



TelstraClear Limited

**Submission on Ministry of Economic Development
Discussion Paper *Legislating Against Spam***

30 June 2004

1. Introduction

TelstraClear welcomes the opportunity to provide a submission on the approach New Zealand should take to dealing with the problem of spam. Spam is a significant problem for our company and our customers. We welcome the announcement by Hon David Cunliffe at the 29 June 2004 Anti-Spam Workshop that the Government intends to introduce anti-spam legislation later this year.

TelstraClear considers that anti-spam legislation is an important element of what needs to be a multi-pronged approach to successfully combating spam. Legislation is needed to prevent New Zealand becoming a base for spammers and to provide the ability for the Government to participate in international co-operative efforts to combat spam. Legislation should be targeted at unsolicited messages that users have not consented to that are sent via email, internet/instant messaging and small messaging services (SMS) on mobile phones. The legislation should require that, before sending a promotional message, senders must obtain or be assured they have the consent of the intended recipient to be sent the message, ie "opt in".

The enforcement provisions of the legislation should target spammers and should not target innocent third parties such as telecommunications companies and ISPs that unknowingly transmit spam through their networks and systems. Spam imposes significant costs on both our company and our customers and we do not consider it appropriate to be further penalised for the actions of others, especially when we have taken all practicable steps to eliminate the problem.

International co-operation is another key element of a successful approach for combating spam. International co-operation is vital as spam is a truly international problem that no country is able to address by itself. TelstraClear would strongly support any initiatives by the Government to promote and participate in international efforts to address this problem.

Other key elements of an effective anti-spam effort are industry self-regulation and technological solutions. TelstraClear has in place significant anti-spam measures to limit the amount of spam received by our customers. Technology may eventually provide solutions that significantly reduce the problem of spam but other actions are needed as well to ensure that it does not re-emerge as a significant problem.

TelstraClear is actively participating in industry initiatives to combat spam. This includes the work by Internet New Zealand to combat spam

and an initiative by the Telecommunications Carriers' Forum to develop an anti-spam code for mobile phone SMS messages.

Following below are our responses to the specific questions posed in the discussion document. We would be happy to further elaborate any of the points made in this submission, if required.

2. Responses to discussion paper questions

General

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

Spam is a significant issue for TelstraClear. As the discussion document notes, spam has many detrimental affects and associated costs. It accounts for a significant portion of email sent to clear.net and paradise.net customers. Because of our customers' concern about this we have committed significant resources to filtering our customers email, configuring our infrastructure and providing on going helpdesk support to cope with spam.

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

While our preference would be to rely on industry self-regulation and general legislation such as the Privacy Act and the Harassment Act, these approaches have their limitations, especially in relation to enforcement. In particular, approaches such as industry codes of practice generally rely on voluntary membership and therefore are limited in their ability to take enforcement actions against producers and distributors of spam that choose not to sign up to such codes. As noted in the discussion document, enforcement under general legislation is problematic. For these reasons, we believe anti-spam legislation has its place.

We note that most other OECD countries have some form of anti-spam legislation. Spam is an international problem and international co-operation is required to address spam effectively. Having anti-spam legislation in New Zealand will prevent New Zealand becoming a safehaven for spammers and is likely to be a key requirement for participating in a co-ordinated international anti-spam initiative.

Existing Legal Framework

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

Our view is that existing privacy protections, including the Privacy Act and Telecommunications Information Privacy Code 2003 are effective in addressing some of the privacy issues with respect to spam but not all. The main problem is that these protections do not appear to be effective in dealing with the problem of address-harvesting software, as we note below. In addition, the protections under the Privacy Act provide no safeguard against misuse of private information outside of

New Zealand. Also, as the discussion document notes, the Privacy Act does not apply to corporate entities but they too have to cope with the problem of spam.

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

In principle, generic legislation would be preferable to specific legislation because of the difficulty of designing and drafting legislation that adequately addresses a specific problem like spam, especially in a rapidly evolving area such as information technology. However, as the discussion document points out, spam is generally of a different nature to what is defined as harassment under the Harassment Act in that it is not directed at an individual and its purpose is not to pester, torment or trouble someone, even if that is its effect. We also agree with the point in the discussion document that the remedy available under the Harassment Act, which focuses on stopping the harassment of particular individuals, may not be appropriate for spam. Specific stand-alone legislation is therefore needed to address the specific issues that arise in relation to spam.

Legislative Issues

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)?

Our view is that any legislation should be targeted at the problem that has been identified, ie electronic messaging, ie emails, internet/instant messaging and short messaging services using mobile phones. There is a risk of unintended consequences if the legislation is made broader than this (ie to include faxes, telemarketing and physical mail), especially since these other activities cover legitimate forms of marketing.

A key reason why anti-spam legislation should apply to electronic spam but not other forms of marketing is that the costs of electronic spam are borne directly by the end-user, ISPs and telecommunications companies and not the spammer. This means that there is no financial disincentive to limit the amount of spam, unlike mediums where the generator of the material has to pay for the costs of its distribution, eg direct mail.

