

netconcepts

36 Anzac Road • P.O. Box 35932 • Browns Bay, North Shore City
Ph: (09) 476-4601 • Fax: (09) 353-1414 • Email: infodesk@netconcepts.com

30 June 2004

IT & Telecommunications Policy Group
Resources & Network Branch
Ministry of Economic Development
P O Box 1473
WELLINGTON

Email: spamsubmissions@med.govt.nz

Background:

Netconcepts is a nine year old interactive agency specialising in email marketing, usability, search engine optimisation, and e-commerce. Clients include Vector, Westpac (NZ), the Fletcher Trust, Business in the Community, Sara Lee Direct, Sharper Image, REI, Cabela's, InfoSpace, Gorton's, and the American Marketing Association. GravityMail is Netconcepts' hosted email delivery service, and features personalisation, segmentation, and tracking capabilities. GravityMail services over 300 clients in the U.S., New Zealand, and Australia, delivering over 1.5 million emails per month to clients' opt-in lists. Of the email service providers in New Zealand, GravityMail is the only one recognised in MarketingSherpa's Global Top 50 list of Email Vendors. The founder and Managing Director of Netconcepts, Stephan Spencer, is on the executive of the DMA's eMarketing Network and on the board of the Sales & Marketing Institute of New Zealand. (Note that although Stephan contributed in part to the Sales & Marketing Institute's submission on the anti-spam legislation discussion document, he does not hold their views on the need or legitimacy of anti-spam legislation.) Stephan is a primary architect of the DMA / eMarketing Network's Standards for Search Engine Marketing, slated to be publicly launched in July 2004.

Responses to questions raised in the discussion document:

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

We indeed consider spam to be an important issue. Spam clogs our inboxes and those of our customers, so much so that the viability of legitimate permission-based email marketing is in trouble. Spam is unlike other media intrusion. No other media sends pornography to children who have email accounts. No other media allows a few hundred miscreants to blanket the earth with their "ads" at very little cost to themselves.

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

Legislation can play a useful role, but the Government needs to be careful about how it implements the legislation. Email is a constantly changing medium and legislation tends to be static. Therefore, we support the DMA's Email Marketing Standards and suggest that these Standards be overlaid on the legislation as an enforceable industry code of practice. The DMA's Standards has already been updated several times over the past two years because of the dynamic nature of email and the marketplace.

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

Existing privacy protections are sufficient to protect privacy, but not sufficient to stop spam. With that said, however, no amount of additional legislated privacy protections enacted by the New Zealand government are likely to significantly reduce the amount of spam.

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

The Harassment Act is not appropriate as spam is directed at nameless, faceless email addresses rather than identifiable individuals. Many people share an email addresses, and many people have multiple email addresses.

5. What message mediums should be caught by the legislation?

Email, possibly also Internet instant messaging. Not SMS, as from a practicality standpoint, the cost of SMS messages are borne by the sender and so the financial incentive for the spammer is much less than email or Internet instant messaging. Faxes, telemarketing, and direct mail should absolutely not be caught by the legislation, as it will just muddy the waters and is unnecessary.

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

Spam is spam regardless of the numbers involved, because it is unsolicited. The recipient doesn't care if they are one of a thousand or one of ten million affected – they care because they have been affected. The amount of spam sent by the offender should only be taken into account when assessing penalties.

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?

The legislation should only apply to messages of a commercial advertising or promotional nature. No exceptions should be given to charities or political parties..

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

Absolutely. The primary focus should be on minimising overseas spamming to New Zealand email addresses.

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?

Vendors and their agents should be covered by the legislation. ISPs, email service providers, email marketing consultants, and telecommunication companies should be exempted from prosecution unless they were knowingly involved in the act of spamming.

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

Opt-in, in our opinion, makes the most sense, as long as the legislation doesn't interfere with the ability of legitimate email marketers within New Zealand to do business. Our view of opt-out is that it burdens the consumer to opt-out of potentially many thousands of spam emails. Furthermore, that consumer still won't be able to trust the unsubscribe process because most overseas-originating spams won't comply with the NZ legislation. The U.S.CAN-SPAM legislation has shown us that. The double opt-in approach overburdens the small businesses because it requires technology that usually only larger businesses possess. Furthermore,

double opt-in, with all those confirmation request emails, will increase the volume of email and the effort required for the consumer, compared with a simple opt-in approach.

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?

This is a very important issue. It's unlikely that NZ marketers have collected opt-in date & time, IP address of opt-in, etc. in their opt-in databases. If an NZ marketer has a website with an opt-in form that only asks for email address, that opt-in database should be considered compliant as express consent according to the legislation. It would be disastrous for NZ marketers to have to go back and obtain a second opt-in on an already opt-in database, as it would likely reduce the list by three-fourths (an obviously NZ business-unfriendly result). Inferred consent should include customer and supplier relationships, and it should include the actions of handing over one's business card (after all, a business card's purpose is to convey contact details to facilitate future contact).

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

It should be a one-time opt-in. We should not have to go back to our database and keep pestering them to repeatedly opt-in after a certain time period.

13. Should there be a requirement for commercial electronic messages to accurately identify the sender of the message? If so, what constitutes accurate identification?

Yes. Only spammers forge or hide their identity, so this is a simple way for the legislation to catch only the spammers. We concur with what's recommended in the DMA's "Standards for Email Marketing," namely the sender's company or trading name along with either their physical address, web address, or phone number.

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, require a functional unsubscribe to be included in promotional messages, but don't require that it has to be by replying to the email. Clicking a link to a web page to unsubscribe should be sufficient, as it is an easier process for the recipient and doesn't clog up his Sent Mail folder with unsubscribe requests. Individual email correspondence should not require this. You you imagine the chaos if all email correspondence a businessperson sent through the course of the day via Outlook had to have unsubscribe instructions – everyone would be labelled a spammer.

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

The requirement should be to not provide false or misleading header or subject information. Then it's consistent with the existing body of legislation relating to fraud.

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

Labelling is an unnecessary complication to the legislation if by law the recipient must have opted in in order to receive the advertising or adult message.

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. Address harvesting software and harvest address lists is not good marketing practice and should be caught by the legislation.

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

The recipient or the ISP or the email service provider. In fact, anyone should be allowed to do in a spammer – even the spammer's subcontractors that they have hired.

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

We recommend the DMA's suggested approach a Government-funded, industry-run complaints body which could be given the power to adjudicate in all but the most serious cases. Then only major breaches of the legislation would be referred to an authority empowered to impose punitive measures.

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 recommend the approach taken by the Australian authority which has an escalating scale of fines depending on the severity of the offence.

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

Civil.

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

Yes. In the case of serious crime referred to the higher authority described in 19 above, the enforcement agency should be given full powers of entry, search and seizure of all material and equipment used in the course of the offence.

Kind Regards,

Netconcepts Ltd.

www.netconcepts.com

www.gravitymail.com