SINGAPORE TELECOMMUNICATIONS LIMITED

SUBMISSION TO IDA AND AGC ON PROPOSED LEGISLATIVE FRAMEWORK FOR THE CONTROL OF E-MAIL SPAM

1. STATEMENT OF INTEREST

1.1 SingTel is licensed to provide telecommunications services in Singapore. It was corporatised on 1 April 1992. SingTel is committed to the provision of state-of-the-art telecommunications technologies and services in Singapore. In addition, the SingTel group has a comprehensive portfolio of services that includes voice and data services over fixed, wireless and Internet platforms. SingTel provides services to both corporate and residential customers and is committed to bring the best of global communications to its customers in the Asia Pacific and beyond.

1.2 As a leading provider of telecommunications services and a leading proponent of innovation and competition, the SingTel group ("SingTel") has a strong interest in effective pro-competition regulation of Singapore's telecommunications industry.

1.3 The IDA and the AGC have released a joint consultation paper entitled "Proposed Legislative Framework or the Control of Email Spam" (**the Consultation Paper**). SingTel's comments in response to the Consultation Paper are outlined below.

2. SUMMARY OF MAIN POINTS

2.1 SingTel's major comments on the proposed legislative framework for control of spam (as outlined in the Consultation Paper) are as follows:

- Legislation alone will not solve the problem of spam in Singapore. Without broader public education initiatives, legislation could mistakenly be seen as a panacea for spam. However, international experience has demonstrated that legislation alone will not prevent spam.

- The Consultation Paper recommends a "multi-pronged approach". SingTel agrees that a "multi-pronged approach", including public education and implementation of anti-spam technology, is likely to be the most effective way of addressing spam;

- However, SingTel is not convinced that legislation is necessary, given that most spam that is received in Singapore is sent into Singapore from offshore. This leaves limited enforcement opportunities under a legislative regime.

- In this context, SingTel notes that many overseas jurisdictions that have introduced anti-spam legislation have done so within an existing privacy legislation framework (eg UK), or to complement existing privacy legislation (eg Australia), or in order to combat the spread of specific unsavory content, such as pornography (eg USA). In determining whether legislation is necessary, Singapore needs to consider the issue of spam by reference to its own regulatory environment.

- If legislation is considered appropriate in Singapore (as part of this "multi-pronged approach"), it will need to be carefully drafted. Otherwise, there is a risk that anti-spam legislation could prohibit legitimate online business communications, and dampen business enterprise and genuine e-commerce in Singapore. As discussed below, not all commercial emails should be considered to be "spam".

- It is important that any anti-spam legislative framework incorporate elements that reflect the following principles:

  (i) the definition of spam should refer to the bulk sending of "unsolicited commercial emails" in "bulk";

  (ii) if "unsolicited commercial emails" are sent in bulk, they will need to contain specified information, and the sender will need to meet minimum standards under an "opt out" regime (**minimum standards**). If these minimum standards are not met, the sending of such emails should be an offence under the proposed legislation;

  (iii) an "opt-out" regime is to be preferred to an "opt-in" approach. An "opt-in" approach would unduly constrain Singaporean businesses from engaging in genuine e-commerce;

  (iv) commercial emails that are sent by Singaporean businesses to existing clients/customers should not be regarded as spam, and should not fall within the prohibition on spam (even if they do not meet requirements of an "opt-out" regime). The legislation should expressly state that that such emails do not fall within the definition of spam (as they are not "unsolicited");

(v) the minimum standards required by the "opt-out" regime should be those summarized in paragraph 11 of the Executive Summary of the Consultation Paper (i.e. a valid return email address, instructions for opting out in English, a functional opt-out mechanism and compliance with opt-out requests within specified time limits);

(vi) the legislative framework should clearly identify the Government agency or agencies that are to be responsible for enforcement of the legislation (e.g. IDA, MDA, AGC). Such agencies should be able to initiate prosecutions against "spammers" who do not comply with the minimum standards (e.g. following the investigation of a consumer complaint);

