

Mercury Telecommunications Limited

**t/a Quicksilver Internet
t/a Splurge Internet**

Discussion Paper

Legislating Against Spam

Introduction:

Mercury Telecommunications is a privately owned telecommunications and internet service provider. Based in Auckland but offering services nationwide , Mercury has over 10,000 internet and telecommunications customers.

It is the intention of the directors of Mercury to respond to the Discussion Paper “Legislating against Spam”. Mercury will attempt to answer each of the 22 questions posed by the discussion paper. The answers will be principally based from the perspective of an Internet Service provider providing services to the New Zealand business community and general public.

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

Answer: Yes ! Spam is one of the two most important issues (along with virus) concerning the internet and internet usage today.

Quicksilver installed spam protection on its network for all users in October 2003. Indicative information is that 40-50% of all email on the Quicksilver network is Spam.

Total email on the Quicksilver network has also grown by 75% in the past 2 years.

Quicksilver has invested over \$200k over the past 12 months in developing tools to fight the spread of spam. This investment decision was based partly on the wishes of Quicksilver’s customer base and partly on the growing network cost of the Quicksilver network be used to deliver spam.

Spam has also been the cause of a significant increase in customer service costs as users constantly inquire about spam, its effects and how to stop it.

Question 2: Do you think legislation has a role to play alongside other complementary measures /

Answer: Yes! We think that legislation will have limited effect on the receipt of spam by NZ businesses and users that has originated overseas however as anti-spam legislation has been enacted in various places around the world , legislation in New Zealand will be vital to stop potential spammers setting up operations in an unregulated NZ environment.

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

Answer: No. The privacy act would appear to contain safeguards and references to the collection of information that may include email addresses and the like however this would not address two issues

- a) the privacy act while mentioning the collection of personal information would seem to only be addressing the action of collecting the information from the person by whatever means. It would also seem to cover the transfer or sale of this information to a third party – It does not seem to cover the use of the information by a third party who did not gain the information from the public involved.
- b) The privacy also does not appear to cover the scenario whereby a spammer does not know the individual addresses of who they are spamming they are just undertaking what we call a sequential spam whereby they email a@whatever.co.nz, aa@whatever.co.nz, aaa@whatever.co.nz etc. In this way they are not breaching anyone's privacy as we understand the act to define privacy because that have not had access to privileged information.

It would also appear that it would be difficult to prove the vast majority of spam as being of a harassing nature. Annoying yes, potentially in contravention to content/censorship legislation but harassment would appear to be a stretch.

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

Answer : Yes: Again for two reasons. Firstly that we don't think the Harassment Act would apply in the vast majority of spam, and secondly that it can be expected over the oncoming years that the nature of spam will change in ways that are unknown or at least unexpected today. A unique or stand-alone piece of legislation will conceivably make it easier for the government and the various stakeholders in this issue to adapt the legislation for future eventualities.

Question 5: What message mediums should be caught by the legislation (eg. Email, short message services using mobile phones, Internet instant messaging, faxes, telephones (telemarketing), physical mail delivery).

This is a difficult question because while the advent of unwanted solicited material in any form is annoying and potentially costly, it cannot be ignored that email, texting and other forms of electronic communication in general are the most powerful communication medium as well as potentially being the most powerful commercial medium of the future.

The discussion of which forms of electronic media should be covered as best addressed by looking at what barriers there are to sending “spam. The two main issues are the cost to send a spam message (ie the cost of a spam message is on the sender not the receiver) and the ease of sending “mass” amounts of messages in a small space of time (ie effectively sending 10 or 100 thousand messages almost instantaneously).

Email spam – there are very few cost barriers in sending spam, as well as this it is very easy to mass send email thus making email an ideal medium for spammers.

SMS – It is not free to send SMS messages so there is a cost deterrent however is very easy to send mass messages.

Internet Messaging – It is free to send an instant message through most systems however it is difficult to send mass amounts of messages through this system

Faxes- There is a cost deterrent however it is very easy to send mass messages

Telephones- there is a significant cost deterrent as well as a problem sending mass messages

Physical mail delivery – Again there is a significant cost deterrent and it is difficult to send mass messages.

We would recommend that only mediums with BOTH factors, free to send and ability to send in a mass format be subject to legislation. In New Zealand only Email fits this profile therefore we would that only EMAIL is subject to spam legislation.

There has been some discussion that mobile texting and SMS should be subject as well however with the recent caps on flat rate texting plans recently introduced by NZ mobile network operators effectively means that the amount of texting possible would not count as spam.

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

Answer: NO, it is our opinion that any legislation directed at spam messages be dictated by the consent of the recipient not the number of messages sent or received. While it will clearly be necessary to add a layer of definition above the issue of consent, we do not believe that basing a definition of spam on specific numbers of messages will produce effective legislation.

