



# New Zealand Law Society

Law Society Building, 26 Waring Taylor Street, Wellington 1, New Zealand  
P.O. Box 5041, Wellington, DX SP20202, Tel (04) 472-7837, Fax (04) 473-7909  
Email [inquiries@lawyers.org.nz](mailto:inquiries@lawyers.org.nz) World Wide Web <http://www.lawyers.org.nz>

30 June 2004

IT and Telecommunications Policy Group  
Resources and Network Branch  
Ministry of Economic Development  
P O Box 1473  
WELLINGTON

And by email: [spamsubmissions@med.govt.nz](mailto:spamsubmissions@med.govt.nz)

## Legislating Against Spam

Please find attached the Electronic Commerce Committee submissions on the Ministry's discussion document *Legislating against Spam*.

Yours sincerely

Dick Edwards  
Acting Secretary

# New Zealand Law Society

## Ministry of Economic Development Discussion Paper – Legislating against Spam

The Society's Electronic Commerce Committee (the Committee) appreciates the opportunity to comment on this discussion paper. Its comments are set out following the chapter headings in the discussion paper and a number of questions in that chapter.

### Background

1. *Do you consider spam to be an important issue?*  
Yes

*Has it significantly affected you in any way?*

Yes - Spam has affected Committee members who responded to the questionnaire, principally by imposing additional costs through the need to deal constantly with unwanted emails. The Committee believes that its members experience is representative of the legal profession. Those costs arise from:

- consumption of network and computing resources;
- use of systems administration time;
- slow down in email services;
- implementation of email/filtering;
- loss of genuine messages filtered out as false positives by email spam filters.

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

Yes – legislation would be beneficial, alongside other complementary measures, in dealing with spam. Although most spam received by New Zealanders originates from overseas, a legislative solution needs to be implemented internationally in a manner that enables anti-spam enforcement agencies to deal with spam at its source, wherever that may be.

### Existing Legal Framework

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

No – existing privacy protections deal only with collection of information relating to natural persons and not corporate entities. Furthermore, personal information about individuals can be obtained from public sources without contravention of the Privacy Act. For example, email addresses can be collected from documents published on web sites and from public Internet forums, such as USENET newsgroups. In terms of enforcement of the Privacy Act, it is important to note that section 66 of the Act requires proof of damage as well as a breach of a privacy principle or code of practice. Furthermore, the damages available relate to pecuniary losses and loss of benefits

incurred in relation to the interference with privacy of an individual rather than the economic costs associated with the delivery of unwanted spam. Targeted anti-spam legislation is required to deal with these gaps.

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

Yes – the Harassment Act 1997 is not adequate to deal with spam because it requires a pattern of behaviour directed against another person that includes doing any specified act to the other person on at least two separate occasions within a period of 12 months. In this context the term specified act involves acting in a way that causes that person, or would cause a reasonable person in that person’s circumstances, to fear for his or her safety. Although most spam is a nuisance it does not generally constitute a threat to a person’s safety. Stand-alone anti-spam legislation is therefore necessary.

### **Legislative Scope**

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)?*

The Committee is unanimous that anti-spam legislation should cover electronic mail via the Internet. However, views were divided as to whether the legislation should apply to other unsolicited messages such as:

- short message service (SMS);
- multi media messaging services (MMS);
- instance messaging (IM);
- faxes;
- telephone marketing;
- physical mail delivery.

We note that the scope of overseas legislation differs from country to country. Australia’s legislation provides a technology neutral definition of “electronic message” that includes all of the messages identified above but does not include voice calls from a standard phone service or facsimile messaging. The United States, CAN-SPAM legislation is primarily concerned with email messages sent via the Internet. However, telemarketing is regulated separately under 1996 legislation banning robotic voice telemarketing and telemarketing by fax machines and through the implementation of the so-called “do not call” anti-telemarketing registry for consumers. In addition, US legislation requires the FCC to promulgate rules to protect consumers from unwanted mobile service commercial messages. The FCC has recently (March 2004) published a paper seeking comments on rules to eliminate spam from wireless devices such as mobile phones.

In our view, emails should be the principal target for legislation simply because volumes of unwanted emails far exceed other forms of unsolicited communications. This may be due to the fact that the cost of sending spam to millions of email addressees is minimal whereas senders of other forms of unsolicited communications incur material costs in doing so.

