the *modus operandi* and conduct adopted by irresponsible spammers may already be offences under the current criminal law. If a spammer uses e-mail to fraudulently induce the recipient to part with his money or property, it would constitute the offence of cheating under section 415 of the Penal Code (Cap. 224). A dictionary attack launched against an ISP's mail server that degrades the performance of the mail server may constitute an offence under section 7 of the Computer Misuse Act (Cap. 50A) as a denial-of-service attack. In the same vein, the use of worms and trojans to take over a server for the purpose of transmitting spam may constitute an offence of unauthorised access to a computer under section 3 of the Computer Misuse Act. The sending of spam containing pornography may also constitute an offence under section 11 or 12 of the Undesirable Publications Act (Cap. 338) as distribution of obscene or objectionable publications on electronic medium.

3.15 Further, the sending of unsolicited commercial e-mail with false or misleading advertising or product claims may amount to an unfair practice under section 4 of the Consumer Protection (Fair Trading) Act 2003 (Act 27 of 2003).

3.16 Hence, current Singapore laws already deal with activities associated with the more serious forms of spamming, for example,

use of e-mail for cheating, spamming leading to denial-of-service, hacking into or taking over computers to send spam and spam containing pornography. However, where these elements are absent, our study shows that the existing laws do not provide for any legal recourse. New spam control legislation is thus needed to fill this lacuna.

3.17 Annex B contains the relevant extracts of the current legislative provisions.

PART 4
INTERNATIONAL SURVEY

4.1 AGC conducted a survey of the legislative and regulatory framework relating to the control of spam of several jurisdictions, namely Australia (Commonwealth), the United Kingdom, the United States (Federal), Japan and South Korea. All the listed jurisdictions and many of the European Union member states have enacted spam control legislation. The results of the international survey are summarised in the comparative table at Annex B.

4.2 As stated at paragraph 3.3, Canada has recently announced on 11 May 2004 that a ministerial task force has been created to oversee the implementation of a comprehensive action plan to reduce spam. The Canadian Spam Task Force will review whether legislation could make a significant impact on the reduction and control of spam.[20] Further, the New Zealand Government has on 17 May 2004 issued a Discussion Paper *Legislating Against Spam*[21] as part of a multi-pronged approach.

4.3 It is clear from the survey that the recent trend in developed IT savvy jurisdictions is steering towards enactment of anti-spam legislation in the context of a multi-layered or multi-pronged approach. It is thus important for Singapore's international profile and reputation as an IT hub to be aligned with this trend.

[20] *An Anti-Spam Action Plan for Canada*, Industry Canada, May 2004, URL: http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00246e.html.

[21] New Zealand Discussion Paper, *Legislating Against Spam*, Ministry of Economic Development, May 2004, URL: http://www.med.govt.nz/pbt/infotech/spam/discussion/.

PART 5
LEGISLATIVE ISSUES

5.1 The key legislative issues relate to the following:

- Definition of spam;
- Application of the proposed legislation;
- Requirements for the sending of unsolicited commercial e-mail;
- Legal action for breach of the requirements;
- Civil action for dictionary attacks and the use of automated spamming tools; and
- Co-Regulation - Codes of practice.

Definition of spam

5.2 An agreed definition of spam is important in making any spam control legislation effective. ISPs and regulatory authorities need to be reasonably confident of the definition before they enforce their terms and conditions or the applicable laws against spammers. Similarly, legitimate direct marketers would want to ensure that their activities remain both legal and ethical.[22]

5.3 It is proposed that spam be defined as "unsolicited commercial e-mail". This is the common definition of spam amongst the jurisdictions surveyed. The Canadian Anti-Spam Action Plan also refers to spam as "unsolicited commercial e-mail"[23]. The New Zealand Discussion Paper *Legislating Against Spam* refers to spam as "unwanted, unsolicited, commercial e-mails via the Internet". Spam therefore consists of 3 distinctive features, as follows:

(a) Spam is unsolicited, in that the recipient usually does not ask to receive such communication;

[22] *Final Report of the NOIE Review of the Spam Problem and How It Can Be Countered*, The National Office for the Information Economy, Australia at 7.
[23] *An Anti-Spam Action Plan for Canada*, Industry Canada, May 2004, URL: http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00246e.html. .

(b) The content of spam is commercial in nature, usually containing advertisements or solicitations for goods or services; and

(c) Spam consists of e-mail.