Question 7: Should the messages caught by the legislation be of a commercial advertising and promotional nature or should other types of messages be caught? Should there be exceptions and if so what should be exempted/

Answer: There are two questions therefore two answers.

- 1) No, there should not be any difference between what is classed as spam and not spam based on content. With the basic definition of spam being one of an unsolicited nature we feel the content shouldn't be an issue as to the definition of spam.
- 2) Yes there should be exemptions; the standard exemptions should be organizations contacting their customer base for whatever reason. For example many organizations send electronic invoices by Email, debt and payment reminders. Quicksilver also regularly sends warnings to its customers (who number more than 10,000, about new virus' they should be aware of and new products and services that they should consider. There may be many reasons why an organization would like to reach their customer base (online surveys are another example) and the size and spread of that customer base would make any media other than email unsustainable. The prospect of a customer refusing to opt in to an email debt reminder is possible and we feel would significantly damage the perception of the appropriateness of legislation.

Question 8: Should the legislation extend to coverage of acts done overseas? If so what acts should be covered?

Answer: Yes. It is our belief that anti-spam legislation will only become genuinely effective when a significant level of international co-operation is possible. Because geographical details are largely immaterial where the Internet is concerned, a spammer's activities may span several jurisdictions. Assuming that some form of international treaty is a likely long-term outcome of anti-spam activities, having legislation that covers acts committed outside New Zealand will likely prove worthwhile in the future.

Question 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 ISP's ?

Answer: Yes all parties involved in the act of spamming should be covered by the legislation. However there is an issue with ISP's and telecommunications companies.

With the sending of spam email there are often two ISP's or telecommunications companies involved. One providing the connection for the SMTP or server sending the spam, and one providing the email services for the people receiving the spam. We feel

that the ISP or telecommunications company responsible for providing the services to receive the spam be exempt from this legislation. The analogy would be to sue the mailman for the contents of a letter and the number of letters received.

We also feel that there should be a process under the legislation for ISP's and telecommunications businesses to rectify a situation where they are an unwilling accomplice to the sending of spam. It may not always be possible for an ISP to know that a spammer is using their network. We feel there should be a notice period defined under a best practice process where ISP's have a certain amount of time to suspend a spammer generating spam or to generally take action.

With a best practice process in place, then when the ISP is notified of a potential spammer on their network, the ISP can follow the best practice process set down by the legislation with a consequence that they are able to use this process and the action of following the process as a defense against the legislation.

Question 10: Should NZ adopt an opt-in or opt-out approach in legislating against spam? Why?

Answer: NZ should adopt an opt-in approach to spam. While perhaps not the most ideal method we feel that it is the most practical method and the easiest method to police. While any opt-in method is open to huge amounts of interpretation and confusion as to when consent is given, we feel that opt-out places too much onus upon the user to police. However we do feel that each solicited email must include an opt-out provision.

However, if opt-in consent becomes too restrictive then it will effectively kill email as a commercial tool at all.

We do feel that basis of any legislation should be to police the abuse of email but not curtail the honest use of email as a business tool. This issue is usually driven by the concept and definition of consent. If you get someone's business card we feel that it is reasonable that you can send them an email to contact them or even to try and sell them something.

Question 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.

Answer: If the opt-in approach was taken we feel that the level of consent required should be reasonably low.

Inferred consent should at least include the following:

- Any customer/supplier relationship within the past 2-3 years.

- Opt-in through an email system or website based form or other electronic means
- Voice verification

Note: Opt-in Issues.

- How long does opt-in consent last or is an opt-out mechanism required anyway.
- What happens if a third party opts a consumer into receiving email. (eg I have 400 addresses in my address book, what if I deliberately or otherwise (virus infection) opt-in someone else - what remedies are their for the person opted-in, what defense is there for the organization sending the emails

We feel that opt-in is the best approach however there must be significant thought given to the potential abuse of opt-in consent in order to maintain the integrity of the legislation.

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

Answer: We would agree with the Australian approach that any opt-in assent be tagged with the reasonable expectation of content that can be inferred from the message or the organization sending the message.

Eg Opt in to the Warehouse then you should expect to receive emails on all items for sale or about to be on sale at The Warehouse, whether everything is mentioned or not.

Question 13: Should there be a requirement for commercial electronic messages to accurately identify the sender of the message ? If so, what constitutes accurate identification (eg name and physical address, name and email address)

Answer: In answer to the first question , YES there should be a requirement to provide accurate sender information.

We feel that this information should include name, email address, website and phone number (so that a phone call be made to verify existence of the company)

Question 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 ?

Answer: We agree and feel that there should be an unsubscribe address in the email. The onus should be on the sender of the spam email to make sure that the unsubscribe address is current and that they have a working unsubscribe process involving this address. However if someone unsubscribes then they should provide proof and as such the onus is

on them to save the unsubscribe email that they have sent in order to gain any relief from the legislation.

