

Anti-Spam Legislation

21 May 2004 / 30 June 2004

To: Ministry of Economic Development

Re: **A Comprehensive Solution**

This document is submitted on behalf of the New Zealand Computer Society, the organisation of the professionals in the computer industry. Current membership is about 2,800.

The NZCS places high value on its responsibilities to the lay users of computers.

This document is based on current practices implemented by most reputable users of the Internet. The NZCS believes that there are technology-based solutions to the Spam problem. However it also believes that these solutions are required to be in place by legislation – the ignorance (or worse) of the few should not detract from the use of the internet by the many, particularly the community at large and not just those with expertise.

There are five basic ideas in this submission:

- ✓ Computers should be sold in a “safe” mode.
- ✓ There are many valid reasons for “lists” of email addresses. Law should address the issue of unsolicited bulk email and not inhibit legitimate commerce.
- ✓ Just because most email arises off-shore does not remove the need for legislation in New Zealand. We should protect our borders.
- ✓ Intentional obfuscation should be illegal.
- ✓ Some specific legislation is required to meet certain specific problems.

No attempt has been made to write this document in a legal “style”.

The technology exists to provide protection to users and is widely recommended by the industry. Excellent products are available to address these concerns – some developed in New Zealand, some associated with or acknowledged by the major suppliers such as Microsoft.

The role of Government and legislation needs clarification, particularly where children are exposed to some problems, and where existing legislation exposes some solutions to commercial risk. For example it must be clear that ISPs can filter emails and block websites which are damaging to legitimate commerce or offensive.

The legislation which other countries have used is based on technologies (or the lack thereof) at least 2 years old. Adopting legislation similar to Australia and the USA would be applying an obsolete solution to a current problem.

Note: Government should be required to follow these guidelines as good practice rather than be required to by legislation because a number of exceptions or specials requirements can be identified.

Note: Spam is used as the primary tool to distribute virus. Therefore some of the purpose of eliminating spam is to reduce the traffic which carries viruses.

Legal Requirements for Consumer Protection

Self-Regulation or Legislation: Some of the ideas expressed here could be addressed by self-regulation by resellers. However the NZCS recommends that the ideas have some support in legislation. The set-up of the software listed below is beyond the ability of most end-users and will remain so because of inherent complexity and the rapid changes in the threats.

Virus are so-named because they spread by **contagion**. If the proportion of the machines protected is increased the contagion is reduced. Several recent viruses had a lesser effect because they did not propagate through Windows'98 which at the time was about half the machines.

Definition of Spam: Spam is Emails generated from a single source in bulk. We exclude bulk emails generated from Double Opt-In Lists, Opt-Out Lists, Targeted Advertising Lists and Membership Lists (see below). Spam also includes unsolicited emails with sender and/or subject obfuscated or not indicative of the contents. Many Spam Filtering tools allow the end-user to set the filtering criteria.

Consumers might be defined as legal persons who are not GST-Registered. This definition may be refined but it has the advantage of clarity. Thus businesses who buy machines and configure the machines themselves are not bound. However business laptops should have the same requirements imposed because they are clearly intended to be used outside the business premises.

Computers need a more restricted definition in this particular context. We suggest they must be: intended for primary use for email, web browsing, word processing, spreadsheet processing, slideshow presentation and similar use. This eliminates various devices such as hand-helds and special purpose machines. Only computers loaded with a "ready-to-run" operating system need be covered.

Patches for the software sold pre-installed should be up-to-date (say within 30 days).

AntiVirus: It is required that all such computers sold to consumers must have AntiVirus software pre-installed and pre-configured with LiveUpdate which is activated and functioning at the time of sale and that outbound filtering be enabled. Most machines are sold with an initially free version of an anti-virus product – so this just enforces it. Many Unix/Linux advocates claimed this was unnecessary for them but the worst worm was a Unix worm.

SurfSafe: It is required that any software sold to consumers which enables access to the Internet must be configured to block access to sites which contain Adult Material AND can be re-set to permit access to such sites whilst **always** blocking sites containing Offensive Material and the software must have a "liveupdate" facility which is activated and functioning at the time of sale. The focus here is on safety for children. A high proportion of spam is associated with the promotion of Adult, Offensive or Erotica sites.

