

DISCUSSION PAPER

**LEGISLATING AGAINST
SPAM**

Contents

Minister's Foreword	3
Introduction	4
Spam	4
Purpose and Scope of Discussion Paper	4
Next Steps	4
Background	5
The forms of spam in New Zealand	5
The extent of spam in New Zealand	5
The detrimental effects and costs of spam	5
Measures aimed at reducing spam	6
Existing Legal Framework	8
Privacy	8
Harassment	9
Transparency	10
Misuse/abuse of computing resources	10
Legislative Issues	11
Legislative Scope	11
The Consent Issue – Opt-in or Opt-out	15
Transparency Issues	17
Privacy Issues – Address Harvesting	19
Enforcement Issues	20
Responses to Discussion Paper	22

Minister's Foreword

Spam is a growing problem for New Zealand computer users and businesses. In this discussion paper, the Government proposes an approach to tackle the problem through legislation. This will form part of a multi-pronged approach alongside industry self regulation, awareness and education campaigns, and international initiatives.

Spam, or unsolicited commercial electronic messages, undermines the use of email and other communications technologies. It clogs up the email boxes of private individuals with irrelevant, unwanted and often offensive messages. The Government seeks to assist New Zealanders who are sick of the annoyance and costs that spam imposes on them.

Spam also imposes significant costs on businesses who lose productivity and staff time dealing with it, and who foot the bill for security and screening software. It also undermines the legitimate needs of communications and marketing users. In so doing, spam undermines the Government's objectives of promoting economic growth and building public confidence in electronic communications.

Spam has become a huge problem worldwide and has now grown to the extent that many countries see legislation as an important step to effectively addressing it. New Zealand must play its part alongside other countries to deal with this growing threat to electronic communications. The Government considers that it is now timely to look at how legislation in this country might effectively contribute to minimising the spam problem.

I encourage all individuals and organisations with an interest in this area to consider the issues raised by this discussion paper and make a submission so that the Government can benefit from widespread input in the development of an effective and timely policy to address the issue of spam.

Hon David Cunliffe
Associate Minister for Information Technology

Introduction

Spam

1 Spam is the term now generally used to refer to unsolicited bulk messages, usually transmitted to a large number of recipients via electronic mediums such as email. They usually have a focus on promoting products, services or fraudulent schemes.

2 Major problems caused by spam are breaches of privacy and a lowering of user confidence, deceptive practices, illegal or offensive content such as pornography and scams, threats to network integrity and security, desired e-mail getting blocked by anti-spam technologies, and the financial costs imposed on ISPs and users.

3 Due to the problems caused by spam and the continuing growth in the volume of spam, a number of governments around the world have enacted or are proposing legislation as one way of curbing spam growth. The New Zealand Government has signalled that legislation against spam may be an appropriate measure for New Zealand also.

Purpose and Scope of Discussion Paper

4 This discussion paper seeks to discuss and obtain feedback on the various policy issues which are raised when considering anti-spam legislation. The objective is to ensure that any anti-spam legislation enacted in New Zealand is an effective tool as part of a multi-pronged attack on spam.

5 The paper does not seek to consider content issues such as the sending of pornography over the Internet as these are dealt with under existing legislation. Its focus is rather on addressing the spam problem in general.

Next Steps

6 It is proposed that a joint Government / InternetNZ industry workshop will be held during the consultation period (mid-May – 30 June) as part of the consultation process.

7 Subsequent to the receipt of submissions, the Ministry of Economic Development, in conjunction with other Government departments, will be preparing a paper for submission to Cabinet on the proposed anti-spam legislation.

8 Views expressed in submissions will be taken into account in the policy development process. It is envisaged that a summary of views will be prepared and published on the Ministry's website (www.med.govt.nz).

Background

The forms of spam in New Zealand

9 Spam largely takes the form of unwanted, unsolicited, commercial emails via the Internet. It can also include other forms such as text messages using short message services via mobile communications technologies. How to define 'spam' is one of the key policy issues raised by this paper.

The extent of spam in New Zealand

10 Anecdotal evidence suggests that most spam received in New Zealand comes from overseas. This highlights the need for international co-operation to address the spam problem.

11 Recent reported figures suggest that the extent of spam received in New Zealand is similar to that experienced overseas. TelstraClear, which filters email for its clear.net and paradise.net customers, indicated that in October 2003 spam accounted for 46% of the email received, in November 2003 52% and in the first week of December 2003 62%.

