IN THE HIGH COURT OF NEW ZEALAND
AUCKLAND REGISTRY

CIV 2012-404-001899
[2013] NZHC 2064

UNDER	the Unsolicited Electronic Messages Act 2007
BETWEEN	CHIEF EXECUTIVE OF THE DEPARTMENT OF INTERNAL AFFAIRS Plaintiff
AND	WAYNE ROBERT MANSFIELD Defendant

Hearing: 8 August 2013

Appearances: B Hamlin for the Chief Executive
No Appearance for the Defendant

Judgment: 14 August 2013

[RESERVED] JUDGMENT OF WYLIE J

This judgment was delivered by Justice Wylie
on 14 August 2013 at 3.30 pm
Pursuant to r 11.5 of the High Court Rules

Registrar/Deputy Registrar

Date:

Introduction

[1] The plaintiff, the Chief Executive of the Department of Internal Affairs (the Department) seeks the imposition of a civil pecuniary penalty against the respondent, Mr Mansfield, under s 45 of the Unsolicited Electronic Messages Act 2007 (the Act).

[2] Mr Mansfield is an Australia citizen, ordinarily resident in Perth. He ran business seminars in New Zealand, initially through a company, Business Seminars NZ Limited, and later on his own account. The pecuniary penalty is sought in relation to what the Department says are unsolicited commercial electronic messages (colloquially known as "spam") promoting the seminars, said to have been sent by Mr Mansfield to persons and organisations resident in New Zealand. It says that this breaches s 9(1) of the Act. The Department also says that Mr Mansfield has been served in Australia, and that he has taken no steps in the proceedings. The matter has proceeded by way of a formal proof hearing. The Department has filed affidavits in support of its assertions. It seeks a pecuniary penalty of $100,000, along with costs of $8,460 and disbursements of $1,806.54.

[3] There are a number of issues which require resolution. I list them as follows:

(a) Does the Court have jurisdiction to make the orders sought? In particular,

(i) does the Court have jurisdiction over Mr Mansfield, as an Australia citizen ordinarily resident in that country?;

(ii) can the Court impose a civil pecuniary penalty under the Act by way of a formal proof hearing?; and

(iii) was the proceeding properly served on Mr Mansfield under the provisions of r 6.27?

(b) Has Mr Mansfield breached s 9(1) of the Act?

(c) Were the messages unsolicited, or did Mr Mansfield have the consent of the recipients?; and

(d) If the Court has jurisdiction, if Mr Mansfield has reached s 9(1), and if the messages were unsolicited, what is the appropriate pecuniary penalty to impose?

The Act

[4] Unsolicited electronic messages have become an increasing problem in recent years. The then Minister for Information Technology, the Honourable David Cunliffe, in introducing the Act, noted as follows:[1]

> In just a few years, unsolicited commercial email, generally known as spam, has gone from being a minor nuisance to becoming a significant social and economic issue. It is also a drain on the business and personal productivity of New Zealanders. Spam impedes the effective use of email and other communication technologies for personal and business communications. It threatens the growth and acceptance of legitimate e-commerce. Spam technology is also increasingly being used as the delivery mechanism for computer viruses, phishing, and identity theft.

The negative effects of spam are significant and far reaching. A Departmental deponent, a Mr Anthony Grasso, records research indicating that it is estimated that around 120 billion spam email messages are sent every day. Such messages clog up the internet, disrupt email delivery, reduce business productivity, raise internet access fees, irritate recipients, and erode people's confidence in using email and other forms of electronic communications.

[5] The Act was introduced in an endeavour to combat the difficulties caused by spam. It came into force on 5 September 2007. Inter alia, it prohibits the sending of unsolicited commercial electronic messages that have a New Zealand link. Further, commercial messages must contain accurate information about the sender and they must have a functional "unsubscribe" facility. The Act also provides that persons must not use address-harvesting software or harvested address lists in connection with the sending of unsolicited commercial electronic messages.[2]

---

1 (13 December 2005) 628 NZPD 1043.

2 Unsolicited Electronic Messages Act 2007, ss 9, 10, 11 and 13.

[6] Persons must not aid, abet or counsel a breach of the Act or be in any way, directly or indirectly, knowingly concerned in, or a party to, a breach of its provision.[3]

[7] The key prohibitions contained in the Act are backed up by a series of comprehensive definitions, for example, of the words "electronic message",[4] "commercial electronic message",[5] "unsolicited commercial electronic message",[6] and "civil liability event".[7]

[8] Section 9(3) provides that a person who contends that a recipient consented to receiving a commercial electronic message has the onus of proof in that regard. Similarly, a party relying on other defences available under the Act has the onus of proving them.[8]

[9] The Court can order a person to pay a pecuniary penalty if it is satisfied that the person has committed a civil liability event.[9] If the perpetrator is an individual, the pecuniary penalty must not exceed $200,000. If the perpetrator is an organisation, the maximum penalty is $500,000.[10] The Court can also order the payment of compensation and/or damages.[11]

[10] Enforcement is undertaken by the Department, being the Department of State that, with the authority of the Prime Minister, is responsible for exercising the enforcement provisions contained in Part 3 of the Act.

