

Submission on SPAM:

By Lyn Hoben

Date: 29/6/2004

To:
IT and Telecommunications Policy Group
Resources and Network Branch
Ministry of Economic Development
PO Box 1473
Wellington

Email to:
Spamsubmissions@med.govt.nz

NB this is a personal submission, NOT related to Auckland City Council

In summary:

Should be email only

NZ should adopt a volume-based, complaint-based system.

If, say, 5 or more individuals complain about a specific email, their ISP will be asked to count the number of identical emails in a 48hr period around the receipt time. If more than 1000 total are counted, and the source is not exempt, this will be prima facie evidence of spamming.

An ISP would also be able to initiate this count.

It should be possible to aggregate counts over more than one ISP, for a total of, say, 10 complaints and 2000 instances.

Responding to the specific questions:

Background

Do you consider spam to be an important issue?

I personally find web popups more disruptive - it is comparatively easy to delete unwanted emails. I accept that overall, in terms of time wasting and overloading networks, spam is a real problem.

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

Yes

Existing Legal Framework

Do you consider existing privacy protections in this area sufficient?

Yes - I think an email address is no more 'private' than a street address.

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

Yes

Legislative Issues

What message mediums should be caught by the legislation (eg email, SMS over mobile phones, internet instant messaging, faxes, telephone, physical mail delivery)?

Only those where the infringement (particularly the volume) can be detected by infrastructure providers.

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

Yes - I think the volume is the distinguishing feature of the offence - it is only because of the statistical chance of commercial return on a large number of messages sent that this activity exists, and it is the unwanted costs caused by the volume of messages over a network that make this a real problem - I doubt that legislation would be considered just to sooth the feelings of offended recipients.

In my opinion, the volume should be quite high, as I think the real offenders are the very high volume statistical marketers. The aggregate NZ total over all ISPs (for email) should be in the 1000s - at least 1000.

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

Ideally the criteria should be the level of offence caused (ie a number of complaints) and the volume, not specifically the content. In practice, because the exceptions are likely to be government, local government, political parties and possibly church groups, the only actionable messages will probably be commercial.

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

Yes, because most of the objectionable material originates overseas. We are legislating largely to prevent NZ being used as a staging post or originator, and to give us the moral right to demand other countries clean up their act.

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 who benefit from spamming should be covered, just as those who suffer from spamming, particularly ISPs, should not be held liable.

Consent Issue

Should NZ adopt an opt-in, double opt-in or opt-out approach on legislating against spam? Why?

I would prefer to avoid any opting approach, concentrating rather on minimising commercial spam by defining the offence in terms of the volume and level of complaint. If opting proves to be a necessary component, I prefer Opt-out - much simpler, the ramifications of double opt-in would probably make any email almost legally impossible. The implications are ridiculous - it is more intrusive to confront someone and ask them personally for permission to email them, than just to email them in the first place.

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?

Do not adopt either Opt-in approach! Any approach which could make it illegal to email someone who has given you their card is just over the top. At least with Opt-out, it would be clear if a complainant had opted-out in the past (I guess commercial emailers would be required to make their opt-out database available to investigators?)

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

Out-out - just click an email link - initiator to maintain functioning database (as discussed in the paper).

Transparency

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

Yes - name, email and physical address. It is important to allow legitimate initiators to send bulk email - this requirement would apply to government and other exceptions to spam definitions.

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 an electronic address is functional?

Yes

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

Yes

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

If it is possible to get agreement on the format/spelling at international level - no point defining it just in NZ.

Address Harvesting

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

Enforcement

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

ISPs and telcos, possibly in conjunction with offended individuals. I would envisage the action being initiated by an ISP in most cases - the legislation could require individuals to complain (by email) to their ISP, who would be required to run a count on the number of instances if there were more than (say) 5 complaints - if a stated number was exceeded, that would constitute a prima facie case. There should also be the possibility of aggregating complaints and numbers across more than one ISP. The ISP would be able to initiate the action by asking their customers if they wished to complain!

What agency should have the enforcement role under the legislation?

Commerce Commission

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

Worst offenders are overseas, so out of reach of our legislation. Best to follow other comparable countries penalties?

Should contraventions give rise to criminal or civil penalties?

Civil, because of lower standard of proof. But if civil penalties cannot be enforced overseas, then perhaps criminal penalties may be necessary?

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

Should not be necessary if the offence is defined by the content and volume at the ISP end.