Singapore Journal of Legal Studies
[2007] 361–379

THE *SPAM CONTROL ACT 2007*[1]

KARTHIK ASHWIN **THIAGARAJAN***

I. INTRODUCTION

In 2003 the Info-communications Development Authority ("IDA") commissioned a survey ("the IDA Survey") to understand the "nature and extent" of unsolicited e-mail in Singapore.[2] It was estimated that 94% of e-mail users in Singapore had received unsolicited e-mail, which cost the economy $23 million in productivity losses every year.[3] These numbers were reason enough for the Singapore government to step in and provide a legislative tool to tackle the problem of unsolicited communication.[4] This legislative tool is the *Spam Control Act 2007* which marks the culmination of a process that has spanned more than four years. While acknowledging that legislation alone is not the panacea for the ills of unsolicited communication,[5] Parliament

---

* B.A., LL.B. (Hons.) (National Law School of India University); Former Law Clerk to Justice Ruma Pal, Supreme Court of India; Advocate, India; International Lawyer, Drew & Napier LLC. The views expressed by the author are those of the author alone. The author is grateful to Anirudh Wadhwa, Foo Yuet Min and Ling Vey Hong for comments on earlier drafts of this note. Responsibility for any errors remains solely with the author.

1 No. 21 of 2007 [the Act]. The Act came into force on 15 June 2007.

2 Info-communications Development Authority of Singapore, "2003 Survey on Unsolicited E-mails" (25 May 2004), online: IDA Singapore <http://www.ida.gov.sg>. Note that the IDA Survey considered spam as being limited to only electronic mail. It did not specifically consider unsolicited *commercial* e-mail (which is the focus of the Act) or other means of communication which have been included in the Act, such as mobile telephony.

3 *Ibid*.

4 The term "unsolicited communication" has been used loosely, and is not a defined term for the purposes of this note. There exist a number of differences in the scope of unsolicited communications across jurisdictions. Where required, terms that have been defined in legislation have been specifically employed.

5 See *e.g*. Tom Zeller, Jr., "Law Barring Junk E-Mail Allows a Flood Instead" *The New York Times* (1 February 2005), online: The New York Times <http://www.nytimes.com>. See also Meyer Potashman, "International Spam Regulation & Enforcement: Recommendations Following the World Summit on the Information Society" [2006] 29 B.C. Int'l & Comp. L. Rev. 323 at 333 (noting that while many prosecutions were launched soon after the coming into force of the legislation, the quantum of spam has not decreased significantly).

considers the Act to be one aspect of a multi-pronged approach which also includes public education, industry self-regulation and international cooperation.[6]

In its long journey from the IDA Survey to its final form, the scope of the legislative response has been widened to encompass mobile telephony, which is a popular and a far more invasive communication medium.[7] While the Act makes a genuine attempt to address the problem at hand, there remain a number of deficient and uncertain features—some fundamental and others that only call for some fine-tuning. An analysis of the provisions of the Act forms the central purpose of this note. The first segment provides an overview of this new piece of legislation and sketches its scope. The second segment attends to conceptual issues which need to be re-evaluated and addresses certain other shortcomings of the Act. Plausible solutions and alternatives have been proposed to tackle these issues and deficiencies. While this note does not seek to revisit the policy objectives of the framers of the Act, it attempts to gauge the precision with which the provisions of the Act reflect the stated policy objectives.[8]

II. Basic Framework of the Act

The Act has its roots in similar legislation in other jurisdictions. Substantial portions of the Act are modelled on the lines of the Australian *Spam Act*[9] and the *Controlling the Assault of Non-Solicited Pornography and Marketing Act*[10] of the United States.[11] As a result, interpretations given to the parent provisions in these jurisdictions may be useful guides in cases where any provision of the Act lacks clarity.

