

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

**[spamsubmissions@med.govt.nz](mailto:spamsubmissions@med.govt.nz)**

**29 June 2004**

**SUBMISSION IN RESPONSE TO  
"LEGISLATING AGAINST SPAM"  
DISCUSSION PAPER  
(MAY 2004)**

**Submission From:  
Michael O'Donnell  
Business Manager  
TradeMe Ltd  
PO Box 11 042  
WELLINGTON**

## **Introductory Comments**

We applaud the Government's moves to develop an approach to tackling the problem of spam. We believe that we are one of New Zealand's largest emailing businesses, sending and receiving close to 20 million authorised emails every month. This high reliance on email as a tool results in a correspondingly high exposure to the risks associated with spam. We have considered the issues raised in your discussion paper and are pleased to respond to them in this paper.

## **Trade Me**

Trade Me is New Zealand's largest internet company, attracting half of all the New Zealand originated page views recorded by Red Sheriff. Our websites include Trade Me - which has over 200,000 items for sale at any time, and lists over one million auctions per month, Finds someone, which has the largest number of paying dating clients in New Zealand and Old Friends with over 350,000 members.

We have been and are continuing to grow at an extraordinary rate, latterly of over 300% per year. Positive user experience is paramount to us at Trade Me, and we pride ourselves on having New Zealand's fastest and easiest to use websites, even with the vast amount of content we deliver. In total we expect to run over 20 million Internet auctions over the next year, the vast majority of which involve New Zealand buyers and sellers.

As part of the normal functioning of our businesses we sent over 8.6 million emails in May, and received, in turn, over 10 million emails per month.

The bulk of these emails are based on our auction and dating processes, where customers receive notification through email of events that have taken place on the site. These events include:

- being outbid on an auction
- buyers and sellers being put in touch with each other following the completion of an auction
- being given notification of a requested item being auctioned
- receiving a personal message from another findsomeone client

Our community of customers also relies on email to contact each other to ask questions of each other, during a classified listing or as

part of the dating process. We estimate that each completed auction generates an average of six emails, while members of the dating site may send and receive an equal number of emails each week.

**Over ninety nine point four per cent of the emails we receive are spam** (118 million annualized for the last 12 months), and we continuously develop systems to cope with both the rapidly increasing numbers and the spikes from virus based attacks. Correspondingly, less than 1% of emails directed to our mail server are actually legitimate.

## **Our Perspective**

It is critical to our business that:

1. the emails we send to our members are received and seen;  
and
2. the emails sent by our members to each other are also received and seen.

The large amount of spam impacts adversely on this happening, both through over-zealous spam filters and the clutter created by large amounts of visible in-box spam.

Trade Me believes in a free internet. We also believe that a combination of legislation, self regulation and internal measures is the best way to combat fraud and spam. Legislation on its own is often slow moving, out-dated, rendered irrelevant by technology and sometimes unenforceable. However it is the only measure that can stop the more aggressive actors, through civil or criminal charges.

Internal measures or industry self regulation and policing will always be required to combat the latest virus, spam or fraud attacks. These attacks grow in sophistication and can (and do) originate from anywhere in the world.

We believe and use a "double opt-in" system to form a relationship with our members, and then use an opt-out system for individual email categories. We also send transactional emails that, much like bank statements, we do not wish members to be able to opt-out from.

However we also ensure that a member may opt-out of all communications simply by de-registering from a site.

We see the main objectives of legislation in New Zealand to be to discourage global spammers from setting up base here, to discourage New Zealand based companies from adopting unacceptable spamming practices and to provide a mechanism to ensure that any malicious and persistent spammers are put out of business.

Our main concerns about new legislation in New Zealand are that it could negatively affect our customer user experiences, and that it may create the potential for highly damaging enforcement activities for relatively innocuous acts.

Our user experience could be threatened by a legislated opt-in requirement, which if poorly considered, could result in customers having to opt in to our process driven emails, such as auction-win notifications. (Many of our process driven emails also contain short promotional statements (e.g. for our other sites), but, much like a mailed bank statement contains promotional inserts, we do not see these as "email marketing".)

We operate a business that is live 24/7/365. We are particularly wary of legislation that grants enforcement agencies rights to effect search and seizure of our servers or other computer equipment. Moreover, we conduct business in three other countries and have customers from many countries. We are very wary of legislation that would grant the right to foreign enforcement agencies to apply their more stringent laws and interpretation of those laws to our domestic business.

The paper will now go on to respond to the 22 questions raised in the original discussion paper.

# **Trade Me Responses To Specific Issues In Discussion Paper**

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

Spam is an important issue as it affects our community's ability to make full use of our sites, increases our costs and slows the uptake of Internet use and trust in New Zealand.

Spam dilutes the effectiveness of our customer's transactional and promotional emails, which reduces our ability to help customers buy and sell items online.

Spam also increases our infrastructure and personnel costs, which take resources from our efforts to improve our customer's user experience.

Finally, we believe that spam is a barrier to fast adoption of the Internet as a transaction medium. The presence of spam makes it tougher for us to demonstrate that the Internet is a place where trust-based, person to person transactions are safe.

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

Yes, to discourage local spammers, to prevent foreign spammers operating from New Zealand, and to provide enforcement for persistent offenders.

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

No. We do not consider that the Privacy Act is the vehicle to address the spam problem.

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

Yes, we consider stand-alone specialist anti-spam legislation to be preferable to other acts.

**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)?**

While we believe that email is the predominant medium at present, we believe the legislation should apply to any electronic message medium where the material cost of the message is not borne by the sender. This would include events where the sender somehow avoided the normal cost.

