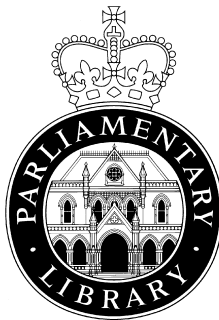


BILLS DIGEST

UNSOLICITED ELECTRONIC MESSAGES BILL 2005

Date of Introduction: 28 July 2005

Bills Digest No. 1309



NEW ZEALAND PARLIAMENTARY LIBRARY

Bills Digest No. 1309

Published by the Parliamentary Library
Parliament Buildings, Wellington
New Zealand.

31 August 2005

Prepared by John McSoriley B.A.L.L.B., Barrister
Legislative Analyst
Ph. (04) 471-9626 (Ext. 9626)
Fax (04) 471-1250

Caution

This Digest was prepared to assist consideration of the Bill by members of Parliament. It has no official status.

Although every effort has been made to ensure accuracy, it should not be taken as a complete or authoritative guide to the Bill. Other sources should be consulted to determine the subsequent official status of the Bill.

Copyright

© NZ Parliamentary Library, 2005

Except for educational purposes permitted under the Copyright Act 1994, no part of this document may be reproduced or transmitted in any form or by any means, including information storage and retrieval systems, other than by Members of Parliament in the course of their official duties, without the consent of the Parliamentary Librarian, Parliament Buildings, Wellington, New Zealand.

This document may also be available through commercial online services and may be viewed and reproduced in accordance with the conditions applicable to those services.

UNSOLICITED ELECTRONIC MESSAGES BILL 2005

Date of introduction:	28 July 2005
Portfolio:	Information Technology
Select Committee:	As at 30 August, 1 st reading not held

PURPOSE

The Bill “implements the Government’s decisions on the regulation of unsolicited electronic messages (commonly called “spam”) as part of a “multi-tiered strategy to combat the growth of spam along with self-regulation in the form of industry codes of practice, education and awareness campaigns, improved technical measures, and international co-operation.

BACKGROUND**The need for the Bill**

“Spam is generally described as unsolicited electronic messages, usually in the form of commercial marketing emails. Most of the spam received in New Zealand originates from overseas. According to New Zealand internet service providers (ISPs) and anti-spam solution companies, spam accounts for about 40% to 75% of all email traffic [in New Zealand] (estimated at over 350 million messages per month). While effective filtering reduces the overall quantity of spam reaching the end user, this is merely a movement of the burden from the recipient to the ISP, not a solution.

“The problems associated with spam include the annoyance and loss of time involved for users in dealing with large quantities of unwanted emails, the consequent loss of user confidence in dealing with business and other communications online, the consumption of network and computing resources (as well as email administrator and helpdesk time), and the loss of worker productivity (eg, a United States survey has estimated the economic cost of spam is US\$874 per year for every US office worker). Spam is also associated with attacks on the security and integrity of computer networks through viruses and the like, identity theft (eg, emails seeking personal information from users and masquerading as emails from a bank), and the sending of offensive or indecent material.

“Existing laws, which can generally deal with spam content issues such as offensive or misleading material, are not specifically designed to deal with the problems associated with large spam volumes or mass e-marketing; and technical solutions do not alleviate the load of spam on the internet infrastructure before it reaches the recipient’s ISP”¹.

¹ Unsolicited Electronic Messages Bill 2005, Explanatory Note, Regulatory impact and compliance cost statement, p. 10.

The proposed anti-spam measures ban the sending of commercial spam without the prior consent of the recipient. Commercial electronic messages are required to include accurate identification details of the sender, and the distribution and use of list-generating software (and address lists) are banned.

The Bill provides a definition of a “New Zealand link” (*Part 1, Clause 4(2)*) specifying when commercial spam becomes subject to the Bill. Basically, the Bill is directed at New Zealand originated spam or where the overseas sender is represented in New Zealand or maintains a server in New Zealand. Spam is delivered electronically over the Internet and the legislation will not directly affect (in a practical sense) the bulk of e-mail from overseas sources.

The Internet

The main drivers of the Internet today are commercial computer firms and a host of Internet Service Providers (ISPs) but the Internet grew out of an advanced research project for an electronic communications network undertaken for the United States Department of Defense². As early as 1969, a network called ARPANET was designed and developed to provide a “network of networks” to link universities, military and defence contractors for the purpose of sharing research information and to study the potential of computer-based command and control systems³. In 1983, ARPANET was split into MILNET (for military communications) and ARPANET (which continued to be used for research into networking) which eventually became absorbed into the broader Internet⁴.

