
Legislating against Spam

A response to Discussion Paper dated 17 May 2004

Telecom Corporation of New Zealand Limited

30 June 2004

SUBMISSION**30 June 2004****To:**

IT and Telecommunications Policy Group
Email: spamsubmissions@med.govt.nz
Resources and Network Branch
Ministry of Economic Development
PO Box 1473
Wellington

This submission is made on behalf of:

Telecom Corporation of New Zealand Limited (*Telecom*)
PO Box 570
Wellington

Telecom Corporation of New Zealand Limited is the parent company of the Telecom group of companies. Telecom provides a full range of telecommunications products and services including a comprehensive range of Internet, e-commerce, data and telecommunications solutions for business and residential customers.

Telecom has reviewed the Discussion Paper and has developed its responses with a view towards ensuring that regulation of spam balances the need to meet legitimate community concerns, while ensuring that regulation does not impose onerous or unjustifiable burdens on Internet Service Providers (ISPs) and other industry participants.

Telecom would welcome the opportunity to discuss any of its attached submissions with the Select Committee in person, should that be helpful.

SUBMISSIONS ON DISCUSSION PAPER: LEGISLATING AGAINST SPAM

INTRODUCTION

Telecom strongly supports the primary objective of the Discussion Paper, which is to develop an approach to tackling the problem of spam through specific legislation. Telecom agrees that it is now timely to look at how legislation in this country might effectively contribute to minimising spam, given that spam is now a huge, and growing, problem worldwide.

As the largest carrier of electronic messages to New Zealand consumers and businesses, principally through its Xtra brand, Telecom is a significant stakeholder in any discussion about spam and is well placed to contribute to the discussion on the scope of the current spam problem and the utility and consequences of any potential legislation.

Set out below are Telecom's responses to the specific questions posed in the Discussion Paper, along with some more general comments and recommendations on how the spam problem should be addressed.

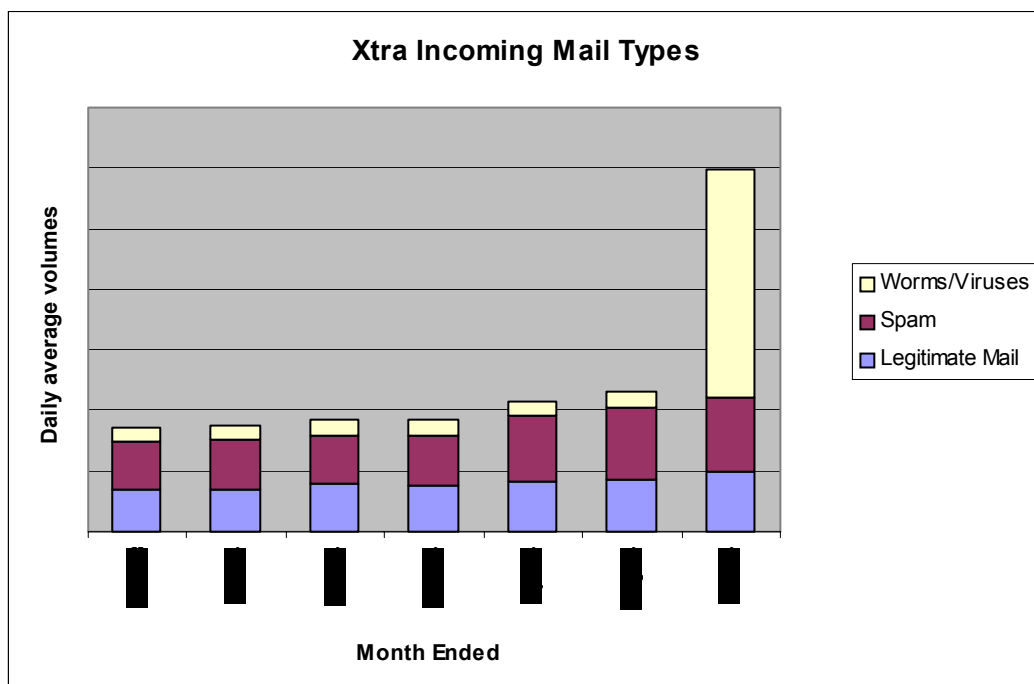
PART A: SCOPE OF PROBLEM

1 *Q1. DO YOU CONSIDER SPAM TO BE AN IMPORTANT ISSUE? HAS IT SIGNIFICANTLY AFFECTED YOU IN ANY WAY?*

- 1.1 Telecom, and, judging from feedback it has received, the vast majority of Telecom's customers, consider spam to be a serious issue that presents a significant and growing threat to email usage and traffic, currently the most important Internet application.