Many such tools are readily available now – enforcing would be simple. Some such software uses a black-list/white-list server – and such sites are readily available internationally with candidate sites being submitted by users, screened and actioned semi-automatically. **Many ISPs offer this service already.** We need to remove the **ambiguity** over the right of ISPs to filter any material and **require** the service to be offered particularly because the telcos benefit by charging for the high volumes involved. This requirement must be harmonised with the Electronic Transaction Act and its definition of "Received".

Port-Closure: It is required that Firewall software sold must be initially configured with only the minimal ports which are needed for email and web access enabled. Expert users can readily open other ports but lay persons must be made aware that they are creating greater risks for themselves and their families. **Microsoft now understands this** and will be a willing partner.

Spyware: It is required that all computers sold to consumers must have software which detects and clearly advises the user of the downloading of any executable software, such spyware filters to be preinstalled and pre-configured with LiveUpdate which is activated and functioning at the time of sale. The problem here is "which anti-spyware can I trust". An authoritative source of such software is required and there may be grounds for a safe host machine to be maintained and the software placed on it after expert scrutiny. This may need a legislative underpinning.

Laptops: Laptops bought by anyone (including corporates) must meet the same requirements. It may be better to require these conditions on all machines which are not permanently installed in a LAN.

Retailed Software: Software sold through retail shops separately from hardware must meet the above requirements if installed in the standard mode without the user having to actively choose such options.

Spam Filtering

Email List: An email list is a text file or database recording multiple email addresses for multiple (legal) persons. Databases (or email software databases or file systems) holding the addresses of emails that have been received are not email lists for this purpose.

Email Lists may be **Double Opt-In Lists** or **Opt-Out Lists** or **Membership Lists** or **Targeted Advertising Lists**.

Double Opt-In List: A name is added to a List (First Opt-In) after it is provided to the list owner by the email address owner entering it on a website. Subsequently an email is sent from the list owner asking for confirmation that the address is for the correct person and that the person wishes to receive email from the sender. A positive reply is the Second Opt-In. A negative reply must cause the address to be marked as "No further emails to be sent". No reply and "bounces" may be processed as the list owner wishes. Date/Time Stamps must be retained for both Opt-Ins. An Opt-In List must also operate as an Opt-Out list.

Opt-Out List: Every email sent from a List must contain a link which leads to web accesses or email replies for the sole purpose of recording that the recipient does not wish to receive further emails from the sender for commercial purposes. The sender must record and act upon the reply.

Opt-Out Lists must be created by receiving a business card, writing on a form, sending an email to the list owner or similar commercial transaction. The List Owner should be required to retain evidence of this transaction. Emails relating to Health and Safety and other "legal" issues may still be sent after a list member has "opted out".

It will be necessary to re-educate the public that if the email appears to come from a ".nz" domain they are safe to reply to the Opt-Out link.

Targeted Advertising Lists: Advertising by email is only legitimate if:

- a) the list is a Double-Opt-In or Opt-Out List as defined above OR
- b) the list has been provided by a Directory Service which has confirmed with the address owner that they understand that their address will be made available in this way and allowed the target company to classify the nature of their business and the product or services offered are clearly relevant to such businesses OR
- c) the email is the Second Opt-In.

AND the subject begins with "[ADV]".

Note: If goods or services have been supplied it is legitimate to retain the address after an Opt-Out for the purposes of product warnings or upgrades but not for promotional purposes.

Note: Collecting addresses off Yellow Pages (and similar) should not be permitted to be used with sales or promotional emails but only for purchases. The major issue here is that addresses are made available by the owner as a contact from prospective **customers** but are then used by **suppliers**.

Membership Lists: Any organisation which has a constitution (under the Companies Act or Incorporated Societies Act) which identifies members who must formally and unambiguously consent to be a member may send emails to its current or recent members about the activities of the organisation.

Bulk eMail is defined as emails with substantial content in common sent from a common site at a rate in excess of 100 per hour.

It should be an offence for New Zealand senders of bulk emails not to meet the above definitions.

It may be simplest to define New Zealand senders as those using a .nz domain and to require an authoritative database of such addresses and to require them to be recorded in the Companies Register (and similar) where they can be readily checked by spam filters.

This provides a clear basis on which to require off-shore bulk emails to be filtered while NZ sources can be handled explicitly.

ISPs **must** make available to all of its customers on request from the customer a service to filter any emails containing "[ADV]".

ISPs may choose to offer a service which filters on content.