Unsolicited communications

5.4 If a user subscribes to an e-mail alert or information service, the e-mail sent would not be unsolicited. E-mails sent in response to communications initiated by the recipient would also not be treated as spam.

Commercial communications

5.5 Spam usually, though not necessarily, has a commercial focus, promoting or selling products or services. It is proposed that the definition of spam in the proposed legislation focus on commercial communications, such as communications between a commercial entity and its customers, as opposed to general communications of a personal nature. The latter category would include communications between private individuals.

5.6 Many jurisdictions[24] have restricted the scope of their anti-spam legislation to commercial communications. The commercial nature may be defined narrowly as in the United Kingdom[25] and the United States[26], or widely as in Australia[27].

5.7 Commercial communications would also exclude non-commercial content such as Government to citizen communications, appeals for

[24] Examples are Australia, the United Kingdom, the United States, Japan and South Korea. It is noted that the Australian Spam Act 2003 does not use the expression "spam" but applies to "commercial electronic messages" unless they are exempted.

[25] In the United Kingdom, the Privacy and Electronic Communications (EC Directive) Regulations 2003 make reference to e-mail for direct marketing purposes.

[26] Section 3(2) of the United States CAN-SPAM Act of 2003 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)". Section 3(3) provides that the term "commercial electronic mail message" does not include a transactional or relationship message.

[27] In section 6 of the Australian Spam Act 2003, a commercial electronic message is defined as a message where the purpose or one of the purposes is to offer to supply goods or services, to advertise or promote goods or services or a supplier of goods or services, to offer to supply land or an interest in land, to advertise or promote land or an interest in land or a supplier of land or an interest in land, to offer to provide or to advertise or promote a business opportunity or investment opportunity, or to assist or enable a person to dishonestly or deceptively take advantage of another person. The Australian Act, however, expressly excludes certain messages.

donations by charities and religious organisations.[28] Messages which are of a purely factual nature accompanied by material that identifies the sender, authoriser or sponsor of the message[29] would also be excluded. In this regard, the factual component of the message must be of such a nature that it would not be considered a commercial message. For instance, a message describing a particular drug may be simply factual, but if it also includes a link to where it can be bought, it would be a commercial message.

E-mail communications

5.8 It is proposed that the legislation focus on e-mails. This is the position in the United Kingdom, United States and Japan. Hence, paper junk mail would not constitute spam and neither would Short Messaging System (SMS) messages sent through a mobile phone. The technical architecture[30] and charging mechanism[31] for SMS and Multi-media Messaging System (MMS) have so far constrained the growth of spam using those technologies. IDA will, however, conduct a separate study on mobile spam in due course.

5.9 Further, a technology neutral approach is proposed to ensure that the legislation would apply regardless of whether the e-mails are received using e-mail software, through an Internet web browser or from a personal computer or portable mobile device such as a mobile phone or Personal Digital Assistant (PDA). Whilst e-mails are traditionally received using e-mail messaging software operated from a desktop personal computer (for example, Eudora, Outlook Express and Netscape Mail), the means of accessing e-mail have increased.

Q1. What are the considerations that should determine whether a communication is solicited or unsolicited?
Q2. What are the considerations that should determine whether a

[28] In Australia, government to citizen messages, messages from charities, religious organisations and registered political parties, messages from educational institutions directed to the households of past or attending students, and messages of a purely factual nature are prescribed as designated commercial electronic messages in Schedule 1 of the Spam Act 2003. Designated commercial electronic messages are not required to be sent with the consent of the recipient or with an included unsubscribe facility. However, they must provide information about the individual or organisation who authorised the sending of the messages.

[29] See paragraph 2 of Schedule 1 to the Australian Spam Act 2003.

[30] For example, SMS messages do not have subject headings and there is a limit on the number of characters that a SMS message can contain.

[31] SMS and MMS messages are charged on a per message basis and thus it would be more expensive to send SMS and MMS messages than bulk e-mail messages.

communication is commercial?

Q3. Should there be exclusions from the definition of spam?

Q4. Do you agree that the proposed legislation should apply to all e-mail messages regardless of the technology used to access them?

Application of proposed legislation

Spam transmitted in bulk

5.10 As spam is usually transmitted to a large number of recipients, it is proposed that the legislation apply to spam transmitted in bulk. This requirement would serve to exclude certain categories of unsolicited commercial communications which are not problematic, for e.g. where a marketing executive discovers that a company intends to purchase office equipment and he proceeds to market his product by sending a single unsolicited e-mail to the office manager of that company.