The Background Facts

[11] Between 5 April 2010 and 27 September 2010, the Department received 53 complaints from members of the public. Each complainant had received an

---

3 Section 15.
4 Section 5.
5 Section 6.
6 Section 4(1).
7 Section 18.
8 Section 12.
9 Section 45(1).
10 Section 45(3)–(4).
11 Section 46.

unsolicited electronic message marketing and promoting the goods and services of an entity known as Business Seminars NZ.

[12] The complaints were investigated. They appeared to be part of a number of separate email marketing campaigns where many emails were sent out to a large number of email addresses over a short period of time. Mr Grasso prepared a schedule of the campaigns which he identified from the complaints received. It is as follows:

	Date	Subject line	From Email address
1	07/04/10	An Evening With A Marketing and Business Legend	info@businessseminars.net.nz
2	07/04/10	Social Media Marketing... Auckland and Christchurch in August 2010	info@businessseminars.net.nz
3	18/05/10	Social Media Marketing... Auckland and Christchurch in August 2010	info@businessseminars.net.nz
4	30/05/10	[Recipient's Name] everything you need to know to be A Social Media Marketing Expert	info@businessseminars.net.nz
5	06/06/10	Someone is waiting for your call - don't be a Cold Calling Scaredy Cat	info@businessseminars.net.nz
6	06/06/10	Social Media Marketing... Auckland and Christchurch in August 2010	info@businessseminars.net.nz
7	09/06/10	Share the best new customer acquistion techniques with a master Auck ChCH Aug 2010	info@businessseminars.net.nz
8	13/06/10	Add POWER to your selling with PowerSell August 2010	info@businessseminars.net.nz
9	16/06/10	PowerSell Seminars in Auckland and Chirstchurh Aug 2010	info@businessseminars.net.nz
10	20/06/10	All you need to know about Social Media Marketing Auck CHCH Aug 2010	info@businessseminars.net.nz
11	04/07/10	NegotiationPOWER seminar highlights skills to do better business	info@businessseminars.net.nz
12	05/07/10	Become more effective - learn the magic of TimeSHIFTING	info@businessseminars.net.nz
13	20/07/10	Everything You Need to Know About Social Media Marketing Aug 24Auck Aug 26 Chch	info@businessseminars.net.nz
14	27/07/10	Cold Calling For Scaredy Cats - Build your business with NEW clients	info@businessseminars.net.nz
15	09/09/10	NegotiationPOWER - Six Deadly Sins of Negotiation Seminar Sept 2010	info@businessseminars.net.nz
16	12/09/10	TimeShifting getting more out of your busy day - Christchurch - Auckland Seminar Seminar Series Sept	info@businessseminars.net.nz

He also prepared a much larger schedule showing the times and dates the messages received, the complainant's name, who the message was sent to, and who the message was sent by.

[13] Mr Grasso contacted a number of the complainants to obtain further information from them. He obtained witness statements from them, copies of which have been made available to the Court. In each case, the complainant indicated that he or she had received an email message or messages from "Business Seminars NZ", but had not consented to receiving the email(s).

[14] Each email purported to come from an entity described as "Business Seminars NZ". Contact details were given. It transpired that the contact details were similar to the contact details for Mr Mansfield. Further, a company by the name of Business Seminars NZ Limited had previously been incorporated in New Zealand. Mr Mansfield had been the sole director of and shareholder in Business Seminars NZ Limited. The company has been struck off the Companies Register since 23 February 2010.

[15] An investigator with the Department made contact by email with "Business Seminars NZ" on 29 July 2010. He asked the recipient of the email to contact him to discuss the complaints that had been received. Mr Mansfield responded by email on the same day. He indicated that he was confident that "we are complying with the legislation's intent, and within the spirit of the rules it imposes on direct marketeers". He explained that Business Seminars NZ had been doing business since 2004, and that it emailed its "databases" nearly every month. He advised that prior to the implementation of the Act, Business Seminars NZ operated in New Zealand as a joint venture with a New Zealand partner, and that "part of the way of building the list was to source relevant business directories and have the marketing details data entered by business listings of Manila".

[16] The Department in reply posed various questions to Mr Mansfield. He again responded promptly. He attached the databases of email addresses he had sent emails to, and he indicated that there were 66,809 email addresses in the databases. This was down from the number which had been in the database at the beginning of March 2010. The number in the database as at that date was 80,705 email addresses. Mr Mansfield also provided confirmation of the number of email addresses to which emails were sent in some of the campaigns, including 10,748 addresses on 18 May 2010, 10,411 addresses on 30 May 2010, 10,922 addresses on 21 July 2010, 9,333

addresses on 27 July 2010, 10,608 addresses also on 27 July 2010, and 9,315 addresses on 3 August 2010.

[17] Mr Mansfield spoke to Departmental investigators. Inter alia, he was seeking an assurance that the Department would not seek "to sabotage" his seminars.

[18] Mr Leach, a Departmental investigator, sent further questions to Mr Mansfield on 5 August 2010, and again, Mr Mansfield responded promptly. Further, Departmental investigators attended a seminar run by Mr Mansfield on 24 August 2010.