(vii) consumers and/or recipients of spam and Internet Service Providers (**ISPs**) should also be given the right to commence their own court actions against "spammers" who do not comply with the minimum standards set out in the legislation. ISPs should not be expected to commence action against spammers on behalf of consumers and/or recipients of spam; and

(viii) ISPs should be given the right to cease providing services to those spammers (at the sole discretion of the ISP) as well as to recover damages and/or losses suffered due to spam; and

(ix) the legislative approach should not impose cost or administrative burdens on ISPs. For example, ISPs should not be expected to assume monitoring functions or to police compliance with the legislation.

2.2 SingTel's general comments in relation to the Consultation Paper are summarized at 3 below, and specific comments in response to the questions posed by the Consultation Paper are at 4 below.

3. GENERAL COMMENTS ON PROPOSED APPROACH TOWARDS SPAM

3.1 SingTel supports focused and practical Government initiatives to address spam. The problems caused by spam are well documented in the Consultation Paper. Some further observations are noted below.

3.2 Spam congests networks and frustrates customers. From a business perspective, spam decreases productivity and the efficient flow of electronic commerce. For example, at a recent meeting hosted by the International Telecommunications Union, a report of an online survey was provided in which 80% of respondents said that spam made them less productive at work[1]. SingTel agrees that spam is a growing problem.

3.3 However, it should be emphasised that not all commercial emails should be regarded as "spam". International experience (which SingTel suggests is also relevant in Singapore) indicates that the "spam" that is most concerning to users and businesses has the following characteristics:

- It is sent in an untargeted and indiscriminate manner, often by automated means;
- It includes or promotes illegal or offensive content;
- Its purpose is fraudulent or otherwise deceptive;
- It is sent in a manner that disguises the originator; and
- Recipients can't "opt-out" from receiving further unsolicited messages[2].

3.4 As outlined below, SingTel considers that the types of electronic messages outlined at paragraph 3.3 above should be distinguished from emails that are sent to recipients who have had prior business dealings with the sender.

3.5 When spam is considered in this context, SingTel agrees that a "multi-pronged approach" is the best policy for addressing spam related concerns. This recognizes that the approach towards spam must include public education (including the use of appropriate technology measures) and international cooperation.

3.6 SingTel queries whether anti-spam legislation is necessary in Singapore. SingTel notes that some overseas jurisdictions that have introduced spam legislation have done so in the context of their own unique legislative regimes. For example, in the UK, anti-spam legislation is incorporated into privacy legislation (e.g. *The Privacy and Electronic Communications (EC Directive) Regulations* 2003). In Australia, anti-spam legislation (*Spam Act* 2003) complements the rules regulating direct marketing under the *Privacy Act* 1988.

---

1 Communications Day, 9 July 2004. Survey conducted by software vendor Sophos, with over 5,000 respondents.

2 Explanatory Memorandum on the Spam Bill 2003 (Australia)

In the US, the *CAN-SPAM Act* 2003 was enacted with the objective of reducing the circulation of pornographic or adult oriented material (among other things).

3.7 In each of the countries noted above, anti-spam legislation was introduced by reference to the existing legislation in those jurisdictions. In Singapore, it is appropriate to place some weight on the fact that there are a number of current legislative provisions that are already operative (as set out in Annex A of the Consultation Paper).

3.8 However, to the extent that a "multi-pronged approach" in Singapore includes new legislation, SingTel is nonetheless concerned that such legislation not be presented as the panacea for spam in Singapore.

3.9 Also, SingTel is concerned that if anti-spam legislation is not carefully drafted, it has the potential to dampen business enterprise and stymie e-commerce in Singapore.

