Unsolicited Electronic Messages Bill

Government Bill

Explanatory note

General policy statement

The Unsolicited Electronic Messages Bill implements the Government's decisions on the regulation of electronic messages. Unsolicited electronic messages, commonly known as 'spam', have become a major problem worldwide because of the significant growth in volumes of such messages, particularly in the form of emails via the Internet. The enactment of legislation that prohibits the sending of unsolicited electronic messages (in the form of emails, text messages, or instant messages) of a marketing nature provides a legislative basis to combat the growth of spam.

This legislation is 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.

The Bill takes an opt-in approach to the sending of unsolicited electronic messages of a marketing nature while taking an opt-out approach to the sending of certain non-commercial electronic messages. Electronic messages covered by the legislation are also required to meet requirements in relation to accurate sender identification and the provision of a functional unsubscribe facility.

The enforcement regime under the legislation is a civil penalty regime, with the emphasis being on internet and telecommunications service providers taking action in response to customer complaints, and with the government enforcement agency acting as the overseer and backstop.

Clause by clause analysis

Clause 1 relates to the Title of the Bill.

Clause 2 provides that the Bill comes into force 4 months after the date on which it receives the Royal assent.

Part 1
Preliminary provisions

Clause 3 sets out the purposes of the Bill. The purposes of the Bill 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; and
- prohibit promotional electronic messages that have a New Zealand link from being sent to a person who has withdrawn consent to receiving those messages; and
- 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; and
- 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.

Clause 4 defines terms used in the Bill. Some of the key terms are address-harvesting software, consented to receiving, harvested-address list, message, promotional electronic message, and unsolicited commercial electronic message. A definition of New Zealand link is set out in *clause 4(2)*. This definition is central to the application of certain parts of the Bill.

Clause 5 provides a definition of electronic message. This definition is central to the definitions of commercial electronic message and promotional electronic message.

Clause 6 defines the term commercial electronic message. This definition is important for understanding the scope of *clause 9*.

Clause 7 provides that the Bill, when enacted, binds the Crown.

Clause 8 deals with the application of the Bill. The Bill, when enacted, will apply to a person who engages in conduct outside New

Zealand if that conduct breaches the Bill, and that person is of a kind described in *clause 8(2)*.

Part 2
Restrictions on electronic messages, address-harvesting software, and harvested-address lists

Subpart 1—Commercial electronic messages and promotional electronic messages

Clause 9 prohibits a person from sending unsolicited commercial electronic messages that have a New Zealand link, or causing such messages to be sent. An unsolicited commercial electronic message is a message—

- sent to an electronic address using a telecommunications service:
- that has, as its primary purpose, marketing or promoting goods, services, land, an interest in land, or a business or investment opportunity, or assisting or enabling a person to obtain dishonestly a financial advantage or gain from another person:
- that the recipient has not consented to receiving.

There is no prohibition on sending a commercial electronic message if the recipient of the message has given his, her, or its prior consent to receiving that message. *Clause 9(2)* states that the onus of proof for proving that a recipient consented to receiving a commercial electronic message lies with the person who is asserting that matter.

Clause 10 prohibits a person from sending promotional electronic messages that have a New Zealand link to any person who has opted out of receiving messages from that person, or causing such messages to be sent. 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.

There is no prohibition on sending a promotional electronic message to any person who has not opted out of receiving such messages. *Clause 10(2)* sets out how a person opts out of receiving promotional electronic messages, and *clause 10(3)* states when opting out takes effect.

Clause 11 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.

Clause 12 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, *clause 12(2)* provides that people can agree between themselves that this requirement does not apply to messages sent to and from each other.

Clause 13 provides that a person who sends an electronic message in contravention of *clause 9, 10, 11, or 12* 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.

Subpart 2—Address-harvesting software and harvested-address lists

Clause 14 defines the terms person and relevant time for the purposes of *clauses 15 to 17.*

Clause 15 prohibits people from supplying, or offering to supply,—

- address-harvesting software or a right to use that software; or
- a harvested-address list or a right to use that list.

However, the prohibition does not apply in 2 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.

Clause 16 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.

The 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.

Clause 17 provides that 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.

Clause 18 places the onus of proof on anyone wanting to rely on an exemption in *clauses 15, 16, or 17* on that person.

Subpart 3—Third party breaches of Act

Clause 19 states 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. 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 sections.

Subpart 4—Rules of general application throughout Act

Clause 20 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*, merely because they provide a telecommunications service that enables an electronic message to be sent.

Clause 21 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 3
Enforcement provisions

Subpart 1—Civil liability events

Clause 22 defines civil liability event for the purposes of *Part 3* of the Bill. Civil liability event means a breach of any of the provisions of *Part 2* of the Bill.

Clause 23 is effectively a guide to the rest of *Part 3* of the Bill. It 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.

Subpart 2—Obligations of service provider

Clause 24 provides that a service provider must consider any complaint made to it under *clause 23(a)(i)*, and in considering that complaint, the service provider must have regard to any relevant, generally accepted industry code that applies to the service provider.

Subpart 3—Powers of enforcement department

Clause 25 provides that the enforcement department must consider all complaints it receives from service providers concerning civil liability events. But it must not consider any other complaint it receives. The department may investigate and take enforcement action, either on a complaint from a service provider or on its own initiative, if it considers that an investigation or enforcement action is appropriate in the circumstances.

Formal warnings

Under *clause 26*, the enforcement department may issue a formal warning to any person the department believes may have committed a civil liability event. This clause also specifies the form the formal warning must be in, and that it must be issued in accordance with regulations made under this Bill, when enacted.

Contravention notices

Clauses 27 to 33 concern the issue of contravention notices by the enforcement department. The department may issue contravention notices if it has reasonable grounds to believe that a person has committed a civil liability event.

Clause 27 provides the enforcement department with the power to issue contravention notices.

Clause 28 specifies when and how a contravention notice must be issued, and when it is deemed to have been issued.

Clause 29 sets out the information that a contravention notice must contain. Amongst other things this includes details of the alleged civil liability events, the penalty that must be paid, and a person's right to object to the notice.

Clause 30 provides that the grounds on which a person may object to a contravention notice and the time period within which they may do so will be specified in regulations made under this Bill, when enacted. It also specifies what an enforcement department must do when it receives an objection and the possible responses that are open to it.

Clause 31 provides that the enforcement department may, by written notice, withdraw a contravention notice and specifies the time period within which it may do so. It also provides for the refund of a penalty paid in accordance with a contravention notice if that notice is subsequently withdrawn.

Clause 32 provides that if a person pays the penalty specified in a contravention notice, then—

- any liability of that person for the alleged civil liability events to which the notice relates is discharged; and
- proceedings under *clauses 42 or 43* may not be brought against that person for those alleged civil liability events.

Clause 33 provides that if a person does not pay the penalty specified in a contravention notice, or the notice is withdrawn before the penalty is paid, proceedings under *clauses 42 or 43* may be brought against that person.

Enforceable undertakings

Clauses 34 to 36 concern enforceable undertakings.

Under *clause 34*, the enforcement department may accept a written undertaking from a person in connection with—

- commercial electronic messages; or
- promotional electronic messages; or
- address-harvesting software; or
- harvested-address lists.

That person may withdraw or vary the undertaking, but only with the consent of the enforcement department.

Clause 35 provides that the enforcement department may apply to the High Court for an order under *clause 35(2)* if it considers that a person who gave an undertaking under *clause 34* has breached its terms. The Court may make an order if it is satisfied that a person breached the terms of the undertaking, including an order directing that person to—

- comply with the terms of the undertaking:
- pay to the enforcement department any financial benefit that person received as a result of breaching the undertaking:
- pay compensation to any other person who suffered loss or damage as a result of the breach of the undertaking.

Clause 36 sets out, for the purposes of making an order for a person to pay compensation under *clause 35(2)(c)*, the matters that the High Court may have regard to when determining whether another person has suffered loss or damage as a result of the breach of the undertaking, and in assessing the amount of compensation payable.

Subpart 4—Powers of High Court

Injunctions

Clauses 37 to 41 concern the power of the High Court to grant injunctions.

Under *clause 37*, the Court may grant a performance injunction requiring a person to do an act or thing if that person has refused or failed to do that act or thing and the refusal or failure is a civil liability event.