[19] The Department examined the form and content of various of the messages. It considered that they were commercial in nature, because they were marketing and promoting a series of business seminars which were intended to be facilitated and conducted at various locations in New Zealand by Mr Mansfield. Recipients of the emails could book for and pay to attend one of the advertised seminars by replying to the commercial electronic message.

[20] The emails examined by the Department had a number of common features:

(a) they were sent from "information@businessseminars.net.nz";

(b) they came from two different IP addresses. (An IP address identifies a particular computer that is using the internet);

(c) the sender's domain name was "businessseminars.net.nz";

(d) the two IP addresses both led to the website, www.businessseminars.net.nz.

[21] The website www.businessseminars.net.nz is registered. The registration details disclose the address — 20/40 Lord Street, Perth, Australia. The registrant's name is recorded as being "Joseph John". The Department emailed Joseph John care of the email address given in the registration details, and it received a reply from Mr Mansfield.

[22] On 23 August 2010, Mr Mansfield was interviewed by a Departmental investigator, a Mr Demetriou. In the course of that meeting, Mr Mansfield explained his business model and how it related to the sending of commercial electronic messages marketing and promoting his goods and services in this country. He provided an overview of the seminars that he had been and was then conducting in New Zealand.

[23] In September 2010, the Department received complaints regarding unsolicited commercial electronic messages. The Department investigated the complaints, and spoke to a Mr Richard Gee. He had worked with Mr Mansfield up until 2009, and he advised that he had been supplied a database by Mr Mansfield. Subsequently, the Department interviewed him in relation to his business relationship with Mr Mansfield, and his knowledge of Business Seminars NZ. The interview was conducted on 22 March 2012. Subsequently, the Department put further questions to Mr Gee, which he answered in writing.

[24] The Department formed the view that Mr Mansfield had breached s 9(1) of the Act. A statement of claim was filed in this Court on 11 April 2012. Inter alia, it recited the relevant facts as they were understood by the Department, and alleged that Mr Mansfield had breached s 9 of the Act. A claim was made for the imposition of a pecuniary penalty pursuant to s 45.

[25] The Court documents were served on Mr Mansfield's solicitors, Elek-Roser Legal, in Perth in Western Australia on 11 May 2012.

Does the Court have jurisdiction to make the orders sought?

(i) Does the Court have jurisdiction over Mr Mansfield, notwithstanding that it appears that he is an Australian citizen resident in that country?

[26] The Department asserts that Mr Mansfield has breached s 9(1) of the Act. It reads as follows:

> **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.

…

[27] An electronic message has a New Zealand link in various situations, including when the message originates in New Zealand, or when the person who sent the message is either an individual who is physically present in New Zealand when the message is sent, or an organisation whose central management and control is in New Zealand. The purview of s 9 is wider than this, however, because a message has a New Zealand link, if the recipient is an individual who is physically present in New Zealand, or if the message is sent to an electronic address that ends with ".nz", or begins with an international access code directly followed by "64".[12] In such cases, it is not necessary that the message originates in New Zealand or that the sender is present in this country.

[28] Section 8 expressly extends the Act's operation to conduct engaged in outside New Zealand, where the conduct is the conduct of a New Zealand resident or a company carrying on business in New Zealand. It provides as follows:

> **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.

The section extends the purview of the Act to the conduct of a New Zealand resident where the conduct is engaged in outside New Zealand. To this extent, it gives the Act extraterritorial reach. However, in its terms, s 8 does not apply to conduct that occurs in New Zealand.

[29] Here, the Department submits that the sending of an unsolicited commercial electronic message into New Zealand from another jurisdiction is conduct which occurs in New Zealand. In the present case, it notes that the emails were intended to

---

[12] Unsolicited Electronic Messages Act 2007, s 4(2).

be received in New Zealand, and that they were directed to persons in this country. The emails invited people to seminars intended to be held in New Zealand and invited people to book for and pay in advance in New Zealand currency to attend the seminars. The emails purported to come from an entity with a New Zealand connection — Business Seminars NZ. Contact details in this country were given.

[30] The Department points to the number of decisions in support of its argument.

[31] First, it refers to a decision of the Federal Court of Australia, *Bray v F Hoffman – La Roche Ltd*,[13] which dealt with a jurisdictional challenge by companies alleged to be involved in a global vitamin cartel. Merkel J found that the defendants did not carry on business in Australia, but that the Court nevertheless had jurisdiction, in part on the basis that the defendants' communications into Australia were acts which occurred in that country. He noted as follows:[14]

> In the present case the facsimile, email, letter, telephonic, telex, or other communications from overseas parents to officers of the Australian subsidiaries, although they were likely, for the most part, to have been initiated outside of Australia, were directed to and were expected to be, and were, received in Australia. In my view, such conduct can, for the purposes of s 45 of the [Trade Practises Act 1974], be regarded as taking place in Australia.