5.11 In the New Zealand Discussion Paper *Legislating Against Spam*, it is recognised that "the issue of bulk is primarily an issue for people of organizations who are attempting to solve or regulate spam because the concern relates to its collective impact. For the recipients of spam, however, the issue of how many other people may have received a message is generally irrelevant. For them, it is the content of the message that is the issue of concern."[32]

5.12 The definition of what amounts to "in bulk" would be important if it is decided that the proposed legislation should apply to spam transmitted in bulk. This may be determined by a subjective test or by reference to a minimum numerical threshold, for e.g. more than 100 e-mail messages during a 24-hour period, more than 1,000 e-mail messages during a 30-day period, or more than 10,000 e-mail messages during a 1-year period. We would invite comments on the definition of "in bulk".

5.13 In the United States, the offence provisions[33] apply to the transmission of "multiple commercial electronic messages" where

[32] New Zealand Discussion Paper, *Legislating Against Spam*, Ministry of Economic Development, May 2004, URL: http://www.med.govt.nz/pbt/infotech/spam/discussion/.

[33] See section 4 of the CAN-SPAM Act 2003, which amends Chapter 47 of title 18, United States Code to make it an offence to transmit multiple commercial electronic mail messages

the term "multiple" means "more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period".

Q5.	Do you agree that the proposed legislation should apply only to spam transmitted in bulk?
Q6.	What are the considerations that determine whether e-mail messages have been transmitted in bulk?

Spam sent from or received in Singapore

5.14 It must be recognized that the preponderance of spam originates overseas where any legislative effort may well not have any bite. Nevertheless, spam control legislation may to an extent control spamming activities that take place within Singapore, that is, where the spammer carries out his spamming activity within Singapore, regardless of whether he spams local or overseas mail servers.

5.15 It is proposed that the legislation applies to spam originating from or received in Singapore. These are activities that have a direct nexus or connection with Singapore. This approach is similar to the Australian position[34]. It enables legal action to be taken against spammers based in Singapore, which would serve to minimise the risk that Singapore may be used as a base for which spamming activities against addressees in other countries can be carried out. Further, there may be situations where a Singapore business arranges for spam promoting or advertising its products or services to be sent from overseas. The proposal would enable the legislation to apply notwithstanding the overseas source of the spam.

5.16 With this limited extra-territorial provision, Singapore will be in a position to participate in discussions with like-minded countries on international cooperation.

---

where fraud is involved. The other provisions in the CAN-SPAM Act 2003 do not require the transmission of multiple commercial electronic mail messages before civil action can be taken. See section 5.

[34] Section 16 read with section 7 of the Australian Spam Act 2003. The Australian Act applies to commercial electronic messages that have an Australian link. Messages having an Australian link include messages sent from overseas to Australian e-mail account holders. See also section 14 which provides that unless the contrary intention appears, the Act extends to acts, omissions, matters and things outside Australia.

Q7.	Do you agree that the proposed legislation should apply to spam sent from or received in Singapore?

Person or business commissioning or procuring spam

5.17 Under the proposed legislation, it is not only the spammer who will be liable for unlawful spam. It is proposed that the merchant or business commissioning or procuring spam should also be liable. This will prevent businesses from hiding behind individual spammers. It will also allow action to be taken against the beneficiaries of spam.

5.18 This proposal is similar to the approach in the United States where the CAN-SPAM Act of 2003[35] provides that it is unlawful for a person to promote or allow the promotion of his trade or business, goods, products or services, in a commercial electronic mail message in violation of section 5(a)(1)[36] if he knows or ought to have known that the goods, products or services were being promoted in such a message, he received or expected to receive an economic benefit from the promotion, and he took no reasonable action to prevent the transmission or to detect the transmission and report it to the Federal Trade Commission.

5.19 Similarly, in Australia, the legislation applies not only to the sender of the message, but also to those who cause the message to be sent, those who aid, abet, counsel or procure a contravention of the requirements and those who are in any way a party to such a contravention.[37]

Q8.	Do you agree that the person commissioning or procuring spam should also be liable under the proposed legislation?

Requirements for the sending of unsolicited commercial e-mail

5.20 Under the proposed law, not all unsolicited commercial bulk e-mail communications would be disallowed. Unsolicited commercial e-

[35] Section 6.

[36] Section 5(a)(1) of the CAN-SPAM Act of 2003 makes it unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading.

