

LEGISLATING AGAINST SPAM

August 2004

Introduction

- 1 The Government has recognised that spam is becoming a major problem, and that a number of governments around the world have enacted or are proposing legislation as one way of curbing spam growth. The New Zealand Government has signalled that legislation against spam is an appropriate measure for New Zealand.
- 2 In May this year, the Government issued a discussion paper to seek feedback on the various policy issues which are raised when considering anti-spam legislation. Forty-three submissions in response to this discussion paper were received - from industry and specialist groups, businesses, ISPs, telecommunications companies, government agencies and individuals. An industry workshop organised by InternetNZ was also held as part of the consultation process.

Summary of Submissions

IMPACT OF SPAM AND ROLE OF LEGISLATION

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

- 3 The response was unanimously yes. Spam has markedly eroded people's confidence in the reliability of email (through false-positive spam detection and anti-spam measures that misfire). While effective filtering reduces the overall quantity of spam reaching the end user, this is merely a movement of the burden, not a solution.

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

- 4 Almost all respondents agreed that legislation is required, especially for global cooperation and to prevent New Zealand from becoming a haven for spamming.
- 5 Some organisations favour self regulation, but understand the need for legislation for the reasons above.
- 6 Email is a legitimate and often effective marketing communication medium, but some businesses have concerns that compliance costs and "the prospect of being accused of spamming in the course of attempting productive communication" will be an "intimidating deterrent" to using email as a marketing tool. There was comment that the legislation in Australia has been labelled a "disproportionate solution to the spam problem".

EXISTING LEGAL FRAMEWORK

Do you consider existing privacy protections in this area sufficient?

- 7 All but two respondents said no. A few respondents pointed out that while the Privacy Act did address specific privacy aspects of spamming it would not be sufficient to deal with the spam problem.

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

- 8 All but two respondents (same ones as above) said yes.

LEGISLATIVE SCOPE

What message mediums should be caught by the legislation?

- 9 Many respondents said that legislation should be technology neutral, but most felt that electronic media, especially those which involve little costs to the sender and/or the burden of costs falls upon the recipient, should be the focus of legislation. The feedback from most submissions and the InternetNZ workshop was that email, instant messaging and text messaging should be covered, while faxes, telemarketing and physical mail delivery should not.

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

- 10 Almost all respondents thought that the number of messages sent was irrelevant – the issue of concern is consent, but that the multiple/bulk aspect of spam should be addressed in the penalty provisions of legislation.

Should the messages caught by the legislation be of a commercial and promotional nature only or should other types of messages be caught? Should there be exceptions and if so what should be exempted?

- 11 Most respondents felt that the definition “unsolicited messages of a commercial or promotional nature” is a good starting point.
- 12 Some defined “promotional” widely to also include messages from political, religious, and charitable (and pseudo charitable) organisations. Others broadened the definition even further to include any unsolicited message.
- 13 Some businesses believe that it is crucial that the content of spam should be defined narrowly, so as not to inadvertently capture normal business communications. It was suggested that the above definition could be narrowed, for example, to “unsolicited messages of a commercial or promotional nature where no prior consent or relevant relationship exists”.
- 14 It was also submitted that any definition of spam will need to be cast so as not to infringe upon the Bill of Rights which provides that “everyone has the right to freedom of expression including the freedom to seek, receive and impart information and opinions of any kind in any form.”

15 All but two respondents did not want any exceptions.

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

16 All respondents said yes, and that the Australian legislation provided a useful model. One respondent did, however, highlight that the extraterritorial impact of legislation in Australia and the potential conflict of laws have created a few problems for Australian corporations and their subsidiaries, for example, offices in the UK must comply with both Australian and EU legislation.

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?

17 The response was a unanimous yes. Most respondents exempted telecommunications companies and ISPs, and some mentioned email marketing companies, if they unwittingly conveyed spam. However, any telecommunications companies and ISPs knowingly involved or reasonably expected to know that spamming was occurring, would not be exempt from legislation.