Clause 38 specifies the matters that the Court must take into consideration when deciding whether or not to grant a performance injunction.

Under *clause 39*, the Court may grant a restraining injunction restraining a person from engaging in conduct that constitutes a contravention of this Bill.

Clause 40 specifies the matters that the Court must take into account when deciding whether or not to grant a restraining injunction. It also gives the Court authority to grant an interim injunction restraining a person from engaging in conduct if, in the Court's opinion, it is desirable to do so.

Clause 41 provides that the enforcement department is not required to give an undertaking as to damages as a condition of an interim injunction being granted. Further, in deciding whether or not to grant an interim injunction, the Court must not take this matter into account.

Pecuniary penalties, compensation, and damages

Clauses 42 to 47 deal with pecuniary penalties, compensation, and damages.

Clause 42 provides that, 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 the maximum amounts set out in *clause 42(3) to (5)*.

Clause 43 applies 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.

Clause 44 allows the High Court to direct that an application for a pecuniary penalty be heard together with an application for compensation or damages, or vice versa, or that 2 or more applications for compensation or damages be heard together.

Clause 45 clarifies the fact that a person may be liable for a pecuniary penalty, compensation, or damages for the same civil liability event. However, in determining whether to order a person to make such a payment, the High Court must have regard to whether or not that person has already made such a payment, and if so, the amount and effect of that payment.

Clause 46 specifies that the usual rules and procedures of the High Court apply to proceedings under *clauses 42 and 43*.

Clause 47 imposes a 2-year time limit within which an application for a pecuniary penalty must be made. The ususal time limits apply to an application for compensation or damages.

Subpart 5—Search and seizure

Clauses 48 to 52 are 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 4
Miscellaneous provisions

Clause 53 gives the Governor-General authority to amend the *Schedule* to the Bill by Order in Council.

Clause 54 sets out the regulation making powers.

The *Schedule* to the Bill relates to the definition of electronic message in *clause 5*. It sets out messages that are not electronic messages for the purposes of the Bill.

Regulatory impact and compliance cost statement

Nature and magnitude of problem and need for Government action

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 (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.

Without Government action to address the problem of spam through legislation, New Zealand risks being seen as a safe haven for spammers as other countries progressively pass anti-spam legislation, and there is the consequent risk that email traffic from New Zealand to other countries could be blocked without sufficient verification. Without anti-spam legislation, New Zealand also lacks a basis from which it can enter into international arrangements to address spam coming into New Zealand from overseas sources. Legislation also serves the purpose of ensuring that businesses adopt sound e-marketing practices, thereby preventing significant growth in spam originating within New Zealand as the Internet becomes progressively more important for business communications.

One of the main objectives for government action is to create a safe and secure environment in New Zealand for the use of information and communication technologies (ICT), in line with the Government's Digital Strategy. The specific policy objectives are to—

- minimise the level of spam entering New Zealand by providing a legislative basis from which New Zealand can participate in international efforts to address the spam problem at a global level, particularly to provide a firm basis for New Zealand to seek and give co-operation from and to overseas government anti-spam enforcement agencies to combat spam sent from overseas to New Zealand:
- prevent New Zealand from being seen as a safe haven for spammers as legislative measures begin to be implemented in other jurisdictions:

- minimise the costs for legitimate businesses that arise from spam by putting in place a legal framework for tackling spam and promoting the adoption of good e-marketing practices.

Options for achieving desired objectives

Status quo

The current regulation regime includes existing legislation, self-regulation, industry and user education, and technical measures.

Existing legislative framework

The existing legislative framework for addressing issues associated with spam in New Zealand comprises the following:

- *Computer network security and integrity*: Section 250 of the Crimes Act 1961 provides that it is an offence to intentionally or recklessly damage or interfere with any data or software in a computer system or cause any computer system to fail or deny service to authorised users. This provision deals with the concern that some spam is used to transport computer viruses or to launch denial of service attacks on computer systems:
- *Misleading and deceptive messages*: Misleading and deceptive conduct and false or misleading representations by persons in trade are addressed by sections 9 and 13 of the Fair Trading Act 1986. These provisions can be used to deal with emails sent by businesses that are misleading in nature or make false or misleading claims in relation to a good or service:
- *Forgery/fraud*: Sections 256 and 257 of the Crimes Act 1961 provide that it is an offence to make or use a false document with the intention of using it to obtain any benefit or advantage. This provision would apply to email scams that involve false email documents sent to elicit money from the recipient on the basis of a false promise:
- *Privacy*: The Privacy Act 1993 provides rules against the collection, transfer and use of electronic address information pertaining to an individual without their consent or knowledge unless the information is already publicly available. It would be a breach of the Privacy Act for a business to collect a customer's email address without their knowledge or to sell a list of customers' email addresses without authorisation:

- *Pornographic/offensive material*: Section 123 of the Films, Videos, and Publications Classification Act 1993 provides that it is an offence to make or supply an objectionable publication, including objectionable material, by way of email:
- *Harassment*: The Harassment Act 1997 provides that where a person is sending emails as a pattern of behaviour designed to harass another person action can be taken against the sender.

Self-regulation, industry and user education, and technical measures

- *Self-regulation*: In New Zealand, the Direct Marketing Association (DMA) has developed a set of standards for email marketing by its members to promote consumer confidence in e-commerce and ensure that proper account is taken of consumers' right to privacy. An anti-spam code of practice for Short Message Services (text messaging) has been developed by the Telecommunications Carriers' Forum, which is also developing a similar code of practice for email spam in conjunction with the Internet Society of New Zealand (Internet NZ) and the DMA. ISPs in New Zealand will generally not tolerate spammers operating from their networks and will have them removed:
- *Industry and user education*: InternetNZ is active in the area of industry and user education and awareness, and has set up a website for helping to deal with spam:
- *Technical measures*: An ISP can use a spam filter at its server that means that users will not see spam that is filtered out.

Multi-pronged approach including specific anti-spam legislation—preferred option

This option also includes the measures outlined under the "Status quo" option. Within legislation to combat spam, there are several key issues, each of which may have various options. The preferred legislation package includes and covers—

- defining spam as unsolicited commercial electronic messages, where—
  - messages can only be transmitted if the recipient has expressly or implicitly consented to such transmission (opt-in):
  - "commercial" covers marketing messages:

  - "electronic" means in the form of email, instant messaging and text messaging:
- the number of messages sent being a relevant factor in determining what penalties apply, but not part of the definition of spam:
- messages generated within New Zealand and all messages sent to a New Zealand email address:
- all parties knowingly involved in the act of spamming, including the vendor sponsoring the spamming:
- express statutory exemptions for telecommunications network operators and ISPs who are mere transmitters of the messages, and for unsolicited messages being sent by mistake or unknowingly by the address holder's computer such as where a computer has been infected by a virus:
- messages being required to have accurate sender information and a functional unsubscribe facility (which means that there is a working, clearly visible means of opting out of future mailings):
- prohibiting the supply, acquisition, and use of address-harvesting software and harvested-address lists in connection with the unlawful sending of marketing or promotional electronic messages:
- civil pecuniary penalties with the maximum penalties at $200,000 for individuals and $500,000 for bodies corporate:
- a government enforcement agency addressing complaints from ISPs and promoting compliance:
- consumers and users being required to resolve spam problems with the sender of the spam and their ISP. If an ISP considers that a complaint should be addressed by the government enforcement agency then the ISP can refer it on for action:
- the Department of Internal Affairs enforcing the new legislation, educating consumers, users, and business, and promoting compliance.

