

Microsoft Singapore

Submission in response to the proposed legislative framework for the control of e-mail spam in Singapore

1 Introduction

1.1 Microsoft welcomes anti-spam initiative

Microsoft welcomes the fact that the Infocomm Development Authority of Singapore (IDA) and the Attorney-General's Chambers of Singapore (AGC) are debating the issue of legislative reform designed to significantly reduce the volume of spam sent to and from individuals and organisations in Singapore. The risk of inaction is that the vital communications medium of email will no longer be seen as a reliable and efficient means of communication and that Singapore risks jeopardising its position as a regional IT hub.

Microsoft believes in a multi-faceted approach to combating spam, which depends on the combined efforts of industry and government and includes the following elements:

- (a) Developing and implementing new technological tools to combat spam;
- (b) Aggressive enforcement campaigns by both the private and public sector to penalise illicit spamming practices;
- (c) Appropriate legislation that encourages the adoption of email best practices and a means for filters and consumers to identify senders that adhere to such practices.

Microsoft is constantly working on new technologies and strategies to create significant improvement in spam volume. Currently, MSN, Hotmail and Outlook 2003 accounts have experienced significant reduction in spam as a result of SmartScreen technology, an advanced spam-filtering tool. Increasingly, technology can help prevent spam, and other threats from ever entering and overburdening networks, which has led Microsoft to create Exchange Edge Services, a new technology that insulates networks from incoming spam and hacker attacks. Edge Services will incorporate the latest filtering and security technologies and will enhance Microsoft's platform for third-party anti-spam solutions.

Microsoft looks forward to working with the IDA and AGC in the future so as to craft an effective approach for combating spam.

2 Response to specific questions

2.1 Questions 1, 2, 3 & 4

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?

Microsoft supports legislation that would prohibit the transmission of unsolicited commercial emails which contain false or misleading information regarding the sender or the nature of the product and recommends that the proposed legislation includes prohibitions against:

- (a) the transmission of a commercial electronic mail message that falsifies email transmission information for the unsolicited commercial email; and
- (b) the transmission of a commercial electronic mail message that contains false or misleading information in the subject line.

Microsoft believes that the definition of unsolicited commercial electronic mail should not include email sent in the context of a pre-existing business relationship, that is a transactional or relationship message. For this purpose, Microsoft believes that an appropriate definition for these types of emails can be found in section 3(17) of the United States CAN-SPAM Act. Provided that the primary purpose of the email message is to facilitate, provide information or further transact with the recipient of the email message which relates to a commercial transaction or relationship already established with the sender, then that email message should not be considered to be 'unsolicited'. For example, it should be lawful for a manufacturer to send an email to a purchaser of a product indicating that there are safety concerns with a particular product requesting the recipient to take appropriate action.

Generally, an electronic mail message sent with the primary purpose of which is to promote or advertise the supply of goods or services, including the advertising of an internet website operated for a commercial purpose should be regarded as a "commercial" electronic mail message.

Microsoft believes that the proposed legislation should not distinguish between the technology used to access email messages. It would be problematical if the proposed legislation was to introduce different tests, dependent upon the technology used by the recipient to access the email message, with which the sender must comply. A sender is, in most cases, unaware of the choice of technology used by the recipient to access an electronic mail message.

Any proposed legislation should also encourage the further deployment of spam filtering and blocking technologies which are largely responsible for limiting the amount of spam that reaches a consumer's email inbox by allowing companies to use these technologies without the imposition of a new liability. ISPs and email service providers should continue to be allowed to block email that violates existing law or the service providers' stated email policies, without attracting any liability.

2.2 Questions 5 & 6

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?

Microsoft welcomes the proposal that sending a single unsolicited commercial electronic mail message will not contravene the legislation.

Difficulties of proof may be a barrier to the application of a working definition of "bulk" electronic email. A tiered statutory scheme for damages based on the number of infringing electronic mail messages communicated is the most effective method to penalise senders of spam in bulk [see responses to questions 13 and 14 below].

2.3 Question 7

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

Any proposed legislation should, as a minimum, apply to spam sent from or by individuals or organisations in Singapore. There are also good reasons as to why the proposed legislation should also apply to unsolicited electronic messages received in Singapore. Microsoft believes that international laws regulating spam should be harmonised wherever possible. The United States, the European Union, Japan, South Korea and Australia have already enacted specific anti-spam legislation and it is important for Singapore to maintain a degree of consistency.

Harmonisation is integral in the context of Singapore's role as a regional business and information technology hub. As more and more jurisdictions seek to enact anti-spam legislation, the compliance burden for businesses trading internationally will increase. We should not lose sight of the overall objective of anti-spam legislation, namely to reduce substantially the quantum of spam that originates largely from unscrupulous operators rather than legitimate businesses. Without harmonisation, we run the risk of unfairly penalising legitimate businesses engaged in international trade, but having little impact on unscrupulous spammers.

Harmonisation may be achieved by a number of methods. One example is the European Union's approach to "adequacy" of personal data protection laws to which personal data is exported. If Singapore was to adopt that approach, a unsolicited commercial email sent from the jurisdiction with "adequate" anti-spam laws would not be a contravention of Singapore law.

Another approach is that taken by the Australian legislature, namely to confer power to make regulations to give effect to an international convention on spam. No doubt there are other approaches that could be taken.