[32] Secondly, it refers to a decision of the Court of Appeal in this country — *Commerce Commission v Visy Board Pty Limited*.[15] Here, the Commission sought to set aside protests to jurisdiction in a civil pecuniary remedy claim made under the Commerce Act 1986. The respondent and three of its senior executives, including a Mr Carroll, had admitted in proceedings brought in the Federal Court of Australia by the Australian Competition and Consumer Commission, participation in cartel conduct. Declarations had been granted by the Federal Court, and pecuniary penalties totalling some $36 million had been imposed. The question before the Court of Appeal was whether the cartel contact extended to the relevant market in New Zealand. The Commission was alleging that the respondent and Mr Carroll, amongst others, had contravened the provisions of the Commerce Act. The proceedings had been served on the respondent and Mr Carroll in Australia, and

---

13 *Bray v F Hoffman – La Roche Limited* [2002] FCA 243, (2002) 118 FCR 1.
14 At [147].
15 *Commerce Commission v Visy Board Pty Ltd* [2012] NZCA 383.

protests to the jurisdiction of the New Zealand Courts had followed. Various emails had been sent by the respondent and Mr Carroll to the respondent's New Zealand subsidiary. The Court of Appeal referred to *Bray* and noted as follows:[16]

> [56] We agree with counsel for Mr Carroll, Mr Mills QC, who accepted that email or telephonic communications (even where they were initiated outside New Zealand) to Visy Board NZ representatives in New Zealand were properly to be regarded as acts taking place in New Zealand. Communications initiated by Mr Lloyd or Mr Carroll in Australia but directed to Visy Board NZ executives (or customers) in New Zealand are received in this country. They are thus characterised as acts done or conduct occurring in New Zealand for jurisdictional purposes.

[33] The Department also refers to a further decision of the Court of Appeal — *Wing Hun Printing Co Limited v Saito Offshore Pty Ltd*.[17] In this case, the plaintiff was alleging that the defendant, an overseas company, had made a misrepresentation to it by email. The Court found that the extraterritoriality provisions in the Fair Trading Act 1986 did not apply, but that the act of sending an email into New Zealand was conduct which occurred in New Zealand. The Court noted as follows:

> [103] Although not raised by the appellants, there is an initial question as to whether the Fair Trading Act applies to the appellants, none of whom are resident or carry on business in New Zealand…
>
> [104] However, the Fair Trading Act does apply to foreign parties to the extent their misleading conduct occurs in New Zealand. Saito must therefore establish a good arguable case that any such conduct occurred in New Zealand. If it did, then the Act would apply to the appellants and the threshold question under r 6.27(2)(j)(i) would also be established.
>
> [105] In the majority judgment delivered by Tipping J in *Poynter,* the judgment of Merkel J in *Bray v F Hoffman-La Roche Ltd* was discussed. A "crucial point of distinction" from *Poynter* was that, in *Bray*, Merkel J was able to find that communications into Australia from overseas by the parent companies of Australian based subsidiaries were sufficient to support a finding that the parent companies had engaged in relevant conduct in Australia for the purposes of the Trade Practices Act 1974 (Cth).
>
> [106] We agree with the Judge that Saito established a good arguable case that this cause of action falls within r 6.27(2)(j) (claims under an enactment) on the basis that an act or omission to which the claim relates was done or occurred in New Zealand. The representation alleged was communicated by emails sent to and received by a New Zealand resident in New Zealand by Mr Kurdin with Mr Lau's knowledge. The representation related directly to

---

16 See also [84], [136], and [137].

17 *Wing Hun Printing Co Limited v Saito Offshore Pty Ltd* [2010] NZCA 502, [2011] 1 NZLR 754.

> the supply of services in New Zealand to a New Zealand-based company. The representation alleged was acted on in New Zealand when Saito agreed to terminate the existing licence and gave up its rights to the existing IT system. This is said to result in loss or damage occurring in New Zealand. (footnotes omitted)

[34] Finally, the Department drew my attention to a decision of the Supreme Court — *R v Walsh*.[18] In this case, the Supreme Court was considering whether acts occurred in New Zealand for the purposes of s 7 of the Crimes Act 1961. The defendant had defrauded people by forging documents, which he had faxed to victims in New Zealand. The Supreme Court found that the faxing of the documents to this country was "uttering" in New Zealand. It held as follows:

> [26] In our opinion, what Mrs Walsh did in reproducing in New Zealand what she represented was a genuine document must be regarded as uttering a forgery in New Zealand. Her intent was to lead the victims to act upon the forged letters as if they were genuine. In causing them to act on the copies she was causing them to act on the underlying forgeries. The actus reus under s 266(1)(b) therefore occurred in New Zealand. Any other view would overlook the realities of modern communication technologies, which enable the simultaneous reproduction of spurious documents, on an immense scale, to any part of the world from any part of the world. The mischief is done, intentionally, where the receiver acts upon the reproduction believing it to replicate the terms or qualities of a genuine document.

[35] In my judgment, it is clear from these authorities, that the sending of an email to a recipient in this country can breach s 9(1), whether or not the sender of the email is resident in New Zealand. As a result, s 8 of the Act has no application. The sending of an unsolicited commercial electronic email into New Zealand is an act or conduct that occurs in New Zealand, and the Court has jurisdiction to deal with the matter.

(ii) Can a civil pecuniary penalty be imposed by way of a formal proof hearing?

[36] The Department is seeking judgment by way of formal proof under r 15.9. It has filed affidavit evidence from a senior investigator, Mr Demetriou, from Mr Grasso and from a service agent in Australia.