Volumes of spam

- 1.2 Telecom's ISP Xtra receives more spam than legitimate email and the spam component is growing faster. The following chart illustrates the current scale of the problem – and the pace at which it has grown in the past few months:



- 1.3 The area of major impact for Telecom is resource usage, as spam accounts for more than 50% of inbound traffic to Xtra. Recently, Xtra identified 85 per cent of incoming mail in one day as either worms or spam. Increased resource requirements mean higher costs to Telecom. As New Zealand's largest carrier of email, Telecom has observed that spam has caused significant resourcing and service issues, as the problem consumes network and computing resources, email administrator and helpdesk personnel time, and reduces worker productivity. Inevitably, the large costs associated with these increased resourcing requirements must be passed on to the more than 500,000 New Zealanders that use Xtra.
- 1.4 Service quality is also periodically degraded by the large volumes of spam, as mail capacity and delivery times for legitimate messages are significantly impacted, leading to customer dissatisfaction. The increasing spam problem has also led Telecom to take more stringent measures to protect its network and customers, for example, by blocking IP addresses, which increases the risks of not delivering legitimate mail.

Sources of spam

- 1.5 It is widely recognised that one of the primary reasons spam is such a global problem is the fact that it is so difficult to accurately identify the true originating source of spam messages. In most cases spam messages do not appear to be sent by identifiable large scale spam operators but rather from individual Internet users whose PC's have been "taken over" without

their knowledge and used to send spam messages without detection. Telecom believes the sources of spam will continue to be highly dispersed.

- 1.6 Telecom's customers have experienced a significant problem with the recent wave of worms and viruses compromising their machines, and are therefore potentially being used as part of a "zombie" network to send out spam.
- 1.7 This trend makes it harder for Telecom to manage spam for its customers because spam can increasingly come from any address on the Internet. This is in marked contrast to email viruses/worms where the standard method of finding new targets is reading addresses of the infected machine's address book, which tends to result in worm attacks following the same patterns as regular email traffic.

Harm caused by spam

- 1.8 The costs of dealing with spam fall disproportionately on both the carrier and the receiver of spam rather than the sender. The actual cost of sending spam, together with the often illegitimate techniques employed to distribute spam means that the natural economic limitations that work to some extent for physical mail or texting do not apply.
- 1.9 While anti-spam vendors provide figures for the costs of dealing with spam, Telecom has found them at times to be unrealistic, as they are based on lost opportunity costs calculated at US rates. However, Telecom is aware that the problem of spam creates real harm and provides some examples here:
 - Internet user time, sorting and deleting mail;
 - ISP time and resources to carry and manage spam;
 - Loss of reputation for email as a message medium;
 - Offensiveness, particularly where adult content or products are promoted;
 - Increase in Internet traffic:
 - affecting ISPs, because spam is often expensive international traffic; and

- affecting Internet users, because many broadband connections charge for or limit traffic;
- Spam increases the risk of missing important legitimate messages by cluttering the medium;
- Risks of filtering actions catching legitimate messages and producing "false positives";
- Costs in installing, operating and maintaining spam filters for both ISPs and Internet users;
- Risks of having email addresses used as a "sender address", bounced messages, false allegations, etc; and
- Encouraging proliferation of malicious worm activity seeking vulnerabilities in Internet users' PCs to be used to send spam undetected.

PART B: EXISTING LEGAL FRAMEWORK

2 *Q2. DO YOU THINK LEGISLATION HAS A ROLE TO PLAY ALONGSIDE OTHER COMPLEMENTARY MEASURES?*

- 2.1 Telecom supports the position that legislation should be a component of the overall solution to combating spam, alongside other complementary initiatives such as technical measures, education campaigns and international cooperation.
- 2.2 Telecom considers that in practice, New Zealand legislation alone is likely to have only a limited impact on the overall spam issue, as:
- despite some recent international reports to the contrary, Telecom believes the majority of spam received in New Zealand originates from overseas; and
 - in many cases, for the types of spam we are most interested in preventing, we cannot identify the true originating source of the spam.

Telecom therefore agrees that there is a pressing need for international cooperation to address the spam problem. However, Telecom maintains that domestic legislation will send a clear message about the acceptability of spam, and reduce the risk of overseas spammers using New Zealand as a

spam 'safe haven', and consequently, overseas organisations blocking email from New Zealand sources.

