

29 June 2004

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

Dear Sir/Madam

SUBMISSION ON “LEGISLATING AGAINST SPAM”

INTRODUCTION

As an ordinary citizen, not representing any organisation, I have studied your Discussion Paper “Legislating against Spam”, and other documents such as David Harris © 2003 paper “Drowning in Sewage - Spam, the curse of the new millennium: an overview and white paper”. I obtained what I consider to be relevant information from the Internet on the topic of Spam, especially from European sources. In my opinion, the European Commission’s approach is much more thorough and well-considered, and should be the prime consideration when drawing up legislation for New Zealand.

I define spam as *“electronic messages for the purposes of direct marketing which the seller of the goods [or its marketer] has sent without the receiver’s prior and explicit consent”*.

In the Discussion Paper, there seems to be a major emphasis on the service provider who sends spam, whereas the emphasis should be on the company that wants to sell its goods and instructs the service provider to send direct marketing messages via electronic means to recipients. The originating company should be targeted in anti-spam legislation in the first instance, closely followed by the service provider of unsolicited messages. I believe it is more effective to target the company that sells the goods or services. If s/he is not satisfied with the service provider because of complaints about spamming, then the selling company will be more effective in black-listing the service provider by switching to an ISP that does not generate complaints, or effectively handles complaints.

THE SUBMISSION

In my submission, I have followed the numbering of the questions in your Discussion Document, and refer to them as ‘points’.

1. Yes, I consider spam to be an important issue. As a private individual, I receive about 40 spam messages per day. I have to go through them carefully in order to make sure that they are not from persons who genuinely try to make contact with me. I strongly disagree with the statement from a German judge at Dachau that “unwanted messages can be deleted quickly and without trouble”. This judge considered that “Spam with other advertising is socially acceptable and

necessary in order to keep the economy going". See http://www.euro.cauce.org/en/countries/e_de.html

In my opinion, spam is socially unacceptable [just like any form of unwanted advertising], if it has not been solicited, because it consumes the recipient's time and increases his/her telephone costs.

2. Yes, I do think that legislation has a role to play alongside other complementary measures, such as voluntary advertising and direct marketing industry agreements. In my experience as a public servant of some 34 years, such voluntary agreements tend to be extremely slow in being established without relevant legislation.
In this context, I wish to draw your attention to the "Code of Behaviour" drawn up by the Dutch organisation "E-commerce Platform Nederland" www.ecp.nl which comprises the three major marketing organisations in the Netherlands. Its "Code: Distribution of Advertising via E-mail" is claimed to go further than the new Dutch Telecommunications Act (see under point 18 below), and consumers can lodge complaints with the RCC ("Advertising Code Commission") which can publicise offending affiliated organisations and have them expelled from the main body. The RCC claims that "This form of self-regulation has been working effectively for more than 40 years". It may also be noted that the three major marketing organisations manage electronic advertising for banks and charitable institutions. See newspaper article 17 June 2004: <http://www.nrc.nl/economie/artikel/1087448370300.html>
3. No, I consider that the Privacy Act does not adequately protect individuals, as pointed out in para 25 of your Discussion Paper. Most search engines can be made to obtain ["harvest"] E-mail addresses without the permission of the individual. It is even easier to get lists of E-mail addresses from "providers".
4. Yes, I agree that stand-alone anti-spam legislation is preferable to reliance on the Harassment Act, with special reference to para 37 on the absence of transparency as noted in your Discussion Paper. I see spammers as the "dark side of humanity" who abhor transparency.
As reported in "The Dominion Post", 28 June 2004, page C13, "Few disagree that adding an authentication mechanism to E-mail services to verify the origin of messages will play a key role in stopping spam". As implied in my introduction, the firm selling the goods, should be clearly identified in the authentication procedures. These procedures should clearly identify the origin of the message and its routing; see under point 11 below, the Belgian approach.
The present "unsubscribe" function on some spam messages is a joke, as it confirms to the spammer that you read your E-mails and that you are thus a "live address". Most anti-spammers strongly advise against using that "unsubscribe" function. I certainly don't use it. You also make this point in para 64, second bullet point, of your Discussion Paper.
5. The message mediums that should be caught by legislation, should follow the EU approach: fax, E-mail, and other electronic messaging systems, such as SMS and MMS.
As reported in "The Dominion Post", 28 June 2004, page C13, the fact that marketing "organisations have to pay to send faxes and make phone calls, this should mitigate against the impact of spam with these mediums". An individual can hang up on telemarketers, and put "no circulars" on his/her letterbox to stop unwanted mail deliveries, but s/he still has to pay for the fax paper. Therefore, I prefer to see faxes included in electronic messages as the EU has done.
6. I don't think it matters how many messages are sent. The criterion should be that any message that an individual does not wish to receive can be effectively stopped from being sent to him/her again and again [ad nauseam].