[37] Pecuniary penalties are provided for by s 45.

---

[18] *R v Walsh* [2006] NZSC 111, [2007] 2 NZLR 109 . See also *Omni Marketing Group, Asia Pte Ltd v Transactor Technologies Ltd* [2008] 3 NZLR 252 (HC) at [29].

[38] Section 49 provides as follows:

> **49 Applicable rules, procedure, and standard of proof**
>
> The proceedings under sections 45 and 46 are civil proceedings to which the usual rules of the court, rules of evidence, and procedure for civil proceedings apply (including the standard of proof).

The "usual rules of court" can only be the High Court Rules. They govern the disposition of civil proceedings. It follows that r 15.9 is potentially applicable.

[39] Mr Hamlin, appearing for the Department, advised that he had not found any case where a civil pecuniary penalty had been imposed by way of formal proof in New Zealand. Nor could I or my research clerk find any authority in this country.

[40] It is, however, clear that such penalties have been imposed using similar default judgment provisions in Australia.[19]

[41] I can see no reason either in principle or as a matter of law, why pecuniary penalties under s 45, and compensation and damages for a civil liability event under s 46, cannot be sought by way of a formal proof hearing pursuant to r 15.9. Indeed, in my view, s 49 compels the conclusion that the formal proof procedure is available in those cases where a defendant has taken no steps.

(iii) Was the proceeding appropriately served on Mr Mansfield?

[42] The Department has filed an affidavit of service. It records that the documents were served on Mr Mansfield through his solicitor, Elek-Roser Legal, in Perth, Western Australia. The documents were served on Elek-Roser Legal following an email sent by Mr Mansfield to the Department on 7 May 2012. The letter confirmed that Mr Mansfield had spoken to his legal representative, Mr Elek-Roser, and that Mr Elek-Roser was to accept service on his behalf. The process server who served the documents served them on an employee of Elek-Roser Legal, and she confirmed that she was authorised to accept the documents.

---

[19] *Australian Competition and Consumer Commission v Yellow Page Marketing BV (No 2)* [2011] FCA 352 – a pecuniary penalty under the Trade Practices Act 1974 (Cth). A pecuniary penalty was imposed under the Spam Act 2003 by a default judgment in *Australian Communications & Media Authority v Mobilegate Ltd, A company incorporated in Hong Kong (No 4)* [2009] FCA 1225, (2009) 180 FCR 467.

[43] The Department submits that it was entitled to serve Mr Mansfield in Australia, without leave, by virtue of r 6.27(2)(j). Relevantly, that rule provides as follows:

> **6.27 When allowed without leave**
>
> (1) This rule applies to a document that initiates a civil proceeding, or is a notice issued under subpart 4 of Part 4 (third, fourth and subsequent parties), which under these rules is required to be served but cannot be served in New Zealand under these rules (an **originating document**).
>
> (2) An originating document may be served out of New Zealand without leave in the following cases:
>
> …
>
> (j) when the claim arises under an enactment and either—
>
> (i) any act or omission to which the claim relates was done or occurred in New Zealand; or
>
> …

[44] As already noted, an electronic communication sent to a recipient in New Zealand is an act that is done or occurs in New Zealand. Rule 6.27(2)(j) applies. Moreover, there is nothing to suggest that service on Mr Mansfield care of his solicitor was contrary to the relevant laws in Australia. Rather, the rules of both the Australian Federal Court and the Western Australian Supreme Court provide for service through a defendant's counsel by agreement.[20] Mr Mansfield requested that his solicitor be served and the documents were served on his solicitor on 11 May 2012. The timeframe to file a defence expired 30 working days thereafter. Mr Mansfield has had ample time to respond. He has taken no steps in the proceeding.

[45] I am satisfied that service has been attended to appropriately, and that the Department was entitled to serve Mr Mansfield without leave, and through his solicitor.

---

[20] Federal Court Rules (Cth), r 10.22; Rules of the Supreme Court (WA) Order 9, r 1(2).

Did Mr Mansfield breach s 9(1) of the Act?

[46] Section 9(1) has been set out above at [26]. In considering whether the section has been breached, the appropriate standard of proof to apply is the civil standard — namely, the balance of probabilities.[21]

[47] Section 9 prohibits "unsolicited commercial electronic messages". These words are defined separately.

[48] An electronic message is a message sent using a telecommunications service, to an electronic address.[22] The Court can take judicial notice of the fact that an email is sent using a telecommunications service, and that it is sent to an electronic address. It is not a voice call made using a standard telephone service, or a voice over internet protocol.[23] Whether the electronic address exists, or the message reached its intended destination, is immaterial.[24] I have no hesitation in concluding that the emails sent into New Zealand were electronic messages.

[49] Further, it is clear from the evidence that the electronic messages sent in this case were commercial electronic messages, as that term is described in s 6(a)(i) of the Act. They marketed or promoted seminars to be held by Business Seminars NZ. Some of the emails specifically referred to Mr Mansfield by name. Others referred to other persons who were to speak at the seminars.

[50] An "unsolicited" commercial electronic message is defined as meaning a commercial electronic message that the recipient has not "consented to receiving",[25] and these words in turn are separately defined. I deal with this issue below at [54] to [59].