2.3 The complementary measures available to Telecom's Xtra customers include:

- Automatic email spam protection automatically at no additional cost through an anti-spam filtering technology provided by the leading security software company, BrightMail;
- Telecom provides its customers with online education tools describing how to reduce their vulnerability to spam (see <http://www.xtra.co.nz/help/0,,4155-937623,00.html>); and
- As a responsible service provider, Telecom also maintains a hard line on spamming by its own customers. Telecom promptly acts to prevent spamming by customers, including by terminating users' Internet accounts under the terms of its Xtra Service Terms (which prohibit spamming).

Our response

2.4 Telecom has a number of filtering technologies deployed across its business. The most significant is the BrightMail spam filter, which is supplied free of charge to customers of Xtra. The product was chosen as it is designed to have the minimum possible false positive rate and gives Internet users the choice about how they wish to deal with spam. They may choose to file it in a separate email folder or delete it before it enters their mailbox.

2.5 Telecom also blocks network addresses that are measured by BrightMail as being large spam sources. BrightMail updates this information hourly, as it is important to have an automatic aging process for network blocks to avoid damaging email connectivity for legitimate users. By aging the list of blocked addresses very rapidly Telecom attempts to avoid an Internet user's connection to our mail systems being limited by the actions of the previous Internet user of that network address. This is because the majority of Internet access accounts use dynamic IP addresses.

2.6 Xtra has avoided using blacklists as a source of addresses for network blocking. Many blacklist services operate from very small data sets and without reference to the amount of legitimate traffic originating from a network. However, Telecom has a dedicated security and abuse function which monitors complaints to ensure that its IP addresses are not blacklisted by ISPs around the world.

- 2.7 Many of the solutions that are commonly proposed to deal with spam exacerbate rather than alleviate the problem. Solutions that require effort on the part of the user, for example training, Bayesian filters, challenge response systems, or systems with high false positives that require manual review of suspected spam may be very suitable to individual Internet users but do not meet the needs of the mass market.
- 2.8 The area where Telecom sees the greatest potential for change is in incremental improvements to technologies designed to identify or authenticate the sending party. Telecom is watching with interest the current technology advancements in this area. We see technology solutions that for example, would significantly reduce a spammer's ability to steal the identities of legitimate email users as critical in the war against spam.

3 ***Q3. DO YOU CONSIDER EXISTING PRIVACY PROTECTIONS IN THIS AREA SUFFICIENT?***

- 3.1 Telecom agrees with the Government's observation that the Privacy Act is of limited use as a means to address this issue. This is because of the available exceptions to the Privacy Principles, limitations on enforcement, and the Privacy Act's application to natural persons only.
- 3.2 Telecom also observes that although the Privacy Act may have some application to web-based email address harvesting, there are other methods of compiling emailing lists favoured by spammers that would not be captured by the Act. For example, Xtra customers' email accounts are often targeted by dictionary attacks, which randomly target addresses (eg, aaa@xtra.co.nz, aab@xtra.co.nz).

4 ***Q4. DO YOU AGREE THAT STAND-ALONE ANTI-SPAM LEGISLATION IS PREFERABLE TO RELIANCE ON THE HARASSMENT ACT?***

- 4.1 Telecom agrees with the Government's position that there are a number of difficulties in seeking to apply the Harassment Act to the problem of spam. In addition to those already highlighted in the Discussion Paper, Telecom considers that difficulties in establishing the identity of the sending party with email and the Harassment Act's requirement for repetitive contact may be significant obstacles. In addition, the Act would be of little use in cases where the originator of the spam is based overseas.

- 4.2 For the above reasons, Telecom supports the introduction of separate anti-spam legislation rather than relying on existing legislative measures, which have not been framed with the problem of spam in mind.

PART C: LEGISLATIVE ISSUES

5 ***Q5. WHAT MESSAGE MEDIA SHOULD BE CAUGHT BY THE LEGISLATION (EG EMAIL, SHORT MESSAGE SERVICES USING MOBILE PHONES, INTERNET INSTANT MESSAGING, FAXES, TELEPHONES (TELEMARKETING), PHYSICAL MAIL DELIVERY)?***