We don't feel that a statement " But I unsubscribed myself" be sufficient burden of proof under any proposed legislation.

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

No and Yes!! Header information is commonly substituted for legitimate reasons however we agree that the subject should approximate the content of the message. Currently the subject is one of the primary areas of an email that is used by anti-spam software. The forging of these subject lines is solely designed for subverting anti-spam software and therefore should be covered within the legislation.

Question 16: Should there be a requirement for the labeling of advertising or adult messages ?

Answer: At its core commercial email is advertising so we feel that labeling email as advertising is a wee bit pointless, however we do agree that dictating that adult material be labeled. We feel that this is appropriate despite a opt-in approach which inherently supposes that the recipient knows the type of content they are receiving, however there are cases (families sharing email addresses, computers etc) where it would be appropriate from a "good citizen" point of view. This obviously has other implications then just spam email so that it is appropriate that the legislation asks that adult material be labeled as such.

Question 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?

Answer: Yes, it would make sense to include these activities in any legislation as it pertains to the unlawful sending of email.

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

Answer: As an ISP we would favour the enforcement of the legislation to be vested in the Commerce Commission or the department of internal affairs. The reasoning for this is two fold:

1) The occurrence of spam is very rarely directed towards a group of specific individuals, it is more often directed at a wider group of the public. It is therefore appropriate that a public advocate be essentially given the responsibility to enforce the legislation from a user or public perspective.

We feel a process should be in place whereby individuals or organizations can present a case with the Commerce Commission or DIA who can then investigate the veracity of the claim and then proceed to a prosecution phase if they see fit.

We would however be supportive of the ability of ISP's or telecommunications companies to be able to prosecute directly under the legislation if they wish or if their resources don't allow it to petition the Commerce Commission or DIA to pursue remedies under the legislation in the event of a targeted spam attack against an ISP or an effective denial of service attack against an ISP.

2) The second reasoning behind the support of a public entity like the Commerce Commission or DIA having the responsibility to enforce the legislation is that we feel that it would be prudent to have a buffer between the private individual or company requesting action under the legislation. We feel that this buffer would provide protection over spurious claims, and potential abuse of the legislation by individuals and/or organisations with hidden agendas.

Question 19: What agency should have the enforcement role under the legislation ?

Answer: Answered in Question 18. We feel it would be appropriate for the Commerce Commission or DIA to be responsible. We would be agnostic as to the choice however we do note that the DIA does already have some involvement with ISP's in policing cases involving objectionable material.

We feel a process should be in place whereby individuals or organizations can present a case with the Commerce Commission or DIA who can then investigate the veracity of the claim and then proceed to a prosecution phase if they see fit.

We feel that the process be well publicized and relatively simple so that individuals understand their rights. We also feel that the process of lodging a claim be either free or mostly subsidized similar to the prices of High Court injunctions before they were increased (\$0 - \$ 500) perhaps. At this point the cost of a claim is enough to make sure petitioners are serious but not too much so that legitimate claimants are not deterred by the cost .

Question 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?

Answer: We are unsure of an actual figure however the anecdotal evidence is that there can be a significant amount of return for the spammer in their activities. We feel that a tiered approach to penalties should be enacted.

We also feel that there should be a 3 strike rule similar to criminal rules publicized overseas. Where the rules can potentially follow the following pattern.

1st offence: A fine of 50% of the proven financial return from the spamming activity or \$10,000 , which ever is the greater.

2nd offence: A fine of 110% of the proven financial return of the spamming activity or \$25,000 , whichever is the greater.

3rd and subsequent offences: A fine of 125% of the proven financial return of the spamming activity or \$40,000, whichever is the greater PLUS a mandatory custodial sentence of 3 months.

We feel that a simple fine approach is appropriate as an initial penalty due to the nature of the offence in terms of not causing actual harm. We also feel that basing a financial penalty based on the financial gains of the spammer would mitigate the risk of the set penalties being insufficient and would provide the ability of the legislation to effectively and efficiently scale its response to the spamming behaviour. We also feel that a mandatory custodial sentence is required after 3 strikes to deter to recalcitrant spammers who just wont stop.

We feel the period of time to determine the 3 strikes should be around 2 years.

Question 21: Should contraventions give rise to criminal or civil penalties ?

Answer: We feel that the enforcement of the legislation should be on a civil basis due to a lower burden of proof required.

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

Answer: The basic answer is yes in terms of property owned by the spammer. We would not agree that property owned by a third party such as an ISP should be subject to seizure. This would be because a server in an ISP's network may service hundreds or thousands of customers. However we do agree that third parties can have a search warrant served upon them in order to help provide information normally protected under the Privacy Act to the relevant authority for the prosecution under the act only and not for unrelated private civil actions.