Other options

The following options were considered and discarded:

- to include faxes and telemarketing as they are also used for sending unsolicited marketing and promotional messages. However, there does not currently appear to be a sufficient problem in this area to warrant regulation, and moreover the

costs of sending messages via these mediums are largely borne by the sender rather than the recipient or ISP:

- to adopt the sending of a minimum quantity of messages in the definition of spam. For example, in United States legislation, spam is defined as multiple commercial electronic messages, where multiple means more than 100 electronic messages during a 24-hour period. The critical factor with spam, however, is its unsolicited nature rather than its quantity, and it would be easy for spammers to circumvent minimum number restrictions through minor distinctions between messages sent to different addresses:
- to have the legislation apply to all unsolicited electronic messages, rather than just to all unsolicited "commercial" electronic messages. Having the scope that broad would unduly restrict email communication and impose too many compliance costs given that the main problem area is in relation to messages of a marketing or promotional nature:
- to adopt an opt-out approach to consent for unsolicited commercial electronic messages. Under this regime, messages can be transmitted until the sender receives an indication from the recipient that they no longer want to receive such messages. The strongest arguments for the opt-out approach are that it would avoid uncertainty around what may or may not amount to consent, and that the opt-in approach places much of the compliance burden on legitimate businesses that have nothing at all to do with the spam problem. However, this approach is not supported because—
  - it places the onus of addressing the issue of consent on the recipient of the message:
  - as long as unsolicited commercial emails meet all other requirements, the opt-out approach gives spammers at least 1 free hit at mailboxes for a particular product, in effect legitimising spam:
  - it is seen as legitimising the sharing of email address lists by businesses with one another:
- to have criminal penalties instead of civil penalties. However, unsolicited marketing messages do not cause sufficient harm or damage to warrant criminal sanction, and a criminal penalty would require proof beyond reasonable doubt (which may be difficult to establish), whereas a civil penalty would only require proof on the balance of probabilities:

- to enable users and consumers who receive spam to be able to complain directly to the government enforcement agency as is the case in Australia and other countries. This does, however, place higher costs on Government and does not emphasise resolution of issues by ISPs who are best placed to take technical measures in relation to spam originating from overseas, which constitutes the bulk of spam received in New Zealand.

Net benefits of proposal

To Government

For the Government, enacting specific anti-spam legislation has the main benefits of—

- assisting to build confidence in the use of ICT for government purposes by minimising the negative effects of spam on ICT use—such purposes include the effective and efficient delivery of services to citizens online, which reduces costs for government; and
- ensuring New Zealand is being seen internationally as a responsible citizen by participating in multinational efforts to deal with the global problem of spam.

The cost to Government is the cost of enacting the legislation, providing written guides to the legislation, administering the legislation, and enforcing the legislation. The cost of enforcement will largely be demand-driven but is estimated at $500,000 per annum (with a contingency of an additional $250,000 should demand require it). The cost of providing written guides to, and of administering, the legislation is estimated at $50,000 per annum plus an additional one-off initial cost of $50,000.

To businesses

The main benefits to businesses are—

- in the longer term, a reduction in the level of spam received with consequent benefits for productivity and the costs of dealing with spam; and
- maintaining and furthering the integrity of, and general confidence in, electronic communication as a means of doing business, with the consequent benefit of enabling businesses to operate more efficiently and reach a wider market base.

The costs to businesses are—

- the compliance costs associated with ensuring compliance with the legislation, as set out in the Business Compliance Cost Statement; and
- the cost of placing a restriction on the advertising practices of businesses (although such a restriction is in accordance with good e-marketing practice) by prohibiting businesses from sending e-marketing messages advertising their goods and services to prospective new clients who have not given their consent to such messages being sent.

For those businesses that already follow e-marketing best practice (these tend to be banks, large corporations and direct marketers) the proposed legislation is likely to have very little, if any, regulatory impact.

To ISPs

The benefit for ISPs is, in the longer term, a reduction in the volume of spam being sent over their networks meaning a lesser burden on bandwidth and network infrastructure. Customers will also have greater confidence in email services if spam volumes are able to be reduced.

ISPs will face the cost in terms of the limits on e-marketing applying to businesses generally. The legislation will not impose any direct costs on ISPs in relation to dealing with customer complaints, which is a cost ISPs face already, but the enforcement regime proposed (which requires spam complaints to be referred by ISPs to the enforcement agency rather than being made direct) will mean that ISPs will have the role of deciding what complaints should be forwarded on for investigation. ISPs will also be encouraged to join a voluntary code of practice for dealing with spam. Extra resources in the form of a dedicated employee may be required to handle complaints from consumers, decide what needs to be referred to the enforcement agency, and deal with code of practice issues.

To society

Individuals in society not only benefit from having to waste less time dealing with unsolicited messages, but they will also potentially receive fewer messages with objectionable material, scams, or viruses. There is also the benefit that electronic communications as a

viable form of communicating will be able to be maintained and developed if spam volumes are able to be curbed.

On the other hand, some may argue that by restricting the ability of businesses and others wishing to send marketing or promotional messages, including messages for political or religious purposes, the freedom of individuals to send and receive information is restricted.

Consultation

Consultation took the form of submissions to a discussion paper and an industry workshop. Forty-three submissions were received from industry and specialist groups, businesses, ISPs, telecommunications companies, government agencies and individuals.

What message mediums should be caught by the legislation (eg, email, instant messaging, text messaging, faxes, telephones (telemarketing))?

Electronic messages in the form of email, instant messaging and text messaging are the mediums usually used by spammers because these mediums involve minimal costs to them in sending large volumes of messages (but impose the burden of cost on ISPs and recipients).

The issue of "bulk"

Spam messages are typically sent in bulk. The issue of bulk is primarily an issue for those who are attempting to solve or regulate spam because it relates to its collective impact. For the recipients of spam, however, the issue of how many other people may have received a message is generally irrelevant.

The element of bulk will not be included in the definition of spam but the number of messages sent will be a relevant factor in determining what penalties should apply. The Australian legislation has taken this approach.

Types of messages

The types of messages that could be covered by anti-spam legislation range from all types of electronic messages, to messages of a commercial nature (Australia), messages sent for the purpose of direct marketing (European Union (EU), United Kingdom (UK)), or messages sent only for the purpose of advertising or promoting a commercial product or service (United States of America (US)).

Extending coverage of anti-spam legislation to all types of unsolicited messages raises difficulties in terms of rights of freedom of speech and creates legality problems for the use of email as a general form of communication. In addition, regulating all commercial electronic messages, as under the Australian legislation, imposes widespread compliance costs as it requires small businesses to ensure that communications with existing and potential customers, such as quotes, meet minimum requirements. However, in New Zealand, there is widespread support for legislation applying to marketing and promotional messages irrespective of whether they are commercial, political or religious in nature.

It is proposed to apply the legislation to marketing and promotional messages in general, as is the case in the EU and UK, because it is considered that this will strike the right balance between regulation of the area of electronic messages, which constitutes a significant risk to users and businesses, while enabling businesses to effectively use the Internet and communications technology for business purposes without undue constraint.

Extra-territorial application

Legislation can be applied to messages generated only within New Zealand or to all messages sent to a New Zealand email address. The second option is considered preferable so as to ensure that vendors who arrange for messages to be sent from an overseas ISP are caught and to provide a basis for approaching overseas enforcement agencies about breaches of New Zealand's legislation by overseas spammers.

Who should be covered?

All parties knowingly involved in the act of spamming, including the vendor sponsoring the spamming, should be covered by the legislation. Express exemptions should be allowed for telecommunications network operators and ISPs who are mere transmitters of the messages, and for unsolicited messages being sent by mistake or unknowingly by the address holder's computer such as where a computer has been infected by a virus.

Issue of consent—opt-in approach

One of the main characteristics of spam is that it is unsolicited and unwanted. To address this issue, anti-spam legislation has either

provided that electronic messages can only be transmitted if the recipient has expressly or implicitly consented to such transmission (opt-in), or that such messages cannot be transmitted if the recipient has already taken action to indicate to the sender that such messages are unwanted (opt-out).

The merit of the opt-in approach is that it places the onus of addressing the issue of consent on those wishing to send messages and is therefore more effective in addressing the spam problem. It means spam that has not been opted-out from is not legalised, and addresses the concern of many recipients of spam that responding with a message requesting the sender not to send any more messages can represent a confirmation of an address that leads to more spam.

Transparency issues

In order that ISPs, businesses, and users are empowered to control the email they receive, marketing and promotional electronic messages should be regulated through legislation requiring messages to have accurate sender information and a functional unsubscribe facility (which means that there is a working, clearly visible means of opting out of future mailings).

Privacy issues—address-harvesting

Address-harvesting is the use of computer software to search the Internet for email addresses and then to collect and compile those addresses. Spammers use address-harvesting to obtain addresses to send messages to. Privacy issues arise because in many cases the addresses are obtained from sources on the Internet, for example, chat rooms, where there was no intention that the address be available for any form of public use.

