
From:
Sent: Thursday, 17 June 2004 4:07 p.m.
To: spamsubmissions@med.govt.nz
Subject: Legislation against SPAM discussion

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

Yes, it has wasted a lot of my time having to determine what were SPAM e-mails and what was legitimate e-mails sent to me. The percentage of spam emails I received was 67%, and that was a machine infected with Sober.H started sending 80-120 German political SPAM e-mails a day to my Domain.

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

Yes, so far Internet Providers have failed to stem the flow of SPAM as it costs them effort/money and they aren't under any obligation to take any action. 3. Do you consider existing privacy protections in this area sufficient? Yes, except in the case of e-mail harvesters. 4. Do you agree that stand-alone anti-spam legislation is preferable to reliance on the Harassment Act?

Yes stand-alone anti-spam legislation is preferable. The Harassment Act as stated only covers actions that causes fear, and would not cover most common categories of SPAM.

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)?

Definitely email and instant messaging as there or too many mechanisms for a sender to mask their identity.

With both SMS, telephones and faxes the telephone service providers can trace the sender and take appropriate action. Although there has been at least one instance where Telecom abused its position by logging calls made to Vodafone cellular numbers made from landlines and provided these to a marketing company to try and sell Telecom Mobile services. Possibly the legislation around this area should concentrate on the responsibilities and limitations on the service providers, and they can then fulfill these responsibilities via their contracts with their clients.

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

It should either be sent/conveyed to multiple recipients, or to the same recipient multiple times to be considered SPAM. A good definition of SPAM can be found at <http://www.spamhaus.org/definition.html>

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?

It shouldn't just cover commercial advertising because as it can also be used to send political messages as demonstrated by the flood of German SPAM that occurred this month, and also has occurred years ago in newsgroups with a Turkish political message. I cannot think of an exemption, if a user has not subscribed to receive e-mails from that source, they shouldn't receive it.

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

It should cover any person or business which is in New Zealand while they commit the act of SPAMming, or has commissioned someone to SPAM on their behalf while they are in New Zealand. Defining where the act was actually committed would be too hard to define because of the international nature of the internet. Would a person in New Zealand who programmed a server located in another country to send SPAM have committed the Act in New Zealand, or where the server was located?

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? Yes, all parties should be covered in the legislation. ISP's and telecommunications companies should be covered in the legislation to have responsibilities and obligations. These responsibilities should include having clauses in their contracts with their clients that prohibit spamming, to monitor and detect SPAMming and a to terminate services to those that SPAM. 10. Should New Zealand adopt an opt-in, double opt-in or opt-out approach in legislating against spam? Why?

Double opt-in is the best approach. This protects the recipients from receiving messages from a source they did not request, and also protects the sender from having an e-mail address in their list that was not submitted by the owner of that address. There is a small chance that the ownership of e-mail address changes hands without the first user unsubscribing from a list so this should be considered in the legislation regarding lists. E-mails sent to mailing lists should always include clear instructions as to how to unsubscribe from the list.

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? The first message that gets sent to the user when a opt-in or subscribe request is received should describe in full what the list is for and what type of messages get sent to it, this same description should accompany any invitation (web site, printed matter etc.) to subscribe to a list. If the purpose of the list is amended or altered in any way, a new message should be sent detailing the changes and giving the recipients time to unsubscribe before the changes take effect. As per any other communications it should have instructions how to unsubscribe.

This first message also contains instructions to confirm their subscription, and specifies a period after which the subscription request expires. 12. How should the scope of any opt-in or double opt-in assent be framed? See answers above. 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. For e-mails as the very minimum, a correct return e-mail address. The name of the sender should not be misleading.

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.

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

Yes.

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

Yes. There should also be a requirement that the e-mail subject should not be misleading as to the contents of the e-mail.

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?

Yes, as that breaches privacy rights.

18. Who should be able to bring an action against an alleged spammer? In the first instance the provider of the service through which the SPAMmer initiated or carried out the SPAM. If more than one provider is involved, the one that has a business or contractual relationship with the SPAMmer. 19. What agency should have the enforcement role under the legislation? If the contents of the e-mail breaks any other laws, that has jurisdiction over that area. If it doesn't break any other laws, the provider of the service through which the SPAMming is being carried out or initiated. 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?

1) Termination of the services used to SPAM with

2 Pecuniary penalties based on the volume of SPAM sent, and costs incurred by other parties.

3) Publication of the offenders details so that other providers of the service can refuse to provide services to them.

21. Should contraventions give rise to criminal or civil penalties? Civil except where other laws were broken. 22. Should the responsible enforcement agency be given the ability to obtain

search warrants conferring powers of entry, search and seizure?

Only where the service provider is unwilling to pursue their legal obligations, or the contents of the e-mail breaks laws for which have the agency which deals with those has the powers to issue search warrants etc.

Colin Dijkgraaf