YAHOO!'S RESPONSE TO THE JOINT IDA-AGC CONSULTATION PAPER TITLED "PROPOSED LEGISLATIVE FRAMEWORK FOR THE CONTROL OF E-MAIL SPAM"

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

Consent is the primary factor for determining whether a communication is solicited or unsolicited. The most appropriate mechanism for a person to express his consent or otherwise would be a default opt-out approach. In other words, where a person has not previously had an opportunity to express his consent or otherwise in respect of a particular sender, an initial communication by that sender to that person should be permitted.

It is only after a person has had an opportunity to express his consent (eg. by explicitly agreeing to accept further communications) or otherwise (eg. by explicitly asking that no further communications be sent to him, ie. by opting out), that enforcement against unsolicited communications should commence.

In the foregoing, the "sender" should be deemed to be the person on whose behalf the communication is sent, even if that person has outsourced the actual transmission of communications to a third party. If the proposed legislation is intended to impose liability on third parties (such as "email houses") who are intentionally aiding and abetting senders, as appears to be the case (see Q8), the proposed legislation should identify such third parties by their behaviour, as opposed to simply including them within the definition of "senders".

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

Commercial communications should be defined as those communications that have the primary purpose of inducing an order or purchase of goods or services by the recipient. This should include communications that are sent solely or primarily for branding or marketing purposes (such as to build up consciousness for a newly-launched product), but which do not directly solicit or induce an order or purchase of goods or services as such. For instance, the message may comprise no information other than a hyperlink to a website about a newly-launched product, without any transactional capability – such a message should be considered commercial. However, a message that is primarily sent to indicate how to use a product or service that was previously sought or already being used by a user should be able to include such a link, without this message being considered to be commercial.

More broadly, it is important that communications with a very minor or incidental commercial component, such as incidental viral marketing in the vein of the words "*Do you Yahoo?*", are not considered commercial. For instance, an automated e-mail notification by Yahoo! to a user to inform that user that his Yahoo! Groups messages have been bouncing, which contains the tagline "*Do you Yahoo?*" in the e-mail signature, should not be considered commercial.

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

The issue should not be so much whether there should be *exclusions* from the definition of spam (ie. unsolicited commercial e-mail), but whether there should be *exceptions* from the definition of spam. An exception may be either something that satisfies the technical definition of spam (ie. unsolicited commercial e-mail) but should not be regulated as such, or something that does *not* satisfy the technical definition of spam but *should* be regulated under the proposed legislation.

With regards to the first category of exceptions, which may be termed "exclusions" as in the question, minor marketing that accompanies critical functions such as billing, renewals or upgrades of existing services, product recalls, employer/employee communications, or confirmation of a commercial transaction should not be considered spam. In other words, communications sent in furtherance of or pursuant to an existing relationship (whether contractual or pre-contractual, and regardless of the nature of such relationship (ie. whether it is official, commercial or personal)) should *not* be considered spam.

On the other hand, with regards to the second category of exceptions, any communications with false or fraudulent header information or deceptive subject headings should be considered spam and regulated, even if a person had consented to receive them or they are not considered commercial in nature. These are especially egregious abuses that require regulation, and hence justify such an exception to the technical 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?

Yes. The technology used by a person to access his e-mail messages is solely at that person's discretion, and is beyond a marketer's control or knowledge. This is especially so, now that messages sent via one format can be easily forwarded to a device that receives the message in a different format (eg. a message sent via TCP/IP being transmitted to the end-user via SMS).

The proposed legislation should therefore apply equally 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?

The focus of the proposed legislation should be on regulating spam, specifically (i) e-mails with false or fraudulent header information or deceptive subject lines, and (ii) commercial e-mails that were sent to a person after that person has had an opportunity to express opt-out consent (as described in response to Q1 above) in relation to that particular sender.

This should be regardless of whether the e-mails are sent in bulk or otherwise, especially when, from the recipient's perspective, it is immaterial whether the unsolicited commercial e-mail was sent only to him or to thousands of others.

However, the bulk transmission of spam could be a criterion for determining the appropriate level of criminal penalties or even enhanced fines.

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

Following on from the suggestion that bulk transmission of spam be a criterion for determining the appropriate level of criminal penalties or enhanced fines, possible factors used may include standards such as several hundred thousand substantially similar messages per day or per hour. A graduated level for increased numbers in a given time period may be appropriate for graduated criminal penalties or fines. The number of e-mails should be substantial for such graduated criminal penalties or fines to be triggered.