We would also note that, in relation to mobile phone SMS messages, the Telecommunications Industry Forum is currently preparing an industry code on this issue. Our intention with this code is that it will be complimentary with any anti-spam legislation, focussing primarily on

the behaviour of mobile network operators and providers of SMS advertising services prepared to sign up to the code, while the focus of anti-spam legislation should be on the behaviour of spammers. While it might be argued that the cost of accessing mobile networks will prevent SMS spam from becoming a significant problem, bulk texting packages can be abused, as was demonstrated recently by the behaviour of some users in response to Telecom's unlimited text campaign. In addition, the internet can be used to route SMS messages via overseas telecommunication providers onto New Zealand mobile networks, which may provide opportunities for SMS spam.¹

Any legislation should be drafted so it is able to cope with changes in technology, especially in a rapidly changing area like electronic communications. It is quite possible that technological change will mean that a technology that is that is invulnerable to spam at present will be vulnerable in the future.

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

The characteristic that separates spam from other unsolicited and unwanted messages is that it is sent in bulk and this is a major reason why it is a problem of such significance that legislation needs to be considered. However, technology means messages can be individualised, which may mean that a definition that includes volume would be ineffective. Moreover, many legitimate messages are sent to large numbers of addressees so it is important that the definition of spam is not restricted to its volume characteristics. For example, we send electronic newsletters to our customers that inform them about changes to our service. Our view is that it is important that the definition of spam should be drafted to exclude such communications.

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?

From an ISP's and telecommunication company's point of view, the cost impact of spam on our infrastructure is the same regardless of its nature. However, there are likely to be a range of attitudes amongst our customers to different types of spam, eg while spam of a religious nature may be acceptable to one customer it may not to another. Equally, spam that solicits support for a particular charity may be acceptable to some customers but not to others. Even if it is of an

¹ See, for example, the 20 June 2004 *Dominion Post* article "Vodafone's SMS undercut".

altruistic nature, it will still have negative cost consequences for ISPs and telecommunications companies and, ultimately, users.

For these reasons, we consider that the definition of spam should not be limited to material that is of a commercial or promotional nature. Other than its bulk, the other key characteristic of spam that should be captured in its definition is that it is unsolicited. A key reason why spam is widely viewed as a problem is the fact that users have not requested it and the definition of spam should reflect this. As we will argue below, material that end-users elect to receive should not be considered as spam, including material that is of a commercial or promotional nature.

If spam is defined as material of a commercial or promotional nature, we think the definition should exclude material that we send to customers on our network where customers have opted to receive that material. The infrastructure costs of sending such material are borne directly by us or indirectly through interconnection charges if the material is sent across other telecommunications networks.

Should there be exceptions and if so what should be exempted?

The definition of spam should exclude messages broadcast by ISPs and telecommunications companies to their network customers that are required for the effective operation of their network. Defining spam as unsolicited promotional messages that end-users have not consented to would achieve this. The inferred consent provisions in the Australian Legislation also appear to cover such messages and we support such an approach.

An opt-in requirement should be adequate to deal with other sorts of messages. For example, we send product information to our customers and this is covered in our terms and conditions for providing internet services.

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

Yes, as the majority of spam on New Zealand networks originates from overseas. However, we acknowledge that there are likely to be significant jurisdictional issues that will require the Government to work with other governments to address this problem.

If so, what acts should be covered?

Our view is that the acts covered extra-territorially should be the same as those covered domestically. The approach in the Australian Spam Act 2003 seems to provide a useful model here, in that that Act applies to any messages to or from or via Australia.

9. Should all parties involved in the act of spamming, such as the vendor sponsoring the spamming, be covered by the legislation?

Our view is that any legislation should cover both those sponsoring and generating spam.

Should there be express exceptions such as for telecommunications companies and ISPs?

Legislation should expressly exclude telecommunications and ISPs that are not aware of the exact nature of the content passing through their systems. This should particularly apply to those telecommunications companies and ISPs that have taken all possible practicable steps to prevent customers receiving and sending spam.

We believe we have significant commercial incentives to prevent spammers operating on our network. In particular, international blacklist organisations blacklist ISPs that they believe are hosting spammers and some spam-filtering software prevents end-users receiving messages sent from ISPs that are on these blacklists. For this reason, included in our terms and conditions is a provision that customers should not use our systems for sending spam.

Another key reason why ISPs and telecommunications companies should not be targeted by anti-spam legislation is that it is not appropriate that we should be held responsible for the actions of other parties when we do not have an ability to prevent them taking actions such as spamming.

Consent Issues

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

If the purpose of anti-spam legislation is to prevent spam an opt-in approach is preferable. As the discussion document suggests, an opt-out approach seems to legitimise an initial unsolicited broadcast message that users have not consented to, which most users would consider as spam.

To minimise compliance costs, we think that a single opt-in is preferable. A double opt-in provision would increase compliance costs and carries the risk of prosecution for unintentional inadvertent failure to comply with follow-up requirements.

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?

Our view is that the approach in the Australian legislation for express and inferred consent provides a good model for both types of consent.

Express consent involves an addressee taking any action that amounts to a specific request for messages from the message sender, eg subscribing to a mailing list.

