

Personal Submission

MED Discussion Paper: Legislating Against Spam

- 1 The following is a personal submission from Mike Pearson. The submission is structured as general comments on the sections of the discussion paper, followed by answers to each of the specific questions (1-22). I have no objection to any information in this submission being publicly released.
- 2 Disclaimer: The views expressed in this submission are not necessarily those of my employer (E-government Unit, State Services Commission), but are a personal view only

General Comments

Introduction

- 3 Principles – The discussion paper has not outlined any high-level principles, and therefore misses an opportunity to have them agreed by the interested parties. Principles are fundamental to good governance, and would help guide the development of the final solution, and any amendments to the solution in the future. Some examples:
 - Practical – the solution must not act as a barrier to genuine unsolicited bulk messages
 - Enforceable – the solution must be enforceable and must be enforced
 - Technology neutral – the solution must be able to cope with unsolicited bulk messages through other channels
- 4 Therefore, there is a risk that interested parties will disagree on fundamental aspects of the solution and continually re-litigate. Similarly, when changes are required in the future, because principles were never agreed, then the change process will be more difficult than it needs to be.

Background

5 Para 9 – This paragraph appears to indicate that the spam issue is actually about unsolicited bulk messages between countries. This raises the question of why introduce legislation that also enforces spam control on New Zealand organisations communicating in New Zealand? If NZ-internal spam is not an issue, then this is an unnecessary compliance cost on the majority of New Zealand organisations.

6 Para 10 – The discussion paper does not clearly distinguish that there appears to be two types of unsolicited bulk messages:

- **Fraudulent spam:** Typically from overseas organisations, sent from an unauthorised source, with a fake return address, promoting dubious products or services. This is a “Tragedy of the Commons” issue.
- **Genuine spam:** Typically from New Zealand organisations, sent from an authorised source, with a valid return address, seeking to establish a commercial arrangement for delivery of a good or service. This is a social issue.

7 Therefore, the paper is confusing, because it is discussing a variety of controls; the controls may be of use to one or both of the spam types. There is a significant risk that the final solution is not satisfactory in dealing with both issues.

8 Para 13 – The statistics quoted for MessageLabs show that the growth of detected spam from 60 to 350 million messages per month, in less than a year. This suggests that genuine spam messages make up a reducing percentage of the volume and are probably negligible. The major issue is actually fraudulent spam.

9 Para 14 – The current fraudulent spam issue should be analysed as a “Tragedy of the Commons” scenario. Any solution can then be measured against commonly used solutions in such scenarios, to test for robustness.

10 The definition of a “Tragedy of the Commons” is:

A "tragedy of the commons" arises when a common resource is degraded by over use. Well-known examples are ocean fisheries, urban roads, air and water. Whenever a public good (or "bad"

PERSONAL SUBMISSION: Mike Pearson
MED Discussion Paper: Legislating Against Spam

as in the case of road congestion) does not belong to some legal entity empowered to manage the resource through usage restrictions and/or fees, there are inadequate incentives for individual users to restrict usage to the socially optimal level. Consequently, the public good deteriorates (or the public bad swells), and the public suffers a loss relative to the potential social benefits of the commons.

The Internet: A Future Tragedy of the Commons?
http://cism.bus.utexas.edu/alok/wash_pap/wash_pap.html

- 11 The Internet is managed with usage restrictions and/or fees. Senders of fraudulent spam typically send messages from third-party computers that have been compromised by malicious software, to be used as distribution points. The sender is using someone else's computer for dishonest purposes. A number of these computers are in New Zealand.
- 12 Para 17 – Mention should be made of the impact on blind and visually impaired users, using text-to-speech software.

For the millions of blind and visually impaired Internet users around the world, using text-to-speech software is often the only way to check e-mail. But as the spam problem gets worse, more and more of those users are finding that having their e-mail read aloud can be a minefield.

Blind users are finding that they are spending disproportionately more time sorting through their junk e-mail than their sighted colleagues. That's because sighted users can simply scan large batches of messages for that one important piece of mail, whereas blind users must listen to the subject line of each message before they know whether it's spam or not.

It's a process that has become so unbearable that some blind users say they are giving up on e-mail altogether.

PERSONAL SUBMISSION: Mike Pearson
MED Discussion Paper: Legislating Against Spam

Blind Get Earful of Spam Daily

<http://www.wired.com/news/technology/0,1282,63934,00.html>

- 13 Para 18 – A more significant technical measure is the authentication of sending computers to confirm they are authorised to use the “FROM:” address, before they send the message. Ensuring a genuine “FROM:” address, allows accountability after the message has been sent. It also ensures fraudulent spam is not moved through the system, consuming resources.

