

---

**From:**  
**Sent:** Wednesday, 30 June 2004 11:53 p.m.  
**To:** spamsubmissions@med.govt.nz  
**Subject:** Submission to discuss legislating against spam

I have read the submission by InternetNZ and on the whole agree with it. I was also present at the workshop in Wellington on June 24, 2004. While I do agree and support the submission by InternetNZ, I am putting together a submission at the last minute to show my support for such a legislation. I will only continue to be supportive if the legislation is well written and not too watered down that it will be ineffective.

We do not need useless legislation, just to pay lip service to the problem. We need something effective that will contribute positively to the fight against spam without making innocent people's lives difficult.

Due to the lack of time, I have skipped some questions or covered them very briefly. This is not because they are not important but because I lack the time. I also apologise for the typos and grammatical errors. There are probably a few weird or unfinished sentences. This was all written without the benefit of spellchecking or proofreading.

If allowed to, I can proof read it and spell check it this weekend. Email me if you want it cleaned up. Cleanup only means correcting grammar and spelling. If there are unfinished sentences, I'll let you know how they would end and leave it to you to work out if you can include them or not

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

Yes. Spam is an important issue. Electronic communication via technology such as email or sms is extremely useful. It has fundamentally changed the way people interact or communicate with others. Unfortunately the pollution caused by spam will make it unusable or too irritating to be used. Once the signal-to-noise ratio gets too low people will stop using it. This means there is a likelihood that the spam will be more than useful email and people will be put off by email and stop using it. An analogy would be the CB radio.

To reduce the amount of spam I receive, the way I use email has changed from before. I have had to disguise my email addresses when posting to public forums. This means people who wish to reply to me personally will have to take the effort to work out my email address to email me.

I have also had to go to the trouble of having two email addresses. One I use for posting in public forums that do not allow munged addresses and another for private email. This means anyone replying to the former, thinking they will get to me will only get a reply when I occasionally clear out the spam email inbox.

In this article on sms spamming (written in 2003), it states that two thirds of mobile customers receive spam. [http://news.com.com/2100-1041\\_3-1015595.html](http://news.com.com/2100-1041_3-1015595.html)

2: Do you think legislation has a role to play alongside other complementary measures? Yes. I don't believe that legislation alone will stop spam. However that together with other measures will ensure that the amount of spam is reduced.

While most spam comes from overseas, the right legislation (and it is important to get it right) will ensure that NZ is not seen as a haven for spammers or a willing conduit to the distribution of spam.

If the appropriate clauses are included, having a spam legislation will enable NZ to assist in the international effort to reduce spam.

3: Do you consider existing privacy protections in this area sufficient? No.

4. Do you believe that stand-alone anti-spam legislation is preferable to reliance on the Harassment Act? Yes. If interpreted correctly, spamming is not harassment using the definitions in the Harassment Act. The Anti-spam legislation should be more than protection from harassment.

If there are any legal measures in NZ sufficient to stop spam, the spammers in NZ or people who are currently part of the spam industry in NZ would have been facing legal proceedings by now.

For example in March last year, NZ Herald technology wrote about this person in Mt Eden who has profitted from the spam industry. As far as I know he has still not been convicted from his various activities. <http://www.nzherald.co.nz/storydisplay.cfm?storyID=3251095>

In another more recent example, there's so far no news that Mr Shane Atkinson has been brought before a NZ court of law for breaches to any current NZ law  
<http://www.nzherald.co.nz/storydisplay.cfm?storyID=3518682>  
<http://www.nzherald.co.nz/storydisplay.cfm?storyID=3518097>

We are still waiting to hear if NZ authorities are able to assist in the FTC who are going after Lance Atkinson (brother of Shane Atkinson)  
<http://www.nzherald.co.nz/business/businessstorydisplay.cfm?storyID=3564274>

5: What message mediums should be caught by the legislation? All electronic media should be included. Fax, email, sms, instant messaging. Also the legislation should not be limited to method of transmission or receipt. Just that it is an electronic media that should be covered.

At this day and age, with unified messaging systems, it is quite possible an email sent from my computer can be received as an sms message or a fax. Similarly a sms message can be sent from a cellphone to be delivered to my email address or even a mailing list. A fax message can be delivered to email inboxes or even cellphones.