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

The majority view of the Committee is that no minimum number of messages should be required before unsolicited commercial email is classified as “spam”. This view is consistent with the approach taken in Australian legislation, which prohibits the sending of a single commercial electronic message that has an Australian link and is not a designated commercial electronic message. However, the prohibition does not apply if the recipient *consented* (as defined) to the sending of the message. It is important to note that consent, for the purposes of the Australian Act, may be inferred from the conduct of the recipient and their relationship with the individual or organisation concerned. In this regard, the Explanatory Memorandum to the Australian legislation provides an example of a person who has an existing business relationship with the sender and, as part of that relationship, has provided an electronic address to the sender. In that situation it would be reasonable to infer that the person has consented to receiving electronic messages from the sender.

An appropriate definition of “consent” should enable persons to send commercial electronic messages to persons with whom they have a pre-existing business relationship. It may also be reasonable to infer consent to email communications where an email address is published on a business card or on a web site, as long as the message is relevant to the business, functions or roles of the recipient and the email address was published without a statement that withheld consent.

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?*

The Committee was divided as to whether or not the legislation should be restricted to messages of a commercial nature or should apply without exceptions. As noted in the Discussion Paper, the Australian legislation exempts certain types of unsolicited commercial electronic messages from its rules. In addition to the exemptions listed in the Discussion Paper, the Australian legislation also exempts purely factual information without any commercial message. A message does not lose its “purely factual” (and therefore exempt) status by reason only of the inclusion of the name, logo and details of a sponsor of that message.

8. *Should the legislation extend to coverage of acts done overseas?*

*If so, what acts should be covered?*

Yes – the legislation should extend to acts done overseas if those acts have effects in New Zealand. We note that under the Australian legislation, only messages with an

“Australian link” are covered, such as the sender, authoriser or recipient being in Australia, or having business or message access devices in Australia. An equivalent test should apply in New Zealand.

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?*

Yes to both questions – the legislation should apply to all persons who knowingly cause non-compliant messages to be sent or who assist others to contravene the requirements of the legislation or are in any way a party to such contravention. However, legislation should be framed in such a way that innocent carriers of information, such as ISPs who have no advance knowledge of the spammer’s actions, are exempted from liability, in the same way as they are exempt in overseas jurisdictions for the mere conveyance of unauthorised copies of copyright works.

### **The Consent Issue—Opt-in or Opt-out?**

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

*Why?*

The majority view of the Committee is that the opt-in approach is the most efficient method of legislating against spam. However, the opt-in approach should be implemented in a way that minimises compliance costs for commercial businesses who wish to communicate with persons with whom they have an existing relationship. In this regard, we note that the Australian legislation provides that consent can be inferred from the fact that an email address has been published. However, because consent is merely inferred in this situation, persons who publish their email addresses but do not wish to receive unsolicited commercial communications can avoid an inference of consent by clearly stating the purposes for which they do or do not wish to receive email.

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?*

The Committee recognises that if an opt-in approach is adopted, it would be appropriate to broaden the definition of consent to receive email messages to include both express consent (i.e., a positive action by the recipient confirming consent to receive commercial messages) and inferred consent based on a reasonable expectation that the customer is willing to receive commercial messages as evidenced from the recipient’s conduct or an existing business or other relationship with the sender. Consent would obviously not be inferred in a situation where a person has made it clear that consent is not given by actions such as unsubscribing from a mailing list or indicating that he or she does not wish to receive certain email messages.

It is evident that the definition of what constitutes “inferred consent” will be of considerable importance. A balance needs to be struck between ensuring that persons who send business communications in good faith to persons whom they might reasonably expect would be willing to receive the communication are not subject to penalties while persons who, for example, indiscriminately send commercial emails to persons whose email addresses they have harvested are not able to argue that consent may be inferred from the mere failure of the recipient to unsubscribe or otherwise respond to their messages.

We consider that the Australian legislation strikes an appropriate balance in this regard.

In Australia “inferred consent” generally falls into two categories:

- Where a work-related email address has been “conspicuously published”; and
- Where certain types of pre-existing business relationships exist and, as part of that relationship, the recipient has knowingly given an electronic address to the sender.

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

We consider that the approach adopted in Australia should be followed.

### **Transparency issues**

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)?*

Yes – in general it should be unlawful for a person to transmit commercial email messages with materially false header information or with a subject heading that is misleading as to the content of the message. The message should clearly and accurately identify the individual or organisation who authorised the sending of the message, although we do not consider that inclusion of a physical address should be mandatory.

We note that in Australia commercial messages must always contain clear and accurate identification of who was responsible for sending the message, and how they can be contacted. Details that are provided must be reasonably likely to be accurate for a period of 30 days after the message is sent.