Existing Legal Framework

- 14 The lack of analysis given to the Crimes Amendment Act (No 6) 1999 seems to indicate that the issue is only viewed as a genuine spam issue, yet:

- The amount of genuine spam is negligible
- The majority of spam is fraudulent spam
- The majority of fraudulent spam crosses international boundaries
- The majority of fraudulent spam is distributed using compromised PCs

- 15 The Crimes Amendment Act has several sections which are relevant to the distribution of fraudulent spam:

- 250 - Accessing computer system for dishonest purpose
- 251 Damaging or interfering with computer system (includes denying of service to authorised users)
- 252 Making, selling, or distributing or possessing software for committing crime
- 253 Accessing computer system without authorisation

The Consent Issue

- 16 The discussion paper only discusses the initial consent process – it does not discuss the removal of consent process, which is equally as important. Specifically individuals must have the right to opt-out later, in a manner that is as easy as it is to opt-in.

- 17 The paper provides the following consent options:
- Explicit consent to a specific sender in advance (opt-in)
 - Explicit denial of consent to a specific sender retrospectively (opt-in)
- 18 The paper has failed to discuss other consent options, which are equally as valid, such as:
- Blanket consent to all senders in advance (opt-in)
 - Blanket denial of consent to all senders in advance (opt-out) “no circulars”
- 19 Since the receiver is paying for the communication, then they should be in control over what messages they receive. The “no circulars” option would be attractive to many receivers.

Specific Answers to Questions

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

Fraudulent spam is an important issue. I receive over 200 spam messages a day, and this has significantly affected me in the following ways:

- I am harder to contact, because I avoid publishing my email contact details on the Internet;
- I have incurred financial cost, because I have purchased spam-filtering software;
- I have incurred business loss, because my Service Provider has put in place filtering software that is not always accurate;
- I have incurred time loss, because I have to visually filter my messages;
- I have incurred reputation loss, because my email address has been falsely attached as the FROM: address on fraudulent spam; and
- I have incurred denial of service, because my mailboxes have filled with spam and I cannot receive genuine messages.

Genuine spam is **not** an issue. Messages from genuine senders have typically offered ways to unsubscribe, and they have been acted upon.

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

Enforcement of existing legislation has a role to play for fraudulent spam. Technical measures are required, to reduce the opportunities to send fraudulent spam.

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

Existing privacy protections are adequate for genuine spam.

There is a wider privacy issue related to the use of personal information gained from public registers. This is not a spam issue.

Fraudulent spam impacts on corporate entities too, yet privacy protection does not cover such entities. Privacy legislation is the wrong place to provide protection against spam.

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

Yes.

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)?

As stated previously, spam is a "tragedy of the commons" arising when a common resource is degraded by over use. Therefore the legislation should be technology neutral and seek to outline controls when such situations arise.

The convergence of technology means it is possible to move messages between mediums very easily. Other mediums may encounter the same issues.

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

Frequency and quantity are only one-way for the "tragedy of the commons" to occur. Other ways may include many individuals all taking the decision to send one message.

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 fraudulent spam should be caught.

No genuine spam should be caught.

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

For fraudulent spam, existing legislation (Crimes Amendment Bill No 6 1999) already covers acts done overseas.

For genuine spam, there does not seem to be an issue.

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?

All parties should be held responsible for fraudulent spam. This includes telecommunications companies and ISPs, where they can check the authenticity of messages being sent through their networks, and the authenticity of senders attempting to send over their network.

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

For fraudulent spam, no approach will work – as the sender does not care.

I do not receive enough genuine spam for it to be an issue.

If it was an issue, then I would prefer opt-in or “no circulars” (see my general comment)

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?

For genuine spam, I believe there are already social conventions over many such matters. Most senders will assume blanket approval to send “critical announcements”. They may ask for approval to send “general announcements” or “product announcements”.

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

Any assent should only be for the explicit organisations named.

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. This would solve fraudulent spam. Genuine spam already has accurate information.

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?

No. The recipient should however, have confidence that they can reply to the sender, and ask to be removed. Similarly that the sender's address will still be active, i.e. messages are not sent in a one-way direction, directing the recipient elsewhere.

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

Yes. This would solve fraudulent spam. There should be an additional requirement that telecommunication companies and Service Providers do not pass on messages that are not accurate.

The above wording is a very technology specific solution. It should be more generic about ensuring a reliable sender name and address, that can be replied to, and traced back.

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

No. Labelling of content is a social and cultural judgment. This would create confusion in an international messaging environment. It is also a very technology specific solution.

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?

Fraudulent spam is already covered by the Crimes Amendment Act No 6 1999.

For genuine spam, this would depend upon what approach is adopted for achieving consent, and how the messages are sent.

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

Anyone.

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

For fraudulent spam, we need an agency that has the capability to enforce the existing legislation.

For genuine spam, an industry group is probably 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?

Fraudulent spam is already covered by the Crimes Amendment Act No 6 1999.

For genuine spam, if legislation is decided, then it should be civil penalties, linked to financial gain.

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

See answer to Q20.

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

See answer to Q20.