- 5.1 In Telecom's view, the key determinant of whether a particular message medium should be caught by the proposed legislation is whether or not it involves the imposition of direct costs to the originator of the message. We see a direct relationship between the absence of real direct costs and the problem of spam.
- 5.2 Traditional direct marketing channels such as the delivery of material to a physical mailbox or the use of telephones for telemarketing involve a direct cost to the marketer. This imposes finite volume limitations on the originator of the marketing materials.
- 5.3 In contrast, however, most electronic message media, such as email, SMS, MMS, and instant messaging, are of low or negligible cost from the originator's perspective, with the recipient and the recipient's service provider bearing the direct costs of dealing with the bulky and repetitive nature of these messages.
- 5.4 However, as technology will continue to evolve at a rapid pace, Telecom notes that any legislative definitions should be technology-neutral, to ensure that new technologies are caught. An example would be messaging systems within gaming environments.
- 5.5 For the above reasons, Telecom submits that the legislation should apply to all electronic message technologies (existing and future), with perhaps the exception of messages by way of voice call made using a standard telephone service (to which the rationale outlined in paragraph 5.1 in relation to cost would not appear to apply). Telecom therefore supports a broad, technology-neutral definition similar to that used in the Australian legislation, the Spam Act 2003 (*Australian Act*), for "electronic messages".

6 ***Q6. DO THE MESSAGES CAUGHT BY THE LEGISLATION HAVE TO BE SENT/CONVEYED TO MANY RECIPIENTS, AND IF SO, HOW MANY?***

6.1 Telecom considers that the volume of messages sent is an important criteria to be applied either in the definition of spam (the US approach) or in the penalty provisions (the Australian approach). Telecom considers that three criterion should be considered in determining whether messages of the specified type should be caught by the proposed legislation:

- the US approach, which focuses on bulk or volumes of messages; and
- the Australian approach, which focuses on intention and characteristics of the messages; and
- an approach which focuses on the delivery mechanism used by the sender and whether it has been automated or not.

US approach – volume of messages

6.2 The bulk of messages sent is an important criterion because spam is typically sent in bulk, and it is the bulk element of the conduct that leads to the injurious consequences set out in Part A above. If bulk is not taken into account in the definition of spam, then, as pointed out in the Discussion Paper, there is a potential for individual to individual messages to be classified as spam with the result that “innocent” and common-place communications would technically breach the Act. As a matter of principle, it would not seem desirable to prohibit activity which no one would consider harmful.

6.3 However, Telecom observes that there may be practical difficulties with a definition of spam that includes a requirement for certain volume thresholds to be reached. For example, because of spammers’ tendency to “spoof” other Internet users’ email addresses and employ other techniques to disguise the source of the spam, there could be significant evidential issues in proving that a particular spammer has reached the required threshold.

6.4 In addition, exceptions for innocent or legitimate bulk emailing need to be accounted for. For these reasons Telecom considers a purposive element is another important criterion in determining spam.

Australian approach – purpose of message

- 6.5 Telecom therefore suggests that a purposive approach such as that adopted under the Australian legislation by the particular enforcement agency would ensure that only genuine cases of commercial email abuse would be targeted. Even if “innocent” emailers are pursued, the Australian legislation contains the added control that the volume of spamming is a relevant consideration in determining the level of the pecuniary penalty.
- 6.6 This approach has the added benefit of aligning our legislation with that of Australia in an area where there are mutual benefits in addressing the same problem.

Alternative approach – use of automated delivery

- 6.7 As an alternative, Telecom has also considered whether the appropriate determinant should not be whether the sender used an automated tool or database to generate the messages. This would result in an appropriate focus on the harm caused in proportion to the volume of messages sent by identifying those doing the most harm, while excluding personal or usual communications. The touchstone of automation addresses the principal driver for the use of spam, which is the very low cost to deliver large volumes of messages by the use of automated tools and databases.

Preferred approach

- 6.8 Overall, Telecom considers that a workable definition of bulk email is a key criterion to determining spam, provided that there is sufficient comfort that the evidential issues can be addressed. The Australian approach provides useful guidance to balance out the concerns raised by an approach solely determinant on volume by introducing a purpose element and a penalty regime that is proportionate to the volume of spamming.

7 Q7. 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?

- 7.1 Telecom observes that the vast majority of spam seen in New Zealand is of a commercial or promotional nature. However, Telecom considers that narrowing the scope to overtly commercial or promotional messages creates the opportunity for loopholes, for example, disguising promotional material as informative messages. For this reason, Telecom endorses

adopting a wider approach such as that taken by the Australian legislation, which encompasses a broader range of undesirable spam email under the definition of “commercial electronic message”. This would include emails that encourage a person, by deception, to dishonestly obtain a financial advantage from another person.