A parallel may be drawn with the 1999 case of ***PP v Tan Cheng Kang*** (DAC 8409–8411/2000). In that case, the accused was found guilty of three charges under Section 7(1)(a) of the Computer Misuse Act, for committing what were essentially "denial of service" attacks. He had sent over 2500 e-mails to each of three government agency e-mails, all within the space of 2.5 hours. Arguably, any numerical benchmark used to ascertain whether e-mail messages have been transmitted in bulk (thereby triggering enhanced penalties) should be consistent with the numbers and time periods involved in this case.

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

The proposed legislation can address spam both sent from and received in Singapore, as there is obviously a territorial nexus in both cases. But it may be difficult to prosecute a person located outside Singapore who sends spam to a resident of Singapore for numerous practical reasons. Therefore, Singapore should seek effective agreements on a multi- and/or bilateral basis, so that countries cooperate in bringing spammers to justice in the international arena.

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

Yes, both the commissioning or procuring party, or sender, and the intermediary who provided the service that was procured, should be subject to liability, if certain conditions are satisfied. As noted in paragraph 5.18 of the consultation paper, the US has adopted such an approach. However, this provision in the CAN-SPAM Act of 2003 has not yet been enforced, so there is little experience with its effectiveness or operation. The provision requires both knowledge and intent on the part of the intermediary, and is designed to apply to new businesses that are created merely to shield either themselves or others from liability under the CAN-SPAM Act for messages they send, when they know and intend that these messages are sent on their systems.

However, the definition of "procure" is critical in this context. For a person to be found to have "procured" spam, something of value should be exchanged between the parties involved. There should also be actual knowledge that spam is being procured.

Generally speaking, intermediaries should not be held liable for the activities of third parties across their networks. On the other hand, it is appropriate and desirable to hold intermediaries liable, where they have the requisite knowledge and/or intent to assist in unlawful spamming.

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

Yes. An opt-out regime allows entrepreneurial marketers to take advantage of the low barriers to new markets on the Internet. This approach will enhance the growth of new companies adopting Internet-based business and marketing models.

However, once a recipient receives the first message from a particular sender, it is imperative that the sender adheres to any opt-out expressed by that recipient. Enforcement of this aspect must be aggressive, in order for an opt-out regime to be effective. Otherwise, the only persons affected by the proposed legislation would be legitimate marketers who incur the necessary expenses to comply, while unlawful spammers continue to proliferate and enjoy the fruits of their abuses.

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

Compliance with an opt-out request should be as expedient as business practices will allow. It is necessary to remember that some companies engaged in marketing may have extensive corporate or affiliate structures that make compliance more difficult or time-consuming. Generally speaking, compliance with such a provision should be accomplished in not more than 10 business days.

Q11. Are these minimum standards sufficient?

The proposed minimum standards will establish a workable framework for users of the Internet and those who engaged in legitimate e-mail marketing. However, they are not likely to deter or stop spammers, who usually are already breaking one or more local laws, for instance by distributing or promoting obscene publications, or advertising or selling pharmaceuticals without the necessary licences or approvals.

It is important to realise that the proposed legislation, or indeed any legislation, is not likely to, in and of itself, reduce the amount of spam received by Internet users. The eradication of spam will require a combination of technology, laws and their enforcement, and robust user education.

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

The key should be to ensure that a user is clear that an e-mail is an advertisement. If that is the overriding concern, then it would be much more effective to require labelling within the e-mail itself. Within a communication, it should be abundantly clear to the reader that he is viewing a commercial e-mail, and that he can choose not to receive any further e-mails from that particular sender. This would be a much more

flexible approach, that ensures that users retain control, without unnecessarily limiting legitimate commercial e-mails that a user might find to be of interest.

The use of "[ADV]" in a subject line, while superficially attractive, may cause a recipient to reflexively reject all e-mails bearing such a label, when there could be e-mails that may be useful to that recipient. In this way, new business opportunities would be unnecessarily stifled.

The consultation paper itself, at paragraph 5.23, recognises the crucial economic objective of permitting "*new and often more innovative firms and organizations to enter markets and compete*". To require an "[ADV]", or any other, label in the subject line of an e-mail would detract from this objective.

