
From:
Sent: Friday, 25 June 2004 6:03 p.m.
To: spamsubmissions@med.govt.nz
Subject: Submission

Questions for Discussion and Response from www.med.govt.nz/pbt/infotech/spam/index.html

Email: spamsubmissions@med.govt.nz
Comments should be received by 30 June 2004.

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

Yes by it's very 'irritative' nature

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

Yes

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

Obviously not.

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

Yes if the Harassment Act is unable to stem the flow of "Spam" or other 'invasive' message techniques.

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)?

ANY message medium from electronic, written or verbal unless it is obviously sought by the recipient. For example, by entering a place of business, phoning a sales outlet, attending a 'show' (e.g. Home show) Put another way any communication that enters a persons 'personal space' should be subject. This would cover those annoying telemarketers that ring at dinner time, spammers, Txt messages at 2am and of course the 'junk' mail that goes into one's letterbox. However messages in a public space would be allowable provided the delivery method didn't invade the private space mentioned above e.g. strolling through a Mall and being subject to loud 'buy, buy, buy messages from a loudspeaker would be a no no.

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

I would ask any Communication promoting / selling / advocating any goods /service / belief that the recipient could reasonably be expected to ignore if it were say in a newspaper / magazine / on television be included in the definition of spam. This by implication means one or more.

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?

All "Unsolicited" messages should be subject. The exceptions would have to be made for 'formal' communications from Government, Local Authority and other such 'State' bodies, and where a business relationship has been entered into consensually e.g. power, phone and other similar companies. It may well be a suitable act to include some 'guidance' to companies about smothering increases / changes in charges with promotional material in the same envelope. It would also be helpful if it addressed the 'affirmative' action type

of advice notice. i.e. 'unless you tell us we will put the fees up/ make changes unilaterally' All of these 'changes' buried in an envelope / email etc that has so much promotional "Spam" the recipient mistakenly tosses it out in the belief it's all "junk" Perhaps if a communication contains more than 10% advertisement/promotion that any 'notice' included shall be illegal/unenforceable if not accepted in writing by the addressee.

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

Yes if possible. Any act or omission covered by legislation in NZ should be applicable to 'Spam' entering the NZ geosphere. This should not extend to "Censorship of Information" of the type one would expect to receive from Radio, TV, newspapers, Websites or similar Broadcast Media. This would give NZ authorities the opportunity to take action against persons or organisations benefiting from the actions of other(s) outside of NZ that would otherwise be subject to the legislation.

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?

Go for the guy at the top, but do make it a crime if it is patently obvious that the legislation is being contravened. If an offender is caught then their employer/superior/contractor should be held responsible. i.e. the "I don't care how you do it but don't get me involved" type of buck passing. Perhaps another way of looking at it is to make it a crime to induce others to commit an offence against the act. The only exceptions I would perceive as acceptable would be for downstream carriers who may reasonably expect the upstream source to have verified the authenticity of the sender. Maybe this would encourage the development of protocols to enforce accurate sender information that can be traced back to the individual that sent the email (or letter, or telemarketing call for that matter)

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

PLEASE, PLEASE, PLEASE Double Opt In ONLY (think of the door to door cooling of period) The only method of obtaining permission should be by a letter posted to the addressee requesting permission to communicate with the addressee. Full disclosure of who is requesting. Acknowledgement in such a letter that if further communication takes place, the offender shall pay the addressee a fee (i.e. dollars up front) for sending the communication.

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?

Signed express consent in writing, nothing less. And that such consent shall apply to that individual person (salesperson) alone and to the immediate organisation. All consents should contain a sunset clause to a maximum of (say) 12 months, any that do not shall be deemed withdrawn one month after signing by the addressee. Such consents to be invalid for 'parent organisations, their Siblings and Child Organisations. Such consents to 'expire' once the authorised 'salesperson' leaves the organisation. (Or transfers to a Parent, Sibling or Child organisation)

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

A letter of 'request to communicate' to the addressee with a second letter or phone call of confirmation only after a positive response has been received to the first letter. See also #10 above.

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)?

Name AND physical address of not only the company but the individual authorising and or

sending such communication. Such disclosure to be truthful, accurate and precise. Truthful Accurate and Precise to include physical address, manned phone numbers, etc. All contact information to be 'actual' ie not one or more steps removed by the use of 'agents' like answering services or Post Office Boxes. I feel it should be a requirement that contact phones must be manned by real live people working for the organisation not a Call centre service, mail is to be answered within one working week, again by company / organisation staff. There should also be a person with authority to act on the companies behalf available at the physical address. This physical address to be accessible during normal business hours. i.e. that there is several methods of making these people understand that I/You/Whoever do not want to hear from them (ever again!)

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. Clear penalties for not maintaining such unsubscribing mechanisms and ensuring they are 100% effective. See also #13

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

Yes. Accurate, Precise and understandable. See #13 again

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

Yes. In Clear (plain) text.

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. As it is difficult to conceive of a reason to 'harvest' email addresses for any other reason than for 'Spamming' just outlaw the use of email address harvesting 'bots' Also make it an offence to knowingly, or by omission pass email addresses to another person or organisation without signed authorisation to do so from the addressee. Single exception should be the passing of a friend/acquaintance/business contact's email to another person so they may contact such people 'personally' e.g. passing the email address of someone who knows about Genealogy to someone interested in finding out about their family's history. It is also interesting to note the recent 'Fair Go' revelation that the Motor Vehicle Register is being abused by organisations using the Registers 'Public' status to obtain thousands of names and addresses for no other good reason than to inundate people with their messages/mailouts etc.