Inferred consent involves any action by the addressee with respect to the sender and/or relationship between the addressee and the sender that would imply that the addressee would reasonably expect to receive messages from the sender. Examples could include provision of a business card, joining an organisation or purchasing a service and providing address details, or publication of an electronic address. However, in the case of the latter, we would note that a business publishing its electronic address would only reasonably expect to receive messages directly relevant to that business, eg a plumber that had provided an email address in a phonebook might reasonably expect to receive offers for gas cutting equipment but not pornography.

These examples suggest that inferred consent implies that message senders must actively consider whether the person would reasonably expect to receive the information they intend sending, which spammers do not do.

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

The broader the scope of an opt-in assent allowed, the less successful the legislation will be in preventing spam. However, we note that a narrow opt-in assent provision is likely to increase the overall costs of any legislation, though of course this will help deter the use of spam. We support the approach in the Australian legislation that limits consent to either express consent or whether consent can be reasonably inferred.

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)?

A requirement for accurate identification of the sender is a pre-requisite to successful prevention of spam as it gives users the opportunity to communicate with the sender and indicate whether they wish to continue to receive material.

Accurate identification should preferably include name, physical address and telephone number. In the case of SMS messages, it may not be possible to provide all this information but a name and phone number would seem to be the minimum. It is important that the sender information is provided in a form that is clearly readable. It is also important that the information provided relates to the person responsible for sending the message and relates to the actual physical address and phone number where the sender can be and is capable of being contacted.

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 – this should be a requirement for all messages included under the definition of spam and it should be effective in enabling users to remove themselves from the list and not receive any more such messages. This requirement should not result in a charge to the end user other than to the extent it has an incidental effect on a user's normal costs of purchasing internet services.

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

While there may be some merits in such a requirement, it may be difficult to comply with and enforce. A better approach may be to require that header and subject information should not be misleading and should reflect the material contained in the body of the message. However, if an opt-in approach is adopted such a requirement seems unnecessary.

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

If an opt-in approach is adopted then this requirement would not be necessary for general advertising material. Imposing this requirement on adult material would allow users to filter out such material if they had elected to receive it but at the same time prevent children viewing it. If an opt-out approach is adopted this approach should be

a requirement for both promotional and adult messages as it would allow users and ISPs to filter out such messages.

Privacy Issues

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?

Removing the ability of spammers to obtain and use address-harvesting software for the purpose of spamming is an important element of any anti-spam legislation. While the Privacy Act should be adequate to address the privacy concerns in relation to individuals, the fact that many New Zealanders receive spam suggests that address-harvesting software is being used in a manner that contravenes the Privacy Act. Even if the Privacy Act were effective for addressing these concerns for individuals, its provisions do not extend to corporate entities where similar concerns about address harvesting exist. In particular, spam also imposes costs on corporate entities and, while corporate entities make available contact details for commercial purposes, such information is not provided so businesses' addresses can be harvested so they can be sent spam.

Enforcement Issues

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

We support the approach proposed in the discussion document of, at a minimum, giving a government agency the primary enforcement role.

While there are arguments in favour of giving ISPs and telecommunications companies the ability to take actions against spammers – principally, the significant cost of spam to us and that such an approach could help overcome any enforcement resourcing problems – we would prefer not to have the ability to take enforcement action. This is because we think there is a risk that customers will put the expectation on us to take enforcement action rather than the enforcement agency. However, it is crucial that the enforcement agency is adequately resourced.

There is a risk that providing end-users with the ability to take actions may result in vexatious actions, though the costs of taking such an action may help prevent this.

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

Our preference is either the Department of Internal Affairs or the Ministry of Economic Development (which we note has some similar enforcement responsibilities to the Australian Communications Authority that enforces the Australian Spam Act.)

While we understand the argument for the Commerce Commission having this role, we have concerns about the adequacy of resourcing for the Commission for its competition role and therefore would prefer that anti-spam enforcement be given to another agency.

Unless it is proposed that spamming is considered a criminal act, which does not seem appropriate (apart from for related actions, such as fraud, that are already covered by criminal law), our view is that it would also not be appropriate to give this role to the Police.

Because the impact of spam is not just on consumers but on corporate entities as well, the Department of Consumer Affairs does not seem appropriate.

Whichever agency is given the enforcement role it is important that the agency is adequately resourced to effectively carry out this function.

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?

We agree with the principle that the penalties of anti-spam legislation should be sufficient to serve as an effective deterrent. Given the financial gains that can be achieved from sending spam the penalties will need to be sufficiently large that the incentives to comply exceed the incentives not to. The Australian legislation may provide a guide on the size of penalty.

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

While spam is a significant problem for us, we consider that civil penalties should be adequate. Relative to other computer offences, eg denial of service attacks and transmission of computer viruses, spamming is not of the same level of seriousness and therefore does not seem to warrant criminal penalties.

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

These requirements would seem to be essential for any anti-spam legislation to be effective. However, we emphasise that these provisions should not apply to innocent third parties such as ISPs or telecommunications companies. We are happy to assist in any way we can in enforcement actions against spammers and do not think that heavy handed measures are necessary to encourage us to do this.