3.10 Currently, email communications are commonly used as a cost-effective tool by businesses in Singapore who are looking to broaden their customer base and to lower their marketing costs. As indicated above, in the context of discussing a framework for anti-spam legislation, it is important to note that there is a difference between emails sent for genuine marketing purposes, and the use of spam for other purposes, e.g. fraudulent or illegal activities, including attempts to capture financial information by masquerading messages as originating from trusted companies ("spoofing" or "phishing"). Such unscrupulous use of spam differs from the use of email marketing by genuine businesses, who find emails an effective means to communicate with their customers.

3.11 The imposition of anti-spam legislation upon such legitimate business activities would only serve to increase the cost of conducting business in Singapore, and would deter and hamper commercial and economic enterprise as well depriving the public of useful sources of information or services.[3]

3.12 There is also an argument that placing too much emphasis on legislative means of combating spam risks wasting precious resources. A survey in late 2003 shows that 77% of total spam received in Singapore originates from

[3] "Spam : A Threat to the Information Society", ITU News 5/2004.

overseas[4]. As a result, legislation is unlikely to deal effectively with the vast majority of spam. The experience in the United States shows that anti-spam legislation has had little effect and has failed to deter spammers[5] whilst in Australia it has been accepted that legislation cannot by itself solve the problem of spam that originates outside the jurisdiction.

3.13 For this reason, a significant proportion of the available resources could be usefully applied in public education campaigns aimed to provide users with the tools to deal with spam and encouraging them to use such tools. About 42% of users surveyed in late 2003 had no knowledge of how to protect against spam[6]. Separately, the survey also showed that 38% of users were aware of anti-spam measures but were not using any such tools (filtering functions and independent software) whilst 26% were not even aware of such measures. In addition, the survey presented at the ITU meeting noted above found that only 42% of recipients had anti-spam software in place[7]. As a result, we support an approach that focuses on self-help, particularly the measures taken by the various industry agencies like the SITF, DMAS and SBF.

3.14 Having said that, if legislation is introduced to apply to spam that originates in Singapore, the objectives of legislation should be balanced, and should not prevent genuine business communications, e.g. email marketing to either existing or new customers.

3.15 Our specific comments about the proposed legislative framework are contained in Section 4 below. A summary of some main points follows below:

(i) if there is already an existing business relationship between a business and its customer or client, it is reasonable to expect that a company can send commercial emails to its customer or client. The customer or client will reasonably expect such communications, and they will have already given consent (either express or implied) to their receipt. Such commercial email communications should not be regarded as

---

4 "Survey on Unsolicited E-mails Key Findings", Precision Research, published 25 May 2004, www.ida.gov.sg

5 "US Anti-spam law fails to bite", BBC News, 9 February 2004.

6 "Survey on Unsolicited E-mails Key Findings", Precision Research, published 25 May 2004, www.ida.gov.sg

7 Communications Day, 9 July 2004

"unsolicited commercial emails' (i.e. they are not spam), and should be outside the legislative regime;

(ii) the legislation should only apply to spam sent in bulk. SingTel suggests that the definition of "in bulk" could refer to 5,000 emails per IP address or per sender every hour or half hour. However, the use of dictionary attacks or automated spamming tools to send emails in bulk should also be prohibited;

(iii) the legislation should allow unsolicited commercial emails (i.e. spam emails) to be sent under an "opt-out" regime, which imposes minimum standards. This is a more practical approach than an "opt-in" approach;

(iv) the legislation should be clear and identify the liable party as the party commissioning and/or procuring the spam; this should exclude parties whose resources or facilities may have been used or leased for sending the spam;

(v) where legislation is ultimately introduced, we note that the proposal to provide only ISPs with the statutory right to commence court action against spammers is contrary to the concerns raised by the IDA and the AGC with regard to the effects of spam on society at large. We submit that consumers and/or recipients (consumers or businesses who are the recipients of spam) should be given the same statutory right to commence action against "spammers" who do not comply with the minimum standards set out in the legislation. ISPs should not be expected to commence action against spammers on behalf of consumers or recipients of spam;