12 Ihug has indicated that in September 2003 it stopped 5.1 million spam emails and in November, 6.5 million. It has also said that for the 29% of its customers who use its voluntary spam filter, spam accounts for 75% of their email. Xtra has given figures ranging from 38% to 68% since it implemented its anti-spam filter in November 2003.

13 According to Brightmail, an anti-spam software company, as of March 2004, unsolicited bulk mail volumes accounted for 63% of all e-mail traffic on the Internet, up from just 8% of traffic in mid-2001. Another anti-spam solution company, MessageLabs, found that 55% of the emails it scanned in May 2003 were spam, and the volume of spam it has detected has increased in the last ten months from 60 million per month to over 350 million per month.

The detrimental effects and costs of spam

14 Spam imposes costs on all Internet users. It is a nuisance to have to continually deal with unwanted emails. More importantly, however, spam uses scarce resources of users and service providers without compensation or approval. Spam consumes network and computing resources, e-mail administrator and helpdesk personnel time, and reduces worker productivity.

15 It is difficult to calculate the total costs of spam, though estimates suggest the costs at the global level are high. For example, a recent European Union (EU) study estimates that the worldwide cost to Internet subscribers of spam is in the vicinity of EUR 10 billion a year. An American firm, Nucleus Research, estimated in 2003 that the economic cost is \$US874 a year for every office worker with an email account, which multiplied by 100 million workers in the USA amounts to about \$US87 billion. Nucleus Research estimated that the average worker receives 13.3 spam messages a day, which takes 6.5 minutes to process. That equates to 1.4 per cent of their

productive time. Other estimates put the cost to productivity higher. It is likely that this cost has grown substantially since 2003

16 The practice of spamming also raises concerns associated with privacy, fraudulent or deceptive messages, the sending of pornographic material, attacks on the security and integrity of computer networks through viruses and the like, identity theft, and reduced consumer confidence in the use of the Internet for the purposes of e-commerce.

17 The indiscriminate sending of offensive or pornographic material through spamming is a particular concern because of the harmful effect it can have on the young and the vulnerable. Effective measures against spam should therefore seek to address this issue.

Measures aimed at reducing spam

18 There are a number of approaches or measures which are aimed at reducing spam. These consist of:

- Legislative or regulatory measures;
- Self regulatory measures such as industry codes:
 - In New Zealand the Direct Marketing Association (DMA) has developed a set of standards for email marketing by its members. The DMA recognises that the adoption of industry-wide standards of best practice and ethical conduct regarding the use of email for marketing purposes will promote consumer confidence in eCommerce and ensure that proper account is taken of consumers' right to privacy (see www.dma.co.nz);
 - Internet Service Providers (ISPs) in New Zealand will generally not tolerate spammers operating from their networks and will have them removed;
- Education and awareness campaigns (in New Zealand the Internet Society of New Zealand (InternetNZ) is active in this area). InternetNZ has set up a website (www.stopspam.net.nz) as an online resource for helping to deal with spam. It includes the following four golden rules for Internet users:
 - Never buy anything advertised in spam;
 - Never reply to spam;
 - Never use "remove" options in a spam;
 - Distrust everything;
- Technical measures such as the use of filtering by ISPs and users. If an ISP uses filters at its server then that means users will not see spam that is filtered out. The issues that arise are the possibility of false positives (legitimate emails being caught by the filter) and the lack of ability of users

to customise filtering software according to their own requirements. Anti-spam technologies are not wholly effective however as spammers develop more sophisticated technologies to overcome the effects of filtering.

19 The general consensus internationally is that a multi-dimensional approach combining all of the above offers the best prospects for reducing spam, while noting that international co-operation is also a critical factor.

20 The benefits for New Zealand of legislating against spam are:

- It enables legal action to be taken against spammers based in New Zealand;
- It prevents New Zealand being seen as a safe haven for spammers as legislative measures begin to be implemented in overseas jurisdictions;
- It assists New Zealand in efforts to obtain international co-operation to combat overseas sources of spam if we have our own house in order;
- It allows the New Zealand Government to effectively co-operate with overseas government anti-spam enforcement agencies, to help trace the senders and beneficiaries of spam sent to New Zealanders.

Questions for discussion and response

1. Do you consider spam to be an important issue? Has it significantly affected you in any way?
2. Do you think legislation has a role to play alongside other complementary measures?