- 7.2 However, Telecom does not see any logical, compelling public policy or other reason for following the Australian approach of providing exclusions for certain types of messages (eg messages originating from government bodies, political parties, religious organisations, charities and educational institutions). In Telecom’s view, although these messages may not be overtly commercial, there is usually a commercial motivation for their transmission, and like other unsolicited messages of a bulk nature, they have the same ability to annoy and offend email users. The rationale that there is an interest in ensuring that certain types of messages with a social value should not be caught as spam ignores the reality that social value is perceived at an individual level, and that individual’s should be given the choice (ie through a consent process) as to which emails they wish to receive.
- 7.3 As an example, Politically motivated spam received by Telecom in the run up to the recent elections for the European parliament have shown us that non commercial spam is a real and increasing problem. A group of test accounts that are monitored by Xtra were receiving German language political messages at an average rate of 3 per hour.

8 ***Q8. SHOULD THE LEGISLATION EXTEND TO COVERAGE OF ACTS DONE OVERSEAS? IF SO, WHAT ACTS SHOULD BE COVERED?***

- 8.1 Telecom supports the approach favoured in the Discussion Paper that anti-spam legislation should extend to coverage of acts outside New Zealand, provided that there is a “New Zealand link”. This is the approach taken by the Australian legislation.
- 8.2 Telecom observes that most spam encountered by Xtra is relayed by the originator through third party machines, which are almost invariably located overseas. This means that even where spam is targeted at New Zealand email addresses, the source in network terms will very rarely be within New Zealand.
- 8.3 While Telecom acknowledges that issues of enforcement and jurisdiction arise, there are situations in which extraterritorial reach is important. For example, Telecom considers that the legislation should specifically extend

to New Zealand vendors of products or services that arrange for spam to be sent from overseas, notwithstanding that the spam originates from outside New Zealand (see below at paragraph 9.1 for further discussion).

9 ***Q9. 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?***

9.1 Telecom recognises that the sender of spam is not the only person who may be a party to the act of spamming. As observed in the Discussion Paper, it is common practice for a vendor of goods or services to sponsor someone else to carry out the spamming for them (which may be from off-shore), in which case Telecom considers it important that liability should attach (for example, to a New Zealand vendor even if the spam was sent from overseas). Further, the sponsor of the message is often the easiest person to locate at a technical level.

9.2 For these reasons, Telecom considers that the legislation should be framed broadly to capture all parties involved in the sending of the message, subject to the specific exceptions set out below. Telecom therefore supports the broad approach taken in the Australian legislation which covers 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.

9.3 However, Telecom considers that the touchstone for liability for the sending of spam should be actual knowledge of the infringing conduct. Persons who knowingly send spam, or assist others to send spam, should be liable under the proposed legislation. However, following generally accepted legal principles, parties lacking the requisite knowledge should not be held accountable. Telecom recommends that three specific exceptions should apply in circumstances where this knowledge element is lacking.

Exception for mere carriers of messages

9.4 Telecom considers that a specific exemption is required to recognise the special position of ISPs in relation to the carriage and distribution of spam messages through their networks and systems. As New Zealand's largest ISP, Telecom's Xtra is responsible for transmitting vast quantities of email each day.

- 9.5 At a technical level, Xtra's primary function is to act as mere distributor or conduit for information but without any actual knowledge or effective control over the content of individual emails. Xtra and other ISPs do not have certain feasible technical means of preventing particular types of email from entering or being distributed through their networks and systems (eg spam and email viruses). There are only limited and uncertain means of reducing the impact of such emails on its customers, for example, through the use of anti-spam and anti-virus filters.
- 9.6 In addition to these crucial technical limitations, it is not desirable in policy terms to impose a burden on ISPs to prevent spam messages from being sent and received through their networks and systems. Imposing such a duty would force ISPs to pass on the vast costs of monitoring to its customers, which would in turn lead to a lower quality of services and higher costs for consumers and businesses.
- 9.7 For these reasons, Telecom submits that a specific exemption should be included in the proposed legislation, to make it clear that ISPs and telecommunications service providers who are acting as carriers and distributors of email are not liable for the sending of spam.
- 9.8 This position is consistent with the approach taken in the Australian Act , which contains an explicit exemption for carriage service providers in section 9. Telecom suggests that this section provides an appropriate basis for framing an equivalent New Zealand exemption:

“Sending of electronic messages – carriage service providers

- (1) For the purposes of this Act, a person does not send an electronic message, or cause an electronic message to be sent, merely because the person supplies a carriage service that enables the message to be sent.
- (2) Subsection (1) is enacted for the avoidance of doubt.”