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

Any person or organisation affected by the receipt of 'Spam' Action by way of reporting to the Agency responsible for enforcing the legislation

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

Internal Affairs, Customs, Police ? whoever would be EFFECTIVE in this role.

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?

Commensurate with comparable privacy legislation. Publication of offender's full name and town (suburb) in suitable media, in electronic media for 'Spammers' No Community Service sentences to escape public notice. Strong fines based on number of messages, how irritating the message is, and the degree of avoidance measures taken to get their message out.

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

No opinion other than make them pay!

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

Yes.

General submission.

1 I would submit the legislation also includes laws preventing 'cloning' of websites as done in the article by Bruce Simpson at <http://aardvark.co.nz/daily/2004/0528.shtml> where a motel had it's web page 'ripped off' (my words) by someone else. Banning of 'Recursion' i.e. multi layered pages / links hiding the real website and creaming a percentage off the top.

2 I would further submit the intent and scope of this legislation be expanded to include all communications and or contact via any medium other than a clearly defined set of methods. This would then cover future technological developments which I can only see as being even more invasive than the present methods.

*3 One anti spam option conceivable is a mechanism (Website?) whereby a person may quite clearly indicate they do not wish to receive "Spam" (or for that matter telephone pitches, advertising mail outs etc) I believe there is a system operating in the USA where you may list your telephone number as 'off limits' to telemarketers. Contravention of this list I understand carries quite heavy penalties.

4 Alternatively a public list may be created on a similar suitable medium that any person may indicate their willingness to receive 'Spam' on payment of an agreed 'fee' to that person. A suitable mechanism would be that employed by the likes of 'Pay Pal' Any such opt in participant shall be duty bound to accept any communication provided it is of no 'cost' to the addressee (cost in this context would include \$, time, and any other 'tangible' resource beyond a few minutes collecting email, or the walk to the letterbox / phone.) There would be no obligation on the addressee to act upon the communications content.

5 Any communication promoting goods or services should carry the word Advertisement as the first word in the communication immediately prior to any other content (pictures, graphic, text etc) This word "Advertisement" to be more prominent than other text or graphic in the communication.

6 I feel it would be fair to also include religious/political/militant groups under the scope of this legislation as personal experience has taught me that some of these people can be just as, if not more, insensitive to the invasive and sometimes offensive nature of their 'Cause'

7 It is interesting to note the Consumers Institute is guilty of mail 'Spam' via inclusions in subscription magazines etc. Could the legislation look at such 'inclusions' as well?

8 Finally may I make a plea for what is termed 'Spyware' to be subject to some sort of provision in the legislation. Spyware (also know as Adware, Malware and other less repeatable terms) is usually included 'within' another computer program and has objective's that can only be described as 'Covert'. This 'Spyware' can literally bring a PC to it's knee's in a relatively short space of time, all without the user of the PC being aware of anything being installed on the PC.

Sometimes this Spyware installation is notified within the 'License' that a person must agree to before any 'wanted' program will install. I would assume this is to satisfy the 'Legal notice' requirement one could reasonably expect to be advised of. However this notice is frequently buried, obfuscated, or otherwise disguised, making reasonable understanding of exactly what is being installed on your PC difficult if not impossible to make. There is also a class of 'applets' that get installed without the user's knowledge simply by 'browsing' the Web. A common example of this is what is known as 'Browser Hijacks' where after visiting a Web site the home page of the browser is reset to the Hijackers Web site and not the one the owner/user of the PC wants. I frequently

see reports of PC's that have heavy infestations with 'Spyware ' to the point where they will not boot, or if they do, perform so slowly or with such 'crankiness' they are patiently unusable. Spyware 'objects' in excess of 100 are common, it is not uncommon to find in excess of 400. Members of nz.tech have reported cases in excess of 1000. For a fuller explanation of Spyware & Adware etc please visit:
<http://www.spychecker.com/spyware.html>.

Conclusion

In my above submissions I hope I have conveyed the sense of frustration that overwhelms the users of Personal Computers when subject to the effects of "Spam" and "Spyware" Also the frustration one is subject to when as a normal member of society one is inundated with other 'Messages' (mail, phone etc) The people subject to this barrage of 'hype' that find it most frustrating are the 'non tech' users, the Mom and Pop's of this country, the harassed secretary trying to get an important email sent or the retiree who finds their home page directed to a porn site. The message I have received from these people to these 'Advertisers' is loud and clear "GET LOST"

Many proponents of these products argue that 'you don't have to read it / install it' or other self interested platitudes. However I find these arguments weak, facile and insipid because, to use an old fashioned analogy, the cards are stacked in their favour. In other words the proponents of these products know the average 'consumer' of their products has either no idea they are subject to their covert operations, or if they are the 'product' is so difficult, convoluted, impossible to remove or plain unavoidable the average user does not have any 'Reasonable' control over those products.

In nature a 'Person' by the benefits of evolution generally has the 'skills' to protect themselves from the rigors of their environment. However academic equality is a quality that a person has to 'learn'. Computer knowledge and skills fall very firmly into this 'academic' area of life. The breadth and depth of Computer learning (knowledge?) is such that it would in my opinion be "Unreasonable" for a person to be aware of the subtleties involved with such a field of expertise.

Therefore it becomes important that 'Society' levels the playing field by requiring the purveyors of such 'Spam', "Spyware" and other 'Hype" products to provide clear, accurate and prominently presented information about their product and all its objectives. Moreover that such purveyors of such 'Hype" be forced to accept that they can not invade a persons 'personal space' It seems patently obvious to me that legislation is the only way to moderate their otherwise unfettered behavior.

After all society makes provision for Deaf, Blind and Handicapped person's to make 'Reasoned' decisions (choices) about something they can not hear, see or comprehend.

Yours Sincerely

Paul Collins