Existing Legal Framework

Privacy

Privacy Act

21 The Privacy Act 1993 already provides suitable rules against the collection, transfer and use of electronic address information (email address, sms number, fax number etc) pertaining to an individual, without their consent or knowledge. However, this is dependent on how the information is collected, from where it is collected, and how it is used.

22 Information privacy principle 3 provides that when an agency collects personal information directly from the individual concerned, that individual must be made aware of:

- the fact that information is being collected (i.e. no secret copying of email addresses);
- the purpose for which the information is being collected;
- the intended recipients of the information; and
- the name and address of the agency collecting the information and that will hold the information.

Individuals must also be told of their rights of access to and correction of information held. "Correction" may include deletion (e.g. deletion from a mailing list).

23 Principle 4 provides that an agency shall not collect personal information by unlawful means, or by means that, in the circumstances, are unfair or intrude unreasonably upon the personal affairs of the individual concerned.

24 Principles 10 and 11 control use and disclosure. In essence they limit agencies to using and disclosing information they hold to the purposes for which they obtained the information unless the individual consents to some other use, or an exception set out in the principles applies. For example, a company that amasses customers email addresses for some legitimate purpose can't simply sell those to marketers unless they've complied with the principles (e.g. by telling customers at the outset of their practice or by getting authorisation later).

25 It is important to note that personal information about an individual can be collected, traded and used from publicly available registers and other publications, such as the motor vehicle register, with or without the permission of the individual.

26 In addition, the Privacy Act only applies to natural persons. The "privacy" of corporate entities is not protected by the Privacy Act. Although corporate entities have some allied interests in controlling their data and preserving confidentiality it has not generally been seen as appropriate to apply privacy laws to non-natural persons.

27 The main way that compliance with the Privacy Act is enforced is by individual complaints to the Privacy Commissioner which are then investigated, conciliated and settled. Cases that don't settle can lead to civil proceedings before the Human Rights Review Tribunal. Remedies are available for actions that constitute an "interference with privacy". This requires not only a breach of a privacy principle but *also* some evidence of harm to a particular individual.

28 While individual complaints and proceedings may sometimes be appropriate, this is not likely to provide a very effective means for a mass problem such as spam. Although the collective harm may be great, the ability to quantify harm to an individual complainant may be quite difficult. The Privacy Act does allow for class actions although successfully pursuing those may be difficult and costly.

29 The Privacy Act would seem to have limited use as a means for addressing the spam problem due to the exceptions to key principles, the manner of enforcement and its application to natural persons only.

Harassment

Harassment Act

30 It has been suggested that the civil harassment regime under the Harassment Act 1997 potentially covers acts of spamming.

31 The object of the Harassment Act is "...to provide greater protection to victims of harassment by –

- (a) Recognising that behaviour that may appear innocent or trivial when viewed in isolation may amount to harassment when viewed in context; and
- (b) Ensuring that there is adequate legal protection for all victims of harassment."

32 Section 3(1) of the Harassment Act states that:

(1) For the purposes of this Act, a person harasses another person if he or she engages in a pattern of behaviour that is directed against that other person, being a pattern of behaviour that includes doing any specified act to the other person on at least 2 separate occasions within a period of 12 months.

33 The term "specified act", in relation to a person, is defined in section 4(1) of the Act as including the following:

(d) Making contact with that person (whether by telephone, correspondence, or in any other way):

(f) Acting in any other way –

- (i) That causes that person ("person A") to fear for his or her safety; and
- (ii) That would cause a reasonable person in person A's particular circumstances to fear for his or her safety.

34 There are a number of difficulties in seeking to apply the Harassment Act to the problem of spam. The two principal difficulties would appear to be first, while spam is generally acknowledged to be a nuisance, it is, in general, of a different character than harassment and second, the Harassment Act works on the basis of individual victims obtaining a civil court order against a named respondent after the repetition of an act, which would be unworkable in relation to most spam.

35 While consideration has been given to using the Harassment Act as a basis for legislating against spam, stand alone legislation seems a more suitable option given the different purposes of the Harassment Act and anti-spam legislation.

36 The Harassment Act would, however, be a useful complement to any legislation against spam as it gives individuals legal protection against personal emails causing distress to the recipient.

Transparency

37 No existing legislation covers the spam issue of transparency – invalid sender addresses (both physical and electronic), no unsubscribe function and misleading/inaccurate headers and subject lines on commercial messages.