[37] See, for example, sections 16(9), 17(5), 18(6) and 20(5) of the Spam Act 2003.

mail communications that comply with the minimum standards for an opt-out regime, the labelling requirements and other prescribed requirements will be treated as legitimate communications. They would not be subject to any legal action under the proposed legislation so long as all opt-out requests have been honoured. Such e-mail can continue to be sent so long as the recipient has not opted-out.

Opt-out regime

5.21 An opt-out regime is "the distribution model of sending unsolicited e-mail (spam) and allowing the recipient to request removal"[38]. An opt-out regime permits senders to send unsolicited commercial communications by e-mail to intended recipients until such time that they are asked, by the recipients, to stop doing so. In contrast, in an opt-in regime, the sender cannot send any unsolicited commercial communications by e-mail until such time the intended recipient has indicated to the sender that he is willing to receive such communications.

5.22 Closely associated with spam is the debate on whether an opt-in or opt-out regime should be adopted to regulate spam. An opt-out regime is considered to be more business friendly as businesses can generally send unsolicited commercial communications to users in their database until they are told to stop. The United States decision to adopt an opt-out regime has, however, attracted criticism on the ground that an opt-out regime legitimises spam. Another criticism is that an opt-out regime can be easily hijacked by unscrupulous spammers as an opt-out request received from an auto-generated e-mail address would indicate that it is in fact a 'live' address. This would be all that is required for the unscrupulous business to send even more unsolicited e-mail messages to that address, regardless of any attempt to opt-out. Opt-out regimes have thus been criticised for encouraging the proliferation of spam. In contrast, an opt-in regime is said to favour the consumer as he receives unsolicited commercial communications by e-mail only if he consents.

[38] *searchWebServices.com Definitions* at http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci212717,00.html. An opt-out regime is contrasted with an opt-in regime which is characterized by "recipients [having] previously requested by signing up at a Web site or special ad banner … for promotional information about one or more categories of products or services. Those who sign up have thus "opted-in".

5.23 An opt-in regime is, however, not without its pitfalls. It would create legal uncertainty as it may not be clear what conduct or relationships should amount to or be deemed to constitute implicit consent. It would also make it necessary to undertake the difficult task of defining the scope of any opt-in assent[39]. More practically, opt-in may deny opportunities to consumers who now receive unsolicited material and have the option to act on those solicitations. It may make it more difficult for new and often more innovative firms and organizations to enter markets and compete. Finally, opt-in will not solve the problem of "unwanted" e-mail as opt-in e-mail can be just as annoying as opt-out e-mail. A recent survey of 500 consumers in the United Kingdom revealed that 51.8% of all opt-in marketing e-mails were considered irrelevant and inappropriate by recipients[40].

5.24 While the arguments for and against an opt-in regime are finely balanced, it is recognised that in reality an opt-in regime will not be effective so long as the preponderance of spam originates from outside Singapore, especially from jurisdictions that either have an opt-out regime or which do not have any spam control legislation at all. The imposition of an opt-in regime locally would increase the burden of regulatory compliance on businesses without garnering commensurate relief for e-mail users.

5.25 Whilst we are aware that the United States' adoption of an opt-out regime has attracted criticism, we are of the view that an opt-out regime, if properly implemented, will be effective in reducing spam originating from Singapore. Indeed, there is some evidence that a combination of technical measures and legal action may be working in the United States. For example, the United States' largest ISP, America On-Line (AOL) reportedly saw a 27% decline in the amount of spam entering its network in the period between mid-Feb and mid-Mar 2004, attributing the decline to improved filtering techniques and fear of litigation under the United States CAN-SPAM Act[41]. Adopting an opt-out regime is also more business friendly. It enables local businesses to responsibly make use of e-mail as another means of conducting legitimate business. However, we recognise that minimum standards have to be set to

[39] These issues have been raised in the New Zealand Discussion Paper, *Legislating Against Spam*, Ministry of Economic Development, May 2004, URL: http://www.med.govt.nz/pbt/infotech/spam/discussion/.

[40] *Opt-In could cause more to switch off*, New Media Age, 15 Jan 04.

[41] On 9 Mar 2004, AOL and several other large ISPs had sued hundreds of spammers in the first test of the new law. Andy Sullivan, *AOL Says it Sees Sharp Decline in 'Spam' E-mail*, 19 Mar 2004.

ensure that recipients of unsolicited commercial e-mail have a means of opting out of receiving them and that businesses that receive opt-out requests comply with the recipients' wishes. We recognise that an opt-out regime should be implemented in tandem with public education and guidelines on the use of "unsubscribe facilities".