Initially, it was proposed that ARPANET access be confined to researchers but the concept began to be adapted for the development of other networks and it became readily apparent that it was a valuable and new method for more widespread communications usage. The Internet still reveals its military origins in one sense in that it is designed to avoid a major catastrophe if a destructive strike was directed at “headquarters”—the Internet has no “headquarters”⁵. It is an interlinked web of networks that move electronic traffic through connecting gateways. Each network system joining the Internet is responsible for its own administration. There is no single service provider⁶.

Electronic mail (e-mail) is the most elementary service on the Internet. E-mail in its simplest form is a carrier of digital messages between two people, or through a mailing list to a group. Initially, it was considered to be an insignificant aspect of

² Brendan Bailey, *The Spam Bill 2003*, [Bills Digest No. 45](#) 2003/04, Australian Commonwealth Parliamentary Library, 07 October 2003.

³ Paul Gilster, *The New Internet Navigator*, John Wiley & Sons, New York, 1995, 21.

⁴ *Ibid.*, p. 23.

⁵ Heinz Tschabitscher, “Spam”, *Email.About.com*, at: <http://email.about.com/library/weekly/aa100697.htm>

⁶ Brendan Bailey, *The Spam Bill 2003*, [Bills Digest No. 45](#) 2003/04, Australian Commonwealth Parliamentary Library, 07 October 2003.

network capabilities⁷. Today it is a worldwide form of electronic communication and it has become a core Internet application offering fast and convenient form of mail transmission across the entire world⁸.

Some Limited Methods to Counter Spam

From the early 1990's, it became evident that problems would occur with the commercialisation of the Internet. One commentator noted in 1994 :

“However, we must remember the old attitudes about commercial use of the Internet. In the past, commercial use was often acceptable if it wasn't blatant, was appropriately directed, and was of significant value to the readers. In other words, I'll be as angry as the next person if I start receiving automatically generated junk mail every day, just as I receive junk mail via snail mail⁹.

One response suggested was to “flame away” (i.e. send back an outrageously nasty message)¹⁰. However, the contemporary problem is the volume of spam that arrives and the time that is involved in replying. Some spam is also deliberately constructed to confirm a valid e-mail address when the recipient responds and the address is then on-sold by the sender (i.e. spammer) to other spammers. Block deletion of spam by receivers is possible but there is then a risk of unintentional deletions¹¹.

Education programs, voluntary codes of conduct for using the Internet, blacklisting and filters have not successfully addressed the problem of determined spammers who switch e-mail addresses or servers to avoid detection. Spammers will also abuse the relay facility that is at the core of the Internet which allows a message to be relayed by one server to another. Internet relay servers are proliferating in a number of countries. One of the more serious threats from spam is its use to perpetrate scams and fraud and to offer access to illicit pornography. Another development is the spamming of chatroom users. Apart from financial scams, there is a growing concern about young users who may be vulnerable to predators¹².

The Top Ten Spam Messages

The Computer Research and Technology (CR&T) website provides a list of the “Spam top 10 hit list¹³. The list (for the USA—but the Internet is universal) for 2002 is:

⁷ Paul Gilster, *The New Internet Navigator*, John Wiley & Sons, New York, 1995, p.31.

⁸ Brendan Bailey, *The Spam Bill 2003*, [Bills Digest No. 45](#) 2003/04, Australian Commonwealth Parliamentary Library, 07 October 2003.

⁹ Adam C. Engst, *Internet Starter Kit for Macintosh*, 1994

¹⁰ Ibid.

¹¹ Brendan Bailey, *The Spam Bill 2003*, [Bills Digest No. 45](#) 2003/04, Australian Commonwealth Parliamentary Library, 07 October 2003.

¹² Ibid.

¹³ CR&T, Information technology Solutions Provider. <http://www.crt.net.au/etopics/irritatingspam.htm> (accessed 30 August 2005 at 10.00am)

- Free adult site passwords;
- Low price drugs (Viagra);
- Refinance your mortgage;
- Nigerian confidential money transfer;
- Tiny remote control car;
- Best online casino;
- #1 Pasta pot;
- Get out of credit card debt;
- Meet singles in your area;
- Copy DVDs in one click.

Because of the difficulty of enforcement outside the jurisdiction of New Zealand, the Bill is unlikely to counter the transmission of the spam items listed above. CR&T estimates that spam now cost businesses worldwide about \$9 billion per year to deal with and that one in twelve e-mails was identified as spam by companies using spam Internet filters. Businesses (and private users) are also concerned “brand spoofing” where personal and financial data is extracted by the spammer who disguises the e-mail to make it appear to be from a reputable business address¹⁴.

Other jurisdictions

The Spam Act 2003 (Commonwealth) instituted for Australia a regime very similar to that to be provided for New Zealand by this Bill.