Misuse/abuse of computing resources

38 There appears to be adequate coverage under the Crimes Amendment Act (No 6) 1999, concerning the misuse or abuse of computing resources applicable to spam, for example denial of service attacks (DoS) and the transporting of viruses such as the Sobig.F worm.

3. Do you consider existing privacy protections in this area sufficient?
4. Do you agree that stand-alone anti-spam legislation is preferable to reliance on the Harassment Act?

Legislative Issues

39 The key legislative issues are:

- Legislative scope – what types of messages should be regulated or prohibited and who should be covered?
- The consent issue – should an “opt-in” or “opt-out” approach be adopted?
- Transparency issues – should there be a requirement for electronic messages to:
 - Include accurate sender information?
 - Contain a functional unsubscribe facility?
 - Provide accurate header/subject information?
 - Provide labels if they are advertising or adult messages?
- Privacy issues - should there be rules against the supply, acquisition or use of address-harvesting software and harvested-address lists?
- Enforcement issues – what sanctions and/or remedies should be specified/available?

Legislative Scope

40 In determining what types of messages should be regulated or prohibited, a number of questions need to be answered. These are:

- What message mediums should be caught by the legislation (e.g. email, short message services using mobile phones, faxes, telephones (telemarketing), physical mail delivery)?
- Do the messages caught by the legislation have to be sent/conveyed to many recipients, and if so, how many?
- 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 any exceptions?
- Should the legislation extend to coverage of acts outside of New Zealand?

41 There is also the question of who should be covered by anti-spam legislation. Should it be just the sender of the message, or should the legislation also cover the ‘sponsor’ of the message (normally the vendor of the product or service being promoted or advertised) and others knowingly a party to the sending of an unlawful message. In the case of telecommunications companies and Internet Service Providers, they are unwitting transmitters of

spam and so the general approach in other countries is to exclude them from being covered.

42 The issue of what should constitute consent to the sending of a message will be addressed in the next section.

Message mediums

43 The approach of the EU is to apply its legislation to fax, email and other electronic messaging systems such as SMS and MMS (Multi-media Messaging Service). Australia's legislation applies to "electronic messages", which also covers emails, faxes and other electronic messaging systems. It does not apply to voice calls. The United States spam legislation is limited in its coverage to electronic mail via the Internet (telemarketing is regulated separately).

44 Difficulties arise in extending the application of anti-spam legislation to traditional direct marketing mediums such as the delivery of material to a physical mailbox and the use of the telephone for telemarketing. The reason for this is that it is the marketer who bears the costs associated with the use of these message mediums, whereas in the case of electronic communications such as email via the Internet, it is the recipient and the recipient's ISP that bears the cost. In the case of Japan, it has a major problem with spam sent via text messages as the cost of such messages is borne by the recipient.

The issue of "bulk"

45 Spam messages are typically sent in bulk. The issue is whether or not legislation should address the "bulk" characteristic, and if so, how. The EU directive does not specifically address the bulk aspect of spam, but rather refers to electronic mail sent for the purposes of direct marketing. It would seem that the reference to direct marketing indirectly refers to email sent in bulk, although there may be exceptions.

46 In the Australian legislation the issue of bulk has been addressed in the penalty provisions rather than in the definition provisions, with more penalty points applying if a greater number of messages have been sent. In the United States legislation the offence provisions apply to the transmission of "multiple commercial electronic messages", where the term "multiple" means "more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period".

47 The issue of bulk is primarily an issue for people or organisations who are attempting to solve or regulate spam because the concern relates to its collective impact. For the recipients of spam, however, the issue of how many other people may have received a message is generally irrelevant. For them it is the content of the message that is the issue of concern.

48 If individual to individual emails are to be classified as spam (as is the case in the Australian legislation), it would seem that this has the potential to

catch emails from an individual who has maybe obtained another individual's email address as a result of an exchange of business cards and has initiated contact over a commercial matter such as an offer to supply goods or services. In this case the email could be described as both "commercial" and "unsolicited" in terms of the Australian legislation, unless consent to the sending of the email could be reasonably inferred.

49 While the above conduct would seem to be no different from sending a letter to the same effect, it is arguable that the sender should send an initial email asking the recipient if they would be interested in receiving this type of information first to expressly cover off the consent issue. While it may be possible to address this sort of situation in the definitions of "commercial" and "unsolicited", requiring that there be a bulk element to spam would be one solution.