It is therefore recommended that legislation prohibits the supply, acquisition and use of address-harvesting software and harvested-address lists in connection with the unlawful sending of marketing or promotional electronic messages.

Enforcement—penalties and other remedies

It is proposed that civil pecuniary penalties be adopted. It is proposed that the maximum penalties be $200,000 for individuals and $500,000 for bodies corporate as these penalties are considered large enough to have a deterrent effect, with the additional option of being

able to impose a further penalty that is equivalent to any financial gain shown to have been received as a result of the contraventions.

Enforcement—addressing complaints and promoting compliance

It is proposed that consumers and users seek to resolve spam problems with the sender of the spam and their ISP. If an ISP considers that a complaint should be addressed by the government enforcement agency then the ISP can refer it on for action.

It is also proposed that a voluntary code of practice for ISPs on dealing with spam be promoted. It is not proposed that the Government would consider regulating ISPs unless a code of practice cannot be agreed to.

It is proposed that the New Zealand Government enforcement agency be established within the Department of Internal Affairs and be given the role of educating consumers, users, and businesses, promoting compliance, dealing with complaints from ISPs, carrying out investigations where appropriate, taking appropriate enforcement action, and co-operating with overseas enforcement agencies.

Business compliance cost statement

Sources of compliance costs

For businesses, organisations, and individuals involved in direct marketing or the sending of promotional messages by electronic means, there will be an initial cost while they move to best e-marketing practice if they have not already done so. This will involve—

- ensuring their address lists are opt-in based or that an appropriate business or other relationship exists. The actual cost of this is unlikely to be significant as only a small number are likely to be caught and the costs for those who are caught are likely to be in the nature of a day or two of a staff member's time. The costs will be short-term and offset by longer-term benefits in terms of improved efficacy of direct online marketing as a channel. In addition, where email addresses are for natural persons, the Privacy Act 1993 already requires that they be held only for the purpose for which they were given:
- ensuring that electronic marketing or promotional messages contain accurate sender identification and include a functional unsubscribe facility (a working, clearly visible means of opting out of future mailings). This mechanism may simply

involve instructing the recipient to return the email with "unsubscribe" in the subject field or providing a link to perform this task automatically if the recipient wishes to unsubscribe. To comply with this requirement an email template change at trivial cost is all that would be required:

- setting up a system for ensuring that lists of email addresses for marketing or promotional purposes are up-to-date and comply with the legislative consent requirements.

Ongoing compliance costs would be the administration costs involved in maintaining an up-to-date email address list for marketing or promotional purposes. This would simply mean acting in accordance with best e-marketing practice and may already be part of most businesses administrative practices.

Parties likely to be affected

The parties that are likely to be affected are businesses, organisations, and individuals who send electronic marketing or promotional messages. It is unclear how many parties are likely to be affected as no data is kept on this. It would certainly cover all businesses involved in direct marketing online such as banks, insurance companies, and retailers who keep customer email lists.

Estimated compliance costs

The estimated compliance costs will vary for each business, organisation and individual and will range from zero for those who already comply with best practice to potentially one-off costs of $1,000 to $2,000 for businesses or organisations that need to make changes to their systems to ensure ongoing compliance. The ongoing administration costs are likely to be minor and part of the wider marketing function already provided for.

Steps taken to minimise compliance costs

In order to minimise compliance costs, industry will be educated on best practices of email marketing, cost effective means of carrying out those practices, and complying with legislation. The definition of "spam" has also been limited to marketing and promotional electronic messages which is narrower than in Australia where all commercial messages relating to an offer of goods or services (eg, quotes and invoices) are caught by its anti-spam legislation.

Hon David Cunliffe

Unsolicited Electronic Messages Bill

Government Bill

Contents

The Parliament of New Zealand enacts as follows:

1 Title

This Act is the Unsolicited Electronic Messages Act **2005**.

2 Commencement

This Act comes into force 4 months after the date on which it receives the Royal assent.

Part 1
Preliminary provisions

3 Purposes of this Act

The purposes of this Act are to—

(a) prohibit commercial electronic messages with a New Zealand link from being sent to people who have not given their prior consent to receiving those messages; and

(b) prohibit promotional electronic messages with a New Zealand link from being sent to a person who has withdrawn consent to receiving those messages; and

(c) require all commercial and promotional electronic messages to include accurate information about the person who authorised the sending of the message; and

(d) require all commercial and promotional electronic messages to contain a functional unsubscribe facility; and

(e) prohibit address-harvesting software and any electronic address list produced using that software from being supplied or acquired for use, or being used, in connection with sending unsolicited commercial electronic messages, or promotional electronic messages, in contravention of this Act.

4 Interpretation

(1) In this Act, unless the context otherwise requires,—

address-harvesting software means software that is capable of, or marketed for use for,—

(a) searching the Internet for electronic addresses; and

(b) collecting, compiling, capturing, or otherwise harvesting those electronic addresses

civil liability event has the meaning set out in **section 22**

commercial electronic message has the meaning set out in **section 6**

consented to receiving—

(a) means—

(i) express consent, whether given by the relevant electronic address-holder or any other person who uses the relevant electronic address; or

(ii) consent that can reasonably be inferred from—

(A) the conduct and the business and other relationships of the persons concerned; and

(B) any other circumstances specified in the regulations; or

(iii) consent that is deemed to have been given when the following circumstances apply:

(A) an electronic address has been conspicuously published by a person in a business or official capacity; and

(B) the publication of the address is not accompanied by a statement to the effect that the relevant electronic address-holder does not

want to receive unsolicited electronic messages at that electronic address; and

(C) the message sent to that address is relevant to the business, role, functions, or duties of the person in a business or official capacity; but

(b) does not include the circumstances specified in the regulations from which consent cannot be inferred

electronic address means an address used in connection with—

(a) an email account; or

(b) an instant messaging account; or

(c) a telephone account; or

(d) a similar account

electronic message has the meaning set out in **section 5**

enforcement department means the department of State that, with the authority of the Prime Minister, is responsible for exercising the enforcement powers in **Part 3**

goods has the same meaning as in section 2(1) of the Fair Trading Act 1986

government body means—

(a) a department named in Part 1 of Schedule 1 of the Ombudsmen Act 1975:

(b) a Crown entity as defined in section 10(1) of the Crown Entities Act 2004

harvested-address list means—

(a) a list of electronic addresses; or

(b) a collection of electronic addresses; or

(c) 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

individual means a natural person, other than a deceased natural person

message means information, whether in—

(a) the form of text or writing; or

(b) the form of data; or

(c) the form of speech, music, or other sounds; or

(d) the form of visual images (animated or otherwise); or

(e) any other form; or

(f) any combination of forms

mistake means a reasonable mistake of fact

organisation includes—

(a) a corporation sole; and
(b) a body corporate; and
(c) an unincorporated body or association; and
(d) a partnership; and
(e) a government body; and
(f) a court or tribunal

person means—

(a) an individual; and
(b) an organisation

promotional electronic message means an electronic message—

(a) that is not a commercial electronic message; and
(b) that has, as its primary purpose, the promotion or marketing of an organisation, or its aims or ideals

recipient, in relation to the sending of an electronic message to an electronic address, means—

(a) the relevant electronic address-holder; and
(b) any other person who uses that electronic address

regulations means regulations made under this Act

relevant electronic address-holder means the person who is responsible for the relevant electronic address

send includes an attempt to send

service provider means a provider of a telecommunications service

services has the same meaning as in section 2(1) of the Fair Trading Act 1986

telecommunication has the same meaning as in section 5 of the Telecommunications Act 2001

telecommunications service means any goods, services, equipment, and facilities that enable or facilitate telecommunication

unsolicited commercial electronic message means a commercial electronic message that the recipient has not consented to receiving.

(2) For the purposes of this Act, an electronic message has a **New Zealand link** if 1 or more of the following applies:

(a) the message originates in New Zealand:
(b) the person who sent the message is—
  (i) an individual who is physically present in New Zealand when the message is sent; or
  (ii) an organisation whose central management and control is in New Zealand when the message is sent:
(c) the computer, server, or device that is used to access the message is located in New Zealand:
(d) the recipient is—
  (i) an individual who is physically present in New Zealand when the message is accessed; or
  (ii) an organisation that carries on business or activities in New Zealand when the message is accessed:
(e) 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:
(f) it is sent to an electronic address that—
  (i) ends with ".nz"; or
  (ii) begins with an international access code directly followed by "64".

