

Legislating against Unsolicited Electronic Messages Sent for Marketing or Promotional Purposes (Spam)

Regulatory Impact and Business Compliance Cost Statement

December 2004

Nature and Magnitude of the Problem and the Need for Government Action

1. Spam is generally described as unsolicited electronic messages, usually in the form of commercial marketing emails. Most of the spam received in New Zealand originates from overseas. According to New Zealand internet service providers (ISPs) and anti-spam solution companies, spam accounts for about 40% to 75% of all email traffic (estimated at over 350 million messages per month). While effective filtering reduces the overall quantity of spam reaching the end user, this is merely a movement of the burden from the recipient to the ISP, not a solution.

2. The problems associated with spam include the annoyance and loss of time involved for users in dealing with large quantities of unwanted emails, the consequent loss of user confidence in dealing with business and other communications online, the consumption of network and computing resources as well as email administrator and helpdesk time, and the loss of worker productivity (United States research has shown that spam results in a 1.4 percent loss in office worker productivity – a similar level of loss of productivity is expected in New Zealand). Spam is also associated with attacks on the security and integrity of computer networks through viruses and the like, identity theft (e.g. emails seeking personal information from users and masquerading as emails from a bank), and the sending of offensive or indecent material.

3. Existing laws, which can generally deal with spam content issues such as offensive or misleading material, are not specifically designed to deal with the problems associated with large spam volumes or mass e-marketing, and technical solutions do not alleviate the load of spam on the Internet infrastructure before it reaches the recipient's ISP.

4. Without Government action to address the problem of spam New Zealand risks being seen as a safe haven for spammers, as other countries progressively pass anti-spam legislation and there is the consequent risk that legitimate email traffic from New Zealand to other countries could be blocked without sufficient verification. New Zealand also currently lacks a basis from which it can enter into bilateral or multilateral agreements to have spam coming into New Zealand from overseas sources investigated and action taken by these partner countries.

Public Policy Objective

5. The public policy objective is to create a safe and secure environment in New Zealand for the use of information and communication technologies (ICT), in line with the Government's draft Digital Strategy. The specific policy objectives are to:

- Minimise the level of spam entering New Zealand;
- Facilitate participation in international efforts to address the spam problem at a global level;
- To provide a firm basis for New Zealand to seek and give cooperation from and to overseas government anti-spam enforcement agencies to combat spam sent from overseas to New Zealand;
- Prevent New Zealand from being seen or used as a safe haven for spammers;
- Minimise the costs for legitimate businesses that arise from spam; and
- Promote the adoption of good e-marketing practices.

Statement of the Feasible Options (Regulatory and Non Regulatory) that May Constitute Viable Means for Achieving the Desired Objectives

6. Details of the options for enforcement of the legislation and the enforcement agency will be presented in a separate Cabinet Paper.

Status Quo

7. The current regime includes existing legislation, self-regulation, industry and user education and technical measures.

Existing Legislative Framework

8. The existing legislative framework for addressing issues associated with spam in New Zealand comprises the following:

- **Computer network security and integrity** – Section 250 of the Crimes Act 1961 provides that it is an offence to intentionally or recklessly damage or interfere with any data or software in a computer system or cause any computer system to fail or deny service to authorised users. This provision deals with the concern that some spam is used to transport computer viruses or to launch denial of service attacks on computer systems;
- **Misleading and deceptive messages** – Misleading and deceptive conduct and false or misleading representations by persons in trade are addressed by sections 9 and 13 of the Fair Trading Act 1986. These provisions can be used to deal with emails sent by businesses which are misleading in nature or make false or misleading claims in relation to a good or service;
- **Forgery/Fraud** – Sections 256 and 257 of the Crimes Act 1961 provide that it is an offence to make or use a false document with the intention of using it to obtain any benefit or advantage. This provision would apply to email scams which involve false email documents sent to elicit money out of the recipient on the basis of a false promise;
- **Privacy** – The Privacy Act 1993 provides rules against the collection, transfer and use of electronic address information pertaining to an individual without their consent or knowledge unless the information is already publicly available. It would be a breach of the Privacy Act for a business to collect a customer's email address without their knowledge or to sell a list of customers' email addresses without authorisation;
- **Pornographic/offensive material** – Section 123 of the Films, Videos, and Publications Classification Act 1993 provides that it is an offence to make or supply an objectionable publication, including objectionable material by way of email;

- **Harassment** – The Harassment Act 1997 provides that where a person is sending emails as a pattern of behaviour designed to harass another person then action can be taken against the sender.