What types of messages should be caught?

50 Spam messages are typically commercial or promotional in nature. Their content nature may be defined narrowly (e.g. sent for the purposes of direct marketing – EU; the commercial advertisement or promotion of a commercial product or service - USA) to widely (e.g. to offer to supply goods or services, promote goods or services, advertise or promote a supplier of goods or services, offer to supply land or an interest in land, offer to provide or to advertise or promote a business opportunity or investment opportunity, assist or enable a person to dishonestly or deceptively take advantage of another person – Australia).

51 The Australian legislation expressly provides for exclusions from the types of messages caught by its rules. The specified exclusions are messages from government bodies, political parties, religious organisations and charities relating to goods or services supplied by them, and messages from educational institutions to students, former students or households of students or former students relating to goods or services supplied by them.

52 There would seem to be merit in adopting the wider approach taken by the Australian legislation as most people would consider messages as spam and undesirable if they were trying to entice people to participate in a scam just as much as if they were seeking to promote a product or service. The approach to exclusions appears to be based on the idea that there is a public interest in ensuring that certain types of messages with a social value should not be caught as spam.

Extra-territoriality

53 Given that much of the spam received in New Zealand is sent from overseas, should anti-spam legislation extend to coverage of acts outside of New Zealand? While issues of enforcement and jurisdiction arise there would seem to be merit in adopting this approach, as has been done in Australia. In the Australian legislation it provides that it extends to acts, omissions, matters and things outside Australia and that it applies to commercial electronic

messages that have an “Australian link”. Messages having an “Australian link” include messages sent from overseas to Australian email account holders.

54 There can be situations where the New Zealand vendor of a product or service arranges for spam promoting or advertising that product or service to be sent from overseas. By providing that the legislation covers acts outside of New Zealand, the New Zealand vendor can then be prosecuted notwithstanding the overseas source of the spam (and assuming that they are covered – see below).

55 In relation to enforcement against persons overseas, this would require co-operation with the authorities from the country concerned. This has occurred with other New Zealand legislation however.

Who should be covered

56 The sender of spam is not the only person who can be a party to the act of spamming. Often a vendor of goods or services will sponsor someone else to do the spamming for them. The Australian legislation has applied its legislation to not only the sender of the message but also those who cause the message to be sent, those who aid, abet, counsel or procure a contravention of the requirements and those who are in any way a party to such a contravention.

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)?
6. Do the messages caught by the legislation have to be sent/conveyed to many recipients, and if so, how many?
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?
8. Should the legislation extend to coverage of acts done overseas? If so, what acts should be covered?
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?

The Consent Issue – Opt-in or Opt-out

57 One of the main characteristics of spam is that it is unsolicited and/or unwanted. To address this issue legislators have either provided that electronic commercial messages can only be transmitted if the recipient has expressly or implicitly consented to such transmission (opt-in), or that such messages cannot be transmitted if the recipient has already taken action to indicate to the sender that such messages are unwanted (opt-out).

Opt-in

58 The opt-in approach has been the approach favoured by those opposing spam and by the majority of legislators (e.g. EU, Australia). Some anti-spam groups favour a double opt-in approach whereby the recipient must respond in 2 different ways to indicate consent. The merit of the opt-in approach is that it places the onus on those wishing to send messages and is thereby more effective in addressing the spam problem. In addition many recipients of spam are reticent to respond with a message to not send any more messages as this can represent a confirmation of an address that leads to more spam.

59 Issues that arise with the opt-in approach are:

- What conduct/relationships should amount to or be deemed to constitute implicit consent?
- What is the scope of any opt-in assent?

60 The Australian legislation defines “consent” as meaning “express consent or consent that can reasonably be inferred from the conduct and the business and other relationships of the individual or organisation concerned”. This definition does seem to create an area of uncertainty as to what conduct and relationships would result in there being a reasonable inference of consent.

61 The fact that 2 individuals know one another and have exchanged business cards including their email addresses may, of itself, not be enough to constitute inferred consent to the sending of an email about a “commercial” matter. The question is, is this too restrictive an approach or should the issue be dealt with by defining spam as being the sending of bulk messages, or the sending of messages by someone where the email address of the recipient was not given personally to the sender by the recipient or published? The Australian legislation provides that consent can be inferred from the fact that an email address has been published.