CONSENT – OPT-IN OR OPT-OUT

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

18 Most respondents preferred an opt-in approach, with a few preferring double opt-in.

19 The respondents who wanted an opt-out approach were mainly concerned with being able to legitimately and cost effectively market or provide information on their products and services to their customer base. They felt that an opt-in approach places “the lion’s share of the compliance burden on legitimate businesses which have nothing to do with the spam problem”. It was also argued that opt-out preserved email as a key contact tool for vendors, who would not (unlike spammers) risk irritating customers with excessive emails. Opt-out supporters also argued that opt-out provides a more definitive approach to consent compared to opt-in, which produces grey areas with concepts such as inferred consent.

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

20 Many differing views were received to these questions – however, most are variations on basically the same approach or different ways of expressing the same approach. This highlights the fact that the issue of consent and in particular, the wording of legislation with respect to consent, will be one of the most difficult aspects of effective anti-spam legislation.

21 Many said that the Australian legislation provides a useful starting point. Consent could involve one or more of the following concepts put forward in submissions:

- Express consent and inferred consent;
- The sender has “reasonable grounds” for believing that a recipient has consented;
- The recipient has a means of opting out of future mailings, even where the recipient had given explicit consent;
- There is a relevant pre-existing business or personal relationship between the sender and recipient.

TRANSPARENCY

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)?

22 All respondents replied yes. However, there was no consensus as to what minimum details should be provided, apart from the sender’s name, company or trading name. Other contact details required, included one or more of website address, email address, physical address or phone number. Some stated that the contact method had to be where the sender could be contacted directly.

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?

23 Almost all respondents replied yes. The few who said no were concerned with “trick” unsubscribe mechanisms.

24 Some respondents said that the unsubscribe mechanism must be usable at no charge to the recipient, and need not be an email address, but can be a website link.

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

25 All respondents replied yes. Some suggested that this requirement would be better framed along the lines of the Fair Trading Act, that is, the header and subject information should not be misleading or deceptive.

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

26 There was no consensus on this issue. The respondents who replied yes were mostly individuals, while those who replied no were businesses and industry groups, who argued that labelling was not necessary in an opt-in regime (a couple of respondents suggested labelling of adult material only).

PRIVACY – ADDRESS HARVESTING

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?

- 27 All respondents replied yes, with some emphasising that the supply, acquisition and use of address-harvesting software per se should not be prohibited, only that undertaken in connection with the unlawful sending of messages.

ENFORCEMENT

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

- 28 Most respondents recommended an appropriate government agency and ISPs as those who should be able to initiate action. Some ISPs, however, were concerned that a provision which allows them to sue may result in pressure on them from customers to take potentially costly legal action.
- 29 Some said anyone who has suffered damage or loss by a spammer's activities should be able to take action, but it was pointed out that in reality, individuals generally will not have the resources to do so.

What agency should have the enforcement role under the legislation?

- 30 There were mixed views. Some named the Commerce Commission or Department of Internal Affairs, while some suggested a Government-funded industry-run agency. This agency would handle complaints, education, codes of practice and powers of adjudication in all but the most serious cases. Major breaches of the legislation would be referred to an existing Crown agency for prosecution or search warrants. Some respondents had no view on what the enforcement agency should be but stressed that the agency must be adequately and appropriately resourced and funded, and be aggressive in its enforcement.

What should be the available penalties and remedies for breaches of anti-spam legislation and what should be the maximum fine or pecuniary penalty?

- 31 Most respondents recommended escalating pecuniary penalties depending on the severity of the breach. The penalties also should be commensurate with those under the Fair Trading Act and Commerce Act. It was also suggested that monies earned from, and equipment used in, spamming could be seized.

Should contraventions give rise to criminal or civil penalties?

- 32 Most respondents recommended civil penalties, but some said both, as some spamming activity could be fraudulent or malicious.

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

- 33 Almost all respondents replied yes, and some emphasised that searches should only be authorised by judicial warrant.

Next Steps

- 34 The Ministry will now seek approval from Cabinet on legislative policy principles, which are being developed taking into consideration views expressed in the submissions. Once approval has been given, a bill will be introduced to Parliament for debate.