

---

**From:**  
**Sent:** Friday, 21 May 2004 11:58 a.m.  
**To:** spamsubmissions@med.govt.nz  
**Subject:** Response to discussion paper

Dear Sir/Madam,

In response to your invitation to provide input into the SPAM issue, I submit the following:

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

Yes, and Yes.

Both in terms of cost, wasted time and adversely impacting resources procured by me for other purposes.

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

Yes.

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

No.

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)?

Any communication medium used with the intent of sending a message that was not solicited by the receiver AND by its receipt incurs cost to AND/OR by its repetition OR content cause inconvenience or loss to, the recipient - electronic or otherwise. All parties running double opt-in for electronic communication, or opt-out for physical communication are automatically exempt.

Telemarketing and direct mail are currently self limiting insofar as they cost the sender time/money, not the recipient and tend to only be of value to NZ Based companies. They could still qualify under the inconvenience clause of the proposed rule. If they were obligated to register through a central regulating body, then recipients who were inconvenienced could opt-out through the governing body and companies would be obliged to remove them from their contact database.

Television and Radio, the receiver is opting in to the service as provided.

SPAMers and Virus distributors would qualify under both parts of the rule. Innocent victims that inadvertently spread a virus would be exempt as they would NOT have prior intent.

This wouldnt cover "shotgun" leaflet marketing to a physical mail box unless there were also legislation for deliverers to honour a sign on the mailbox explicitly refusing bulk mail.

With the correct wording, non-commercial and not-for-profit entities like charities,

political messages, religious groups, local community news, interest groups etc would be unaffected unless the mail box rule above applies

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

Anyone having the intention to bulk communicate for commercial gain for profit AND/OR with the intent of causing inconvenience subject to the terms above. Definition of BULK would need further work/consultation. Personally, I would define bulk as 100+ The wording should be such that it should cover many times to one recipient as well as one time to many recipients.

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?

See above. I cant think of any SPAM that isnt commercial however, and most bulk marketing involves a commercial component or financial gain for profit.

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

See above. This would currently hit SPAM as I doubt it would be commercially viable to bulk market direct from abroad using other means. [Readers Digest excepted :)]

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 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?

Any party employing double opt-in for electronic communication, or opt-out for physical communication is exempt from the above.

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?

For email, opt-in with a digital signature or double opt-in without is the only feasible way of electronically giving express permission. The problem is making sure that a third party verifies a digital signature before inferring permission is given. Double opt-in is the only safe, practical way to go in the current environment.

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

See above. Public key infrastructure support for digital communication would permit greater flexibility with regard to authorisation and government support should be seriously considered (like in Germany). Double opt-in implies that recipient has requested and by confirming the query sent as challenge - given consent.

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)?

Digital signatures would help here, too, and would provide credibility. ~ But yes - senders need to be identified to be credible and accountable. Enforcing that is entirely another matter.

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?

Ideally yes, but this is totally unworkable, so impractical and unrealistic.

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

Yes provided they are not already captured by the actions in 5.

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

Yes provided they are not already captured by the actions in 5.

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?

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?

ISP's and Teleco's are best placed to gather metrics and judge severity. A designated government body should bring the action, and allow class action from other parties.

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

See above.

Police should only be involved if there are other criminal activities associated with the mail-out.

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?

Heavy, pro-rated fines in line with the magnitude of the breach (using the Aussie solution as a guide). Confiscation of all devices/equipment directly capable of contributing to the offence. (Note ISP's and Teleco's are explicitly exempt from this, unless active intent to contribute is proven.)

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 only on a per case basis with firm evidence provided for obtaining the warrant.

This should NOT be permissible on suspicion alone, nor provide 'blanket' powers.

Regards,  
Colin Templeman