MAIN PROVISIONS

Purpose clause

The Bill states that its purposes are to:

- prohibit commercial electronic messages that have a New Zealand link from being sent to people who have not given their prior consent to receiving those messages;
- prohibit promotional electronic messages that have a New Zealand link from being sent to a person who has withdrawn consent to receiving such messages;

¹⁴ Brendan Bailey, *The Spam Bill 2003*, [Bills Digest No. 45](#) 2003/04, Australian Commonwealth Parliamentary Library, 07 October 2003.

- require all commercial and promotional electronic messages to include accurate information about the person who authorised the sending of the message, and contain a functional unsubscribe facility;
- prohibit address-harvesting software and any electronic address list produced using that software from being supplied, acquired for use, or used in connection with sending unsolicited commercial electronic messages, or promotional electronic messages, in contravention of this Bill.

Unsolicited commercial electronic messages must not be sent and onus on sender

The Bill provides that a person must not send, or cause to be sent, an “unsolicited commercial electronic message”¹⁵ that has a “New Zealand link”¹⁶. A person who contends that a recipient consented to receiving a commercial electronic message has the onus of proof in relation to that matter (*Part 2, Subpart 1, Clause 9*).

Promotional electronic messages

The Bill prohibits a person from sending a “promotional electronic messages”¹⁷ that has a New Zealand link to any person who has opted out of receiving messages from

¹⁵ “Unsolicited commercial electronic message” means a commercial electronic message that the recipient has not consented to receiving” (*Part 1, Clause 4(1), definition of “unsolicited commercial electronic message”*).

¹⁶ The Bill provides that an electronic message has a “New Zealand link” if one or more of the following applies:

- the message originates in New Zealand;
- the person who sent the message is an individual who is physically present in New Zealand when the message is sent or is an organisation whose central management and control is in New Zealand when the message is sent;
- the computer, server, or device that is used to access the message is located in New Zealand;
- the recipient is an individual who is physically present in New Zealand when the message is accessed or is an organisation that carries on business or activities in New Zealand when the message is accessed;
- if the message cannot be delivered because the relevant electronic address does not exist, assuming that the electronic address existed, it is reasonably likely that the message would have been accessed using a computer, server, or device located in New Zealand;
- it is sent to an electronic address that ends with “.nz”; or begins with an international access code directly followed by “64” (*Part 1, Clause 4(2)*).

¹⁷ A “promotional electronic message” is a message:

- sent to an electronic address using a telecommunications service;
- that is not a commercial electronic message;
- that has, as its primary purpose, the promotion or marketing of an organisation, or its aims or ideals (*Part 1, Clause 4(1) (definition of “promotional electronic message”) and Clause 5(1) “meaning of electronic message)*).

that person, or causing such messages to be sent. The Bill sets out how a person “opts out”¹⁸ of receiving promotional electronic messages (*Part 2, Subpart 1, Clause 10*).

Identification required

The bill requires every commercial electronic message and promotional electronic message that is sent, and that has a New Zealand link, to:

- clearly and accurately identify the person who authorised the sending of the message; and
- include accurate information about how the recipient of the message can readily contact the person who authorised the message to be sent.

Regulations made under the Bill, when it is enacted, may specify further conditions about the information that must be included in commercial electronic messages and promotional electronic messages (*Part 2, Subpart 1, Clause 11; Part 4, Clause 54 (the regulation-making clause)*).

Unsubscribe facility must be provided

The Bill requires every commercial electronic message and promotional electronic message that is sent, and that has a New Zealand link, to include a functional unsubscribe facility that allows the recipient of the message to instruct the person who authorised the sending of the message that no further messages authorised by the sender should be sent to the recipient's electronic address. It also sets out various requirements in relation to the unsubscribe facility. However, people can agree between themselves that this requirement does not apply to messages sent to and from each other (*Part 2, Subpart 1, Clause 12*).

Defence

The Bill provides that a person who sends an electronic message in contravention of Clause 9, 10, 11, or 12 (all described above) has a defence if that person sent the message by mistake; or the message was sent without that person's knowledge. The onus of proving a defence lies with the person who is relying upon it (*Part 2, Subpart 1, Clause 13 (defence in respect of Clauses 9, 10, 11, or 12)*).

Address-harvesting software and harvested-address lists

The Bill prohibits people from supplying, or offering to supply, to another person “address-harvesting software”¹⁹ or a right to use address-harvesting software or a

¹⁸ An unwilling recipient “opts out” of receiving a promotional electronic message from a sender if:

- one or more promotional electronic messages have been sent to the unwilling recipient's electronic address by or on behalf of the sender; and
- the unwilling recipient sends, delivers, or gives the sender a message to the effect that the unwilling recipient does not want to receive, at that electronic address, any further promotional messages from or authorised by that sender (*Part 2, Clause 10(2)*).