Compare: Spam Act 2003 ss 4, 7, Sch 2 (Aust); 2001 No 103 s 5

5 Meaning of electronic message

(1) For the purposes of this Act, an **electronic message** is a message sent—
  (a) using a telecommunications service; and
  (b) to an electronic address.

(2) However, the messages listed in **clause 1 of the Schedule** are not electronic messages.

(3) For the purposes of **subsection (1)**, it is immaterial whether—
  (a) the electronic address exists; or
  (b) the message reaches its intended destination.

Compare: Spam Act 2003 s 5 (Aust)

6 Meaning of commercial electronic message

For the purposes of this Act, **commercial electronic message**—

(a) means an electronic message that has, as its primary purpose,—

(i) marketing or promoting—

(A) goods; or

(B) services; or

(C) land; or

(D) an interest in land; or

(E) a business or investment opportunity; or

(ii) assisting or enabling a person to obtain dishonestly a financial advantage or gain from another person; but

(b) does not include an electronic message that—

(i) provides a quote or estimate for the supply of goods or services if that quote or estimate was requested by the recipient; or

(ii) facilitates, completes, or confirms a commercial transaction that the recipient previously agreed to enter into with the person who authorised the sending of the message; or

(iii) provides warranty information, product recall information, or safety or security information about goods or services used or purchased by the recipient; or

(iv) provides notification of factual information about a subscription, membership, account, loan, or similar relationship involving the ongoing purchase or use by the recipient of goods or services offered by the person who authorised the sending of the message, or the recipient's ongoing subscription, membership, account, loan, or similar relationship; or

(v) provides information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or

(vi) delivers goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously entered into with the person who authorised the sending of the message; or

(vii) provides the recipient with information about goods or services offered or supplied by—
(A) a government body; or
(B) a court or tribunal; or
(viii) has any other purpose set out in the regulations.

Compare: Spam Act 2003 s 6 (Aust)

7 Act binds the Crown

This Act binds the Crown.

Compare: Spam Act 2003 s 12 (Aust)

8 Application of Act outside New Zealand

(1) This Act extends to the engaging in conduct outside New Zealand by a relevant person to the extent that that conduct results in a civil liability event occurring.

(2) In this section, **relevant person** means—
(a) an individual who is a resident of New Zealand; or
(b) an organisation that carries on business or activities in New Zealand.

Compare: Spam Act 2003 s 14 (Aust)

Part 2
Restrictions on electronic messages, address-harvesting software, and harvested-address lists

Subpart 1—Commercial electronic messages and promotional electronic messages

9 Unsolicited commercial electronic messages must not be sent

(1) A person must not send, or cause to be sent, an unsolicited commercial electronic message that has a New Zealand link.

(2) A person who contends that a recipient consented to receiving a commercial electronic message has the onus of proof in relation to that matter.

Compare: Spam Act 2003 s 16(1), (2), (5), (6) (Aust)

10 Promotional electronic message must not be sent to person who opts out

(1) A person (the **sender**) must not send, or cause to be sent, a promotional electronic message that has a New Zealand link to any person (the **unwilling recipient**) who has opted out of receiving messages from that sender.

(2) For the purposes of **subsection (1)**, an unwilling recipient opts out of receiving a promotional electronic message from a sender if—

(a) 1 or more promotional electronic messages have been sent to the unwilling recipient's electronic address by or on behalf of the sender; and

(b) 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 electronic messages from or authorised by that sender.

(3) Opting out of receiving promotional electronic messages takes effect at the end of a period of 5 working days beginning on—

(a) the day on which the message was sent if the message referred to in **subsection (2)(b)** is an electronic message; or

(b) the day on which the message was given if the message referred to in **subsection (2)(b)** was given over the telephone; or

(c) the day on which the message would be delivered in the ordinary course of post if the message referred to in **subsection (2)(b)** was sent by post; or

(d) the day on which the message was sent, delivered, or given in any other case.

Compare: Spam Act 2003 s 16(1), Sch 2 cl 6 (Aust)

11 Commercial electronic messages and promotional electronic messages must include accurate sender information

A person must not send, or cause to be sent, a commercial electronic message or a promotional electronic message that has a New Zealand link unless—

(a) the message clearly and accurately identifies the person who authorised the sending of the message; and

(b) the message includes accurate information about how the recipient can readily contact that person; and

(c) the information referred to in **paragraph (b)** complies with any conditions specified in the regulations; and

(d) the information referred to in **paragraph (b)** is reasonably likely to be valid for at least 30 days after the message is sent.

Compare: Spam Act 2003 s 17(1) (Aust)

12 Commercial electronic messages and promotional electronic messages must contain functional unsubscribe facility

(1) A person must not send, or cause to be sent, a commercial electronic message or a promotional electronic message (the **principal message**) that has a New Zealand link unless—

(a) the principal message includes a functional unsubscribe facility that the recipient may use to instruct the person who authorised the sending of the principal message (the **sender**) that no further commercial electronic messages or promotional electronic messages from or authorised by the sender should be sent to the electronic address at which the principal message was received; and

(b) the unsubscribe facility is expressed and presented in a clear and conspicuous manner; and

(c) the unsubscribe facility is reasonably likely to be functional and valid for at least 30 days after the principal message is sent; and

(d) the unsubscribe facility complies with any conditions specified in the regulations.

(2) **Subsection (1)** does not apply to the extent (if any) to which it is inconsistent with the terms of a contract, arrangement, or understanding between—

(a) the person who authorised the sending of the principal message; and

(b) the recipient.

Compare: Spam Act 2003 s 18(1), (3), (9) (Aust)

13 Defences

(1) A person who sends an electronic message, or causes an electronic message to be sent, in contravention of **section 9, 10, 11, or 12** has a defence if—

(a) that person sent the message, or caused the message to be sent, by mistake; or

(b) the message was sent without that person's knowledge (for example, because of a computer virus or a malicious software programme).

(2) A person who wishes to rely on a defence in **subsection (1)** has the onus of proof in relation to that matter.

Compare: Spam Act 2003 ss 16(4), (5), 17(3), (4), 18(4), (5) (Aust)

Subpart 2—Address-harvesting software and harvested-address lists

14 Application of sections 15 to 17

(1) In **sections 15 to 17**, **person** means—

(a) an individual who is physically present in New Zealand at the relevant time; or

(b) an organisation that carries on business or activities in New Zealand at the relevant time.

(2) In **subsection (1)**, **relevant time** means, as appropriate, the time of—

(a) the supply or offer; or

(b) the acquisition; or

(c) the use.

Compare: Spam Act 2003 ss 20(1), 21(1), 22(1) (Aust)

15 Address-harvesting software and harvested-address lists must not be supplied

(1) A person (the **supplier**) must not supply, or offer to supply, to another person (the **customer**)—

(a) address-harvesting software; or

(b) a right to use address-harvesting software; or

(c) a harvested-address list; or

(d) a right to use a harvested-address list.

(2) **Subsection (1)** does not apply if the supplier had no reason to suspect that the customer, or another person, intended to use the address-harvesting software or the harvested-address list, as the case may be, in connection with sending—

(a) unsolicited commercial electronic messages in contravention of **section 9**; or

(b) promotional electronic messages in contravention of **section 10**.

(3) **Subsection (1)** does not apply if the supplier did not know, and could not, with reasonable diligence, have ascertained, that the customer was—

(a) an individual who was physically present in New Zealand at the time of the supply or offer; or

(b) an organisation that carried on business or activities in New Zealand at the time of the supply or offer.

Compare: Spam Act 2003 s 20(1), (2), (3) (Aust)

16 Address-harvesting software and harvested-address lists must not be acquired

(1) A person must not acquire—

(a) address-harvesting software; or

(b) a right to use address-harvesting software; or

(c) a harvested-address list; or

(d) a right to use a harvested-address list.

(2) **Subsection (1)** does not apply if the person did not intend to use the address-harvesting software or the harvested-address list, as the case may be, in connection with sending—

(a) unsolicited commercial electronic messages in contravention of **section 9**; or

(b) promotional electronic messages in contravention of **section 10**.