[51] Section 9(1) also requires that any electronic message has a New Zealand link. Here, it is clear from the affidavits filed that the electronic messages had a New Zealand link, as defined in s 4 of the Act. They were sent to electronic

---

21 Section 49.
22 Section 5(1).
23 Clause 1, Schedule to the Act.
24 Section 5(3).
25 Section 4(1).

addresses that ended with ".nz" — s 4(2)(f)(i). Moreover, it is likely that the messages were received on computers in New Zealand, by persons who were in New Zealand when the messages were accessed — s 4(2)(c) and (d).

[52] The evidence also establishes on the balance of probabilities that Mr Mansfield sent the electronic messages in issue. I note the following:

(a) When the Department attempted to contact the sender of the electronic messages, using details obtained from them, it received an email back purporting to be from Mr Mansfield;

(b) In resulting email correspondence received from Mr Mansfield, he accepted responsibility for sending the electronic messages, albeit using the term "we" rather than "I" to describe his operations;

(c) Mr Mansfield also acknowledged responsibility for the electronic messages when he met with Department investigators on 23 August 2010;

(d) The electronic messages purported to be from the entity Business Seminars NZ. A company under that name had been incorporated in 2006. As noted, it was struck off the Register of Companies on 23 February 2010. Mr Mansfield was the sole director and shareholder of that company;

(e) The Department interviewed Mr Richard Gee, who had worked with Mr Mansfield. In the course of his interview, Mr Gee stated that Mr Mansfield did the technical work, including the sending out of the electronic messages. When asked in a follow up email to clarify who sent the messages, Mr Gee confirmed that it was Mr Mansfield. While this evidence is unsworn, it is consistent with the other evidence I have noted;

(f) The website "businessseminars.net.nz" and an associated website, "businessseminars.co.nz", seem likely to have been registered by Mr Mansfield under the pseudonym Joseph Jones. As noted, when the Department sent an email to Mr Jones, it received a reply from Mr Mansfield.

[53] I conclude, on the balance of probabilities, that the electronic messages were either sent by Mr Mansfield, or that he was directly or indirectly, knowingly concerned in, or a party to, the sending of the electronic messages. Subject only to the issue of consent by the recipients, the Department has proved to the requisite standard that Mr Mansfield breached s 9(1).

Were the electronic messages unsolicited?

[54] In his email reply on 29 July 2010, Mr Mansfield asserted that the electronic messages had been sent in accordance with the Act. He indicated his belief that the recipients had consented to receiving the messages. He referred to the definition of the words "consented to receiving" in s 4(1) of the Act.

[55] A person who contends that a recipient consented to receiving a commercial electronic message has the onus of proof in relation to that matter.[26] Notwithstanding that there has been no evidence put forward by Mr Mansfield to justify his assertion, the Department out of caution responded to his claim.

[56] The words "consented to receiving" are defined in s 4 of the Act. Broadly, a person consents to receiving emails if there is express consent, or consent that can reasonably be inferred. Consent can also be deemed to have been given when, inter alia, an electronic address has been conspicuously published by a person in a business or official capacity, 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 the message sent to that address is relevant to the business role, functions or duties of the person in a business or official capacity.

---

[26] Section 9(3).

[57] Again, I am satisfied, on the balance of probabilities, that the recipients did not consent to receipt of the electronic messages and cannot be deemed to have consented. I note the following:

(a) A number of the complainants to the Department expressly stated that they did not have any business relationship with Mr Mansfield or Business Seminars NZ, and that they did not subscribe to receive the electronic messages;

(b) Some of the complainants went further, and stated that the email address to which the messages were sent was used for domain name registration only, and for no other purpose;

(c) One complainant noted that she had continued to receive the emails, even after sending an "unsubscribe" message.

(d) While Mr Mansfield initially claimed in discussions with the Department that he had not purchased any databases of email addresses, in a later discussion, he accepted that he had purchased email addresses from a third party, a firm called Image Marketing Group. In such circumstances, express, inferred or deemed consent to the receipt of emails from Mr Mansfield or Business Seminars NZ is inherently unlikely.

(e) Mr Mansfield at one stage told the Department that he became aware that his electronic messages were being blocked by various internet service providers (presumably as spam), and that he changed his IP address to try and circumvent this restriction. Again, this indicates that the consent of the recipients had not been obtained.

(f) The Department's analysis of the email lists provided by Mr Mansfield also supports the inference that the email addresses were inherently unlikely to belong to consenting recipients. The Department sampled 19,239 addresses and found 7.6 percent of the

> addresses belonged to not for profit organisations, 4.1 percent were technical addresses used for website administration, and 2.3 percent of the addresses were for organisations that were inherently unlikely to use social media for commercial purposes, such as military email addresses, or addresses including terms such as "community" and "trust".

[58] The evidence negates any claim of express or inferred consent. It also negates any claim that the electronic addresses were conspicuously published and that the emails sent were relevant to the business role, functions or duties of the addressee in a business or official capacity, as required by the deemed consent provisions.