Self Regulation, Industry and User Education, and Technical Measures

- **Self regulation** - In New Zealand the Direct Marketing Association (DMA) has developed a set of standards for email marketing by its members to promote consumer confidence in eCommerce and ensure that proper account is taken of consumers' right to privacy. ISPs in New Zealand will generally not tolerate spammers operating from their networks and will have them removed.
- **Industry and user education** - The Internet Society of New Zealand (InternetNZ) is active in the area of industry and user education and awareness, and has set up a website for helping to deal with spam.
- **Technical measures** - An ISP can use a spam filter at its server which means that users will not see spam that is filtered out.

On its own the status quo cannot achieve the public policy objectives.

Multi-Pronged Approach Including Specific Anti-Spam Legislation – Preferred Option

9. This option also includes the measures outlined under the “Status Quo” option. It is proposed that a new Act will be developed. Within legislation to combat spam, there are several key issues, each of which may have various options. The key features of the preferred option are:

- The legislation would prohibit the sending of unsolicited “commercial” electronic messages sent for marketing or promotional purposes, where:
 - “unsolicited” means that the recipient has not expressly or implicitly consented to such transmission (opt-in). Implicit or inferred consent is defined as being consent that can reasonably be inferred from the conduct and the business and other relationships of the individual or organisation concerned, for example, the act of handing over a business card or a bank-customer relationship.
 - “commercial marketing and promotional” means for the purpose of marketing or promoting goods, services, land or an interest in land, a business or investment opportunity, or for the purpose of assisting or enabling a person, by a deception, to dishonestly obtain a financial advantage or a gain from another person.
 - “electronic” effectively means in the form of email, instant messaging and text messaging, as facsimile messages and voice calls are excluded.

- The legislation would prohibit the sending of non-commercial electronic marketing messages where:
 - “non-commercial” means the primary purpose is to promote an organisation’s aims or ideals (for example, a political, religious or charitable organisation seeking support for their cause), **and**
 - the recipient has previously specifically opted out from receiving such messages from the sender.
- A number of matters, such as quotes, estimates, providing warranty or product recall information, will be excluded from the prohibitions and requirements in the legislation.
- The legislation would also regulate the sending of all electronic marketing or promotional messages. Messages would be required to have:
 - accurate sender information, and
 - a functional unsubscribe facility (which means that there is a working, clearly visible means of opting out of future mailings).
- The legislation would apply to all messages generated within New Zealand and all messages to a New Zealand email address whether generated in New Zealand or overseas.
- All parties knowingly involved in the act of spamming, including the vendor sponsoring the spamming would be committing an offence under the Act.
- Express statutory exemptions would be put in place for telecommunications network operators and ISPs where messages are transmitted over their networks in contravention of the legislation without their knowledge, and in relation to unsolicited messages being sent by mistake or unknowingly by the address holder’s computer such as where a computer has been infected by a virus.
- The legislation would prohibit the supply, acquisition, and use of address-harvesting software and harvested-address lists in connection with the unlawful sending of marketing or promotional electronic messages.
- The number of messages sent will be a relevant factor in determining what penalties would apply but it will not form part of the definition of spam.
- There will be a four month transition period.