The Act, as the name itself suggests, deals with "unsolicited communication." This is commonly viewed as an inconvenience to users and a burden on the communication infrastructure and resources. On the flip side, it could be a very useful tool for businesses to reach out to existing and potential customers. This argument is further strengthened in the case of digital communications, where the marginal cost of sending electronic messages is close to zero, allowing even small enterprises (without copious ad-spends) to access a large number of people. Recognising these benefits, the thrust of the Act is *regulation* and not *prohibition* of unsolicited communication.[12]

Further, a choice had to be made between two approaches to spam control—the "opt-out" approach and the "opt-in" approach. There is considerable debate between

---

6 Infocomm Development Authority of Singapore *et al.*, "Multi-Pronged Measures Developed to Curb E-Mail Spam in Singapore" (25 May 2004), online: IDA Singapore <http://www.ida.gov.sg>.

7 During the same time the volume of spam rose rampantly. From a miniscule 5% in 2001, spam is now estimated to be around 90% of all Internet traffic in some regions of the world. See Michael Specter, "Damn Spam: The Losing War on Junk Email", *The New Yorker* (6 August 2007), online: The New Yorker <http://www.newyorker.com>.

8 See Infocomm Development Authority of Singapore & the Attorney-General's Chambers, *Proposed Spam Control Bill (Joint IDA-AGC Consultation Paper)* (12 September 2005) at para 1.4, online: IDA Singapore <http://www.ida.gov.sg> [Second Consultation]. The first consultation paper [First Consultation] was released in May 2004. For further details of this paper, see *infra* note 46.

9 Act No. 129 of 2003 (Cth.).

10 15 U.S.C. §7701, *et. seq.* (2003) ('CAN-SPAM Act').

11 See Table of Derivatives, *Spam Control Bill*, Bill No. 6/2007, for sources from which certain provisions of the Act have been derived.

12 As may be evident from the short title and long title of the Act, its objective is to control and not prohibit spam.

these two philosophies, and any choice between the two necessarily depends upon the balance that is sought between privacy rights and business interests—a balance which is unique to each jurisdiction. The opt-out framework to spam control allows the sending of unsolicited communication, while only mandating that the recipient be provided with an option not to receive any further communication. When compared with the opt-in mechanism, this is more favourable to business interests. On the other hand, the opt-in framework, as followed in the European Union,[13] proscribes sending commercial communications without the prior consent of the recipient. This reflects a greater concern for rights of the individual, and in the context of the European Union fits in with its long-standing history of strong privacy rights.[14] The opt-out approach was adopted for the Act, as it was considered more business-friendly and better suited to the requirements of Singapore. This note avoids a potentially endless debate between the relative merits of the opt-in and opt-out mechanisms. The choice is necessarily particular to each jurisdiction, and the Act's framers in Singapore have chosen the opt-out requirement after much thought and deliberation.[15] However, one question remains. Seeking (as the fundamental premise) to walk the thin rope between business interests and the public's concerns, how far do the provisions of the Act actually achieve this balance?

A. *Regulation of Unsolicited Commercial Electronic Messages*

The Act is primarily concerned with unsolicited commercial electronic ("UCE") messages[16] sent in bulk. This may be explained by deconstructing its constituent parts. First, an *electronic message* refers to an e-mail sent to an e-mail address or a text or multimedia message sent to a mobile telephone number.[17] Next, an electronic message is considered *unsolicited* when the recipient has neither requested nor consented to the receipt of the electronic message.[18] Whether the unsolicited electronic message is *commercial* or not is to be judged having regard to the content of the message, the reference content (by way of links provided in the message, to websites and other sources) and the way in which the message is presented.[19] The message

---

13 EC, *Council Directive 2002/58 of 12 July 2002 of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector* [2002] O.J.L. 201/37 ['EC Directive on the protection of privacy in the electronic communications sector'].

14 Steven Salbu, "The European Union Data Privacy Directive and International Relations" (2002) 35 Vand. J. Transnat'l L. 655 at 666.

15 See Second Consultation, *supra* note 8 at paras 3.26-3.32.

16 "An Act to provide for the control of spam, which is unsolicited commercial communications sent in bulk by electronic mail or by text or multi-media messaging to mobile telephone numbers, and to provide for matters connected therewith." See the Preamble to the Act, *supra* note 1.

17 *Ibid*. s. 4(1), read with s. 2.