5.26 It is therefore proposed that the spam control legislation establish an opt-out regime, requiring senders of unsolicited commercial e-mail to provide an opt-out mechanism which complies with the following minimum standards:

(a) Each unsolicited commercial e-mail should contain a valid return e-mail address to which an opt-out request can be sent by a recipient. Alternatively, it should provide an Internet location address at which a recipient can access the opt-out mechanism.

(b) Instructions for opting out of future unsolicited commercial e-mails can be in any language but there should be one version in English. This concern is perhaps more pertinent in Asia where there is a likelihood that unsolicited commercial e-mail messages, including opt-out instructions, are received in a language that the recipient is not literate in. Having one version of the opt-out instructions in English, which is an internationally recognized language and probably the language of the Internet, will address this concern. South Korea imposes this requirement.

(c) Where an automated opt-out mechanism is adopted, whether it works via e-mail messages or through a mechanism accessible via a web page, the opt-out mechanism should be functional. This would address concerns that opt-out mechanisms are used as a means to detect whether an auto-generated e-mail address is in fact a 'live' e-mail account. We are aware that spammers may use the opt-out facility fraudulently in order to confirm the validity of an e-mail address. Public education is needed to guide users as to when and how to make use of opt-out facilities. For example, users should not opt-out of spam with obviously false headers, misleading subject titles, or which peddle illegitimate material such as pornography or prescription drugs.

(d) Where an opt-out request has been received, the sender should not transfer the e-mail address of the recipient in a manner contrary to his request, e.g. where the recipient has requested to opt-out of future unsolicited commercial e-mails from the sender as well as his partners, the recipient's e-mail address should not be transferred to business partners for the purposes of enabling them to send unsolicited commercial e-mail.

(e) Senders of unsolicited commercial e-mails must comply with opt-out requests within a specified time frame. With a highly automated system, such requests should be capable of being complied with within a short period of time. Less automated systems will require more time.

Q9.	Would you agree that an opt-out regime for spam control is more beneficial to Singapore as a regional IT and commercial hub?
Q10.	What is a reasonable time period for compliance with opt-out requests?
Q11.	Are these minimum standards sufficient?

Labelling and other requirements

5.27 In order to facilitate self-help, especially the adoption of spam control technologies, it is necessary that minimum standards be established to identify unsolicited commercial e-mails. Compliance with these minimum standards will enable spam control technologies to function properly and prohibit attempts to circumvent them.

5.28 The following requirements are proposed:

(a) The subject title of e-mail messages should not be labelled in a manner that misleads the recipient as to their content;

(b) The subject title should contain the characters '[ADV]' to identify unsolicited commercial e-mail messages as such;

(c) The e-mail messages should not contain a false header;

(d) The e-mail messages should have a genuine e-mail address; and

(e) The e-mail messages should include a valid postal address.

5.29 Compliance with the above requirements will provide sufficient information to the recipient for him to decide whether he wishes to access the content of the e-mail message. It will also permit the recipient to configure his anti-spam software to sieve out such messages. If the commercial e-mail is solicited, labelling would not be imposed. There may, however, be a need for a technological means of distinguishing between commercial e-mail which a user finds desirable and chooses not to opt-out of, and undesirable spam. The user may, for example, add the sender to his "safe" list of senders which the anti-spam program will not block.

Q12. Are the recommended labelling requirements sufficient? Is '[ADV]' an appropriate label? Should there be any other requirement?

Legal action

By ISPs

5.30 As the loss suffered by a single individual end-user is not likely to be significantly substantial and we would not want to encourage a multitude of frivolous litigation, individuals will not be permitted to take civil action on their own. The New Zealand Government in its Discussion Paper *Legislating Against Spam*[42] recognises that individuals and firms that are the recipients and victims of spam generally do not have the resources necessary to carry out an investigation and bring court action.