Other Options

10. The following aspects for the proposal were considered and not preferred or discarded:

- To include faxes and telemarketing as they are also used for the sending of unsolicited marketing and promotional messages. However, there does not currently appear to be a sufficient problem in this area to warrant regulation, and moreover the costs of sending messages via these mediums are largely borne by the sender rather than the recipient or ISP.
- To adopt the sending of a minimum quantity of messages in the definition of spam. For example, in United States legislation, spam is defined as multiple commercial electronic messages, where multiple means more than 100 electronic messages during a 24-hour period. The critical factor, however, with spam is its unsolicited nature rather than its quantity, and it would be easy for spammers to circumvent minimum number restrictions through minor distinctions between messages sent to different addressees.
- To have the legislation apply to all unsolicited electronic messages or all unsolicited “commercial” (as defined under Australian legislation) electronic messages. Extending coverage of anti-spam legislation to all types of unsolicited messages raises difficulties in terms of rights of freedom of speech and creates legality problems for the use of email as a general form of communication. In addition, regulating all “commercial” electronic messages as it is defined under the Australian legislation imposes widespread compliance costs as it requires small businesses to ensure that communications with existing and potential customers, including quotes and invoices, meet minimum requirements.
- To adopt an opt-out approach to consent for commercial messages. Under an opt-out regime, messages can be transmitted until the sender receives an indication from the recipient that they no longer want to receive such messages. The strongest arguments for the opt-out approach are that it would avoid uncertainty around what may or may not amount to consent, and that the opt-in approach places much of the compliance burden on legitimate businesses which have nothing at all to do with spam problem. However, this approach for commercial messages is not supported because:
 - It places the onus of addressing the issue of consent on the recipient of the message.
 - As long as unsolicited commercial emails meet all other requirements, the opt-out approach gives spammers at least one free hit at mailboxes for a particular product, in effect legitimising spam.

- It is seen as legitimising the sharing of email address lists by businesses with one another.
- To have criminal penalties instead of civil penalties. However, unsolicited marketing messages do not cause sufficient harm or damage to warrant criminal sanction, and a criminal penalty would require proof beyond reasonable doubt (which may be difficult to establish), whereas a civil penalty would only require proof on the balance of probabilities.

Statement of the Net Benefit of the Proposal, Including the Total Regulatory Costs (Administrative, Compliance and Economic Costs) and Benefits (Including Non-Quantifiable Benefits) of the Proposal, and Other Feasible Options

11. In the short to medium term, there is unlikely to be any significant reduction in the level of spam received. Combating spam requires harmonisation of global legislation and international cooperation; however, not all countries have anti-spam legislation or have multilateral agreements to cooperatively address the problem. Also anti-spam legislation in most countries has only been introduced in the past year or so and therefore has not yet been able to realise their full potential. Only aggressive enforcement of anti-spam legislation on a global basis will reduce spam levels in the longer term.

To Government

12. For the Government, enacting specific anti-spam legislation has the main benefits of:

- assisting to build confidence in the use of ICT for government purposes by minimising the negative effects of spam on ICT use – such purposes include the effective and efficient delivery of services to citizens online which reduces costs for government;
- ensuring New Zealand is being seen internationally as a responsible citizen by participating in multi-national efforts to deal with the global problem of spam.

13. The cost to Government is the cost of, providing written guides to the legislation, and administering and enforcing the legislation. Details of the cost to Government will be submitted to Cabinet in a separate paper, along with the enforcement options.

To Businesses

14. The main benefits to businesses are:

- in the longer term, a reduction in the level of spam received with consequent benefits for productivity and the costs of dealing with spam; and
- maintaining and furthering the integrity of and general confidence in electronic communication as a means of doing business with the

consequent benefit of enabling businesses to operate more efficiently and reach a wider market base.

15. The costs to businesses are:

- The compliance costs associated with the legislation – see the attached Business Compliance Cost Statement;
- The costs associated with the lost opportunity caused by placing a restriction on the advertising practices of businesses (although such a restriction is in accordance with good e-marketing practice) by prohibiting businesses from sending e-marketing messages advertising their goods and services to prospective new clients who have not given their consent to such messages being sent.

16. For those businesses that already follow e-marketing best practice (these tend to be the banks, large corporations and direct marketers) the proposed legislation is likely to have very little, if any, impact.