[59] Once again, on the balance of probabilities, I am satisfied that the recipients did not consent to receiving the commercial electronic messages sent by or on behalf of Mr Mansfield, and that the messages were unsolicited.

Pecuniary Penalty

[60] Relevantly, s 45 provides as follows:

> **45 Pecuniary penalties for civil liability event**
>
> (1) On the application of the enforcement department, the 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) and (4), the pecuniary penalty that the 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 commercial electronic messages sent:
>
> (b) the number of electronic addresses to which a commercial electronic message was sent:
>
> (c) whether or not the perpetrator has committed prior civil liability events.
>
> …

[61] The words "civil liability event" are defined in s 18. Inter alia, a civil liability event includes a breach of s 9(1). It also includes a breach of s 15, which deals with third party breaches of the Act.

[62] Section 45 is drawn from s 24 of the Spam Act 2003 (Cth). There are, however, significant differences. First, the maximum penalty in Australia for an individual is $500,000 and $10 million for a body corporate. Secondly, in considering the imposition of a pecuniary penalty in Australia, the courts are expressly empowered to look at breaches committed by a perpetrator in foreign countries.

[63] In imposing civil pecuniary penalties, the courts in Australia have applied principles developed under the Trade Practices Act 1974 (Cth).[27] That Act is the counterpart to the Commerce Act in this country, and there is now a substantial body of jurisprudence relating to the imposition of civil pecuniary penalties under the Commerce Act. In my judgment, that approach adopted in Australia is also appropriate in this country.

[64] Further, it is appropriate to adopt a modified version of the three-step approach to sentencing in the criminal context discussed by the Court of Appeal in cases such as *R v Taueki*.[28] This methodology has been adopted in the Commerce Act context.[29] In broad terms, the courts should arrive at a starting point pecuniary penalty by considering the breach and any aggravating and mitigating factors attaching to it. It should then consider factors personal to the perpetrator, to determine whether a pecuniary penalty higher or lower than the starting point is required. Finally, it should deduct from the starting point penalty any allowance for an admission of liability and/or cooperation offered by a defendant in relation to others who are suspected of having breached the Act.

[65] The analogy with sentencing cases in the criminal context can only be taken so far. The overriding objective of a civil pecuniary penalty is deterrence, including

---

27 See for example *Australian Communications & Media Authority v Mobilegate Ltd, A company incorporated in Hong Kong (No 4)*, above n 18, at [27]–[28].

28 *R v Taueki* [2005] 3 NZLR 372 (CA); *R v Clifford* [2011] NZCA 360, [2012] 1 NZLR 23 at [60].

29 *Commerce Commission v Alstom Holdings SA* [2009] NZCCLR 22 (HC) at [14].

the deterrence of others who might seek to breach the Act for financial gain.[30] Deterrence in achieved by imposing pecuniary penalties that remove the financial gain that was obtained by, or could reasonably have been obtained, from the breach of the Act.[31]

[66] I have endeavoured to apply these various principles in fixing the pecuniary penalty in this case.

[67] As required by s 45(2)(a), I have considered the number of unsolicited commercial electronic messages sent by Mr Mansfield. It is however difficult to be precise as to how many unsolicited electronic messages were sent. There were at least 15 marketing campaigns, perhaps more. Mr Grasso has prepared a schedule indicating, insofar as the Department is aware, the database lists used for each campaign, and the number of likely recipients. That schedule reads as follows:

Date	Email list	Recipients
7 April	4	Up to 18,922
18 May	1, 2, 3, 4	Between 10,748 and 47,229
30 May	1, 2, 3, 4	Between 10,748 and 47,229
June 6	Unknown	Up to 80,705
June 9	Unknown	Up to 80,705
June 13	Unknown	Up to 80,705
June 16	Unknown	Up to 80,705
June 20	Unknown	Up to 80,705
July 4	Unknown	Up to 80,705
July 5	Unknown	Up to 80,705
21 July	5	Up to 19,493
27 July	2, 5	Up to 28,826
3 August	1, 2	Up to 9,315
9 September	Unknown	Up to 80,705
12 September	Unknown	Up to 80,705

It seems probable that the number of electronic messages sent were in the hundreds of thousands. It could have been close to a million.

---

30 *Commerce Commission v Alstom Holdings SA* above n 29; *Australian Communications & Media Authority v Atkinson* [2009] FCA 1565 at [49].

31 *Australian Communications & Media Authority v Mobilegate Ltd, A company incorporated in Hong Kong (No 4)*, above n 18, at [31]–[35].

[68] It is also clear that a number of the electronic messages were sent to the same recipient. For example, the email addresses on list 4 were the subject of the marketing campaigns conducted on 7 April, 18 May and 30 May. The total number of addresses on the five databases was somewhere between 66,722 and 80,705. It is likely that most of the electronic addresses received more than one electronic message from Mr Mansfield.

[69] Mr Mansfield has not committed a prior civil liability event, as those words are defined, in this country. While a pecuniary penalty has been imposed against him in Australia for sending spam, I do not take that into consideration in fixing the starting point for the appropriate pecuniary penalty.

