
From:
Sent: Tuesday, 29 June 2004 10:38 p.m.
To: spamsubmissions@med.govt.nz
Subject: Submission on anti-spam legislation paper

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

I have long considered it to be an important issue. Approximately 70% of my mail is spam. At this level, I suspect that it is not simply advertising, but an attempt to wreck the email medium, and a weapon to be used against those one disagrees with. If you don't like what someone says, you sign them up to receive embarrassing spam. I believe I have been attacked in this way.

The possibility of such attacks biases me towards the safeguard of "confirmed" or "double" opt-in.

I have received spam messages with probably illegal attachments, traces of which may still remain on my disk storage, and put me in danger of unfounded prosecution. I would find it very difficult to disprove that I had downloaded such material myself.

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

Undoubtedly. To fail to legislate when other countries are legislating against spam poses the risk of New Zealand becoming a "spam haven".

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

No. The Privacy Act is directed to settlement. Spam is a problem that needs civil and probably criminal penalties.

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

The Harassment Act applies to actions directed against a particular person. It is unsuitable for the one-to-many abuse that constitutes spam. There should be specific anti-spam legislation

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)?

All of them: why not? Let's have a "technologically neutral" law. Persistent unsolicited and unwanted marketing messages should be legally prohibited.

Those who would limit these provisions to email argue that the recipient pays for email while this is not true of the other media. I ask these people: who do you think *does* pay for your local supermarket's junk mail? Thoughtless mass marketing costs us all in monetary terms and in terms of irritation. At the very least, I should be able to "opt out" of telemarketing (even when the marketer is not a member of the DMA) and junk mail. There is no reason why junk mail cannot carry a genuine return address or telephone number for opt-out requests, and phone telemarketers likewise honour a request to cease phoning a particular number.

A “no circulars” notice on my letter box still does not work for persistent junk-mailers and there should be legal sanctions to stop them.

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

There would be difficulty counting the number of recipients reliably, and if you make a law stipulating, say 1,000 as the limit, spammers would send an identical message to 999 recipients, then change the wording slightly and claim it was a different message.

There is, however, clear evidence of a “bulk” nature in some messages. When I receive a mail addressed to “s.ballmer@isp.net, s.bearman@isp.net, s.bell@isp.net, s.bellamy@isp.net,...that is clear evidence of an unselective sending. It may be difficult to define precisely, but such evidence of spacing should be taken as evidence that the message has been sent in bulk, as should a certain proportion of rejected messages from non-existent addresses. The latter is a metric that the spammer would be unable to control.

Following prosecution, the bulk of the spam should in any case be taken into account when deciding penalties (see retrospectivity of definition, below).

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?

To quote a well-known anti-spam activist: ‘ “Repent for the end is nigh” or “vote for Joe Bloggs” are just as much spam as “buy my widgets” .’ Political, religious, all are ‘promotional’ and all should be barred. At the very least, every kind of promotional message liable to be repeated should carry a functioning “unsubscribe” facility. By exempting certain kinds of messages, the Australians found themselves caught in a technicality which meant they could not insist on an unsubscribe facility in exempted messages. That situation should be avoided by regarding “promotion” as including political, religious and personal promotions.

As was pointed out at the Wellington workshop, xenophobic hate-mail such as that sent by a German-speaking source in large volume recently would not qualify as a commercial promotion; but few people would wish to receive it and most would call it spam, indeed one of the most damaging and undesirable forms of spam.

In summary, it is as difficult to define “spam” as to define the kinds of pornographic images that should be illegal (or, for that matter, to define what is “pornographic”). The ultimate solution is at hand from the censorship arena; where there is doubt whether something is “spam”, the sender and recipients should make their case before a panel similar to the Office of Film and Literature Classification. What the panel says is spam, becomes spam, and, if we followed censorship’s retrospective model, always was spam. If this week a message someone else received is declared to be spam, I should still be entitled to register a complaint about having received it last week and my reception of it should be counted in the assessment of any penalty.

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

Any kind of promotion in any medium, as above, which is directed to a New Zealand resident, should be illegal under New Zealand law. Assiduous effort should be expended in bilateral and multilateral agreements covering at least email messages.

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?

The vendor (sponsor) and original sender should be covered. The ISP should not, any more than they are, or should be, held to account for transmission of illegal pornography or copyrighted material initiated by their users.

Some ISPs, however, deliberately provide a channel for spammers, and there should be a way of holding such companies liable. An ISP should be expected to take reasonable technological precautions to filter spam; but this is probably a matter for a “code of practice” rather than inclusion in anti-spam law.

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

Definitely opt-in, preferably double opt-in, to prevent false subscription to spam services by malicious third parties (see answer to Question 1).

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?

There should be a standard form of words: “I consent to receiving material of (this/these kind (s)) from (this person) until (date) or until I give notice to that person to cease, whichever is the sooner.” Such a message should be kept on file by the marketer, who should be able to produce it on demand, or be judged guilty of sending unsolicited messages.

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

It should be defined under “material of this (these) kind(s)” as above, and in cases of doubt, referred to the “Spam Classification Office” for a ruling.

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)?

Yes, there should be such a requirement, which should include at minimum, name and physical address. An email address should ideally also be provided, so a recipient who wishes to stop receiving the messages can notify this and have it acted on quickly.

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.

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

This should be encouraged as a matter of good marketing practice, but I do not consider it should have legal force.

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

Again, the former might be adopted as a matter of good marketing practice, especially where the intent of a message might be unclear much as a newspaper advertisement that looks like editorial is labelled. But in view of the other sanctions against spam, it would be inappropriate to give this additional measure legal force.

“Adult” messages: my instinct says yes: give them a label so they can easily be filtered and kept from the eyes of children and sensitive people. But there is a potential minefield in defining what is “adult”; this is seen in many incidents involving censorship filters, particularly in the US, where minors have defended their right to receive, for example, messages seriously discussing homosexuality. There is no easy answer. Obviously erotic, pornographic or violent subject matter should be so marked, but it should be made clear that some matters are on the borderline and there should be no guarantee of enforcement to everyone’s sensitivities; more of a “best efforts” policy. Again, judgment of the need for an “adult” label should in cases of doubt, be referred to a panel with the power to rule on such matters.

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; such lists should not be dealt with unless every person on them has opted in or been given the opportunity to opt out.

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

A recipient should have the right to complain to an official body (I suggest the Department of Internal Affairs, in the same area as gaming and censorship) and if the complaint is found to have substance that body should bring the action.

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

Internal Affairs, with its experience in enforcing censorship and gaming legislation, seems the best choice.

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?

Since the profit to be made from spamming increases virtually without limit, it is difficult to put a firm limit on penalties. I would say at least a six-figure sum as standard, with increased penalties for subsequent offences. There should also be a provision to confiscate profits demonstrably derived from spamming, as with drug trading.

Imprisonment should be an option in serious (large bulk) cases, or for persistent repeat offending.

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

Both.

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

Yes.

ends

Regards

Stephen Bell