

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

### **Anti-spam legislation**

Dear Sir,

As I receive hundreds of spams a day, I've a vested interest in this issue. Spam has been so annoying to me that I've created an Open Source anti-spam tool (<http://www.berenddeboer.net/emc/>).

The following issues are, in my opinion, the most important for this legislation:

1. Making it clear under what circumstances companies can legitimately send commercial email.
2. Giving the legal boundaries for spam fighters. I prefer no government boundaries here. ISP's should be able to specify any boundaries in their contract with their customers.

I don't see anti-spam legislation helping a lot against spam. Spammers don't earn that much money and the amount of time spend in tracking down spammers will most of the time not be recovered.

In my submission I've just answered the questions as they cover all the issues. My compliments to the writers of this discussion paper for the comprehensive treatment of this issue.

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

I consider it so significant that it will be the end email if it is not stopped.

It has cost me significant time. As I was not satisfied with existing anti-spam products, I even wrote my own anti-spam tool.

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

I do, but only as deterrent for people who obey the law. Prosecution costs are high however, and spammers don't make that much money that significant fines can be asked. The possibility of imprisonment must therefore be an essential part of the legislation.

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

No idea.

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)?*

All delivery methods where a significant part of the delivery costs is borne by the recipient.

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

I think this is irrelevant. Is a message the same of one word is different? Is the sender different if it comes from a different computer? The issue is the delivery cost: next to nothing.

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?*

No exceptions.

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

If it can be prosecuted in NZ, it should be covered. If that cannot be done, it's useless to put it in the law.

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?*

No. Only the originators of the message should be covered.

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

Opt-in. Because opt-out cannot work:

- a. Opt-out works only per email address, not per person: People new to email might have just one email address, but people who use it a lot, have many. Spammers spam all those email addresses. I have at least 10 different email

addresses. A day just doesn't have enough hours to opting-out for all spam I get for all 10 email addresses I use.

- b. An email address can be more appropriately seen as a role. People might have email addresses as secretary@company.com or info@organisation.org or sales@business.co.nz. All for the same person. But as soon as the role is transferred to another person, the email address is transferred as well. Email addresses can be bound to a person, but not necessarily so, and certainly not in businesses and organisations.
  - c. Domains can have a catch-all email address. A catch-all email address means that any email sent to that domain is forwarded to a single person. As the number of possible email addresses for a domain is unlimited, it is impossible to unsubscribe them all.
  - d. Spammers could simply start a new business and people have to opt-out all again.
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?*

Consent can only be given if:

- a. The email address was given with a series of other clues that without doubt establish the identity of the person (for example credit card details were also supplied).
- b. If only an email address is asked, the company must send an email to that email address and ask for consent. Consent is then expressed as a reply or visiting a particular non-guessable URL or specifying a non-guessable password.

Else anyone can just supply the email from someone else to a company. Basically consent should be how mailing lists currently work as they face the same problem.

Getting opted-in should be hard, not easy.

12. *How should the scope of any opt-in or double opt-in consent be framed? This is perhaps best left to the individual company. The law should provide for suing in case the given consent is breached.*
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)?*

A physical address, can be a PO Box address. That makes it much easier to track down the actual senders. And it serves as a deterrent.

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?*

Every commercial email should contain unsubscribe information at the bottom of the email. Could be an unsubscribe, but can also be a website. Opting-out must be easy.

Note that if a subscriber unsubscribes from all mailing lists from a company, its email address *should be deleted*. This to prevent misuse or the (inadvertent) selling of that email address. This is optional, but should be best practise.

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?*

Every commercial email should also be properly tagged. Either by a field in the header or by a prefix in the subject.

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?*

No. It doesn't really matter if someone has 1 million email addresses if they are never used.

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

Anyone who is spammed. But as spam is so widespread, it is up to the person bringing the allegation to the police to give the physical address of the spammer. Just an email won't do. The police will be swamped. But if the spammed person has a physical address, the police can take action with reasonable success.

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

The police.

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?*

It should include imprisonment as I don't expect spammers to make a great deal of money. They make some, not a lot.

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.