

31 August 2004

IT and Telecommunication Policy Group
Resources and Network Branch
Ministry of Economic Development
P O Box 1473
Wellington

Dear Sirs

Information Systems Audit and Control Association (ISACA – Wellington) Incorporated is pleased to be able to offer its submission on the Spam discussion paper, published on the Ministry's website.

ISACA Wellington is a professional trade organisation supporting educational and promotional objectives for its 118 professional members. To prepare this submission, members' views have been canvassed, and the response incorporates written and verbal comments of the individual members, some of whom will submit individual feedback.

In general, views expressed by individuals were very consistent. ISACA's specific response is as follows:

1. Do you consider spam to be an important issue? Has it significantly affected you in any way?

YES, an important issue with nuisance value, costly and time wasting, and utilising resources procured for other purposes.

2. Do you think legislation has a role to play alongside other complementary measures?

YES, need to punish distributors to deter them.

3. Do you consider existing privacy protections in this area sufficient?

NO, email addresses used by spammers are in breach of item 12 in discussion paper. Email addresses are registered with ISPs for the purpose of receiving mail from known sources and replies and are not provided for receipt of 'mass mailing'. Spamming breaches point 22 bullet point 2. In this case we suggest that the legislation should allow for the Privacy Commissioner to act on any complaint sourced from more than one ISP, and if he decides it is in breach, would pass it to the commerce commission to prosecute. In this way the Privacy Commissioner who largely has the 'rules' but not the 'enforcement capability' can utilise existing law and the

Commerce Commission can act under the 'Fair Trading Act' or 'Anti Spamming Act' with 'privacy breaches' as supporting evidence.

4. Do you agree that stand-alone anti-spam legislation is preferable to reliance on the Harassment Act?

YES

5. What message mediums should be caught by the legislation (e.g. email, short message services using mobile phones, Internet instant messaging, faxes, telephones (telemarketing), physical mail delivery)?

All unsolicited mail, including all electronic forms of messaging, including facsimile, SMS, and hard copy mail.

6. Do the messages caught by the legislation have to be sent/conveyed to many recipients, and if so, how many?

No, just unsolicited marketing messages. If a limit of say at least 10 is set, the spammers will just set up programs to subtly change the message after every 9 'sends' so they will achieve the same result within the law. So it is not feasible to set limits without compensating controls and it is hard to see what those could be. If you had a compensating control of 'similar messages' this will just result in lawyers arguing about what 'similar' means for years on end. Conclusion is that limits will not work in practical terms. We suggest that you consider definitions of "bulk" messages in US legislation, where the intention to bulk communicate for commercial gain or profit is expressed. The definition of "bulk" should also include many times / one recipient scenarios.

7. Should the messages caught by the legislation be of a commercial advertising and promotional nature only or should other types of messages be caught? Should there be exceptions and if so what should be exempted?

At this time our view is that such messages would have a commercial motive, but we would encourage legislation that is flexible enough to be amended if non-commercial spam proves a problem.

8. Should the legislation extend to coverage of acts done overseas? If so, what acts should be covered?

It should cover all countries with existing policing or enforcement agreements with NZ.

9. Should all parties involved in the act of spamming, such as the vendor sponsoring the spamming, be covered by the legislation? Should there be express exceptions such as for telecommunications companies and ISPs?

Only the parties spamming, their sponsors, and any other party that actively aids and abets or gains financially from the act of doing so.

This would exclude ISPs and Teleco's provided they can demonstrate due diligence in their operations (no open relays or proxies).

10. Should New Zealand adopt an opt-in, double opt-in or opt-out approach in legislating against spam? Why?

The legislation can simply state that spam is an unsolicited message, and allow common law to decide when a message is solicited or not.

11. If an opt-in or double opt-in approach was to be adopted, what should amount to express consent and what actions and/or relationships should amount to inferred consent to the sending of a "commercial" electronic message?

See 10.

12. How should the scope of any opt-in or double opt-in assent be framed?

See 10.

13. Should there be a requirement for commercial electronic messages to accurately identify the sender of the message? If so, what constitutes accurate identification (e.g. name and physical address, name and email address)?

YES – but enforcing this will be problematic. Digital signatures could be used as a means of authentication.

14. Should there be a requirement for commercial electronic messages to include a statement to the effect that the recipient may use an electronic address set out in the message to send an unsubscribe message to the sender, and to ensure that such electronic address is functional?

YES – but enforcing this will be problematic.

15. Should there be a requirement that commercial electronic messages provide accurate header and subject information?

YES – but enforcing this will be problematic.

16. Should there be a requirement for the labelling of advertising or adult messages?

YES – but enforcing this will be problematic.

17. Should anti-spam legislation include rules against the supply, acquisition and use of address-harvesting software and harvested-address lists in connection with the unlawful sending of electronic messages?

The recognised global leader in IT governance, control and assurance

GST Registration Number 50-621-006

P O BOX 440, WELLINGTON, NEW ZEALAND

www.isaca-wellington.org

Supply and/or possession of the software, NO. Use of for illicit purposes defined in 5, YES.

18. Who should be able to bring an action against an alleged spammer?

Either Privacy Commissioner or Commerce Commission ultimately, but push back on ISPs to enforce through self-regulation.

19. What agency should have the enforcement role under the legislation?

Commerce Commission.

20. What should be the available penalties and remedies for breaches of anti-spam legislation and what should be the maximum fine or pecuniary penalty?

Scaling penalties, confiscation and destruction of all computer related equipment.

21. Should contraventions give rise to criminal or civil penalties?

Civil

22. Should the responsible enforcement agency be given the ability to obtain search warrants conferring powers of entry, search and seizure?

Yes, but warrant to be obtained with the same diligence and process as for existing offences.

Yours faithfully

Rupert Dodds

President

Information Systems Audit and Control Association (ISACA – Wellington) Chapter