

---

**From:**  
**Sent:** Wednesday, 7 July 2004 5:34 p.m.  
**To:** spamsubmissions@med.govt.nz  
**Subject:** Submission from the E-Government Unit on MED's Discussion Paper: Legislating against Spam.

This message is a submission from the E-Government Unit, State Services Commission on MED's Discussion Paper: Legislating against Spam.

General Comment

EGU, like MED, recognises that merely making spam unlawful is unlikely to stop it. However, EGU believes that it is a necessary part of a wider group of measures including education, technical measures, enforcement, and international co-operation, which together may reduce the size of the problem.

Furthermore, the current trend toward technical measures risks rendering email far less useful as a tool since it reduces the confidence that 'innocent' email will actually be delivered. Other policies which have been suggested by large companies could restrain Internet growth and innovation by raising artificial barriers to sending email in an attempt to control spam.

Since the passing of the Australian legislation, industry surveys have shown a jump in spam apparently sent from New Zealand. EGU therefore believes that legislation such as that proposed in the paper is necessary and urgent, but that it needs to be accompanied with an enforcement regime which has the authority and resources to investigate and prosecute.

Q1 - Do you consider Spam to be an important issue? Has it significantly affected you in any way?

Yes.

- Spam threatens the usefulness of email, and public confidence in email. Consequently spam threatens the e-government programme and the investments the government is making in it.
- The volume of spam is stressing the Internet infrastructure, particularly ISP mail servers and bandwidth. Some of the measures taken by spammers to evade detection (particularly the use of worms to compromise home PCs) also causes damage to the Internet and inconvenience to its users.
- While most government departments have effective spam filters, the sheer volume is clogging gateways and mail servers in government and so causing delays in email between departments. Q2 - Do you think legislation has a role to play alongside other complementary measures?

Spammers appear to believe that what they are doing is perfectly reasonable, or at least a valid marketing model. Legislation will change this.

Spam is a global problem. Almost all the countries we compare ourselves with have introduced spam legislation or are moving to do so. New Zealand will be seen as a haven for spam if we do not. Eventually, Internet providers may start simply refusing to accept messages from countries with inadequate legal protections. Q3 - Do you consider existing legal protections in this area sufficient? No. Existing legislation has proved inadequate to deal with spammers in New Zealand Q4 - Do you believe that stand-alone anti-spam legislation is preferable to reliance on the Harrassment Act? Yes. The Harrassment Act is intended to deal with ongoing harassment of one individual by another with the intent of annoying or threatening them. Spam is completely different, it is a series of one-off messages sent to a huge group of unknown individuals. The annoyance is an unintended by-product of the volume and content. Also see comment on Q3 above. Q5 - What mediums should be caught by the legislation? The main reason spam is prevalent on email and not so much on other mediums (in New Zealand anyway) is that email is free to

send, whereas other mediums are not. Usenet (which is also free to the sender) is also riddled with spam. The law should be technically neutral as far as possible. The Australian approach of 'electronic messages' seems appropriate. Other issues such as telemarketing and direct marketing by mail should be the subject of a separate debate, not rolled into this legislation. Q6 - Should the messages caught by the legislation be of a commercial / promotional nature only, or should other types of message be caught? "Promotional" would need a broad definition. In a recent example, there has been a German language racist tract widely distributed by spam before a European election, which illustrates the point that not all unwelcome messages are commercial. Q7 - Do the messages caught by the legislation have to be sent/conveyed to many recipients, and if so, how many? This would appear a better test than the content of the message. However, Australia considered this approach and decided that the burden of proof would be too great. In EGU's view, a "bulk" test should be employed, but only if MED believes that this would not pose an impossible barrier for prosecutions. Q7b - Should there be exemptions, and if so, what should be exempted No. Exemptions would weaken the law. They would also be seen as special pleading by any group seeking one. Q8 - Should the legislation extend to cover acts done overseas? Yes. The Internet is a global medium, other NZ legislation does this, so does the Australian spam law. Q9 - Should all parties involved in the act of spamming, such as the vendor sponsoring the spamming, be covered by the legislation? The vendor and the spammer should both be covered. Q9b - Should there be express exemptions, such as for Telecommunications Companies and ISPs? ISPs should be made liable if mail servers they own or host (including their direct customers) are passing on spam in bulk, for the reason above. This could be contracted out of by advising the customers that they will be cut off if they start spamming.

