



Stephen Revill Partner

## Lawmakers sending message to spammers New Zealand is set to join the worldwide legislative battle against spam.

The Unsolicited Electronic Messages Bill (the Bill) was introduced to Parliament on 28 July 2005 and represents the Government's attempt to bring us in line with other countries such as Australia, the United Kingdom and the United States in fighting the increasing cost of spam.

A recent European Union study has estimated the worldwide cost of spam at approximately 10 billion Euros per year.

The Bill is also intended to meet a commitment made by the Government, in its recently published Digital Strategy, to introduce laws that help preserve legitimate business and promotional activities, while also encouraging the responsible use of electronic messaging.

### Purpose of the Bill

The Bill seeks to promote the responsible use of electronic messages by:

- prohibiting the sending of commercial electronic messages that have a New Zealand link, except where the message is sent to people who have given their prior written consent to receiving those messages;
- prohibiting promotional electronic messages that have a New Zealand link, where the recipient has indicated that it does not want to receive those messages anymore;
- requiring all electronic messages with a New Zealand link to identify the person authorising the sending of the message and how that person may be contacted; and include a functional unsubscribe embedded in that electronic message.

- prohibiting the use of software to harvest electronic addresses, and the use of harvested address lists.

### Who will it affect?

The Bill changes the "ground rules" for business involved in digital marketing by requiring an "opt-in" process before commercial electronic messages (as defined by the Bill) can be sent to customers or potential marketing targets. It will also require business to distinguish between commercial electronic messages, promotional electronic messages and other kinds of marketing delivery channels, for which different rules apply.

Fines of up to \$200,000 for individuals and up to \$500,000 for organisations can be incurred for breaching the Act.

The Bill is also significant for internet service providers. People who wish to make a complaint about a breach of the Act must first go to their service providers rather than to government, except where they are prepared to take direct legal proceedings themselves.

Service providers are required to consider complaints and must do so in line with any applicable generally accepted industry codes. This could mean that additional costs will be imposed on service providers in managing complaints, upgrading filtering software and liaising with other ISPs from whom spam is originating.

**"A recent European Union study has estimated the worldwide cost of spam at approximately 10 billion Euros per year."**

**“An individual faces fines of up to \$200,000 while an organisation faces fines of up to \$500,000. A breach of the prohibition relating to promotional electronic messages can result in a fine of up to \$50,000.”**

**“A key feature of the Bill is the requirement restricting the enforcement department from considering complaints except from service providers.”**

## **The new rules for electronic messaging**

### **Electronic messages**

The Bill applies to messages sent to an electronic address using a telecommunications service, and includes email, instant messaging or text messaging. It doesn't apply to voice calls (including voice messages using voiceover internet protocol technology) or to fax transmissions.

### **New Zealand link**

The Bill only applies to electronic messages with a New Zealand link. The definition “New Zealand link” is very wide and covers not only messages originating in New Zealand, but also, among other things, any electronic messages accessed by a computer located in New Zealand. However, liability for breaches of the Act apply only to people resident in or organisations carrying on business or activities in New Zealand.

### **Commercial and promotional electronic messages**

The Bill distinguishes between “unsolicited commercial electronic messages” and “promotional electronic messages”. The opt-out principle continues to apply to promotional electronic messages, while the new opt-in process must be adopted before unsolicited commercial electronic messages are sent.

A commercial electronic message is a message whose:

- primary purpose is the marketing or promoting of goods or services; or
- object is to obtain a dishonest financial advantage (to cover off the kind of messages used by Nigerian scam operators).

A promotional electronic message is an electronic message that does not fall within the definition of commercial electronic message and whose primary purpose is the promotion or marketing of an organisation, its aims or ideals.

There are exceptions as to what represents a commercial electronic message. These

include quotes or estimates (if requested); messages facilitating, completing or confirming an already agreed commercial transaction; and messages that provide the recipient with information about goods or services offered by a government body.

### **Consent**

This is fundamental to stopping unsolicited commercial electronic messages. Consent can be either express or inferred (from the conduct and business and other relationships between the parties). The Bill also deems consent to have occurred where:

- an electronic address has been published by a person in a business capacity,
- where there is no accompanying statement that there is no consent to the sending of messages; and
- where the message sent is relevant to the business, role, functions, or duties of that person.

### **Required particulars**

The Bill requires that any electronic message covered by it clearly and accurately identify the person who authorised the sending of the message and include accurate information about how to “readily” contact that person. The information must reasonably be likely to be valid for at least 30 days after the message is sent.

It also mandates that electronic messages must include a functional “clear and conspicuous” unsubscribe facility allowing the recipient to opt out from receiving further messages. Again this facility must be reasonably likely to be functional for at least 30 days after the principal message is sent.

### **Defences**

The Bill offers two defences against the violation of its core requirements. A person who sends or who authorises the sending of an electronic message in breach of the Bill's rules on electronic messaging, has a defence if that person can show the message was sent by mistake, or if the message was sent without the sender's knowledge (for example, because of a computer virus).



Simon Martin Partner

### **Regulations**

The Bill itself does not complete the picture on electronic messaging prohibitions. Regulations may be passed to further streamline its application. Some areas of importance that may be affected by such regulations include:

- what amounts to inferred consent;
- exceptions to the definition of commercial electronic message; and
- conditions for unsubscribe facilities.