62 A further issue arises concerning the scope of any opt-in assent. If someone does respond to an email by opting in, the question arises of what this should authorise the sender to do. Should this mean that the sender can only send promotional material relating to the subject matter of the email responded to or should the sender be able to send messages relating to different subjects? Should the sender be entitled to pass your email on to other organisations? The approach of the Australian legislation seems to

relate the issue of the scope of any 'consent' to whether a particular message was expressly consented to or consent could reasonably be inferred.

Opt-out

63 The opt-out approach has been supported by some direct marketing organisations on the basis that the Internet is a legitimate and efficient way of advertising and promoting goods and services to customers or prospective customers and that its members will respect any response by an individual indicating that they no longer wish to receive such email. The opt-out approach has been adopted by the United States in its CAN-SPAM Act of 2003.

64 The problems with the opt-out approach are:

- It legitimises anyone sending emails to an individual's mailbox without any assent at all;
- There is a concern that if an individual responds to a message with an opt-out response that they will confirm their address and end up receiving more spam;
- It is seen as legitimising the sharing of email address lists by businesses with one another.

65 The above problems with the opt-out approach are seen by anti-spam groups as helping to make the spam problem worse rather than minimise it.

66 Based on the issues and arguments described above, the Government's current preference is towards an opt-in approach. However the Government is wanting feedback from interested groups on their views on this matter.

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

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?

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

Transparency Issues

67 Some of the transparency concerns that arise around spam are that the sender is not able to be identified by the recipient from the message, the message does not contain a functional unsubscribe facility, the header /subject information is misleading or inaccurate and there is no clear labelling that the message is of an advertising or adult nature. The lack of transparency associated with spam appears to be designed to avoid identification and detection and avoid anti-spam filter mechanisms.

68 The Australian legislation has specifically addressed the first two of these concerns by providing that a person must not send a commercial electronic message unless the message:

- clearly and accurately identifies the individual or organisation who authorised the sending of the message; and
- includes 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 individual or organisation who authorised the sending of the message, and such electronic address is functional.

69 The United States legislation also addresses the concern over misleading or inaccurate header and subject information by providing that it is unlawful for a person to transmit commercial electronic mail messages with materially false header information and with a subject heading that is misleading as to the content of the message.

70 Another way of requiring transparency and to assist in the filtering of spam is to require messages of an advertising or adult nature to include a label such as ADVT (for advertising) and ADLT (for adult).

71 Requiring transparency for commercial electronic messages would seem to have merit as such transparency would assist in minimising the spam problem.

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)?

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?

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

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

Privacy Issues - Address Harvesting

72 Address harvesting is the use of computer software to search the Internet for email addresses and then collect and compile those addresses. Spammers use address harvesting to obtain a list of addresses to send messages to. It does raise issues relating to privacy as in many cases the addresses obtained are from sources on the Internet where there was no intention that the addresses be available for any form of public use, such as chat rooms.

73 The Australian legislation sets out rules against the supply, acquisition and use of address-harvesting software and harvested-address lists in connection with the unlawful sending of electronic messages. The Australian approach has been adopted in order to ensure a comprehensive code against all aspects of a spammer's activities.

74 There is an argument that New Zealand's privacy legislation already provides adequate protection against the collection, transfer and use of electronic address information pertaining to an individual without their consent. However, the advantage of specific rules against address harvesting connected with spam activities is that it gives greater tools for enforcement against the actions of spammers and therefore assists to minimise the spam problem.

75 There are some problems involved in seeking to legislate against address harvesting. Address harvesting can be used for legitimate purposes and it can be difficult to determine whether the purpose of address harvesting software is legitimate or not. In addition, if the addresses being harvested are publicly made available on the Internet there is an argument that the sending of unsolicited email messages to those addresses is legitimate as any privacy rights have been forgone.

76 There is also the argument that the key problem with spam is the actual sending of spam messages rather than the collection of email addresses which, by itself, does not cause any harm.

<p>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?</p>
--

Enforcement Issues

77 The enforcement issues that arise around any anti-spam legislation concern who may bring an action, whether there should be criminal or civil penalties imposed, what should be the nature of those penalties and what types of remedies should be available.

Who may bring an action

78 The general approach to enforcement of anti-spam legislation has been to give a particular government agency primary responsibility for carrying out investigations and taking enforcement action. In Australia that agency is the Australian Communications Authority (ACA) and in the United States it is the Federal Trade Commission (FTC).