5.31 On the other hand, ISPs are affected by spam in a major way and more likely to have the resources to take legal action. Therefore, in the United States, ISPs are given rights of action. This approach appears to be supported by the New Zealand Government.[43]

5.32 In the context of Singapore, we propose to give ISPs which have suffered loss or damage as a result of unlawful spam a statutory right to commence an action in court to sue the person sending the

[42] New Zealand Discussion Paper, *Legislating Against Spam*, Ministry of Economic Development, May 2004, URL: http://www.med.govt.nz/pbt/infotech/spam/discussion/ at 18.
[43] Ibid at 19.

spam (spammer) or the person commissioning or procuring the spam. This will be a new cause of action created by legislation. It will not require any existing contractual relationship for action to be taken. It is necessary to create a new statutory right of civil action because firstly, spamming *per se* does not fit into current legal grounds for initiating civil action, and secondly, the current law does not generally allow the recovery of pure economic loss which is not directly connected to physical damage.

5.33 It is proposed that the court be empowered, where it finds that a person has engaged in unlawful spamming activity, to award the ISP:

(a) damages for pure economic loss suffered because of the spamming activity; or

(b) statutory damages for notional loss to facilitate the proof of damages; and

(c) costs and expenses of the action.

An ISP may also apply to the court for an injunction to stop the spamming activity. A person in breach of the injunction can be dealt with for contempt of court.

5.34 Under the United States CAN-SPAM Act of 2003[44], a district court of the United States in a civil action by an ISP is empowered to award statutory damages, the amount of which is calculated by multiplying the number of violations (with each separately addressed unlawful message received by or addressed to affected residents treated as a separate violation) by up to US$25 or US$100, depending on the type of violation. For certain violations[45], the amount of statutory damages may not exceed US$1,000,000.

[44] Section 7(g).

[45] Examples of such violations include those arising from deceptive subject headings (section 5(a)(2)), non-inclusion of return address or comparable mechanism in commercial electronic mail (section 5(a)(3)), transmission of commercial electronic mail after objection (section 5(a)(4)), and non-inclusion of identifier, opt-out and physical address in commercial electronic mail (section 5(a)(5)). It is noted that for a violation arising from a commercial electronic mail that contains or is accompanied by header information that is materially false or materially misleading (section 5(a)(1)), the amount of statutory damages that the court may award is not limited to US$1,000,000.

Q13.	Do you agree that ISPs should be empowered to commence legal action for unlawful spam?
Q14.	What would be an appropriate quantum for the computation of statutory damages? For instance, would $1 for every unlawful spam e-mail sent be adequate? Should there be a cap on the quantum of statutory damages that can be awarded by the court?

Civil action for dictionary attacks and use of automated spamming tools

5.35 Spammers may sometimes engage in dictionary attacks. A dictionary attack utilises software that opens a connection to the target mail server and then rapidly submits millions of random e-mail addresses. Many of these addresses have slight variations, such as "jdoe1abc@hotmail.com" and "jdoe2def@hotmail.com". The software then records which addresses are "live" and adds the "live" addresses to the spammers' list.[46]

5.36 Spammers also use automated spamming technologies for the purposes of address harvesting[47], dictionary attacks and auto-generation of throw-away accounts[48]. This contributes to the transmission of bulk e-mail messages which can have a severe impact on the operations of ISPs, for example, by degrading the performance of ISPs' mail servers. In the past, there were occasions where foreign ISPs blocked all e-mail messages coming from an affected local ISP in an attempt to block spam. Legitimate e-mail messages were also blocked.

5.37 Where spam is sent through the use of a dictionary attack or any automated spamming tool, it is proposed that ISPs be allowed to commence legal action against the spammer without having to prove that the e-mails fail to comply with the minimum requirements proposed at paragraphs 5.26 to 5.29 of this Paper. The court, on proof of the existence of a dictionary attack or use of

[46] "Hotmail: A Spammer's Paradise?" by Michelle Delio, *Wired News*, 9 January 2003, URL: http://www.wired.com/news/infostruture/0,1377,57132,00.html.

[47] Address harvesting is another method of spammers. It consists of using computer programmes that search public areas on the Internet to compile, capture or otherwise "harvest" lists of e-mail addresses from web pages, newsgroups, chat rooms, and other online destinations. See "E-mail Address Harvesting: How Spammers Reap What You Sow", November 2002, URL: http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm

[48] In order to evade detection and anti-spam software, spammers frequently use throw-away accounts, which are inexpensive Internet accounts purchased from a legitimate ISP for the sole purpose of sending spam.

an automated spamming tool, will be empowered to award damages for economic loss or statutory damages, and to grant an injunction.

Q15. Do you agree that ISPs should be allowed to take legal action against the spammer who uses dictionary attacks or automated spamming tools without having to prove that the e-mails fail to comply with the minimum requirements?