(vi) ISPs should be given the right to cease providing services to those spammers (at the sole discretion of the ISP) and to recover damages and/or losses suffered due to spam;

(vii) the framework must also clearly identify the enforcement agencies and such a role is best assumed by the regulatory agencies who have the necessary expertise and knowledge (e.g. IDA, MDA, AGC). Enforcement agencies should also be able to commence court proceedings against spammers;

(viii) ISPs should be able to commence court action against spammers who use dictionary attacks or automated spamming tools without having to prove that the emails sent did not comply with the minimum requirements under the "opt out" regime. In such circumstances, ISPs may also elect to cease providing services to spammers (at the sole discretion of the ISP). Similarly, consumers and/or recipients of spam that are the result of dictionary attacks or automated spamming tools should be able to commence court action too;

(ix) there is no need for the legislation to impose an obligation upon ISPs to develop an additional code of practice, and the legislative approach should not impose cost or administrative burdens on ISPs. For example, ISPs should not be expected to assume monitoring functions or to police compliance with the legislation; and

(x) the sending of SMS and MMS does not need to be regulated.

3.16 Detailed comments in relation to the issues raised by the Consultation Paper are set out below.

4. SPECIFIC COMMENTS

Definition of spam

4.1 It has been proposed in the Consultation Paper that spam be defined as "unsolicited commercial emails". The use of the word "unsolicited" is important, and appears to require further clarification.

4.2 The word "unsolicited" is not the same as the word "unwanted", and connotes an "opt-in" approach (i.e. it suggests that the email needs to have been requested). Without clarification, the definition may apply to emails that are sent by organizations to users/customers who already have a form of relationship with the organizations.

4.3 For example, an organization may already have established a relationship with customers or clients who have bought products from them and are currently using the organization's products and services. Under such circumstances, it is reasonable to expect that the organization should be able to send emails to the users informing them of the organization's new services or products, or new promotional offers, or even informing them of ways to subscribe to services. Such email alerts should not be classified as "unsolicited commercial emails"

as they are based on an existing relationship between the sender and recipient.
.

4.4 To provide some further telecommunications/IT industry examples, email communications between businesses and their users with regard to upgrades to new software, or notices like expected maintenance times for services, or ways to subscribe to new services are expected by customers. These should not be regarded as "unsolicited commercial emails".

4.5 The definition of "unsolicited commercial email" appears to require users to specifically subscribe to email alerts or information services, or to initiate the communications to the regulated entity. This is not an appropriate approach.

4.6 Hence, it is proposed that the definition of spam should exclude emails that a business sends to its existing customers (i.e. the legislation could deem such emails to be sought or "reasonably expected").

4.7 SingTel notes that the effect of this would be similar to the effect of the *Spam Act* 2003 in Australia. The approach under that legislation is to treat all "unsolicited commercial electronic messages" as spam, but to deem commercial electronic messages sent in the context of an existing business relationship to have been impliedly consented to (and thus not to be unsolicited). However, SingTel suggests that a better approach could be to make this clarification in the definition of "spam" itself.

4.8 Therefore, the legislative regime could apply to unsolicited commercial emails (which do not include electronic messages sent in the context of an existing business or customer relationship). The legislative regime would require such messages to meet the minimum standards set out in the legislation (as summarised in paragraph 11 of the Executive Summary of the Consultation Paper, and as discussed in more detail below).

4.9 As a separate point, SingTel also supports the proposal to focus on email communications only. As is mentioned in the consultation documentation, the sending of SMS and MMS today is already constrained through cost (as SMS and MMS are charged for on a per message basis) and for technical reasons (as there is a limit to the number of characters that will fit into an SMS). There appears to be no justification for regulatory intervention in respect of SMS and MMS.

Spam transmitted in bulk

4.10 We note that the Consultation Paper proposes that the legislation will apply to spam emails sent in bulk, regardless of the content transmitted, as it is expected that the volume of the emails transmitted should therefore have some level of impact on consumers or society.