7. I believe that all unsolicited messages of whatever nature should be able to be stopped by legislation. There should be no exemptions. The most effective way will be by insisting on authentication procedures, followed by effective anti-spam filters.
8. It would be nice if legislation (see para 55) could be extended to cover acts done overseas but I think that it is impractical and likely to be extremely costly to implement. An EU information sheet delicately states on this issue: “Modalities for cooperation with authorities in third countries will need to be developed”, see http://europa.eu.int/information_society/topics/ecom/all_about/todays_framework/privacy_protection/index_en.htm#unsolicited
The pragmatic Dutch don't attempt that either, but they do prosecute Dutch vendors who use overseas services, just as is proposed in para 54 of the Discussion Paper for NZ-based firms. I support this.
9. The vendor sponsoring the spamming and the sender of the spam should be covered by anti-spam legislation, but not the transmitters of spam, as long as they are unwitting transmitters. Once the telecom companies and the ISPs knowingly transmit spam, they should also be covered by legislation. In this context, the major telecommunication companies in NZ are to be commended for installing and updating anti-spam facilities on their networks. They are of course fully aware that transmitting spam places an avoidable burden on their facilities.
10. New Zealand should adopt an opt-in approach, just as the EU and Australia have done, and reject the US opt-out approach for reasons outlined in para 64 of your Discussion Paper. For the European Community approach, I refer to Article 13 “Unsolicited Communications” of “Directive 2002/58/EC of the European Parliament and of the Council, of 12 July 2002”, and to “Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC adopted on 27 February 2004”, which provides additional opinions on aspects of the EU opt-in regime.
11. Express consent should mean that the receiver of messages has consented to receiving specified messages from the seller/promoter. The receiver should be able to stop receiving such messages at any time if they contravene the specified approval in his/her opinion.
The sender of promotional material should adhere strictly to what s/he has been given approval for, and should not be entitled to pass E-mail addresses to other organisations, unless given specific and unequivocal approval to do so. The Belgian “Information Society Services (Bill)” states it very clearly in “Article 15 Advertising by electronic mail”:
§2. When advertising by email, the service provider [sender] is to ensure the following:
1. supplying clear and comprehensible information concerning the right to refuse such advertising in the future.
 2. to indicate an appropriate method to exercise this right efficiently by electronic means
- §3. when advertising by electronic mail, it is forbidden
3. to use the electronic address or identity of a third party
 4. to falsify or disguise information which makes it possible to identify the origin of the message or its routing. See http://www.euro.cauce.org/en/countries/c_be.html

In this context, notice should also be taken of the opinion “Lists of email addresses” in the above-mentioned Opinion 5/2004 (see point 10) which reads on p.6:

Lists which have not been established according to the prior consent requirement may in principle not be used anymore under the opt-in regime, at least until they have been adapted to the new requirements. Selling such incompatible lists to third parties is not legal either. Companies wishing to buy lists of e-mail addresses should be cautious that those lists are in

accordance with applicable requirements, and in particular that prior consent was given in accordance with those requirements.