Compare: Spam Act 2003 s 21(1), (2) (Aust)

17 Address-harvesting software and harvested-address lists must not be used

(1) A person must not use—

(a) address-harvesting software; or

(b) a harvested-address list.

(2) **Subsection (1)** does not apply in relation to the use of address-harvesting software or a harvested-address list, if the use was not in connection with sending—

(a) unsolicited commercial electronic messages in contravention of **section 9**; or

(b) promotional electronic messages in contravention of **section 10**.

Compare: Spam Act 2003 s 22(1), (2) (Aust)

18 Onus of proof

A person who wishes to rely on **section 15(2), 15(3), 16(2), or 17(2)** has the onus of proof in relation to that matter.

Compare: Spam Act 2003 s 20(4) (Aust)

Subpart 3—Third party breaches of Act

19 Third party breaches of Act

A person must not—

(a) aid, abet, counsel, or procure a breach of **sections 9 to 12 or 15 to 17**; or

(b) induce, whether by threats or promises or otherwise, a breach of **sections 9 to 12 or 15 to 17**; or

(c) be in any way, directly or indirectly, knowingly concerned in, or party to, a breach of **sections 9 to 12 or 15 to 17**; or

(d) conspire with others to effect a breach of **sections 9 to 12 or 15 to 17**.

Compare: Spam Act 2003 ss 16(9), 17(5), 18(6), 20(5), 21(3), 22(3) (Aust)

Subpart 4—Rules of general application throughout Act

20 Supplying message service

A service provider does not send an electronic message, or cause an electronic message to be sent, or contravene **section 19**, merely because the service provider provides a telecommunications service that enables an electronic message to be sent.

Compare: Spam Act 2003 ss 9, 16(10), 17(6), 18(7) (Aust)

21 Person who authorises sending, or sends, electronic messages

(1) For the purposes of this Act, if a relevant individual authorises the sending of an electronic message on behalf of an organisation, then—

(a) the organisation is taken to authorise the sending of that message; and

(b) the relevant individual is taken not to authorise the sending of that message.

(2) For the purposes of this Act, a person (**A**) is taken to authorise the sending of an electronic message if—

(a) that message is sent by A; and

(b) the sending of the message is not authorised by any other person.

(3) For the purposes of this Act, an organisation is taken to have sent an electronic message if—

(a) an individual sent that message on behalf of that organisation; and

(b) that organisation authorised the sending of that message.

(4) For the purposes of **subsection (1)**, **relevant individual** means an individual—

(a) who is a director, officer, employee, or contractor of the relevant organisation; or

(b) in accordance with whose directions or instructions the relevant organisation is required or is accustomed to act.

(5) **Subsection (2)** overrides **subsection (1)**.

Compare: Spam Act 2003 s 8 (Aust)

Part 3
Enforcement provisions

Subpart 1—Civil liability events

22 Meaning of civil liability event

In this Part, a **civil liability event** is a breach of 1 or more of the following:

(a) **section 9(1)**:

(b) **section 10(1)**:

(c) **section 11**:

(d) **section 12(1)**:

(e) **section 15(1)**:

(f) **section 16(1)**:

(g) **section 17(1)**:

(h) **section 19**.

Compare: Spam Act 2003 ss 16(11), 17(7), 18(8), 20(6), 21(4), 22(4) (Aust)

23 Possible responses to civil liability event

If a civil liability event is alleged to have occurred,—

(a) any person affected by that event may do either or both of the following:

(i) make a complaint to the relevant service provider:

(ii) seek an injunction from the High Court under **section 37** or **section 39**; and

(b) a person who suffers loss or damage as a result may do 1 or more of the following:

(i) seek an injunction from the High Court under **section 37** or **section 39**:

(ii) make an application to the High Court for compensation or damages under **section 43**:

(iii) apply to join any Court action initiated by the enforcement department under **section 44**; and

(c) a service provider may do 1 or more of the following:

(i) make a complaint to the enforcement department:

(ii) seek an injunction from the High Court under **section 37** or **section 39**:

(iii) make an application to the High Court for compensation or damages under **section 43**:

(iv) apply to join any Court action initiated by the enforcement department under **section 44**; and

(d) the enforcement department may do 1 or more of the following:

(i) issue a formal warning under **section 26**:

(ii) issue a contravention notice under **section 27**:

(iii) accept an enforceable undertaking under **section 34** and seek an order in the High Court under **section 35** for a breach of that undertaking:

(iv) seek an injunction from the High Court under **section 37** or **section 39**:

(v) make an application to the High Court for a pecuniary penalty under **section 42**:

(vi) make an application to the High Court for compensation or damages under **section 43** on behalf of another person:

(vii) apply to join any Court action initiated by any other person under **section 44**:

(viii) apply for a search warrant under **section 48** and exercise the powers of search and seizure granted by the warrant.

Subpart 2—Obligations of service provider

24 Service providers must consider complaints

(1) A service provider must consider any complaint made to it under **section 23(a)(i)**.

(2) In considering a complaint, the service provider must have regard to any relevant, generally accepted industry code that applies to the service provider.

Subpart 3—Powers of enforcement department

25 General obligations and powers of enforcement department

The enforcement department—

(a) must consider all complaints it receives from service providers concerning an alleged civil liability event, but must not consider any complaint it receives from any other person; and

(b) may investigate and take enforcement action on a complaint received from a service provider if it considers that an investigation or enforcement action is appropriate in the circumstances; and

(c) may investigate and take enforcement action on its own initiative if it considers that an investigation or enforcement action is appropriate in the circumstances.

Formal warnings

26 Formal warnings

(1) The enforcement department may issue one or more formal warnings to a person if the enforcement department has reasonable grounds to believe that that person has committed a civil liability event.

(2) A formal warning must be—

(a) in the prescribed form; and

(b) issued in the manner specified in the regulations.

Compare: Spam Act 2003 s 41 (Aust)

Contravention notices

27 Contravention notices

If the enforcement department has reasonable grounds to believe that a person has committed 1 or more civil liability events, the enforcement department may issue a contravention notice relating to those events to that person.

Compare: Spam Act 2003 Sch 3, cl 3 (Aust)

28 Issue of contravention notices

(1) A contravention notice must be issued within 12 months after the day on which the earliest civil liability event referred to in the notice is alleged to have occurred.

(2) A contravention notice may be issued—

(a) by delivering it to the person alleged to have committed the civil liability event; or

(b) by post, addressed to that person's last known place of residence or business.

(3) A contravention notice issued to a person in accordance with **subsection (2)(b)** is deemed to have been issued on the day it was posted.

Compare: Spam Act 2003 Sch 3, cl 3 (Aust)

29 Form of contravention notices

A contravention notice must—

(a) contain sufficient particulars to inform the person issued with the notice of the time, manner, and nature of the alleged civil liability events; and

(b) specify the penalty to be paid for each civil liability event alleged to have occurred, which must not exceed the amount specified in the regulations; and

(c) specify the time within which the penalty must be paid; and

(d) give an explanation of how payment of the penalty is to be made; and

(e) contain a statement of the person's right to object to the notice; and

(f) contain a statement of what may happen if the person neither pays the penalty nor objects to the notice; and

(g) contain the information specified in the regulations.

Compare: Spam Act 2003 Sch 3, cl 4 (Aust)

30 Objections to contravention notices

(1) An objection to a contravention notice—

(a) may be made only on the grounds specified in the regulations:

(b) must contain all of the information specified in the regulations:

(c) must be made within the time and in the manner specified in the regulations.

(2) The enforcement department—

(a) must consider every objection that is properly made under **subsection (1)**; and

(b) may turn down the objection, alter the contravention notice, or withdraw the contravention notice in accordance with **section 31**; and

(c) must, as soon as reasonably practicable, notify the objector in writing—

(i) as to whether the objection has been turned down, upheld, or upheld in part; and

(ii) of the effect of the enforcement department's decision.

(3) A person may not object to a contravention notice that has been altered by the enforcement department under **subsection 2(b)**.

31 Withdrawal of contravention notice

(1) The enforcement department may, by written notice (the **withdrawal notice**) given to a person who has been issued with a contravention notice, withdraw the contravention notice.

(2) To be effective, the withdrawal notice must be given to the person within 28 days after the later of the day on which—

(a) the notice was issued; or

(b) if applicable, the enforcement department issues its final response to an objection to the contravention notice.