Neither ISPs nor telcos should be liable for spam transiting through their networks or being delivered.

Q10 - Should New Zealand adopt an opt-in, double opt-in or opt-out approach in legislating against spam? Opt-in. Opt-out is too open to abuse. It places the onus on each individual of unsubscribing themselves from each company mailing list - even of these requests were honoured, which is highly unlikely, this represents a large amount of wasted time and more waste of email bandwidth. Opt out also cuts across the advice that people are given of 'never reply to spam'.

Double opt-in also greatly increases network traffic without adding much security.

Q11 - In an opt-in environment, what should amount to express consent, and what actions and/or relationships should amount to inferred consent to the sending of an electronic message? The key should be the context in which an email address is supplied. Providing an email address e.g. on a website or a business card should be consent to send messages related to the business expressed on the website or business card, but not for something totally unrelated.

Where customers are required to provide an email address to as part of a transaction, e.g. on a paper or web form, this address should not be available to the supplier except in connection with the transaction at hand, or for potential future similar transactions. It should not be available for selling different products or passing on to third parties.

Q12 - How should the scope of any opt-in assent be framed?

The Privacy Act sets out that information may only be used for the purpose for which it is collected. Opt-in assent needs to make it clear what purpose is in mind. It should not be acceptable for people to have to agree to their email address being used for unrelated purposes or being passed to third parties as a condition of doing business; also it should be easy and obvious for people to determine what they are agreeing to when supplying their address.

Q13 - Should there be a requirement for commercial electronic messages to accurately identify the sender of the message? If so, what constitutes accurate identification? All messages (regardless of intent) should contain a valid reply address and either the real human name of the sender or a verifiable and accurate company name.

Q14 - Should there be a requirement for commercial electronic messages to include a statement to the effect that the recipient may sue an electronic address set out in the message to send an "unsubscribe" message to the sender, and to ensure that such

electronic addresses be functional? Yes. Furthermore, this should be the "reply to" address of the email. This is exactly what "reply to" addresses are for. This requirement would also have the following benefits:

- It would be simple in concept and execution - anyone can just hit reply and say "unsubscribe".
- Clicking a link in mail is high-risk behaviour, which should not be encouraged or required. For instance, a website could exploit a weakness in the user's browser to take over their computer.
- Any reply which bounced would (as well being unlawful under the terms of this legislation) alert the user to the probable status of the sender.

Q15 - Should there be a requirement that commercial electronic messages accurate header and subject information? Header information would be difficult to define legally, and is not all under the control of the sender. Rather, it should be an offence to deliberately falsify or mislead about the sender or subject matter of the email.

Q16 - Should there be a requirement for labelling of advertising or adult messages? Labelling advertising as such should unnecessary. There may be a case for labelling adult messages. However, labelling regimes are subject to a problem which is that there are many ways to label which appear the same, e.g. Adlt, Adult, A dult etc.

Q17 - 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? It should not include rules about the software per se, since it is easy to promote software as one thing and use it for another. It would be very straightforward to modify a simple web spider to harvest addresses. Intent is the key. There should be a rule against supply etc of such software with intent to generate lists of addresses for electronic mailing.

Email lists should not be traded or passed around. This would be against the Privacy Act already, but there may be value in adding it to the anti-spam legislation.

Q18 - Who should be able to bring an action against a spammer? The Crown. It is necessary to preserve a balance between enforcing against the bulk of spam (pun intended) and retaining the use of email as a useful tool of business, government and individuals. If individuals were permitted to bring action there is a risk of vexatious lawsuits. There should be a mechanism for public complaints about specific instances of spam so the Crown can consider action.

Q19 - What agency should have the enforcement role under the legislation? The responsible agency should have:

- Technical investigative expertise
- Operational links to technical investigative agencies overseas
- An operational focus, but not one so broad as to distract it from spam.
- Experience in the exercise of powers of search and seizure.

Q20 - What should be the available penalties and remedies for breaches of anti-spam legislation, and what should be the maximum fine or pecuniary penalty? Spam can be profitable so penalties need to reflect this or the legislation will be seen as another cost of doing business. Penalties should escalate for second offences.

The Australian legislation allows the seizure of the profits of spam. While this is yet to be tested in court it seems an excellent idea.

Q21 - Should contraventions give rise to civil or criminal penalties? No comment. Q22 - Should the responsible agency be given the ability to obtain search warrants conferring powers of entry, search and seizure? Yes, it will be very difficult to prove without this.