



PO Box 9361 Hamilton
www.wlug.org.nz

On behalf of the Waikato Linux Users Group Incorporated (WLUG), we wish to put forward this submission in response to the request for feedback found at <http://www.med.govt.nz/pbt/infotech/spam/>.

We are a group of concerned individuals, who try to provide help and support for the local users of the Linux operating system. We are a very technical group of users, who have a great depth of knowledge and experience with not only using the Internet, but running services on it. We are also a very atypical group of users, who have the knowledge, and ability to use technology against spam, and many of us run very sophisticated filters incorporating technology such as machine learning. We try and make this technology available to as many people as we can. However, there are large groups of people who are not able to benefit from such technology, and as such they are having to deal with spam the best they can. Current research is showing some promising results at stopping spam, however it will most likely be at least a few years before these systems can be widely agreed upon by the Internet community and deployed.

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

Spam affects us in many ways. Many of us are system administrators and have to deal with spam on our servers. One company reports that they handle over 100,000 emails a day, of which 2.5% are legitimate, 51.5% are spam, and the remaining 46% are email viruses. This requires a significant additional spending on provisioning extra resources to deal with the unwanted email, as well as time by the system administrators to maintain the system that is now complicated by anti-spam and anti-virus software.

Another biotechnology company in New Zealand recently discovered that spam for Viagra was being sent with forged From: addresses appearing to come from their domain without their knowledge or their consent. Some of the products they advertise on their domain are closely related to Viagra. They were very concerned that their customers may receive this spam and that they would be associated with spamming, which would ruin their reputation both nationally and internationally.

Other members of the Waikato Linux Users Group (WLUG) have had to deal with receiving dozens of spam messages each day which they have to read through, and many members are

stopping their children from getting email accounts because they are concerned that they will end up with pornographic spam.

Members of WLUG have had to deal with people overseas who are banning mail from the Asia/Pacific region in general (including New Zealand) because of the bad reputation that this region has for spamming.

Spam is something which regularly uses up our time and resources. It renders a great new communications medium nearly useless. Spam is a big problem.

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

Members of WLUG believe that other laws should be able to target a large portion of spam. We believe that much of the spam we receive is already illegal in New Zealand. For example, since most spam is currently sent from compromised personal computers where the owner is unaware that the spammer is running programs on it, we believe that this would be considered computer trespass under the Crimes Act. Sending mail with misleading subjects and with other forged headers sounds like it would be covered under legislation targeting fraud. Advertising pills and medicines is already covered under existing legislation. Similarly, pornographic texts and images are covered under current laws. If these laws can not be adequately enforced when it comes to electronic media, then we believe that new laws will not change that.

Extending the coverage of current laws to cover spam also helps clarify the current laws' stance when it comes to other abuses of electronic, but perhaps non-email resources, such as SMS text messaging, or instant messaging.

However, there is also room for laws covering the other areas of spam that do not currently infringe, such as the harvesting of addresses, and the sponsoring of spammers.

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

As stated in paragraph 25 it is possible to trade email addresses that are considered to be publicly available. This is causing people to actively conceal their contact information on the Internet, thus destroying one of its most important uses, which is as a communications medium. People should be able to expect that email addresses that are publicly published individually are not collated into a large database to be used for spamming.

The Privacy Act already specifies that people must be informed about information that is collected about them, and given the opportunity to correct out-of-date or wrong data about them.

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

The Harassment Act does not seem to be applicable, as spam is irritating even if it is a single occurrence. People may be tempted to send a single email a year to everyone they can which would still cause the problem (email boxes being filled with irrelevant information) even though it does not meet the legal requirements for harassment under the act. The harassment is not necessarily in one person doing it, it is in everyone doing it.

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)?

Spam is not limited to email; however email is one of the few forms of communication where the cost of the message is borne by the recipient instead of the sender. Spam originated on Usenet, and moved into email, which shows that there are at least two different systems that have been plagued by this problem. Many other new communications technologies are starting to show similar characteristics, such as instant messaging. Restricting new laws to only cover email would be short-sighted.

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

This has raised a large amount of debate within our community. Many people believe that what makes spam a problem is the unsolicited nature of the email messages, while an opposing group believe that it is the bulk nature of spam which means that they receive the unsolicited email. Limiting the number of unsolicited recipients to some communication to no more than one hundred seems to be a reasonable compromise to both parties that would still serve the requirement of preventing large amounts of unsolicited email arriving in people's mailbox.