18 *Supra* note 1, s. 5. Section 5 clarifies the meaning of unsolicited by stating:
(2) For the purposes of subsection (1), a recipient shall not be treated as having requested to receive the message or consented to the receipt of the message merely because the electronic address of the recipient was given or published by or on behalf of the recipient.
(3) For the purposes of subsection (1), where a recipient of an electronic message, other than an unsolicited electronic message, submits an unsubscribe request, he shall not be treated as having requested to receive or consented to the receipt of any message sent after the expiration of 10 business days after the day on which the unsubscribe request is submitted.

19 *Ibid*. s. 3(1).

will be considered commercial where its "primary purpose" is to offer to provide or supply, or to advertise or promote certain types of subject-matter (regardless of the actual existence of the subject matter or the illegality involved in the same). Such subject-matter may include goods, services, land, interest in land, business or investment opportunity, or advertising the provider or supplier (existing or prospective) of any such subject-matter.[20] Further, drawing from the Australian *Spam Act*[21] (and the Australian *Criminal Code*[22]) section 3 also considers electronic messages the primary purpose of which is to assist or enable, "a person, by deception, to dishonestly obtain property belonging to another person"[23] or to "dishonestly obtain a gain from another person"[24] to be commercial. This extends the scope of the Act to cover fraudulent activities such as advance fee fraud and Nigerian e-mail scams where the target is made to advance small sums of money with the promise of receiving a large bounty later.[25]

The various requirements specified under the Act are only applicable to UCE messages that are "sent in bulk." Certain numerical thresholds have to be reached before an unsolicited commercial electronic message can be considered to have been sent in bulk.[26] This is to provide certainty (by specifying a bright-line test) for compliance[27] and to ensure that personal or 'one-to-one' communications remain unaffected by the Act.[28]

Section 11 of the Act stipulates that senders of UCE messages (sent in bulk) are required to comply with the requirements laid out in the Second Schedule to the Act.[29] First, all UCE messages are required to contain an e-mail address, Internet location address, telephone number, facsimile number or postal address that a recipient may use to submit an "unsubscribe request" in order to stop receiving any further UCE messages from the sender.[30] The existence of the unsubscribe facility has to be

---

20 *Ibid*.

21 *Supra* note 9, s. 6.

22 No. 12 of 1995 (Cth.), ss. 134 and 135.

23 *Supra* note 1, s. 3(1)(x).

24 *Ibid*. s. 3(1)(xii).

25 There are numerous variants of this, popular among which is the Nigerian 4-1-9 scam. For an understanding of advance fee frauds, see U.S. Department of State, Bureau of International Narcotics and Law Enforcement Affairs, "Nigerian Advanced Fee Fraud" (April 1997), online: U.S. Department of State <http://www.state.gov>.

26 *Supra* note 1, s. 6. These thresholds have been provided in section 6 which defines "sending in bulk" to mean, sending of (a) more than 100 electronic messages containing the same or similar subject-matter during a 24-hour period; (b) more than 1,000 electronic messages containing the same or similar subject-matter during a 30-day period; or (c) more than 10,000 electronic messages containing the same or similar subject-matter during a one-year period. This provision was derived from the definition of the term 'multiple' in the United States Code. See 18 U.S.C. § 1037 (2003). § 1037 is part of the Federal criminal law of the United States and deals with fraud and related activity in connection with electronic mail.

27 The converse argument is that spammers may avoid the application of the Act by sending electronic communication just a trifle less than the thresholds stipulated. See the Second Consultation, *supra* note 8.

28 *Ibid*. at para. 3.10.

29 The sender in relation to an electronic message, means the person who sends, causes the sending of or authorises the message to be sent: *supra* note 1, s. 2.