12. The scope of any opt-in assent should be:
 - Full disclosure of contact details of the seller of the product/service
 - Full disclosure of the use that may be made of one's E-mail address
 - An efficient and effective option to cease or continue receiving E-mails with every message sent to the recipient
 - A requirement that the subject line shall accurately reflect the contents of the message.

13. The originator and the sender of electronic marketing messages should be required to identify him/herself via an authentication procedure: name, physical address, phone and fax number, and clearly identify the origin of the message and its routing.

14. Because of the lack of action on most "unsubscribe" facilities, and worse, the use of such facilities to send more spam (see para 64, 2nd bullet point, of the Discussion Paper), I have little faith in "unsubscribe" facilities, except as indicated in the next point. Therefore, I would give much more support for effective authentication procedures, and improved anti-spam software.

15. Yes, commercial electronic messages should provide accurate header and subject information; see point 12 above. Companies that provide annual reports etc via E-mail do this already. They also have effective "unsubscribe" facilities.

16. See answer under point 15 above, and for adult messages, that should an absolute requirement.

17. Anti-spam legislation should most definitely include rules against the supply, acquisition and use of harvested address lists; see comments under point 11 above.

18. While I support the suggestion in para 80 of the Discussion Paper that the Commerce Commission may be best placed to investigate and bring court action on behalf of victims of spam, I wish you to note that the Dutch Government has enacted a new Telecommunications Act on 19 May 2004. That Act is based on six European guidelines and forms the principal basis for the operations of the "Independent Post and Telecommunications Authority" (OPTA). This Authority is a quango and operates at a distance from the Dutch Ministry of Economic Affairs. The primary role of OPTA is the promotion of durable competition in the telecommunication and postal markets. The Minister of Economic Affairs is politically responsible for a number of OPTA's tasks, but cannot influence the decisions made by that Authority.
 The Authority is also responsible for the combating of spam and has established a "Spam Complaints Service" with its own website: www.spamklacht.nl OPTA points out that it is not the only body that ensures compliance with legal requirements relating to spam. There is also an "Personal Data Protection Agency" (CBP); see www.cbpreweb.nl
 Under Article 15.4 of the Dutch Telecommunications Act, maximum fines of €450,000 (NZ\$900,000) can be imposed, or 10% of the turnover of the company operating in the Netherlands, if warnings are not effective. OPTA can only control spam in the Netherlands, not in other countries, but just as proposed for NZ, it can prosecute Dutch firms that instruct service providers in other countries to send spam on their behalf.
 I strongly recommend that serious consideration be given to this Dutch approach and its possible compatibility with the role of the NZ Telecommunications Commissioner. As an alternative, it may be necessary to set up a separate Authority under the Telecommunications Act 2001 (or an amendment thereof, possibly of part 3 of the Act).

19. I recommend that serious consideration be given to expanding the role of the NZ Telecommunications Commissioner for reasons outlined under point 18 above.
20. The penalties should be primarily of a pecuniary nature as under the Australian [and Dutch] Spam Act. But the Australian penalties seem moderate in comparison to the penalties imposed by an Amsterdam District Court on 7 March 2002 in the case of XS4ALL vs. AB.FAB: €50 (NZ\$100) per message to a maximum of €2.5 million (NZ\$5 million). See http://www.euro.cauce.org/en/countries/c_nl.html The Australian penalties seem to be about on a par when compared to the maximum fines permitted under the Dutch Telecommunications Act; see point 18 above. I suggest that NZ follows a similar scaling of penalties as outlined in para 84.
21. Contraventions should give rise to civil pecuniary penalties as under the Commerce Act, for reasons outlined in para 86 of the Discussion Paper: the required standard of proof is less strict.
22. The responsible enforcement agency should be given the ability to obtain search warrants conferring powers of entry, search and seizure, because in my opinion spammers are the “dark side of humanity” who abhor transparency.

OFFICIAL INFORMATION ACT 1982

I have no objections to my submission being made publicly available by the Ministry.

PRIVACY ACT 1993

I have no objection to my name being included in a summary of submissions that the Ministry may publish.

Yours faithfully,

Nick C Lambrechtsen