¹⁹ “Address-harvesting software” means software that is capable of, or marketed for use for, searching the Internet for electronic addresses and collecting, compiling, capturing, or otherwise harvesting those electronic addresses (*Part 1, Clause 4, definition of “address-harvesting software”*).

harvested address list or a right to use a “harvested-address list”²⁰. However, this prohibition does not apply in two circumstances. First, if the supplier had no reason to suspect that the address-harvesting software or the harvested-address list was to be used in connection with sending unsolicited commercial electronic messages or promotional electronic messages in contravention of this Bill. And secondly, if the supplier did not know, and could not with reasonable diligence have ascertained, that the person to whom they supplied the software or list was either an individual who was physically present in New Zealand or an organisation that carried on business or activities in New Zealand (*Part 2, Subpart 2, Clause 15*).

Prohibitions in relation to software or list

The Bill prohibits a person from acquiring address-harvesting software or a right to use that software or a harvested-address list or a right to use that list. This prohibition does not apply if the person did not intend to use the software or list in connection with sending unsolicited commercial electronic messages or promotional electronic messages in contravention of this Bill. Likewise, a person must not use address-harvesting software or a harvested-address list. However, this prohibition does not apply if the use of the software or the list is not in connection with sending unsolicited commercial electronic messages or promotional electronic messages in contravention of this Bill (*Part 2, Subpart 2, Clauses 16 and 17*).

Third party breaches

The Bill provides that a person must not aid, abet, counsel, procure, or induce a breach of Clauses 9 to 12 or 15 to 17 of this Bill (described above). Further, a person must not be in any way knowingly concerned in, or a party to, or conspire with others to effect a breach of those clauses (*Part 2, Subpart 3, Clause 19*).

Rules of general application

The Bill clarifies the position of service providers. For the purposes of this Bill, service providers do not send an electronic message, or cause an electronic message to be sent, or contravene Clause 19 (described immediately above), merely because they provide a telecommunications service that enables an electronic message to be sent. The Bill also sets out who is deemed to have authorised the sending of an electronic message, and who is deemed to have sent an electronic message. In particular, it clarifies which individuals may be deemed to have authorised the sending of an electronic message on behalf of an organisation for the purposes of this Bill (*Part 2, Subpart 2, Clauses 20 and 21*).

Enforcement

Under Part 3 of the Bill, a “civil liability event” means a breach of any of the provisions of Part 2 of the Bill. The Bill sets out the actions that the following people may take if a civil liability event is alleged to have occurred: any person affected by the civil liability event; any person who suffers loss or damage as a result of the civil liability event; service providers; the enforcement department. The range of remedies available are set out in the Bill. These cover formal warnings, contravention notices

²⁰ “Harvested-address list” means a list of electronic addresses, a collection of electronic addresses or a compilation of electronic addresses “where the production of the list, collection, or compilation is, to any extent, directly or indirectly attributable to the use of address-harvesting software” (*Part 1, Clause 4, definition of “harvested-address list”*).

and enforceable undertakings (*Part 3, Subpart 1, Clauses 22 and 23; Subpart 3, Clauses 25 - 33*).

Obligations of service provider

The Bill provides that a service provider must consider any complaint made to it under the bill, and in considering that complaint, the service provider must have regard to any relevant, generally accepted industry code that applies to the service provider (*Part 3, Subpart 2, Clause 24*).

Powers of High Court

The High Court is given power to grant injunctions under the Bill. Also, on the application of the enforcement department, the High Court may order a person to pay a pecuniary penalty if it is satisfied that that person has committed a civil liability event. The Court can order that the penalty be paid to the Crown or to any other person. A number of matters are specified for the Court to consider when setting the amount of the pecuniary penalty to be paid, but it cannot exceed certain maximum amounts as follows: if the perpetrator is an individual, the High Court payment of a pecuniary penalty of up to \$200,000 or, if the perpetrator is an organisation, up to \$500,000. The High Court may order the perpetrator to pay a pecuniary penalty of up to \$50,000 in respect of breaches of Clause 10(1) (prohibition on sending of electronic message to a person who opts out). If the High Court is satisfied that a person has committed a civil liability event and, as a result, another person has suffered loss or damage. In these circumstances, the Court can order a person to pay compensation for any loss suffered, or damages, or both (*Part 3, Subpart 4, Clauses 37 – 43*).

Search and seizure

The Bill sets out standard search and seizure provisions that provide for the issue and execution of a search warrant if there are reasonable grounds for believing that a civil liability event has been, or is being, committed at the place or thing to be searched, or there is evidence of a civil liability event at that place or thing (*Part 3, Subpart 5, 48 – 52*).