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?

It is not the content of the messages which is the problem. It is the number of them which arrive each day which cause issues. Allowing exceptions for certain senders or content would be counter-productive to this cause.

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

We strongly believe that it should cover acts done overseas. The Internet is a global communications medium, and no matter where in the world people are spamming, it causes problems for people in New Zealand. There are large numbers of people that are involved in spamming, ranging from people who harvest the email addresses, to people that hire the spammers, through to the people who host the spammers' websites and the compromised machines that they use. We believe that all of these people should be covered by this act.

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?

All parties involved in the act of spamming should be covered. ISPs and telecommunications companies are in technologically superior positions to spam and should not be exempt from these laws. ISPs should be required to act upon abuse complaints in a timely manner to remove abusive customers from their networks.

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

Unfortunately, spammers have fraudulently used opt-out systems in the past to collect lists of addresses to spam, and as such they are no longer trusted to be safe. Even if spammers were to use opt-out systems legitimately, people would not make use of them because of their fear of attracting even more spam.

Opt-in has issues with people accidentally subscribing themselves, or maliciously subscribing others. When combined with the above phobias people have of opt-out systems this

solution is not workable either. Once again spammers have claimed (fraudulently) that people have subscribed to opt-in lists, when people disagree.

Double opt-in seems to be the only workable solution, and has had tremendous success on the Internet already. Double opt-in messages should contain information that clearly identifies who requested the opt-in (such as the source IP address, and any headers that are relevant).

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

With the idea of a double opt-in scheme, the scope of what you are signing up for should be explicit in the authorisation confirmation request. Otherwise, the scope should be for one "mailing list" or equivalent concept.

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)?

There is a requirement that any information that is in the message be correct. Disguising the source of a message as being someone else should be considered to be fraud no matter who is sending the email. There has been a tradition on the Internet that anonymity is respected, however commercial entities should be required to provide at least a correct From: email address.

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?

You should be able to request your address is removed, using the medium that the message arrives in (for example, you should be able to respond via email to have your email address removed), however it should also be possible to remove yourself via other methods, including via phone numbers, and/or the postal system.

If any of these systems are advertised and are non-functional, or do not do as they are advertised to do, that should be illegal.

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

We very strongly believe that header and subject information should be correct. Forged

information can have a serious impact in lost goodwill on a person or company falsely named as the sender.

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

We believe that this should be covered already by existing laws, or, if it's not then existing laws should be extended to cover this. We believe that this is an important issue, however it may not be deserving of its own legislation. Also, having this labelling be in a specific format allows for computer programs (at say schools) to scan for inappropriate content and block it.

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?

We believe that software in itself should not be regulated. There are many legitimate uses for address harvesting software (such as for statistical studies based on the content of the email addresses, or investigating how the software works for better detection/prevention of address harvesting in the future). However, the use of address harvesting software to collect email addresses to send unsolicited email to is something that we disagree with and believe should be banned. We also disagree with allowing people to collect email addresses (through any means) and distributing them.

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

Anyone who is affected by their actions. This includes recipients, owners of forged domains, ISPs who had the mail travel through their network, and companies or individuals whose computers who may have been hijacked.

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

As mentioned earlier, we are not well educated with the roles of the various agencies that enforce laws within New Zealand, and do not believe that we are qualified to express an opinion on this matter.

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?

The penalties should be similar to other fraud, pornography, false advertising or telephone related behaviour. Currently large-scale fraud involving large sums and/or many victims normally results in jail sentences and large fines.

21. Should contraventions give rise to criminal or civil penalties?

Large scale offending for commercial gain should be a crime. As mentioned above, we believe the penalties should depend on the scale of offending as consistent with fraudulent behaviour and false advertising.

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

While we believe that the enforcement agency be given the ability to obtain search warrants for entry, search and seizure of equipment and records related to spamming, we believe that the quality of the evidence should be very high before a warrant is issued, as the loss of computer equipment can result in severe disruption to an individual or company.

In summary, we support more legislative involvement with the issues surrounding spam. Spam is an important issue to almost everyone that uses the Internet, and we are eager to see this legislation progress.

The Waikato Linux Users Group Incorporated.