### **Enforcement, procedures and penalties**

#### **Enforcement**

The Bill's enforcement regime uses civil penalties and a three tier system.

Any person affected by a breach can complain to the relevant service provider (they may also seek an injunction in the High Court or sue for damages if they can they have suffered damage arising out of, for example, a denial of service attack).

A service provider must consider any complaint made to it, and in doing so have regard to any relevant, generally accepted industry code that applies to the service provider.

The service provider may refer any complaint to the relevant enforcement department of government (which is to be the Department of Internal Affairs). The provider may also seek an injunction, apply to the High Court for compensation or damages (if the service provider has also suffered loss), or apply to join any Court action initiated by the enforcement department.

The enforcement department on receiving a complaint may not only initiate legal proceedings for breach of the Bill, but also has powers to apply for and execute search warrants, issue formal warnings, issue contravention notices (which will require the payment of a fine) or accept an enforceable undertaking, the breach of which will result in "fast track" legal remedies before the courts.

A key feature of the Bill is the requirement restricting the enforcement department from considering complaints except from service providers. The victim of a "spam" attack (who is not also a service provider) cannot directly initiate an enforcement action through the Department of Internal Affairs. The Department does, however, retain the discretion to start its own legal proceedings.

#### **Penalties and fines**

An individual faces fines of up to \$200,000 while an organisation faces fines of up to \$500,000. A breach of the prohibition relating to promotional electronic messages can result in a fine of up to \$50,000. Factors to be assessed in deciding the level of fine include the number of messages sent, the number of addresses to which an electronic message was sent, and whether the perpetrator has previously contravened the Bill.

#### **Some issues**

Government consultation has shown widespread "in principle" support for the introduction of "anti-spam" legislation. In its current form, the Bill does raise some practical issues for business, such as:

- will new business processes have to be adopted for business to comply with the "opt-in" requirements for commercial electronic messages and what might these be?
- how far can a business rely on inferred consent as opposed to express consent in relation to the sending of commercial electronic messages?
- will it be easier to adopt a single "opt-in" approach for all electronic messages?
- should more marketing effort be focussed on other forms of marketing not covered by the Bill (such as telemarketing)?
- what steps should be taken by business to avoid being deemed to have given its consent to receiving unsolicited commercial electronic messages?
- what issues arise for businesses based here and also overseas for complying with different legal requirements in different countries for the regulation of unsolicited electronic messages?

“The difficulty in considering New Zealand legislation is that, despite spam accounting for 40 to 75 per cent of New Zealand email traffic, only 10 per cent of spam actually originates in New Zealand. Measures beyond simple legislation will be needed.”

To receive your updates faster, please subscribe to our electronic newsletter service on:  
[info@bellgully.com](mailto:info@bellgully.com)

To view all our publications or update your details please visit our website: [www.bellgully.com](http://www.bellgully.com)

For further information, please contact your usual Bell Gully adviser or:

#### AUCKLAND

**Simon Martin**

[simon.martin@bellgully.com](mailto:simon.martin@bellgully.com)  
64 9 916 8972

#### WELLINGTON

**Stephen Revill**

[stephen.revill@bellgully.com](mailto:stephen.revill@bellgully.com)  
64 4 915 6997

- what new policies are required for compliance with other parts of the new legislation?
- what further training is required to ensure that staff are in a position to support your company's compliance efforts?

There are additional issues for ISPs to whom frontline complaint management is delegated. The Bill only requires the service provider to “consider” complaints, having regard (where applicable) to generally accepted industry codes. However, it is likely that there will be an expectation among some customers that its service provider should be able to solve the problem or give a very good reason why it cannot.

Service providers will need to consider what resources and new procedures they will need to meet the Bill's requirements and to manage their relationships with their customers. This will involve not only dealing with customer complaints, but also introducing new processes for referring complaints to the Department of Internal Affairs.

### A multi-pronged attack

A question remains over how effective legislation will be in solving the spam problem. The difficulty in considering New Zealand legislation is that, despite spam accounting for 40 to 75 per cent of New Zealand email traffic, only 10 per cent of spam actually originates in New Zealand. Measures beyond simple legislation will be needed.

The Government has decreed the Bill is just part of a “multi-pronged attack on spam”. The Bill is intended to prevent the country from being a safe haven for spammers and to support the global legislative effort in this area. It will also allow us to take part in international measures to combat spam like the recent Memorandum of Understanding on Mutual Enforcement Assistance in Commercial Email Matters signed by Australia, the United Kingdom and United States.

The introduction of spam legislation in New Zealand is not so much a matter of “keeping up with the Joneses” as it is of “tidying up our own backyard”. A successful solution to the spam problem will require not only legislation but also international cooperation, technical solutions, individual and industry awareness, and industry responsibility through self-regulation.

**Disclaimer:** This publication is necessarily brief and general in nature. You should seek professional advice before taking any further action in relation to the matters dealt with in this publication.  
All rights reserved © Bell Gully 2005.

#### AUCKLAND

Vero Centre  
48 Shortland Street  
PO Box 4199, Auckland  
New Zealand, DX CP20509  
Telephone +64 9 916 8800  
Facsimile +64 9 916 8801

#### WELLINGTON

HP Tower  
171 Featherston Street  
PO Box 1291, Wellington  
New Zealand, DX SX11164  
Telephone +64 4 473 7777  
Facsimile +64 4 473 3845

[www.bellgully.com](http://www.bellgully.com)

**Bell Gully**