To ISPs

17. The benefit for ISPs is, in the longer term, a reduction in the volume of spam being sent over their networks meaning a lesser burden on bandwidth and network infrastructure. ISPs will also benefit from their customers having greater confidence in email services if spam volumes are able to be reduced.

18. ISPs will face the cost in terms of the limits on e-marketing applying to businesses generally.

To Society

19. For individuals in society, not only will they ultimately benefit from having to waste less time dealing with unsolicited messages (once volumes are reduced in the long term), but they will also potentially receive less messages with objectionable material, scams or viruses. There is also the benefit that electronic communications as a viable form of communicating is able to be maintained and developed if spam volumes are able to be curbed.

20. On the other hand, in restricting the ability of businesses and others wishing to send commercial marketing or promotional messages, the freedom of individuals to send and receive information is restricted.

Consultation

21. Consultation took the form of submissions to a discussion paper and an industry workshop. Forty-three submissions were received from industry and specialist groups, businesses, ISPs, telecommunications companies, government agencies and individuals.

22. There were two areas of concern for some respondents. Some respondents preferred industry self-regulation; however, they appreciated the need for legislation for global cooperation and to prevent New Zealand from becoming a haven for spamming. The other concern would be that the sending of unsolicited non-commercial promotional messages from political, religious and charitable organisations has not been prohibited. However, this will be addressed to some extent by the requirement for these messages to have an unsubscribe function to allow recipients to opt-out of receiving further messages in the future.

23. The following government agencies were consulted: Commerce Commission, Department of Internal Affairs, Department of Justice, Ministry of Consumer Affairs, Ministry of Economic Development – Legal, and Regulatory and Competition Policy, State Services Commission, and Treasury.

24. The above government agencies did not have any significant concerns with the preferred option.

Business Compliance Cost Statement

25. For businesses involved in direct marketing or the sending of promotional messages by electronic means there will be an initial cost while they move to best e-marketing practice if they have not already done so. This will involve:

- Ensuring their address lists are opt-in based or that an appropriate business or other relationship exists. The actual cost of this is unlikely to be significant as only a small number are likely to be impacted and the costs for those who are impacted are likely to be in the nature of a day or two of a staff member's time. In addition, where email addresses are for natural persons the Privacy Act already requires that they only be held for the purpose for which they were given.
- Ensuring that electronic marketing or promotional messages contain accurate sender identification and include a functional unsubscribe facility (a working, clearly visible means of opting out of future mailings). This mechanism may simply involve instructing the recipient to return the email with "unsubscribe" in the subject field or providing a link to perform this task automatically if the recipient wishes to unsubscribe. To comply with this requirement an email template change at trivial cost is all that would be required.
- Setting up a system for ensuring that lists of email addresses for marketing or promotional purposes are up to date and comply with the legislative consent requirements.
- Learning the new requirements

26. Ongoing compliance costs would be the administration costs involved in maintaining an up to date email address list for marketing or promotional purposes. This would simply mean acting in accordance with best e-marketing practice and may already be part of most businesses administrative practices.

27. The parties likely to be affected by the legislation are businesses that send electronic marketing or promotional messages. It is unclear how many parties are likely to be affected as no data is kept on this. It would certainly cover all businesses involved in direct marketing online such as banks, insurance companies and retailers who keep customer email lists.

28. The estimated compliance costs will vary for each business will range from zero for those who already comply with best practice to potentially one-off costs of \$1,000 – \$2,000 for larger businesses that need to make changes to their systems to ensure ongoing compliance. The ongoing administration costs are likely to be minor and part of the wider marketing function already provided for.

29. Steps taken to minimise compliance costs will include educating business on best practices of e-mail marketing and on cost effective means of carrying

out best practices and complying with legislation. A four-month transitional period will be provided to allow time to adjust to the new requirements. The definition of “spam” has also been limited to marketing and promotional electronic messages which is narrower than in Australia where all commercial messages relating to an offer of goods or services (e.g. quotes and invoices) are caught by its anti-spam legislation.