4.11 SingTel agrees that the anti-spam legislation should only apply to spam that is transmitted in bulk. However, in making this submission, SingTel emphasizes that the introduction of an "in bulk" element of the definition of spam should not result in ISPs being required to monitor email transmissions, or to report to the relevant regulatory authorities if it suspects that any individual or company is sending spam. In short, ISPs should not have to assume a "policing" role, as this would quite simply impose an unreasonable financial and administrative burden upon ISPs.

4.12 Instead, insofar as the legislative regime needs to involve the ISP, it should be complaints driven (e.g. if a recipient complains to the relevant regulatory authority, the regulator will investigate, and in that context, it could ask the relevant ISP to confirm whether the email had been part of a bulk email transmission).

4.13 The definition of "bulk" should be clear and the volume must be measurable, based on a commonly agreed sent of parameters and guidelines for easy implementation. Setting a limit that is too low will lead to micro management and wastage of resources in enforcement.

4.14 For this reason, we propose that a clear definition of "bulk" should include the number of emails sent per IP address or per sender every hour or every half hour. A suggestion is to start with 5000 emails per IP address or per sender every hour or every half hour.

Spam sent from or received in Singapore

4.15 The Consultation Paper states that *"It must be recognized that the preponderance of spam originates from overseas where any legislative effort may well not have any bite"*. It then suggests that spam control legislation may nevertheless control spamming activities that take place in Singapore.

4.16 A survey in late 2003 indicates that 77% of the spam received by Singaporean users surveyed originated from overseas and not locally[8]. The figure may well be even higher than this, noting that the spam regulator in Australia has claimed that 98% of spam received in Australia originates from outside its shores[9].

4.17 The Consultation Paper proposes that the anti-spam legislation applies to spam originating from or received in Singapore, as in those instances there is a nexus to Singapore. As an enforcement matter, this would enable spammers based in Singapore to be regulated (including Singapore-based spammers who arrange for spam to be sent into Singapore from offshore).

4.18 While all spam received in Singapore (that does not contain the required particulars) will be prohibited, as a matter of practicality, this will only be able to be enforced against spammers with a Singaporean base. The imposition of legislation only on spam sent from or received in Singapore is clearly insufficient in addressing the issue of spam. This illustrates why more than legislation is required to combat spam.

Person or business commissioning or procuring spam

4.19 The legislation should be clear and identify the liable party, i.e. the liable party should be the party commissioning and/or procuring the spam. SingTel agrees with the approach outlined in the Consultation Paper that the spammer and the merchant or business commissioning the unlawful spam should be liable for that unlawful spam.

4.20 SingTel also wishes to emphasize that entities or parties whose resources or facilities may have been used or leased by spammers should not be liable for sending the spam. It would be extremely difficult for entities or parties who lease out resources or facilities, or whose resources or facilities are used, to monitor how these resources or facilities are being used and the legislation would impose an unreasonable cost burden on such parties.

Requirements for sending of unsolicited commercial email

---

8 "Survey on Unsolicited E-mails Key Findings", Precision Research, published 25 May 2004, www.ida.gov.sg

9 Interview with Anthony Wing, Australian Communications Authority, 23 July 2004, on ABC Radio: http://www.abc.net.au/science/news/scitech/SciTechRepublish_1159697.htm

4.21 SingTel's view is that spam (i.e. unsolicited commercial email) should be required to comply with specified regulatory requirements (described in this submission as "minimum standards"). The sending of spam that does not do so should be an offence.

4.22 We note that the government has already identified the need for an approach that "balances the need of local businesses to publicise themselves with the wish of computer users who do not want to be swamped with unwanted mass – marketing emails"[10]. Singapore is an already highly developed IT hub with an impressive household computer ownership rate of 73.7% in 2003[11] and a high level of internet usage at 51% in 2003[12]. Increasingly, business communications are taking place through emails, including the conducting of marketing activities. SingTel is concerned that proposed legislation does not limit the usefulness of electronic communications as a tool for genuine businesses.