(3) The enforcement department must refund the penalty specified in a contravention notice if—

(a) the penalty specified in the contravention notice has been paid; and

(b) the contravention notice is withdrawn after the penalty was paid.

Compare: Spam Act 2003 Sch 3, cl 6 (Aust)

32 What happens if penalty is paid

(1) This section applies if—

(a) a contravention notice relating to 1 or more alleged civil liability events is issued to a person, even if that notice is subsequently withdrawn; and

(b) the penalty is paid in accordance with the contravention notice, even if that penalty is subsequently refunded.

(2) If **subsection (1)** applies,—

(a) any liability of the person for the alleged civil liability events to which the contravention notice relates is discharged; and

(b) proceedings under **section 42** or **section 43** may not be brought against the person for those alleged civil liability events.

Compare: Spam Act 2003 Sch 3, cl 7 (Aust)

33 Effect of contravention notice on civil proceedings

A contravention notice issued to a person does not prevent proceedings under **section 42** or **section 43** being brought against the person for an alleged civil liability event if—

(a) the person does not pay the penalty specified in the contravention notice for that event; or

(b) a contravention notice relating to the event is issued to the person and subsequently withdrawn before the penalty specified in the notice is paid.

Compare: Spam Act 2003 Sch 3, cl 8 (Aust)

Enforceable undertakings

34 Enforceable undertakings

(1) The enforcement department may accept a written undertaking given by a person in connection with—

(a) commercial electronic messages; or

(b) promotional electronic messages; or

(c) address-harvesting software; or

(d) harvested-address lists.

(2) The person may withdraw or vary the undertaking at any time, but only with the consent of the enforcement department.

Compare: Spam Act 2003 s 38 (Aust)

35 Enforcement of undertakings

(1) If the enforcement department considers that a person who gave an undertaking under **section 34** has breached 1 or more of its terms, the enforcement department may apply to the High Court for an order under **subsection (2)**.

(2) If the High Court is satisfied that the person has breached 1 or more of the terms of the undertaking, the Court may make any or all of the following orders:

(a) an order directing the person to comply with the relevant terms of the undertaking:

(b) an order directing the person to pay to the enforcement department an amount up to the amount of any financial benefit that the person has obtained directly or indirectly and that is reasonably attributable to the breach:

(c) any order that the Court considers appropriate directing the person to compensate any other person who has suffered loss or damage as a result of the breach:

(d) any other order that the Court considers appropriate.

Compare: Spam Act 2003 s 39 (Aust)

36 Assessment of compensation for breach of undertaking

For the purposes of **section 35(2)(c)**, in determining whether another person (the **victim**) has suffered loss or damage as a result of the breach, and in assessing the amount of compensation payable, the High Court may have regard to the following:

(a) the extent to which any expenses incurred by the victim are attributable to dealing with the messages:

(b) the effect of dealing with the messages on the victim's ability to carry on business or other activities:

(c) any damage to the reputation of the victim's business that is attributable to dealing with the messages:

(d) any loss of business opportunities suffered by the victim as a result of dealing with the messages:

(e) any other matters that the Court considers relevant.

Compare: Spam Act 2003 s 40 (Aust)

Subpart 4—Powers of High Court

Injunctions

37 Performance injunctions

(1) The High Court may, on the application of the enforcement department or any other person, grant an injunction requiring a person to do an act or thing if—

(a) that person has refused or failed, or is refusing or failing, or is proposing to refuse or fail, to do that act or thing; and

(b) the refusal or failure was, is, or would be a civil liability event.

(2) The Court may rescind or vary an injunction granted under this section.

Compare: Spam Act 2003 ss 32, 34 (Aust)

38 When High Court may grant performance injunctions

(1) The High Court may grant an injunction requiring a person to do an act or thing if—

(a) it is satisfied that the person has refused or failed to do that act or thing; or

(b) it appears to the Court that, if an injunction is not granted, it is likely that the person will refuse or fail to do that act or thing.

(2) **Subsection (1)(a)** applies whether or not it appears to the Court that the person intends to refuse or fail again, or to continue to refuse or fail, to do that act or thing.

(3) **Subsection (1)(b)** applies whether or not the person has previously refused or failed to do that act or thing or there is an imminent danger of substantial damage to any other person if that person refuses or fails to do that act or thing.

Compare: Spam Act 2003 s 35 (Aust)

39 Restraining injunctions

(1) The High Court may, on the application of the enforcement department or any other person, grant an injunction restraining a person from engaging in conduct that constitutes or would constitute a contravention of a provision of this Act.

(2) The Court may rescind or vary an injunction granted under this section.

Compare: Spam Act 2003 ss 32, 34 (Aust); 2003 No 52 s 96

40 When High Court may grant restraining injunctions and interim injunctions

(1) The High Court may grant an injunction restraining a person from engaging in conduct of a particular kind if—

(a) it is satisfied that the person has engaged in conduct of that kind; or

(b) it appears to the Court that, if an injunction is not granted, it is likely that the person will engage in conduct of that kind.

(2) The Court may grant an interim injunction restraining a person from engaging in conduct of a particular kind if in its opinion it is desirable to do so.

(3) **Subsections (1)(a) and (2)** apply whether or not it appears to the Court that the person intends to engage again, or to continue to engage, in conduct of that kind.

(4) **Subsections (1)(b) and (2)** apply whether or not the person has previously engaged in conduct of that kind or there is an imminent danger of substantial damage to any other person if that person engages in conduct of that kind.

Compare: Spam Act 2003 ss 33, 35 (Aust); 2003 No 52 ss 97, 98

41 Undertaking as to damages not required by enforcement department

(1) If the enforcement department applies to the High Court for the grant of an interim injunction under this subpart, the Court must not, as a condition of granting an interim injunction, require the enforcement department to give an undertaking as to damages.

(2) However, in determining the enforcement department's application for the grant of an interim injunction, the Court must not take into account that the enforcement department is not required to give an undertaking as to damages.

Compare: Spam Act 2003 s 33 (Aust); 2003 No 52 s 98

Pecuniary penalties, compensation, and damages

42 Pecuniary penalties for civil liability event

(1) On the application of the enforcement department, the High Court may order a person (the **perpetrator**) to pay a pecuniary penalty to the Crown, or any other person specified by the Court, if the Court is satisfied that the perpetrator has committed a civil liability event.

(2) Subject to the limits in **subsections (3) to (5)**, the pecuniary penalty that the High Court orders the perpetrator to pay must be an amount which the Court considers appropriate taking into account all relevant circumstances, including—

(a) the number of electronic messages sent:

(b) the number of electronic addresses to which an electronic message was sent:

(c) whether or not the perpetrator has committed prior civil liability events.

(3) If the perpetrator is an individual, the High Court may order the perpetrator to pay a pecuniary penalty not exceeding $200,000 in respect of the civil liability events, other than a breach of **section 10(1)**, that are the subject of the enforcement department's application.

(4) If the perpetrator is an organisation, the High Court may order the perpetrator to pay a pecuniary penalty not exceeding $500,000 in respect of the civil liability events, other than a breach of **section 10(1)**, that are the subject of the enforcement department's application.

(5) The High Court may order the perpetrator to pay a pecuniary penalty not exceeding $50,000 in respect of the breaches of **section 10(1)** that are the subject of the enforcement department's application.

Compare: Spam Act 2003 ss 24, 25, 26 (Aust)

43 Compensation and damages for civil liability event

(1) This section applies if the High Court is satisfied that—

(a) a person (the **perpetrator**) has committed a civil liability event; and

(b) another person (the **victim**) has suffered either direct or consequential loss or damage as a result of that civil liability event.

(2) The High Court may make a finding under **subsection (1)**—

(a) on the application of the victim; or
(b) on the application of the enforcement department.

(3) If this section applies, the High Court may make an order that the Court considers appropriate directing the perpetrator to pay to the victim either or both of the following:
(a) compensation for any loss suffered by the victim as a result of the civil liability event:
(b) damages not exceeding an amount equal to the financial benefit obtained by the perpetrator as a result of the civil liability event.