- 9.9 In addition, Telecom considers it important that the proposed legislation does not interfere with or restrict the ability of ISPs to independently manage spam through their own technical solutions. For example, it would not be desirable for the legislation, by implication, to suggest that any communication falling outside of its scope is not spam. Telecom considers that this could inadvertently create an obligation on ISPs to ensure that customers' emails are delivered. As the Discussion Paper points out, the Government's primary objective is to attack the spam problem through legislation complemented by industry self-regulation, awareness and education campaigns. Telecom emphasises that in order to maintain their

effectiveness, these other measures must be viewed as complementary, yet separate and not restricted in scope by the proposed legislation.

- 9.10 Telecom therefore submits that the right for ISPs to act in what they perceive to be the best interests of their customers should be preserved, preferably through an express provision to this effect in the legislation. Based on this position, Telecom would be reluctant also to support the adoption of an industry-wide code of practice, or similarly generalised form of self-regulation, that would prescribe specific rules for dealing with spam. In Telecom's view, this would inhibit a service provider's ability to provide innovative solutions that are aimed at the particular needs of its customer base. Similarly, Telecom does not consider it appropriate for the proposed legislation to regulate or prescribe the actions of service providers in relation to spam.
- 9.11 Telecom therefore recommends the following clause, primarily for the avoidance of doubt:

Ability of service providers not limited

For the avoidance of doubt, nothing in this Act shall restrict or interfere with, or create any obligation in relation to, a carriage service provider's ability to control and manage spam as it sees fit.

Exception where requisite knowledge lacking

- 9.12 As set out above in paragraph 1.5, the majority of spam encountered by Xtra is sent through the unauthorised use of someone else's resources. For example, it is now fairly commonplace for users' machines to be compromised via network attacks which facilitate the sending of messages from that user's machine, without knowledge of the user.
- 9.13 An exception should therefore apply in cases where a person's computer or other resources have been used to send or assist the process of sending spam without their knowledge or consent. In such a case, liability would attach unless the person could prove that they did not have actual knowledge of the email being sent. Telecom notes that a similar concept is adopted in the Australian legislation, under section 16(3), which provides that a person is not liable for spamming where he/she did not know, and could not (with reasonable diligence) have ascertained that the message had an "Australian link". Telecom therefore recommends the following example clause as an appropriate exception, which is derived largely from section 16(3) of the Australian Act:

Exclusion for lack of actual knowledge

A person will not be liable for sending a commercial electronic message if the person:

- (a) did not know; and
- (b) could not, with reasonable diligence, have gained knowledge; of the message prior to its sending.

Exception in cases of mistaken recipient

- 9.14 Telecom considers that an exception for cases where an email is sent by mistake to the wrong recipient would also be appropriate, if the legislation were to follow the Australian approach of technically prohibiting all individual to individual unsolicited commercial emails (see paragraphs 6.1 to 6.8). This would capture situations where an originator of a message has incorrectly spelt the intended recipient's email address (eg, joebloggs@xtra.co.nz instead of jobloggs@xtra.co.nz). As with the exception set out above, the onus of proving the mistake would be placed on the sender. A similar exception is provided for in section 16(4) of the Australian Act, which Telecom endorses:

Exclusion for mistake

A person will not be liable for sending a commercial electronic message if the person:

- (a) sent the message, or caused the message to be sent, by mistake to a particular recipient; and
- (b) intended to send the message, or cause the message to be sent, to a different recipient (and such sending would not have contravened any provision of this Act).

PART D: THE CONSENT ISSUE – OPT-IN OR OPT-OUT

10 *Q10. SHOULD NEW ZEALAND ADOPT AN OPT-IN, DOUBLE OPT-IN OR OPT-OUT APPROACH IN LEGISLATING AGAINST SPAM? WHY?*

- 10.1 Telecom considers that the definition of consent is critical to distinguishing solicited bulk email (an important and legitimate mechanism for keeping

consenting customers informed of products or service news) from unsolicited bulk email or spam (an unwanted nuisance to, and drain on time and resources of, the recipient).