Instant messaging like ICQ, Yahoo Messaging, Jabber etc are spammed a lot. Fortunately they have developed ways where we can block instant messages that are advertising but only after we get the messages or block it such that we can't be messaged apart from those who we know. This blocks any spontaneous connections. For example if I were looking for an old friend and found someone by that name who is an ICQ user, I may possibly not be able to send an ICQ instant message to that person if they have their ICQ client set up to only accept messages of the people in their contact list.

6: Do the messages caught by the legislation have to be sent/conveyed to many recipients, and if so, how many? I don't think any limits should be set. The only reason heaps can be sent is because they can do it. If you legislate it with a limit, they will just set up ways to work around the loophole.

eg if you set a limit of at least 10,000, they will just send each spam to 9999 recipients to be below it. How would you differentiate someone sending a message to 10 x 9999 recipients from someone who sends it to 100 recipients?

Furthermore how would you know specifically how many emails were sent? What constitutes identical emails? For example in a distributed system, each zombie can be used to send 200 emails, and if you have 10000 zombies, it is the same as have one machine sending 2000000 emails. In fact it is even better because it is easier to shut down one machine than to try shut down 10000 machines.

The fact is is spam is down to the definition of what consitutes spam and this shouldn't be limited to how many were sent.

7: Should the messages caught by the legislation be of a commercial/promotional nature only, or should other types of message be caught? Yes all types of messages should be caught.

7b: Should there be exceptions, and if so, what should be exempted? There should be no exceptions. There was discussion at the workshop as to whether exceptions should be given to charities and political parties. Someone even said, if those qualify then extend it to anything that isn't commercial like sporting groups, religious groups, schools and Universities (some of the former are already charities).

By writing in exceptions, you are signaling that it is ok for those groups within the exceptions to spam.

Charities, religious organisation , political parties, sporting groups and the like may then be able to use spam. While they are not commercial organisations, they usually seek to raise funds or promote their cause. Many churches now expect their members to contribute to their funds. Most religious groups either seek to promote their cause, convert more followers and in turn are able to raise funds or "soldiers" for their cause.

Many charitable organisations hire professional fundraisers to raise their funds and only a percentage of the fee goes towards the charity. The rest goes towards the cost of fundraising, including the pockets of the fundraisers.

Does an email inviting to a sponsored event for a charity constitute as advertising for the sponsor too? "We would like to invite you to the WorldBrandHere's school fair for XYZ Primary School". So WorldBrandHere gets their advert in the email spam out inviting all and sundry to the school fair.

What is to stop a big company in NZ from signing up 500 of their employees as members for a political organisation for a 10c fee and use their ability to a. Advertise their logo on every electoral ballot b. Send spam to all and sundry because they are allowed to as

they are a political party (and political parties were granted an exemption in the act).  
c. Able to put up billboards for free (the ones you advertise your candidates in each electorate, each board has a logo etc) and so on...

Rather than come up with scenarios, there have been more recent examples. For example the German spam is politically rather than commercially driven. The Italian Premier Berlusconi sent out sms to persuade people to vote. Unfortunately it backfired. He was very unpopular for it. However in this country where political parties can require broadcast time allocated to them during a political campaign, there is nothing stopping them from requiring sms broadcast ability during such campaigns too. The Italian govt legislated to allow sms broadcast "'in cases of disaster or natural calamities' and 'for reasons of public order or public health and hygiene' but this is the first time it was used to remind people to vote." <http://www.cellular-news.com/story/11291.shtml>

By writing the exemption, it also means ISPs will not be able to stop their customers who are charities or political parties/politicians for breach of Acceptable use policies or terms and conditions. After all the terms and conditions or AUP should be legal and if it is legal for that group to spam, there is nothing the ISP can do to stop them.

So having done that, you will end up reviewing the legislation in a review and closing the loophole. In my opinion it is best to do it right in the first place.

Having said all of that, I do not want someone charged for spamming simply because they put out a feeler or reached out to someone. ie such emails are unsolicited by nature and possibly for their commercial benefit. It is different to write something unique than to send a form/template or identical message to a few people that is unsolicited and in bulk.

The task you have isn't easy.

8: Should the legislation extend to coverage of acts done overseas? Most definitely. It is very easy to send emails from a machine overseas even when I am here in NZ. It is also possible for someone overseas to have spam sent from NZ to either other NZers or people overseas.

9: Should all parties involved in the act of spamming, such as the vendor sponsoring the spamming, be covered by the legislation?