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

Yes, ISPs are in the best position to recognize spam flowing across their networks and to formulate strong cases against spammers. They should be given incentives to use additional legal tools to fight spammers, in addition to the technological and educational tools they already wield.

In this regard, "*ISPs*" should not be limited to Internet Access Service Providers (which is a term used in the MDA's content regulations), but should include all providers of Internet services who are affected by spam. This would include providers of e-mail services that do not provide Internet access as such.

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?

S$1.00 per unlawful spam would be appropriate for a statutory damages regime. There could also be a provision for aggravated damages, for knowing and/or wilful and/or flagrant violations and/or the use of intentional spammer techniques such as those mentioned in Q.15.

However, it is imperative that there be a cap on the statutory damages that can be awarded, so that legitimate businesses that make honest mistakes are not unduly punished. This is especially true for companies with high volumes of clients or users, who may send a form communication to literally millions of addresses at once. S$50,000 would appear to be a reasonable aggregate cap.

The above proposals can be contrasted with Section 7 of the Computer Misuse Act (pertaining to "denial of service" attacks, which are the closest approximation to spam in the Act), where the penalties are a fine of up to S$10,000 or up to 3 years' imprisonment for a first offender, a fine of up to S$20,000 or up to 5 years' imprisonment for a repeat offender, and a fine of up to S$50,000 or up to 7 years imprisonment where damage is caused to the target of the attack.

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?

Dictionary attacks or automated spamming tools are clearly intentional acts, and can be quite damaging to ISP networks. It would be most appropriate to deal with the use of such techniques, by making their use in cases where the transmission in question and/or the underlying e-mail is prohibited by the proposed legislation, a trigger for enhanced penalties.

Furthermore, it is necessary to ensure that in situations where the transmission of e-mails (whether to a single, a few or many recipients or in bulk) is permissible under the proposed legislation, the use of an automated tool should not be unlawful and should not render that transmission or the underlying e-mails unlawful. In other words, the mere use of an automated tool to send e-mails should not be unlawful in and of itself. For instance, where a legitimate marketer is highly successful and has a large volume of e-mails to send to recipients who have consented to receive them, it is frequently (if not always) more efficient to use an automated tool, and this must be permissible. Any other position would only serve to unfairly penalise successful marketers.

A related issue is the ability of ISPs to maintain control of their networks. It must be clear that ISPs retain the ability to protect their networks from overload through dictionary attacks or automatically generated mail. Nothing in the proposed legislation should diminish or detract from such control by ISPs.

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

All the different stakeholders in the e-mail debate should work together to develop a code of industry best practices. Possible participants include the Singapore infomm Technology Federation, the Direct Marketing Association of Singapore and the Consumers Association of Singapore.

If this code of practice is required under the proposed legislation, then those marketers who participate in and comply with the code should receive at least some degree of protection from liability for any actions fairly taken to abide by the code. However, the proposed legislation should not compel participation in or compliance with the code. Instead, participation in or compliance with the code should be voluntary, with the benefit of additional legal protection under the proposed legislation as the incentive.

Q17. What should the code of practice cover?

An industry code of practice should cover the actions that all of industry, senders of commercial mail or individuals can and should take to diminish the overall problem of spam for everyone. It should encourage ISPs to explain to their customers and the public what they can do to reduce the amount of spam, and to protect themselves from it. Those who send e-mails should also adopt the relevant best practices, thereby ensuring that legitimate players avoid those types of messages that are most problematic. It may therefore be appropriate to either have different codes for

different types of stakeholders, or a single over-arching code with individual components devoted to each different type of stakeholders.

A useful starting point in relation to ISPs, e-mail service providers and large senders of e-mails could be the proposal of the Anti-Spam Technical Alliance, which released its proposal in June 2004 after over a year of work. The members of the ASTA include key industry stakeholders involved in the issue of spam, and includes industry leaders such as Yahoo! and America Online. The complete ASTA proposal can be found at http://antispam.yahoo.com.

Q18. Who should enforce the code of practice?

The code of practice should be enforced by either industry organizations that have the authority to expel or otherwise penalise a non-compliant party, or a third party altogether. This approach has generally been successful around the globe. However, if it appears to be ineffective, then it may be appropriate for the Government to step in and play a role in ensuring compliance with the code.