2.4 Question 8

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

It is important to ensure that the businesses who stand to profit from spam (in the sense that their business or products are promoted in an unsolicited email) are not able to shield themselves from liability if they were knowingly involved in the transmission of the spam. Both the US CAN-SPAM Act and the Australian Spam Act deal with this issue on the basis that if a person or business allows or knowingly assists in the promotion of their goods or services through the use of unsolicited commercial email, then they should be liable for such transmission. We doubt there is much practical difference between the US and Australian provisions on this point.

Given the tremendous amount of commercial emails sent over their networks, email providers and ISPs should not be held liable for merely providing intermediate transmission services for the delivery of email between the sender and recipient.

2.5 Questions 9, 10 & 11

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?

Microsoft agrees that an opt-out regime for email spam control is beneficial to Singapore as a regional IT and commercial hub. The proposed legislation should include a prohibition against the transmission of unsolicited commercial electronic mail that fails to provide a mechanism allowing recipients to easily and at no cost remove themselves from the sender's electronic mail address lists so that they do not receive any future emails from that sender.

Microsoft believes that the 10 business day timeframe specified in the US CAN-SPAM Act for compliance with opt-out requests is reasonable if it is coupled with a definition of a "sender" (on whom an obligation to comply with an opt-out request is imposed) similar to that in section 3(16) of the CAN-SPAM Act, which deals with separate lines of business or divisions. That provision recognises the practical difficulties faced by large corporations with business units that operate essentially on an independent basis. If adopted, it would mean that corporations with separate business units are not unfairly disadvantaged when compared to enterprises consisting of a number of separate corporations each of which operates a separate business.

Microsoft acknowledges that many (but not all) organisations rely on automated processes to act on opt-out requests. It may be possible to impose a shorter timeframe if (1) the sender relies on such a system and (2) the recipient makes the opt-out request strictly in accordance with the sender's instructions. In other words, the regime must recognise that the efficiencies of an automated system will not be achievable if the recipient fails to follow the required procedures when opting-out.

2.6 Question 12

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

The introduction of a requirement by a sender to label an unsolicited electronic mail message either in the subject or elsewhere will assist filter makers to provide a more efficient service and will promote a more effective system of blocking unsolicited commercial email.

2.7 Questions 13 & 14

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?

ISPs and other service providers invest considerable effort and resources in combating the current spam epidemic. Furthermore, these service providers suffer incur significant costs associated with events such as surges in bandwidth as a result of the passage and presence of unwanted spam on their servers. Microsoft believes that it is essential that service providers who are adversely affected by spam, such as ISPs and email providers are empowered with private rights of action against spammers. Providers of web-based email services, who may not also provide internet access, also suffer considerable damage and should be treated equally with Internet access providers.

Microsoft does believe, however, that private rights of action should be coupled with the government or a government instrumentality playing a regulatory role in the campaign against spam. It is unreasonable to expect the ISP sector to bear the entire burden of enforcement.

Microsoft further submits that the legislation or that any proposed legislation should set out detailed guidelines for civil remedies and damages. However, damages must take into account the notion of proportionality, specifically that penalties must fall hardest against those entities that are responsible for the lion's share of the spam problem. Therefore, damages should be capped at a pre-determined amount, while giving courts the ability to increase damages in cases where the defendant has acted wilfully or knowingly. Conversely, courts should be required to reduce damages in cases where entities have established and implemented email best practices and procedures designed to prevent the delivery of commercial email that would violate the new law. Such an approach will encourage good actors to adopt best practices and

create incentives for penalties to be levied against bad actors, not entities who are not contributing to the spam problem but have nevertheless made an inadvertent mistake. Civil remedies available must also include injunctive relief.

2.8 Question 15

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?
-----	--

Spammers rely heavily on the use of harvesting tactics and dictionary attacks to obtain electronic mail addresses to which they can send unlawful spam. Spammers who engage in these activities impose increased costs on both consumers and service providers. ISPs and email service providers alike should be allowed to initiate legal action under the proposed legislation against spammers who use dictionary attacks or employ automated email address harvesting tools such as spiders without having to prove that the emails fail to comply with the minimum requirements in the proposed legislation.

2.9 Questions 16, 17 & 18

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?

At present there is no formal ISP industry association in Singapore. If the IDA and the AGC are seeking to encourage the development of a self-regulatory ISP code of practice on spam, Microsoft would be prepared to co-operate with the major ISPs in Singapore to assist in the development of such a code.

A code could cover issues such as: service providers raising awareness amongst their customer base of technical solutions to minimise spam and any laws relevant to spam; offering spam filters to customers; closing open relays on servers operated by the service providers; topics to be addressed in acceptable use policies or terms of use; and methods for customers to report violations of spam laws. The topics to be addressed by the code will depend to some extent on the content of the legislation.

Microsoft believes that if such a code is developed, the industry should be given an opportunity to enforce the code itself. It would only be appropriate for government to play a role in enforcement of an industry code if there have been demonstrable failures by the industry to self-regulate.

3 Conclusion

The success of any legislative intervention on spam may be measured against these five criteria:

- (i) Dramatically reduced volumes of spam;
- (ii) Lower costs to consumers, service providers and businesses who currently bear the cost of spam;
- (iii) Greater consumer control over whether and how to receive, filter or delete messages;
- (iv) Broader commercial adoption and enforcement of email best practices;
- (v) Preservation of existing tools employed by service providers to fight spam.

Microsoft would be pleased to discuss this submission with the IDA and AGC. Please contact Sheila Saw, Corporate Affairs Manager, Microsoft Law and Corporate Affairs, Tel: (65) 6337 6088.