Co-Regulation - Codes of Practice

5.38 From the experiences of other countries, a co-regulatory model involving industry participation and codes of practice together with the relevant legislation would work well. Codes of practice, which are transparent, practical, verified, vigorously monitored and enforced by all in the communications and marketing chain, are essential to protecting the viability of e-commerce.[49] They should provide clear information on acceptable commercial e-mail practices and policies, and ensure that Internet users are provided with the tools they need to make informed choices.[50]

5.39 It is proposed that the spam control legislation impose a duty on industry players, such as ISPs, to promulgate and adopt a self-regulatory code of practice, which will, for example, set minimum standards of technical spam control measures, and provide for best practices, and which will be self-enforcing. It is proposed that the code of practice be drawn up by the industry.

Q16. Who do you think should draft the code of practice?
Q17. What should the code of practice cover?
Q18. Who should enforce the code of practice?

[49] *An Anti-Spam Action Plan for Canada*, Industry Canada, May 2004.
[50] Ibid.

Annex A

EXTRACTS OF CURRENT LEGISLATIVE PROVISIONS

Penal Code
(Chapter 224)

Cheating

415. Whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to "cheat".

Explanation 1.
A dishonest concealment of facts is a deception within the meaning of this section.

Explanation 2.
Mere breach of contract is not of itself proof of an original fraudulent intent.

Computer Misuse Act
(Chapter 50A)

Unauthorised access to computer material

3. —(1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the act in question is not directed at —

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

Unauthorised obstruction of use of computer

7. —(1) Any person who, knowingly and without authority or lawful excuse —

(a) interferes with, or interrupts or obstructs the lawful use of, a computer; or

(b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

Undesirable Publications Act
(Chapter 338)

Offences involving obscene publications

11. Any person who —

(a) makes or reproduces, or makes or reproduces for the purposes of sale, supply, exhibition or distribution to any other person;
(b) imports or has in his possession for the purposes of sale, supply, exhibition or distribution to any other person; or

(c) sells, offers for sale, supplies, offers to supply, exhibits or distributes to any other person,

any obscene publication (not being a prohibited publication) knowing or having reasonable cause to believe the publication to be obscene shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 2 years or to both.

Offences involving objectionable publications

12. Any person who —

(a) makes or reproduces, or makes or reproduces for the purposes of sale, supply, exhibition or distribution to any other person;

(b) imports or has in his possession for the purposes of sale, supply, exhibition or distribution to any other person; or

(c) sells, offers for sale, supplies, offers to supply, exhibits or distributes to any other person,

any objectionable publication (not being a prohibited publication) knowing or having reasonable cause to believe the publication to be objectionable shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 12 months or to both.

Consumer Protection (Fair Trading) Act 2003 (Act 27 of 2003)

Meaning of unfair practice

4. It is an unfair practice for a supplier, in relation to a consumer transaction —

(a) to do or say anything, or omit to do or say anything, if as a result a consumer might reasonably be deceived or misled;

(b) to make a false claim;

(c) to take advantage of a consumer if the supplier knows or ought reasonably to know that the consumer —

(i) is not in a position to protect his own interests; or

(ii) is not reasonably able to understand the character, nature, language or effect of the transaction or any matter related to the transaction; or

(d) without limiting the generality of paragraphs (*a*) to (*c*), to do anything specified in the Second Schedule.

Annex B

AN INTERNATIONAL COMPARISON OF SPAM CONTROL LEGISLATION

	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 uses "unsolicited communications for the purposes of direct marketing by means of electronic mail": reg 22(2) PECR 2003. NB. Some obligations	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".

	Australia	United Kingdom	United States	South Korea	Japan
		applicable to commercial communications generally.			
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	*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.	*Opt-out* Transmission of specified emails to person who has requested not to receive them prohibited.

	Australia	United Kingdom	United States	South Korea	Japan
		from recipient in previous negotiations; – direct marketing of similar products and services; and – unsubscribe facility at time contact details collected and at each subsequent communication.			
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	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.

