
From:
Sent: Monday, 28 June 2004 4:03 p.m.
To: spamsubmissions@med.govt.nz
Subject: Submission on Spam discussion document

Hi,

The following is a submission on the Legislating against Spam discussion document.

I have been a system administrator for about four years. In the past year the problem has grown from being a nuisance to quite a flood and spam protection is very important to be able to make any sense out of your inbox.

I am one of several administrators that look after the running of the mail servers for the Department of Statistics at The University of Auckland. Within the past few weeks the volume of spam has become so great that we are having to move our mail server to a higher spec'd server so that it can process all the email.

This email is not official policy at my employer. I speak in a personal capacity.

Onto the discussion questions ...

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

Spam is an important issue. I discard email addresses annually, causing some stress from my friends who haven't got the latest one. It has effected us by slowing down our mail server and forcing us to upgrade the hardware.

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

Legislation by itself is useless. There needs to be technological solutions, and also a change in the mindset of people so that sending spam is more disreputable than currently.

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

Yes. Principle 3 should cover it. However, people need to be able to track who is sharing their email address around.

I usually supply to companies an email address that includes a note of who had the address. Then when spam is received, I check the address, and can find out who leaked the address. So far three companies in the United States of America have given away my email, an employee at an Auckland company left the firm with a copy of the email database, and a friend who enjoys forwarding emails passed a message on to the wrong person.

Other than the employee in Auckland, there is no way the Privacy Act can stop these other people.

Also, the privacy provisions do not apply to publically available

information. The other two dozen email addresses that have received spam are publically available. I posted to a public mailing list with them, or put them on my website.

eg, <http://www.google.com/search?q=kimihia%40maxnet.co.nz>

The Act allows those email addresses to be shared around because they are public.

But, the Act also allows me access to my data and correction. Those companies are not allowing me to update my details. Due to the way that email lists get passed around, attempting to chase down my details and update them would be akin to closing stable doors now the horse has bolted.

Another area you may wish to consider is where a mailing list owner is careless with the addresses they have. Village Roadshow (www.roadshow.co.nz) have a monthly mailout. At the bottom is a link to update your details. By changing the number (in random leaps of about three - it's quite hit and miss) you can receive other people data, including names.

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

How different do messages have to be before they are counted as "bulk"?

Sometimes mail is done in a large shot and expanded by the receiving mail server. Other times each message is sent individually, with a different Message-ID header, and with slightly different content, eg, calling you personally in the title. Perhaps even the Message-ID is the same, and the content is different?

Are these messages the same?

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

As a lot of spam originates outside our borders, yes.

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

Single opt-in.

Receiving confirmation emails is a bit hit-and-miss. Often the recipient is too lazy to confirm. Some companies continually nag the user to confirm their address, and are very tight-lipped about how to get yourself off the list, even though you haven't confirmed the second time.

As a sender of automated single email, such as notification that your question in the online FAQ has been answered, having a double opt in would make the process so cumbersome it would negate any benefits.

However those messages are not of a commercial nature. They are informational.

Some sites may only have email access, so requesting a web or phone confirmation would be unsuitable. It shouldn't need to cross protocols to opt-in.

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?

They must have collected the information from you directly, at a minimum.

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)?

No.

Seedy commercial entities are like a hydra, with new heads replacing the old as they become blacklist. They are changing their names more frequently than I change my socks. Knowing their real business name is useless.

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. Their mail server must also work. IE, while they may have a functional email address, they may have, possibly intentional, "technical difficulties" that constantly defer any unsubscription requests.

Not only must the address be functional, requests to it must be enacted in a timely fashion. Under five days for an upper limit, as that is the standard time a mail message will remain in a delivery queue.

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

Yes.

In addition, they MUST include valid 'List-Unsubscribe' headers, as in RFC 2369.

Neufeld G. and J. Baer, "The Use of URLs as Meta-Syntax for Core Mail List Commands and their Transport through Message Header Fields", RFC 2369, July 1998.

<http://www.faqs.org/rfcs/rfc2369.html>

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?

This will be difficult to identify. Refer to comments on question 3.

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

The recipients of email, and the owners and administrators of servers that had to carry the email.

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

Only in more serious cases. If the spammers is willing to admit guilt and settle the case, then there should be no need for a warrant. What does a warrant offer that a subpoena doesn't?

That concludes my comments. Thank you for the opportunity.

You may publish my name and employer, but please do not publish my email address.

Thank you.

--