[70] There are other matters which I consider should also be taken into account in the present case because they are aggravating features of the offending:

(a) First, there is the gain derived by Mr Mansfield from breaching the Act. Mr Grasso notes the number of people who attended the business seminars convened by Mr Mansfield at the Langham Hotel in Auckland. The cost per seat for those seminars, according to the website, was $199 (NZ). The email suggests that Mr Mansfield ran four seminars per day. Some seminars were held at various locations elsewhere in New Zealand. The potential gross profit from holding the seminars was not insignificant. There is, however, nothing from which I can accurately quantify the financial gain resulting to Mr Mansfield. Nor is there anything to suggest that anybody suffered any loss or damage as a result of Mr Mansfield's breach of the Act.

(b) Secondly, Mr Mansfield's conduct was clearly either deliberate, or reckless. It is clear from his discussions with the Department that he was aware of the Act, and the prohibitions contained in it. He, in effect, was "chancing his arm". There is nothing to suggest that there were any steps taken by Mr Mansfield to try and ensure compliance with the Act.

[71] I have looked at the two authorities in this country where pecuniary penalties have been imposed for breach of the Act. In both cases, the appropriate pecuniary penalty was agreed. In one case, a defendant admitted being knowingly concerned in the sending of approximately 2 million spam email messages between 5 September and 31 December 2007. The Court considered that the breach warranted a starting point at the top end of the available range, but accepted that a substantial discount was required to reflect the defendant's cooperation, and the fact that the conduct began when it was not unlawful. A penalty of $100,000 was imposed.[32] In a follow up case, a defendant who agreed to provide assistance to the Department in relation to its investigation was also subjected to a pecuniary penalty of $100,000, and another defendant, who had a substantially reduced involvement, was subjected to the imposition of a $50,000 pecuniary penalty.[33]

[72] Pecuniary penalties imposed in Australia do not assist markedly, given the very different penalties available in that country.[34]

[73] In my judgment, the appropriate starting point for the imposition of a pecuniary penalty in the present case, given the matters detailed in s 45(2) and the additional matters noted above, is $100,000.

[74] There are no aggravating features personal to Mr Mansfield which require a higher pecuniary penalty. There is, however, a mitigating feature. Mr Mansfield did cooperate with the Department, at least initially, and he provided the Department

---

32 *Chief Executive of the Department of Internal Affairs v Atkinson* HC Christchurch CIV 2008-409-2391, 19 December 2008.

33 *Chief Executive of the Department of Internal Affairs v Atkinson* HC Christchurch CIV 2008-409-2391, 27 October 2009.

34 *Australian Communications & Media Authority v Clarity1e Pty (No 2)* [2006] FCA 1399, (2006) 155 FCR 377 – 70 million spam emails to approximately 5 million recipients – penalty of $4.5 million on the corporate perpetrator, and $1 million on the individual defendant (Mr Mansfield); *Australian Communications & Media Authority v Mobilegate Ltd, A company incorporated in Hong Kong (No 4)*, above n 18, and *Australian Communications & Media Authority v Mobilegate Ltd, A company incorporated in Hong Kong (No 6)* [2009] FCA 1533 – penalty of $5 million on one company, $3.5 million on another, $3 million each on two individuals, $1.25 million on another individual, $4.5 million on another company involved, and $2.5 million on another individual; *Australian Communications & Media Authority v Mobilegate Ltd, A company incorporated in Hong Kong (No 9)* [2010] FCA 1383 – $2 million to individual found liable as an accessory; *Australian Communications & Media Authority v Atkinson* [2009] FCA 1565 – 140,000 spam emails – penalty agreed, $210,000 (A) on individual. All currencies are in AUD.

voluntarily with the information sought by it. However, the cooperation did not last throughout the inquiry.

[75] I also note that Mr Mansfield did not try and defend these proceedings. He did not however file an admission, nor cooperate with the Department to prepare an agreed statement of facts. Nor did he offer an enforceable undertaking not to breach the Act in the future, notwithstanding that the Department was also seeking an injunction against him. That course would have been open to him under s 34.

[76] In my view, it is appropriate to allow Mr Mansfield a reduction in the pecuniary penalty which might otherwise be appropriate. I allow a reduction of $5,000 to recognise the not unhelpful, but ultimately limited, cooperation given to the Department.

[77] It follows, that in my view, the appropriate penalty in this case is one of $95,000, and I impose a civil pecuniary penalty in that sum. It is to be paid to the Crown.

Costs

[78] As noted, these proceedings are civil proceedings. It follows that the Department is entitled to its reasonable costs and disbursements determined by reference to the applicable High Court Rules. In this regard, it seeks costs of $8,460, being scale costs on a 2B basis for the various steps taken by it, and disbursements of $3,071.54, comprising filing fees, and the hearing fee payable in respect of the formal proof hearing.

[79] It is appropriate to allow both the costs claimed and the disbursements.

Conclusion

[80] For the reasons outlined in this judgment, I impose a pecuniary penalty of $95,000. That penalty is payable to the Crown. I also award costs against Mr Mansfield of $8,460, and disbursements of $1,806.54. The costs and the disbursements are payable to the Department.

[81] Finally, I acknowledge the comprehensive and helpful submissions made by Mr Hamlin on behalf of the Department. I am grateful to him for his thorough approach to this matter.

_____

Wylie J