4.23 Accordingly, SingTel agrees that there should be some minimum standards that apply to spam email.

4.24 SingTel would support a requirement for spam emails to include an "opt-out", which would allow recipients to unsubscribe or to request not to receive future commercial communications.

4.25 SingTel considers that an "opt-out" approach would also give users/consumers more flexibility than an "opt-in" regime. With an opt-in regime, users will not have the right and flexibility to make a decision as to whether they wish to continue receiving such emails that could contain value to them. On the other hand, an opt-out approach as described in the consultation would provide recipients with the opportunity to continue receiving emails, unless they choose to opt-out.

4.26 It should be noted that many consumers do find commercial emails sent by businesses as a useful source of information; for example, an interactive poll conducted by the Straits Times on attitudes towards spam showed that about 66 per cent of the 1,200 polled saw these messages as useful information, and about 70 per cent 'don't mind' such unsolicited messages as these let them

---

10 "Fighting spam : Opting out is in", Straits Times, 23 June 2004

11 Annual Survey on Infocomm Usage in Households and by Individuals for 2003, 11 June 2004.

12 Ibid.

know 'all that's out there'[13]. The same poll indicated that about 70 per cent polled preferred an opt-out approach.

4.27 In terms of the other minimum standards, we are in favour of providing users with a valid and simple opt-out mechanism with a return email address to which an opt-out request can be sent. We also support the need for opt-out instructions to be in English, at a minimum.

4.28 We also support the requirement for complying with an opt-out request within a specified time frame. With this, we believe that there would be some level of confidence and certainty provided to recipients of spam who wish to opt-out. We recommend that a reasonable time period for responding to an opt-out request would be two (2) weeks as this gives senders sufficient time for updating their database.

Labelling

4.29 Whilst we agree with the general approach towards responsible and informative labeling, we note that some of the labeling requirements may be overly restrictive and are perhaps unnecessary. For example, it may not be necessary to require the characters [ADV] in the subject title as most subject titles already indicate somewhat the nature of the email. We recommend that as long as the subject title carry sufficient indication that the email is a marketing communication or advertisement, no other labeling is required.

4.30 Further, we do not see the relevance of requiring a valid postal address. In the case of business communications, email is chosen for its convenience and its cost-effectiveness; follow-up communication through email is the norm. Requiring both a genuine email address and a valid postal address is somewhat unnecessary. We recommend that the minimum standard be reduced to either a genuine email address, which can either be the email address used for sending the original email or another genuine email address used by the company, to facilitate the administrative process for opt-out requests.

Legal Action

[13] Straits Times, 16 July 2004, http://straitstimes.asia1.com.sg/techscience/story/0,4386,261747-1090015140,00.html

4.31 The proposal to provide only ISPs with the statutory right to commence court action is contrary to the concerns raised by the IDA and the AGC with regard to the effects of spam on society at large. Also, the Consultation Paper is silent about the relevant regulator's rights to enforce compliance with the legislation (and to prosecute offences). These matters are noted separately below.

4.32 We agree that ISPs should have the right to commence court action (and to cease providing carriage services to spammers, if the ISP at its sole discretion elects to do so). ISPs should also be able to recover damages and/or losses suffered due to spam

4.33 However, we do not agree that consumers (users or businesses who are the recipients of spam) need not be given the same statutory right to commence action. Contrary to the reason given in the consultation document, recipients of emails frequently have the ability and resource level to bring court action. In some cases, the recipients of spam could be large multinational corporations or business entities who may have suffered economic loss and have the resources to take action. They should not be denied the right to bring court action.

4.34 Spammers, especially recalcitrant spammers, would thus be aware that their actions could attract legal action from the actual recipients of their spam, ie those who have suffered actual economic loss and damage as well as ISPs who may have suffered economic loss and damage. We recommend that consumers and/or recipients themselves also be empowered to commence legal action for unlawful spam.