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?*

Yes – legislation should include a statement to the effect that the recipient of unsolicited commercial email may use an electronic address set out in the message to send an unsubscribe message to the individual or organisation who authorised the sending of the message. Furthermore, such electronic address must be functional and the unsubscribe request should be actioned within a prescribed period of time. Nevertheless, an unsubscribe option may not be utilised by educated Internet users, who believe that best practice is to avoid responding to spammers.

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

Yes – we agree that requiring transparency for commercial electronic messages would assist in minimising the spam problems. Accurate and non-misleading information is an essential requirement for transparency and also enables self-help measures to be taken by an email recipient to block email from senders from whom the recipient does not wish to receive electronic messages.

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

Yes – the majority view of the Committee is that messages of advertising or adult nature should include labels specifying them as such. Alternatively, this issue could be addressed by prohibitions against materially false header information and subject headings that are misleading as to the content of the message.

### **Privacy Issues—Address Harvesting**

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 – address harvesting should be prohibited in cases where it is undertaken in connection with the unlawful sending of electronic messages. This approach has been taken in Australia in order to control an activity that is closely associated with the actions of spammers.

### **Enforcement Issues**

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

We agree that the approach of the United States in giving rights of action to Internet service providers has merit. ISPs have a considerable incentive to stop spam because they are directly affected by the activities of spammers and bear significant costs in dealing with it. The major New Zealand ISPs are likely to have sufficient knowledge and resources to take actions against spammers.

In principle, anyone who suffers damage or loss as a result of spam should be able to bring a civil action to obtain compensation from the spammer. In practice, such actions are unlikely to be viable unless the impact on the organisation is substantial or actions on behalf of classes of affected persons are available.

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

We agree with the view expressed in the Discussion Paper that the Commerce Commission is best placed to assume the role of carrying out investigations and taking enforcement action under anti-spam legislation.

20. *What should be the available penalties and remedies for breaches of antis spam legislation and what should be the maximum fine or pecuniary penalty?*

We note that overseas legislation provides for substantial penalties for breaches of anti-spam legislation. We agree that New Zealand penalties should be set at similar levels but consideration should be given to ensuring that the levels are commensurate with penalties under the Fair Trading Act. Nevertheless, the penalties prescribed under the Fair Trading Act were set some time ago and, although the penalties in overseas anti-spam legislation seem high, the level of penalty needs to reflect the very high returns that successful spammers can receive through their activities.

As in Australia, the enforcement agency should be given powers to:

- enforce undertakings by originators of spam;
- issue formal warnings and apply for court injunctions;
- issue infringement notices;
- seek court imposed penalties.

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

We agree that the penalties should generally be in the form of a civil pecuniary penalty, and that the required standard of proof should be a civil standard. However, consideration should be given to ensuring that existing criminal laws covering fraud are broad enough to encompass fraudulent spam-related activities as well as the activities of persons who knowingly cause damage by embedding malicious code or viruses into email.

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

The Committee does not have an agreed view as to what powers should be given to the investigating authority. However, given the potentially serious civil liberties implications involved in granting powers of entry, search and seizure of evidence, it considers that it would be appropriate for such powers to be exercised only pursuant to a judicial warrant by persons with specialist skills and training. The application of entry, search and seizure powers should be restricted to persons who are reasonably suspected of having breached the anti-spam legislation.

## **General**

23. *Other comments*

In the end, of course, no legislation will stop this kind of activity. It can be done too

easily and there is easy money to be made by doing it. However, this is not a valid reason not to pursue legislative remedies particularly since there are now examples where legislation has been used to initiate proceedings against spammers with the assistance of regulatory authorities in other jurisdictions.

For example, on 29 April 2004, the US Federal Trade Commission announced that cases have been brought against two organisations that had violated the CAN-SPAM Act, which went into effect in the United States on 1 January 2004. One of those organisations, Global Web Promotions Pty Limited, operated in Australia and New Zealand. The case against them was brought with the assistance of the ACCC and the New Zealand Commerce Commission. If these cases are successfully concluded and substantial penalties are awarded against the spammers this outcome may provide a modicum of deterrent and reduce the incentive for others to engage in activities that are currently adversely affecting Internet users all over the world.

Although the scope of the Discussion paper does not extend beyond unsolicited email, the Committee considers that it would be appropriate for the Ministry to review other forms of potentially harmful Internet activity, such as the transmission of “spyware” that infringes privacy or interferes with the operation of a recipient’s computer without the permission of the recipient. In this regard, we note that a ComputerWorld article dated 28 June 2004 reports that proposed US Federal legislation to regulate spyware has moved another step towards enactment.

Ross Johnston  
NZLS Electronic Commerce Committee  
30.6.04