- 10.2 Telecom agrees with the Government's position in the Discussion Paper that an opt-in approach should be preferred to an opt-out approach, due to the significant disadvantages of an opt-out approach as highlighted in the Discussion Paper. It is highly likely that legitimising an opt-out approach would lead to the creation of vast opt-out lists of New Zealand email addresses, which could then be freely traded overseas, thereby leading to higher volumes of spam. For this reason, Telecom strongly opposes an opt-out approach.
- 10.3 Telecom notes that there are varying levels of opt-in, with two of the most common forms referred to as "single" opt-in, and "double" opt-in. A single opt-in process involves an organisation inviting Internet users to join a mailing list by filling out details (including their email address) in a web form. Once the form has been submitted, the user is signed up to the mailing list and will receive emails from the organisation. The disadvantage with a single opt-in process is that users may misenter their email address into web-based forms (perhaps entering someone else's address by accident or maliciously). In such a case, the user associated with the misentered email address will not have consented to being included on the mailing list – ie there is no opportunity for that person to verify that they wished to be added to the list.
- 10.4 The double opt-in approach involves a user filling out a web form, and being sent an initial message to confirm the subscription to the mailing list.¹ To activate the subscription, the user is then required to either click on a special link in the initial email, or reply. The key point with double opt-in is that it is an email address verification process – it validates that an email list is truly permission-based. This process has become the standard for qualifying a list as a legitimate, non-spam means of business communication.²
- 10.5 In some cases organisations may have other means to authenticate and validate an Internet user with an email address. For example services which associate an email address with a user name and password. In those cases, provided the organisation can show it has authenticated the user name and password with the email address, a double opt-in approach should not be required.

¹ The double opt-in approach is also referred to as a closed loop opt-in, confirmed opt-in, or verified opt-in. See <http://www.spamresource.com/closedloop.html> for further information.

² See http://www.lyris.com/products/listmanager/about_opt-in.html.

10.6 Telecom therefore submits that the proposed legislation should reflect as a default position a concept of consent that is modelled on a double opt-in approach. However care should be taken to ensure such an approach does not create disproportionate compliance costs for small organisations.

11 ***Q11. 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?***

11.1 Telecom considers that the definition of consent adopted by the Australian Act is a useful starting point in terms of framing the proposed New Zealand legislation. In the Australian legislation, consent means express consent, or consent that can be inferred from the conduct, and business and other relationships, of the individual or organisation concerned. Telecom agrees with the comment made in the Discussion Paper that this definition creates an area of uncertainty as to what conduct and relationships would result in there being a reasonable inference of consent. For this reason, Telecom considers that consent should be limited to express consent, or a more prescribed set of circumstances in which it is possible to infer that consent has been given implicitly.

12 ***Q12. HOW SHOULD THE SCOPE OF ANY OPT-IN OR DOUBLE OPT-IN ASSENT BE FRAMED?***

12.1 Telecom agrees with the approach of the Australian legislation that relates the issue of the scope of any “consent” to whether a particular message was expressly consented to or consent could reasonably be inferred.

PART E: TRANSPARENCY ISSUES

13 ***Q13. 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)?***

13.1 Telecom submits that all commercial electronic messages should clearly and accurately identify the individual or organisation who authorised the sending of the message.

14 ***Q14. 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?***

14.1 A functional unsubscribe facility is desirable but it need not be via an electronic email address. Because of the ease with which a person can forge an email address and the difficulties with tracking compliance with such a requirement, insisting on this could result in innocent parties receiving vast amounts of unsubscribe messages. Telecom therefore considers that as most people use HTML email clients that open a connection to the sender's website to retrieve content in a way that is easily tracked by the sender, the easiest way for the already inconvenienced end user to unsubscribe is via a button or web link

15 ***Q15. SHOULD THERE BE A REQUIREMENT THAT COMMERCIAL ELECTRONIC MESSAGES PROVIDE ACCURATE HEADER AND SUBJECT INFORMATION?***

15.1 Telecom agrees in principle that senders of commercial email should not intentionally mislead by providing inaccurate header and subject information. However, misleading conduct is already addressed by existing legislation (eg Fair Trading Act). Telecom submits that specifically regulating header and subject information is therefore unnecessary, and unduly restrictive for legitimate emailers. For example, there are cases where a third party may legitimately be involved in sending the mail (eg electronic greeting cards, and where email is sent by international roaming customers).

16 ***Q16. SHOULD THERE BE A REQUIREMENT FOR THE LABELLING OF ADVERTISING OR ADULT MESSAGES?***

- 16.1 Telecom considers that imposing a requirement to label adult or restricted content would be immensely beneficial for both service providers and Internet users. From a technical perspective, it would enable the Internet user to filter emails more easily and efficiently at the email client. Telecom's experience is that spam containing adult or otherwise restricted content is often reasonably upfront about its nature, but imposing a standard form of labelling would greatly enhance the efficacy of email filters. We believe that in an environment where messages are only sent with consent, adding an advertising label is unnecessary and difficult to define where a message becomes primarily an advertisement.