Yes but only if they knew it was being done Or could have known. What would you do to a parent who sends out an email to his colleagues using his work email list asking them to see him if they wish to buy some girl guide cookies? Is the parent spamming? Is the girl guide association spamming? Is the association responsible for the parent's actions?

9b: Should there be express exceptions, such as for Telecommunications Companies and ISPs? Yes if they aren't spam friendly but have taken all efforts to ensure their customers know spam isn't condoned.

10: Should New Zealand adopt an opt-in, double opt-in or opt-out approach in legislating against spam? NZ should adopt opt-in or double opt-in While the best is have double opt-in, it will be hard to legislate it. Perhaps mention that ideally or best practice should be double opt-in with the minimum being opt-in

The benefit is for the spammer (or marketer). opt-in means I am allowing them to spam me. Opt out is too easy for spammers to get away with spamming. They can only spam me if I give them permission to do so (using opt-in)

Also legislating against opt-out will go against any sensible user education where people

are told not to reply to spam.

16: Should there be a requirement for the labeling of advertising or adult messages? Not really if you have opt-in. Spam by definition is advertising. There are many ways to evade the labelling and there is no foolproof method. That is why antis spam tools are only effective if they continue to evolve. It is a race between the prevention tool and the spamming toll. The spammers can as easily evade prevention tools as they can labelling. SO the only thing this will achieve is control the spam of the "good" spammers.

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 most definitely. People can be paid to harvest email address, mobile phone numbers, and instant messaging identities. Having the addresses enables the spammers to send the emails somewhere.

18: Who should be able to bring an action against the spammer? While it is nice that anyone can bring action (ie be they private citizen or an organisation), I believe in reality only the approved governmental organisation should be able to.

The problem here is that the governmental organisation should be properly resourced and limits set on prosecution should not be due to trying to reduce workload. Otherwise the fight against spam would be lost.

For example currently the problem with false accounts at ISPs are ignored by the police because the loss is too low or not enough to be worth their while. Fraud must be financially big enough to be worth them looking into it.

The only way to keep on this is to ensure everything is taken seriously.

The problem with private citizens bringing action is they may not have the resources (unless they are rich enough) to pursue this. For example to track it down to the right person, they would need to be able to serve papers on each organisation from the ISP to the phone company to track down the person. Not only will this come with legal cost but there could possibly be a search fee imposed. Any ISP or telco is unlikely to volunteer the information due to privacy considerations unless legally required to do so.

The other problem is the use of such powers to harrass people.

19: What agency should have the enforcement role under the legislation? There is no one agency and so perhaps a team set up of various agencies or people who have expertise within each agency be used to enforce this legislation.

22: Should the responsible enforcement agency be given the ability to obtain search warrants conferring powers of entry, search and seizure? Yes except for where it will harm an innocent third party or thirdparty who isn't aware of what is happening. For example if a spammer is spamming from an ISP and the ISP doesn't know or abide by it (ie not spam friendly), confiscating the ISP equipment is causing more harm. As long as the ISP cooperates and produces the information required by the warrant/legal piece of paper, they should not be penalised for it.

Other matters:

a. Spam economy

Please be aware that there are now evidence that shows hackers or virus writers have links to spammers. Also there are some who believe that there are links to terrorists or organised crime. Whatever you believe, there is an economy behind this. Price of zombies [http://www.theregister.co.uk/2004/05/12/phatbot\\_zombie\\_trade/](http://www.theregister.co.uk/2004/05/12/phatbot_zombie_trade/)

Look at what this person in NZ pays and is paid for the spamming he does or activities to support the spam industry (eg address harvesting and cleaning).  
<http://www.nzherald.co.nz/storydisplay.cfm?storyID=3251095>

The story below is titled "Spammer tells all: the Underground Spam Economy"  
<http://rejo.zenger.nl/abuse/1085493870.php>

b. Costs

I think care should be taken that costs to comply with any legislation should not be too high or unreasonable for a small business. A small ISP's ability to shoulder costs of new equipment is vastly different from that of a big ISP like TelstraClear and Telecom. It would be a shame if any unreasonable expectations lead to more consolidation or less competition within the industry.

Small ISPs raising fees for their subscribers because the cost of implementation is spread over small number of subscribers could mean losing customers. Or possibly selling the business to bigger ISPs because they are unable to economically run their business.