TAN & TAN
ADVOCATES SOLICITORS

**Tan & Tan Partnership**
20 Cecil Street #06-07
Equity Plaza, Singapore 049705
Tel: +65 6534 3348 Fax: +65 6532 2511
www.tanandtan.com.sg

**We do not accept service of court documents by fax.**

| | | | |
|---|---|---|---|
| Sender's Name | Bryan Tan | Recipient's Name: | IDA |
| Sender's Ref | BTT/misc | Recipient's Ref | - |
| Sender's EXT | 101 | Recipient's DID | - |
| Sender's Email | bryan.tan@tanandtan.com.sg | Date | Monday, July 26, 2004 |

Policy and Competition Development Group,
Infocomm Development Authority of Singapore,
8 Temasek Boulevard, #14-00
Suntec Tower Three,
Singapore 038988

antispam_submissions@ida.gov.sg

26 July 2004

Dear Sir,

**Re: Anti-spam law public consultation**

We are convinced by the figures cited by IDA and anecdotal evidence that spam is a serious and growing problem. We agree that not taking any action is not an option in response to the growing threat of spam. It is therefore an important step for legislation to be introduced in the fight against spam.

While legislation is never the answer to all the world's problems, legislation nevertheless sends a strong signal that a problem will be addressed and sets the minimum acceptable levels of conduct tolerated by society at large. Spam in general is a social problem, exploited by the errant few for monetary or other purposes against the Internet community at large and we do have the chance to stem in before it becomes systemic.

Therefore, we are pleased to submit our responses to the Joint IDA–AGC Consultation Paper on the Proposed Legislative Framework for the Control of Spam.

We wish to add that although Tan & Tan Partnership does advise clients in the information technology, telecommunications and Internet sectors, our response herein is our own and does not necessarily reflect the views of any of these clients. In addition, this response paper was prepared with the assistance of Ms Judy Yee, a law student from Santa Clara University.

Kind regards

**Bryan Tan**
Tan & Tan Partnership

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

We wish to point out that the solicitation requirement could potentially create a double-barreled test for consent, with the first test (at the definition of spam) being the weaker point. The second stage – whether opt-out or opt-in, is more definitive. For instance, could a website collecting email addresses, contain in its terms and conditions, an obscure provision that the user agrees to receive e-mails and by definition, such e-mails will not be considered spam and subject the user to being a target for indefinite and uncontrollable spam?

We acknowledge that a strict requirement as to solicitation may create undue burden. Therefore, perhaps it must also be said that's solicitation must be express, limited to the purpose expressed to be solicited for and with the full authority of the user to revoke such consent.

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

Some considerations whether a communication is commercial:

(a) whether it involves the offer to sell or invitation to treat of a good or service, whether from the sender or not, whether for consideration or not;
(b) if it involves the exchange of monies (whether for charitable donations or not);
(c) if it is of a business nature;
(d) if it is for marketing, whether the good is identified or not (this would cover market surveys).

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

We would suggest that only pure factual messages and messages from government should be excluded. Charitable appeals could potentially represent a significant source of spam from all kinds of unverified sources unless only approved charities are exempted.

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

The principle is acceptable. However, we note that where SMS-to-email messages are concerned, it is technically impossible for such emails to incorporate the proposed requirements, if such emails are considered spam. However, such inadequacies may be overcome with time and technology improvements. In addition, for the moment, cost barriers would not encourage spam through the SMS-to-email mode. The related question is – would the connecting factor be the mode of receipt of the e-mails or the mode of sending of the e-mails? We think it should be both.

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

Yes it should apply to spam in bulk. However, we think there is a presumption where certain forms of spam are used indiscriminately – for example, spam sent to non-existent email addresses such as sales@abc.com.sg which are eventually directed into default addresses or spam sent using dictionary attacks, the presumption of bulk spam transmission should be applied.

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

A quantitative test would be the clearest – 2,000 emails in any consecutive 30 day period on the same subject matter.

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

Yes, we agree. While Singapore must necessarily protect its users who are the targets of spam, in addition, Singapore cannot allow itself to be used as a launch pad of or haven for spam.

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

Yes. The simple equation is that the person standing to gain the most is not necessarily the computer operator but the business selling the said products. Since the business is willing to be unscrupulous in making sales target using a low cost public resource which burdens other people, then such business should also stand before the judgment of the law.

An additional point to consider would be persons who sell entire databases of (Singapore) email addresses. The argument would be that such persons are abetting the commission of a wrong. The only problem would be that such databases might be argued to have certain legitimate use, such as the verification of email addresses although this argument does not hold much water.

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

Although it may draw criticism for not effectively addressing the problem, we think it is more viable than the opt-in approach, which may be difficult to regulate. At least the opt-out approach has a higher probability of working to reduce spam originating from Singapore. Since the opt-out approach is a more business friendly than the opt-in approach in making it easier for new firms or organizations to enter the marketplace and compete with more established, well-known businesses, we think the opt-out approach would not unnecessarily burden businesses and may help introduce new innovations and products to consumers.

The only fear is that an opt-out regime may cause continued loss of confidence or even worse, irreversible damage if well-meaning users requesting to be opted-out have their information abused. We think it is important therefore for the opt-out provisions to be closely monitored and preferably, regulated by industry.

However, our general comment is that if for some reason any part of such measures prove inadequate to control spam, then we would support continued refinement to achieve the desired policy objectives.

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

Three working days. With modern technology, this should not be too hard to adhere to. We note that the Singapore Credit Bureau takes one business day to rectify information when informed by data owners.

*Q11. Are these minimum standards sufficient?*

Yes, we believe they are sufficient.

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

The slight concern is worrying whether a certain spam adheres to the requirements under the Singapore legislation. The end user will have to make a determination that it does before he has

the confidence to opt out. It is not sufficient to say that the end user should be educated not to reply to obvious spam. Instead, a trust mark to say that the spam is compliant with the Singapore legislation could be considered. The disadvantage is that if the trust mark costs money and is voluntary, and errant spammers can get away without having the trust mark, then most spammers will not undertake the trust mark.

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

Yes, but the definition of ISPs should be expanded. Spam is targeted at email and while ISPs do host emails, not all entities that host email servers are ISPs. In addition, some Singaporeans who use the services of an ISP for internet connection (such as SCV), use a third party for hosting their e-mails. Some other examples of such entities are web-hosting companies, private companies who operate their own email servers and other service providers such as Hotmail who offer e-mail accounts.

*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?*

I think there should be a tier system – for 1 to 50 spams, there should be a minimum of say $100. For every spam after 50, it should be a figure like $1 per spam.

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

I think that the code of practice should be a joint effort by the two sides with interest – the consumer and the direct marketing industry with possibly input from the Internet industry.

*Q17. What should the code of practice cover?*

The code of practice should cover technical control measures, operation of consent and opt-in procedures, auditing and use of a trust mark.

*Q18. Who should enforce the code of practice?*

If it is a code of practice implemented by the industry, then the industry should enforce it. However, having said that, the breach of the code, albeit a voluntary one, should be made a wrong under the legislation to add bite. It would be repugnant for a party to claim compliance under such a code when in fact, it was not the case.

Other comments:

We foresee that the spammers will be scrutinizing the legislation closely for loopholes to exploit. Some possible areas of weakness would be in the definitions adopted. Therefore, while we believe that the drafters will take every care to avoid this situation, the legislation should be available for continuing improvement.