New Zealand Legislation and Border-Protection

We must ensure our legal environment is compatible with our trading partners and that investigations and prosecutions can be conducted internationally.

Much spam and particularly that promoting Offensive Material originates off-shore. While we should legislate against NZ-originated spam it is often argued that we cannot do much about offshore-originated spam. However nearly all major ISPs do offer useful filter services.

All traffic **must** be filtered for viruses using services which have a “LiveUpdate” facility. It is required to filter at any point where traffic from off-shore reaches a New Zealand located machine except where by contract certain traffic will be forwarded to other machines which are obliged to perform the filtering. This should be required by legislation.

It is already widely done – we need to close the gaps in our defensive wall.

However it is recommended here that Bulk Email (as defined) filtering also be compulsory on the same machines. Thus the senders of bulk emails are identified, New Zealand sources validated and those from off-shore be filtered with acknowledgement to the sender that filtering has been imposed. Subsequent emails from those sources will also be filtered. This will require a database to be built by (or jointly by) ISPs to identify legitimate sources of bulk emails.

Most of the large ISPs are already filtering emails for spam and virus. If this was required to be for all ISPs crossing our border then spam could be blocked at the first level. Most attacks are still directed through email attachments. We would have a high profile if we handled spam as a whole country.

Empowering Filtering: Legislation should make clear that filtering is a legitimate practice. When a mail message is filtered at least one message per day advising the sender of the filtering must be sent.

Closing Down Domains: The legislation should apply to any domain used by a NZ-registered company or any domain with cc of “.nz”. InternetNZ or the custodian of .nz country-level domain must be required to block any domain from which an offence has occurred.

ISP SafeSurf: All ISPs with consumer customers must offer them a service to filter for Adult Material and/or Offensive Material to all subscribers.

Note: Bulk emails can only be sent by NZ organisations using domains recorded on the Companies Register database and a similar database for Incorporated Societies. Legislation should require such organisations to use only sending addresses recorded in these databases thus allowing these databases to be used as a “white-list” facility to spam filters. This would require legislation.

Legislation is Required

Definition of Commercial Purposes: Any activity to promote or sell products or services is a Commercial Purpose unless by Government. The following only applies to Commercial email.

There is no need for exceptions for political parties, charities or trusts because of the fairly broad definitions of such entities. The Membership List option covers these.

Identification: Every email sent for “commercial purposes” must clearly contain as the name of the sender the name of a legal person (including Officer of an Organisation and generic addresses such as “info@” or “sales@”) and an email address (the Reply Address) which will be serviced by the original sender for at least a further 30 days. The sender is required to receive responses to such an address as per the Electronic Transactions Act.

Subject: The Subject of an Email must adequately reflect the contents of the body and not be empty or contain multiple adjacent spaces or “tabs” and not attempt to bypass commonly used spam filters by the insertion of special characters or excessive punctuation.

Also Legally Prohibited

Web-scraping is where software on one machine responds to a website as if it is a Browser and thus captures a substantial portion of a database hosted by the website for the purpose of commercial use of that data (other than as a search engine which must clearly ascribe to the data the correct URLs of its immediate source).

Web-Scraping should be prohibited unless permission is expressly given by the site owner.

Spidering or **Crawling** to collect email addresses must be illegal (except by search engines).

SpyWare is downloaded software which usually without the knowledge of the user (or where the user does not know that the software acts in this way as well as doing what it says it does) which sends information such as keystrokes or security information back to another machine. It must be prohibited.

Phishing Solution

Phishing is where an email is sent purporting to come from another source such as a bank is becoming a problem. Such emails are usually part of a scams or fraudulent activity. They exploit the fact that the web address included looks like a valid address known to the recipient but are actually different addresses.

Phishing is probably already illegal under the ETA.

However it would be possible to provide technical solutions (program code) which must be installed on the user’s machine. The problem is that the user does not know if they can trust the source of this code.

The government can set up a specific site hosting software addressing the areas identified above and validated as not containing any malicious components. This is an issue of public confidence rather than a technical issue.

Providers of the software would pay for the examination and certifying of the code which would be done by independent experts.

PKI Validation

Digital Certificates require a high level site which can certify transactions. One such site must be the trusted top level of a hierarchy of sites which issue the certificate validation.

The Government can set up such a site. Its issue of certificates can be fully automated. It could be managed under contract.