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

We would tend towards the Australian approach where the focus is on penalties rather than definitions, with more penalty points applying if a great number of messages are sent. Legislation should take into account that spammers are capable of sending different emails to each recipient.

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

We believe that the legislation should cover all forms of messages, as it is very difficult to define the difference between promotional, informational, transactional and personal messages. While these different message types should be covered, we also believe that the primary purpose of a message should determine how it is treated.

On our dating site Findsomeone, for example, multiple message types are often combined in the same message, such as when we notify our members, using a process driven transactional emails, that they have new personal messages from another member of the site, and include in the email a promotion for another site.

There should be no exceptions. We do not see that Government organizations, political parties, charities or any other organizations have a right to spam. Indeed, these organizations should realize that spamming is a poor way to communicate with constituents.

## **8. Should the legislation extend to coverage of acts done overseas? If so, what acts should be covered?**

There are several different categories of acts that can be done either in New Zealand or overseas. We believe that these separate instances should be dealt with independently, with appropriate penalties for each type of offence. The different categories are, in reducing order of severity:

- Spam relating to goods or services offered from within New Zealand
- Spam relating to goods or services offered from overseas to New Zealanders
- Spam is sent from within New Zealand to overseas clients, offering overseas products and services
- Spam sent from overseas, relating to goods or services that are not offered to New Zealanders, or not related to goods or services.

## **9. Should all parties involved in the act of spamming, such as the vendor sponsoring the spamming, be covered by the legislation? Should there be express exceptions such as for telecommunications companies and ISPs?**

Both the originator of the spam and the sponsoring vendor should be covered by the legislation.

Telecommunications companies and ISP's should not be liable for routing spam from others. However, they should maintain and enforce terms and conditions that prohibit the generation of spam by their customers.

While potentially desirable, it would be impractical to enforce any penalties against negligent parties that facilitate the propagation of spam because they did not properly secure their network.

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

We advocate (and use) a double opt-in system for initial membership to our sites, and more generally consider it an appropriate model for the registration of interest to a service. (The double opt-in process may require sending more than one "reminder" email.)

Once a customer is registered with one of our family of sites, they are able to opt-out of appropriate email notifications and promotions with a single opt-out system. However, there are some crucial transaction-oriented email notifications that we do not wish customers to be able to opt-out from. The primary purpose of emails in this category is notification of a financial (or potentially financial) implication for the customer. These emails may also contain promotional messages.

**New Zealand should adopt a double opt-in approach** for initial site registration. Initial registration should imply opt-in for emails sent for primarily process oriented transactional purposes, and may include opt-in for other types of emails, as appropriately stated in linked terms and conditions. Customers should have the ability, at any time after registration, to opt-in and opt-out of emails sent for primarily promotional or informational purposes.

Legislation should also require that customers can remove themselves from all email lists by de-registering from a site.

## **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?**

Registration with a website should constitute consent, provided that it is clearly stated (e.g. in terms and conditions) that electronic messages will be sent.

(We cannot explicitly ask each customer to opt-in to each of the number of types of email that we send. We do, however, allow customers to choose whether or not they receive emails that are not core to the transaction processes of our business)

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

Once the recipient has opted-in, the scope of consent should be broad enough that they may be sent any emails relevant to the service. This includes transactions performed as part of the service, and related informational or promotional material so long as the recipient chooses to maintain a relationship with the sender.

We do not support the sharing of email addresses between different commercial entities.

**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)?**

Commercial messages should be required to accurately identify the sender of the message. A link to the appropriate website which contains further identification and contact details should be sufficient.

**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?**

Where the primary purpose of a message is informational or promotional (not transactional), then there should be a requirement for messages to provide a mechanism to easily unsubscribe.

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

Yes.

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

We do not believe is necessary (or enforceable) to request categorisation of promotional or adult messages.

**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?**

Yes, anti-spam legislation should include rules of this nature. Harvesting email addresses is obviously a precursor to spamming itself, and has little legitimate purpose.

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

Only government agencies should be able to bring actions against spammers.

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

We believe that the Commerce Commission appears to be the most appropriate agency. We are concerned that the resources available to the Commerce Commission may not be sufficient.

**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?**

The Fair Trading Act penalties appear reasonable, with the proviso that persistent offenders may need more severe measures.

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

While civil action may allow for compensatory damages, we believe that these are criminal offenses, require a "beyond reasonable doubt" test and should be subject on summary conviction to a fine.

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

While granting powers of search and seizure against spammers may seem reasonable, it is positively frightening for a company like us, where our computers and servers constitute our entire business. We recommend a high hurdle before the right of entry is bestowed, including a warning, or cease and desist, process.

We also recommend that legislation provides the ability for alleged spammers to assess damages against the investigating agency in the event that the seizure caused material harm, and the subsequent legal proceedings result in no action against the alleged spammer.

## **Concluding Remarks/Next Steps**

Again we congratulate the Government in being proactive around the issue of spam by creating the well-written discussion paper.

We trust this response adds value to the process and look forward to seeing the resultant progress. We also look forward to being involved in the process going forward.

As part of this involvement we are keen to give Government insight into how a large scale New Zealand Internet business deals with a large volume of spam. We could do this by presenting to officials or arranging a visit to our premises to see how the mechanics of large scale spam control work in our business.

Similarly, should the IT & Telecommunications Policy Group proceed to hearing oral submissions, we would be pleased to present an oral submission.

Yours sincerely,

Michael O'Donnell  
Business Manager  
Trade Me