17 ***Q17. 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?***

- 17.1 Telecom submits that harvesting software should not be illegal in itself. This is because there are a variety of legitimate uses for such software, including in relation to search engines and caches, which are often essential to the smooth operation of the Internet.
- 17.2 Telecom considers that legislation should instead target the use of addresses collected by these methods for spamming.
- 17.3 For this reason, Telecom considers that the Australian legislation provides useful guidance on this issue. Under the Australian legislation, it is an offence to supply, acquire, or use address-harvesting software or harvested lists unless the person did not intend to use them in connection with sending spam. Telecom also considers that the use of dictionary attacks (applications that generate possible email addresses by combining names, letters, or numbers into numerous permutations) should also be prohibited on the same basis as address-harvesting software and harvested lists, which is consistent with the position taken in the CAN-SPAM Act 2003 (US) (*US Act*), section 5(b)(1)(A)(ii).

18 ***Q18. WHO SHOULD BE ABLE TO BRING AN ACTION AGAINST AN ALLEGED SPAMMER?***

18.1 Telecom agrees with the general approach adopted in other jurisdictions in relation to the enforcement of anti-spam legislation, whereby primary responsibility for carrying out investigations and taking enforcement action is given to an appropriate government agency.

18.2 Telecom also submits that ISPs should have the right to bring actions under the proposed legislation, as they are likely to have the highest risk of incurring substantial loss as a result of spam due to wasted network and computing resources, email administrator and helpdesk personnel time, and decreased worker productivity. Telecom notes that section 7(g)(1) of the US Act provides a precedent for allowing ISP actions to proceed.

19 ***Q19. WHAT AGENCY SHOULD HAVE THE ENFORCEMENT ROLE UNDER THE LEGISLATION?***

19.1 Telecom does not have a settled view on the appropriate agency, but recommends that an agency with proven expertise in investigation and enforcement is advisable. Whichever agency is used should have appropriate resource to ensure that sufficient action is taken to provide a useful deterrent effect.

20 ***Q20. WHAT SHOULD BE THE AVAILABLE PENALTIES AND REMEDIES FOR BREACHES OF ANTI-SPAM LEGISLATION AND WHAT SHOULD BE THE MAXIMUM FINE OR PECUNIARY PENALTY?***

20.1 Telecom considers that pecuniary penalties are likely to be the most effective form of remedy. Telecom agrees that given the costs that spam can impose and the difficulties in carrying out a successful court action, the penalties imposed should be significantly high to serve as a deterrent. In terms of maximum levels, Telecom submits that New Zealand should follow international norms, which suggest that substantial penalties are appropriate. For example, under the Australian Act, a single day's contravention can amount to AUD\$220,000, with a penalty of AUD\$1.1 million for further breaches.

20.2 In relation to actions brought by ISPs, Telecom considers that ISPs should be entitled to claim compensation for the full amount of loss suffered as a result of a spammer's actions, including the costs of pursuing legal actions. In addition, exemplary damages and restitutionary remedies (which look to

the profit made by the spammer rather than the loss suffered by the ISP) should be available as alternatives to loss-based damages claims.

21 ***Q21. SHOULD CONTRAVENTIONS GIVE RISE TO CRIMINAL OR CIVIL PENALTIES?***

21.1 Telecom considers that civil penalties are likely to be the most appropriate means of enforcing the proposed legislation. Criminal liability, especially where there is imprisonment, is generally thought internationally to be inappropriate unless there is repeat serious offending involving widespread harm to the public interest.

22 ***Q22. SHOULD THE RESPONSIBLE ENFORCEMENT AGENCY BE GIVEN THE ABILITY TO OBTAIN SEARCH WARRANTS CONFERRING POWERS OF ENTRY, SEARCH AND SEIZURE?***

22.1 Telecom agrees that enforcement powers similar to those conveyed on the Commerce Commission under the Fair Trading Act and Commerce Act would seem to be appropriate to ensure that the provisions of the proposed legislation are enforceable.

22.2 However, Telecom is also conscious that these powers should be carefully balanced with the issue of costs to third parties. As New Zealand's largest ISP, Xtra is perhaps likely to be involved closely with the activities of the New Zealand enforcement agency, particularly in relation to providing investigative resources such as information and technical expertise. While Telecom wishes to cooperate with and assist enforcement agencies, as is evidenced by its current practice, Telecom emphasises that this support is costly. Telecom notes that the concept of cost-sharing in relation to investigative resources is already recognised in other legislation, such as the Telecommunications (Interception Capability) Act 2004. Telecom therefore submits that express provision should be made in the proposed legislation to enable service providers to recover their reasonable costs from the government of providing resources in the context of investigations carried out by the particular enforcement agency.