79 The approach of the Australian legislation is to give the ACA the right to bring actions for breach of civil penalty provisions and seek injunctions and undertakings while giving victims the right to join any action by the ACA to seek compensation. The approach of the United States legislation is to give the FTC the right to bring both criminal and civil actions while also giving rights to bring particular types of actions to State authorities and to the providers of Internet access services.

80 For individuals or firms that are the recipients and victims of spam, the resources necessary to carry out an investigation and bring court action are generally beyond them, hence the approach of other jurisdictions to assign primary responsibility for this to a government agency. In New Zealand, the agency best placed to take on this role is probably the Commerce Commission, which currently has the responsibility of carrying out investigations under and enforcing the Fair Trading Act. Other possibilities are the Police, Ministry of Consumer Affairs and Department of Internal Affairs.

81 The approach of the United States in giving rights of action to Internet Service Providers would seem to have merit as they can be affected by spam activities in a major way and are more likely to have the resources to take an action. In the United States, for example, four Internet Service Providers have recently taken action under the CAN-SPAM Act against six Internet marketers. There would also seem to be merit in giving victims the right to join actions for the purpose of seeking compensation.

Penalties and other remedies

82 Given the costs that spam can impose and the difficulties involved in carrying out a successful court action, the penalties able to be imposed under anti-spam legislation should be sufficient to be able to serve as a deterrent.

83 The penalty options include the imposition of a civil pecuniary penalty (e.g. Australia) and the imposition of a fine or a term of imprisonment (United States).

84 In terms of the amount of any penalty or fine, the New Zealand Fair Trading Act is one possible guide. Under that Act a contravention can result in a maximum fine of \$60,000 for individuals or \$200,000 for bodies corporate. The maximum penalties under the Australian Spam Act are quite substantial, being \$220,000 for a single day's contraventions and \$1.1m for further breaches.

85 A further issue is whether the penalty should be in the form of a civil pecuniary penalty or in the form of a fine and/or imprisonment as part of an offence provision. The Commerce Act, for example, imposes civil pecuniary penalties for contraventions of many of its provisions with the ability to seek damages for consequential loss as well as exemplary damages also included. The Fair Trading Act, on the other hand, provides that any person who contravenes specified provisions commits an offence and is liable on summary conviction to a fine.

86 One of the differences between taking the civil penalty approach and the criminal offence approach is that concerning the required standard of proof. For civil proceedings the standard is on the balance of probabilities while for criminal proceedings it is beyond reasonable doubt, which is a stricter standard.

87 Other possible remedies include the ability to seek injunctions against the actions of spammers as well as the ability of victims to seek compensation or damages and the ability to seek exemplary damages.

Powers of investigation

88 Another issue is what powers should be given to the investigating authority. Under the Fair Trading Act and Commerce Act, for example, the Commerce Commission is given the ability to obtain search warrants to investigate possible contraventions of those Acts. These search warrants confer powers of entry, search, and seizure of evidence in the form of documents and goods. If enforcement is to be effective it would seem that there is merit in the investigating authority having the ability to obtain search warrants.

18. Who should be able to bring an action against an alleged spammer?
19. What agency should have the enforcement role under the legislation?
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?
21. Should contraventions give rise to criminal or civil penalties?
22. Should the responsible enforcement agency be given the ability to obtain search warrants conferring powers of entry, search and seizure?

Responses to Discussion Paper

87 Comment on the issues raised in this paper should be sent to:

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

Email: spamsubmissions@med.govt.nz

88 Comments should be received by **30 June 2004**.

Official Information Act 1982

89 The content of submissions provided to the Ministry in response to this discussion document may become subject to public release under the Official Information Act 1982. Please advise if you have any objection to the release of any information contained in a submission to this discussion document, and in particular, which part(s) you consider should be withheld, together with the reason(s) for withholding the information. The Ministry will take into account all such objections when responding to requests for information on submissions to this document under the Official Information Act 1982.

Privacy Act 1993

90 The Privacy Act 1993 establishes certain principles with respect to the collection, use, and disclosure of information about individuals by various agencies including the Ministry. It also governs access by individuals to information about themselves held by agencies. Any personal information you supply to the Ministry in the course of making a submission will be used by the Ministry only in conjunction with consideration of matters covered by this document. Please clearly indicate in your submission if you do not wish your name to be included in any summary of submissions that the Ministry may publish.