	Australia	United Kingdom	United States	South Korea	Japan
			thus promoted: s 6.		
Functional unsubscribe facility	Commercial electronic messages must contain a functional unsubscribe facility: s 18(1).	Simple means of refusing use of contact details for the sending of electronic mail for the purposes of direct marketing to be provided at time contact details initially collected and at time of each subsequent communication: reg 22(3)(c) PECR 2003. Valid return address to which opt-out request can be sent: reg 23(b) PECR 2003.	Functional internet-based opt-out mechanism: s 5(a)(3). Inclusion of clear and conspicuous notice of opportunity to opt out: s 5(a)(5)(ii).	Art 11 Ordinance of the Ministry of Information and Communication of the Act: – 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.	(see under Labelling requirements) Unsolicited commercial e-mail must include opt-out e-mail address.
Identify sender	Commercial electronic message to clearly and	E-mail for the purposes of direct marketing not to	Line identifying person initiating message to	Art 50(2) Restrictions on transmission of	Unsolicited commercial e-mail must include

	Australia	United Kingdom	United States	South Korea	Japan
	accurately identify sender: s 17(1)(a).	be transmitted where identity of person on whose behalf communication is sent has been disguised or concealed: reg 23(a) PECR 2003. Commercial communications to clearly identify person on whose behalf it is made: reg 7(b) ECR 2002	accurately not to be materially false or misleading: s 5(a)(1)(B) Secondary liability for businesses knowingly thus promoted: s 6.	advertisement information: to indicate the following: – types of transmission and major contents in there; – name/ contact means of addressor.	sender's name and address.
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.	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.

	Australia	United Kingdom	United States	South Korea	Japan
		Promotional offers, competitions or games and conditions to be clearly identified: s 7(c) & (d) ECR 2002.			
English language requirement	—	—	—	Art 11 Ordinance of the Ministry of Information and Communication of the Act: – encourages Korean companies and individuals to insert English language buttons or links with which foreign users may reject and block future spam from the same source.	—
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 ficticious e-mail addresses Telecommunications carriers are permitted not to provide a volume of e-

	Australia	United Kingdom	United States	South Korea	Japan
					mail transmission services if the emails include random ficticious 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.	—

	Australia	United Kingdom	United States	South Korea	Japan
				Art 50(2) Restrictions on transmission of advertisement information: to indicate source of e-mail address harvested.	
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).	—	—

	Australia	United Kingdom	United States	South Korea	Japan
Remedies	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
Persons who may be liable	Sender of commercial electronic messages.	Any person transmitting or instigating the transmission of a	Sender of commercial electronic mail message.	Any person transmitting advertisement information.	Sender.

	Australia	United Kingdom	United States	South Korea	Japan
	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.	communication: PECR 2003	Any person who initiates/ procures transmission of commercial electronic mail message (s. 5)		
Multi-pronged approach	Australian Communications Authority (ACA) has the following additional functions: – education: s 42(a); – research: s 42(b); and	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	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.

	Australia	United Kingdom	United States	South Korea	Japan
	– international co-operative arrangements: s 42(c).			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.	Future plans to promote self-regulatory and technical solutions by ISPs and mobile operators. Awareness actions.

Annex C

LIST OF QUESTIONS

Q1. What are the considerations that should determine whether a communication is solicited or unsolicited?

Q2. What are the considerations that should determine whether a communication is commercial?

Q3. Should there be exclusions from the definition of spam?

Q4. Do you agree that the proposed legislation should apply to all e-mail messages regardless of the technology used to access them?

Q5. Do you agree that the proposed legislation should apply only to spam transmitted in bulk?

Q6. What are the considerations that determine whether e-mail messages have been transmitted in bulk?

Q7. Do you agree that the proposed legislation should apply to spam sent from or received in Singapore?

Q8. Do you agree that the person commissioning or procuring spam should also be liable under the proposed legislation?

Q9. Would you agree that an opt-out regime for spam control is more beneficial to Singapore as a regional IT and commercial hub?

Q10. What is a reasonable time period for compliance with opt-out requests?

Q11. Are these minimum standards sufficient?

Q12. Are the recommended labelling requirements sufficient? Is '[ADV]' an appropriate label? Should there be any other requirement?

Q13. Do you agree that ISPs should be empowered to commence legal action for unlawful spam?

Q14. What would be an appropriate quantum for the computation of statutory damages? For instance, would $1 for every unlawful

spam e-mail sent be adequate? Should there be a cap on the quantum of statutory damages that can be awarded by the court?

Q15. Do you agree that ISPs should be allowed to take legal action against the spammer who uses dictionary attacks or automated spamming tools without having to prove that the e-mails fail to comply with the minimum requirements?

Q16. Who do you think should draft the code of practice?

Q17. What should the code of practice cover?

Q18. Who should enforce the code of practice?

T:/Spam:/Joint IDA-AGC Consultation Paper (final) (24.5.04)