Compare: Spam Act 2003 ss 28, 29 (Aust)

44 Joinder of parties

(1) On the application of the enforcement department or any other person, the High Court may direct that—
(a) an application for compensation or damages under **section 43** be heard together with an application by the enforcement department for a pecuniary penalty under **section 42**; or
(b) an application by the enforcement department for a pecuniary penalty under **section 42** be heard together with an application for compensation or damages under **section 43**; or
(c) 2 or more applications for compensation or damages under **section 43** be heard together.

(2) The High Court may make a direction under **subsection (1)**—
(a) at any stage of the proceedings; and
(b) upon any terms that it thinks fit; and
(c) according to the merits and equities of the circumstances.

45 Interrelationship of civil liability remedies

(1) A person may be liable for a pecuniary penalty, compensation, and damages for the same civil liability event.

(2) However, in determining whether to order a person to pay a pecuniary penalty, or compensation, or damages (individually, a **civil liability remedy**), the High Court must have regard to—
(a) whether that person has already paid another civil liability remedy for the same civil liability event; and

(b) if so, the amount and effect of that first civil liability remedy.

Compare: Spam Act 2003 ss 28(3), 29(2) (Aust)

46 Applicable rules, procedure, and standard of proof

The proceedings under **sections 42 and 43** are civil proceedings to which the usual rules of the High Court, rules of evidence, and procedure for civil proceedings apply (including the standard of proof).

47 Time limit for applying for pecuniary penalty, compensation, and damages

(1) An application for a pecuniary penalty may be made at any time within 2 years after the date on which the matter giving rise to the civil liability event was discovered or ought reasonably to have been discovered.

(2) The usual time limits apply to all applications for compensation or damages.

Compare: Spam Act 2003 ss 26(2), 28(4), 29(3) (Aust)

Subpart 5—Search and seizure

48 Search warrant

(1) The enforcement department may apply for a search warrant to search a place or thing.

(2) The application must be made in writing and on oath to the District Court.

(3) The District Court may issue a search warrant if there are reasonable grounds for believing that—

(a) a civil liability event has been, or is being, committed at the place or thing; or

(b) there is in, on, over, or under the place or thing anything that is evidence of a civil liability event.

(4) The District Court may issue the warrant to—

(a) a person authorised by the enforcement department in writing to execute the warrant; or

(b) any member of the police; or

(c) a member of the police by name.

49 Form and content of search warrant

(1) A search warrant must not be exercised later than 14 clear days after the day on which it was issued.

(2) A search warrant must be in the prescribed form and must contain all of the following information:

(a) the place or thing that may be searched; and

(b) the civil liability event or events in respect of which the warrant is issued; and

(c) a description of the kind of property or thing that may be seized; and

(d) the period during which the warrant may be executed; and

(e) any special conditions on which the warrant is issued.

50 Powers conferred by search warrant

(1) A search warrant may be executed by the person to whom it was issued or, if it was issued to the police in general, any member of the police.

(2) Subject to any special conditions specified in the warrant, a search warrant may authorise the person executing the warrant to—

(a) enter and search the place or thing specified in the warrant at any reasonable time; and

(b) use the assistance that is reasonable in the circumstances to enter and search the place or thing; and

(c) use the force that is reasonable in the circumstances to gain entry and to break open anything in, on, over, or under the place or thing searched; and

(d) search any person found in or at the place or thing; and

(e) search for and seize any property or thing referred to in **section 49(2)(c)**; and

(f) take copies of documents, or extracts from documents, that the person executing the warrant believes on reasonable grounds may be relevant; and

(g) require a person to reproduce, or assist any person executing the warrant to reproduce, in usable form, information recorded or stored in a document.

(3) A person who is called to assist to execute a search warrant may exercise the powers described in **subsection (2)(c), (e), and (f)**.

(4) The power to enter and search a place or thing under a search warrant may be exercised only once.

51 Requirements when executing search warrant

(1) The person who executes the warrant (**person A**) must carry the warrant with him or her, and produce it for inspection, with evidence of person A's identity,—

(a) when person A first enters the place or thing specified in the warrant, to the person who appears to be in charge of that place or thing; and

(b) whenever person A is subsequently required to do so at the place or thing specified in the warrant, by any other person who appears to be in charge of that place or thing or any part of it.

(2) If the owner or occupier of the place or thing is not present at the time person A executes the search warrant, person A must leave at the place or thing, in a prominent location, a written statement that includes the following information:

(a) the time and date of the search; and

(b) person A's name; and

(c) the address of the office of the enforcement department or (if person A is a member of the police) the police station to which inquiries should be made.

(3) If any property or thing is seized in the execution of a search warrant, person A must leave in a prominent location at the place or thing, or deliver or send by registered mail to the owner or occupier within 10 working days after the search, a written inventory of all property or things seized.

52 Disposal of property or thing seized under search warrant

(1) In any proceeding for a civil liability event relating to any property or thing seized under a warrant under this Act, the High Court may order, either at the trial or hearing or on application, that—

(a) the property or thing must be delivered to the person who, in the Court's view, appears to be entitled to it; or

(b) the property or thing must otherwise be disposed of as the Court thinks appropriate.

(2) The enforcement department or a member of the police may, at any time, unless an order has been made under **subsection (1)**,

return the property or thing to the person from whom it was seized, or apply to a District Court Judge for an order for its disposal.

(3) On an application under **subsection (2)**, the District Court Judge may make any order that the High Court may make under **subsection (1)**.

(4) If proceedings for a civil liability event relating to the property or thing are not brought within a period of 3 months from the date of seizure, any person claiming to be entitled to the property or thing may then apply to a District Court Judge for an order that it be delivered to that person.

(5) On an application under **subsection (4)**, the District Court Judge may—

(a) adjourn the application, on any terms that he or she thinks are appropriate, for proceedings to be brought; or

(b) make any order that the High Court may make under **subsection (1)**.

Part 4
Miscellaneous provisions

53 Alterations to Schedule

The Governor-General may, by Order in Council, amend the Schedule by, with respect to the list of messages that are not electronic messages,—

(a) adding a type of message to the list and, if required, a description of that type of message:

(b) omitting a type of message from the list and, if relevant, an associated description of that type of message:

(c) amending a type of message on the list:

(d) amending a description of a type of message.

54 Regulations

The Governor-General may, by Order in Council, make regulations for all or any of the following purposes:

(a) specifying circumstances from which a recipient may or may not be inferred to have consented to receiving an electronic message:

(b) setting out further purposes that exclude an electronic message from being a commercial electronic message under **section 6**:

(c) specifying conditions for the purposes of **section 11(c)**:

(d) specifying conditions for the purposes of **section 12(1)(d)**:

(e) prescribing the form of formal warnings and specifying the manner in which they must be issued under **section 26**:

(f) specifying the maximum penalty that may be required under a contravention notice under **section 29(b)**:

(g) specifying the information that must be contained in a contravention notice under **section 29(g)**:

(h) specifying, in accordance with **section 30**,—

(i) the grounds on which an objection to a contravention notice may be made; and

(ii) the information that must be contained in an objection; and

(iii) the time within which, and the manner in which, an objection must be made:

(i) prescribing the form of search warrants under **section 49(2)**:

(j) authorising the enforcement department to enter into agreements or arrangements with overseas enforcement agencies concerning international enforcement of anti-spam legislation, sharing of information between national enforcement agencies, and the pursuit of cross-border complaints concerning spam:

(k) providing for any other matters contemplated by this Act or necessary for its administration or necessary for giving it full effect.

Compare: Spam Act 2003 ss 45, 47 (Aust)

s 5

Schedule
Messages that are not electronic messages

1 Excluded messages

The following messages are not electronic messages for the purposes of this Act:

(a) voice calls made using—
  (i) a standard telephone service; or
  (ii) voice-over internet protocol (IP):

(b) facsimiles.

2 Definition

In this Schedule, **voice call** means, whether or not a recipient responds by way of pressing buttons on a telephone handset, a keyboard, or similar thing,—

(a) a voice call within the ordinary meaning of that expression; or

(b) a call that involves a recorded or synthetic voice; or

(c) a call that is equivalent to a call covered by either **paragraph (a) or (b)** if a call covered by either of those paragraphs is not practical for a particular recipient with a disability (for example, because the recipient has a hearing impairment).

Wellington, New Zealand: Published under the authority of the New Zealand Government—2005

6002V6
27-JUN-05
281bar1

Price code: K