4.35 In addition, there may also be instances where it is not appropriate nor is it applicable for an ISP to commence court action, e.g. the ISP may not have suffered sufficient economic loss to merit court action against the spammer but the consumer and/or recipient could have genuinely suffered economic loss and would need the right to court action to recover damages. Hence, the legislation should allow the consumer and/or recipient to commence court action against spammers; ISPs should not be expected to commence action against spammers on behalf of consumers or recipients of spam.

4.36 In the event that there are still concerns over consumers' and / or recipients' resource levels, the legislation could then provide for specific associations to

take court action on behalf of groups of consumers and/or recipients who have suffered economic loss or damage. For example, it is possible for industry bodies or associations like the Singapore Business Federation or the Consumer Association of Singapore to take action on behalf of businesses and consumers respectively.

4.37 In addition, the relevant enforcement agency or agencies (e.g. IDA, MDA, AGC) should be able to initiate actions against spammers (e.g. following the successful investigation of complaints). This is noted at 4.43 below.

Civil action for dictionary attacks and use of automated spamming tools

4.38 The Consultation Paper suggests that ISPs should be able to commence court action against spammers who use dictionary attacks or automated spamming tools without having to prove that the emails sent comply with the minimum standards.

4.39 SingTel agrees with this proposal. Directory attacks and the use of automated spamming tools are prima facie evidence of "spamming" activity, and are unlikely to ever comply with the minimum standards. Spam that is created by use of these attacks and tools generates much of the spam that is in circulation globally. Addressing the problem of spam that is created in this way eats into the resources of ISPs and impose a cost burden on them.

4.40 Similarly, SingTel submits that consumers and/or recipients of spam that are the result of dictionary attacks or automated spamming tools should be able to commence court action against such spammers too.

Co-regulation - Codes of Practice

4.41 We do not see a need for legislation to impose a duty on industry participants to promulgate and adopt additional self-regulatory code of practice. Currently, there are already several initiatives by the industry to provide self-regulatory guidelines or codes of practices (e.g. the Direct Marketing Association of Singapore has a Email Marketing Guidelines) that provide clear information on acceptable commercial email practices and policies. Similarly, the ISPs currently already provide information and tools to their users on anti-spam measures. An imposed duty for a code of practice is not necessary under such circumstances.

4.42 At most, the industry participants could voluntarily co-operate (under voluntary codes of practices) to coordinate their efforts in the area of common definitions (eg dictionary attacks), and to share information on new developments regarding spam. Such voluntary codes of practices should be self-regulatory in nature and must not pose as a cost burden to industry players like ISPs. The participation in such activities should be discretionary, not mandatory.

Enforcement

4.43 The proposed framework does not identify who is to enforce the legislation. In doing so, the framework provides no certainty except in so far as to provide a right for ISPs to commence court action. However, SingTel's submission is that there should be an identified regulatory agency who is able to prosecute offences under the legislation. The relevant regulatory agency or agencies, whether the IDA, MDA, AGC or otherwise, would have the necessary expertise and knowledge to perform this role effectively.

Others

4.44 As a final point, the legislative and regulatory approach should also ensure that ISPs should not have to bear additional costs burdens. To illustrate, the introduction of legislation should not result in ISPs having to respond to all complaints about spam that do not meet the minimum standards at no charge or to offer anti-spam solutions at no charge. Rather, the ISPs should only be required to assist in investigations, to a reasonable extent and where appropriate, where an investigation is deemed necessary by the necessary regulatory enforcement agency. There should not be any requirement for ISPs to implement sophisticated and resource-intensive email scanning engines and systems to ensure, for example, that all emails adhere to the minimum standards.

5. CONCLUSION

5.1 In conclusion, SingTel supports initiatives to reduce spam, but urges a balanced and commercial approach be adopted in Singapore (with a significant emphasis on public education, and the use of technologies such as anti-spam software).