30 *Ibid*., Second Schedule, para. 2. In case the unsolicited commercial electronic message is received by recipients by electronic mail, provision of an e-mail address for sending an unsubscribe request is compulsory. For an unsolicited commercial electronic message received by recipients via text or

brought to the specific notice of the recipient in a "clear and conspicuous manner," through a statement in the English language and any other language that is used in the message.[31] The sender is prohibited from sending any UCE messages to the concerned recipient ten days after the day on which the unsubscribe request is submitted[32] and is not allowed to provide any third party with any information in the unsubscribe request.[33] Further, the Second Schedule to the Act mandates that all UCE messages need to indicate at the outset that they are commercial in nature through a fixed format label.[34]

In addition to the regulation of UCE messages, the Act prohibits the sending of any electronic message to an e-mail address or a mobile phone number that is generated either by way of a dictionary attack or obtained through address-harvesting software.[35] While a dictionary attack[36] is an automated means to generate e-mail addresses and mobile phone numbers by using permutations and combinations of letters, number and other characters, address-harvesting software[37] is software that trawls and collects electronic addresses from the Internet. It is to be noted that unlike the "sending in bulk" requirement for UCE messages, here there is a total prohibition against the use of a dictionary attack and address-harvesting software and no electronic message can be sent to an address obtained through these means.

B. *Scope of the Legislation*

Mirroring the philosophy of the Australian *Spam Act*, the Act only applies to those electronic messages that have a "Singapore link."[38] The Singapore link is present if:

(a) the message originates in Singapore;
(b) the sender of the message is (i) an individual who is physically present in Singapore when the message is sent; or (ii) an entity whose central management and control is in Singapore when the message is sent;
(c) the computer, mobile telephone, server or device that is used to access the message is located in Singapore;
(d) the recipient of the message is (i) an individual who is physically present in Singapore when the message is accessed; or (ii) an entity that carries on business or activities in Singapore when the message is accessed; or
(e) if the message cannot be delivered because the relevant electronic address has ceased to exist (assuming that the electronic address existed), it is reasonably

---

multi-media messaging, recipients should be provided with a mobile telephone number to which an unsubscribe request may be sent through a text message. See para. 2(3). See too *infra* note 65 and accompanying text.

31 *Ibid*.

32 *Ibid*. Second Schedule, para. 2(7).

33 *Ibid*., Second Schedule, para. 2(8).

34 *Ibid*., Second Schedule, para. 3(1). The requirements of paragraph 3(1) include, the use of the letters '<ADV>' at the beginning of the subject field (where a subject field exists) or preceding the message; the title (where a subject field exists) and the header information should not be false or misleading; and, a functional mail address or telephone number at which the sender can be readily contacted.

35 *Ibid*. s. 9.

36 *Ibid*. s.2.

37 *Ibid*. s.2.

38 *Ibid*. s.7.

> likely that the message would have been accessed using a computer, mobile telephone, server or device located in Singapore.[39]

The scope of the Act may be split into two. First, it attempts to prohibit the abuse of the communication infrastructure in Singapore. This is achieved through the expansive definition of Singapore link, which allows the Act to be applicable in a wide variety of situations. For example, section 7(2)(a) appears to be a catch-all provision to establish a link in Singapore should sections 7(2)(b), (c) or (d) be unable to establish the Singapore link. This provision would be applicable in a situation where neither the "sender" (the person offering marketing services through UCE messages) nor the "actual sender" (the person causing the message to be sent by the marketer) are in Singapore.

Second, the Act contains provisions that provide extraterritorial effect—this at best can be seen as a hortatory message about Singapore's stance on UCE messages. The IDA Survey revealed that more than three-quarters of all spam received by users in Singapore originated from individuals and entities outside Singapore.[40] Mindful of this reality, Parliament needed to address this issue at least on paper by providing 'extraterritorial effect' to the Act. Accordingly, the definition of "Singapore link" allows the Act to be enforced against individuals and entities not resident in Singapore.[41] However, extra-territorial enforcement is likely to be a formidable challenge in practice.

Further, even if an electronic message has a Singapore link it may be exempted from the requirements of the Act if the message is authorised by the Government or a statutory body in the wake of a public emergency, to promote public interest or to maintain national security.[42]

III. Fissures in the Enactment

Even if technology provides the most effective shield against UCE messages, the importance of a legislative tool cannot be overemphasized. The potency of the legislation, however, lies in how comprehensively it tackles the problem at hand. It is submitted there are numerous shortcomings that may take the wind out of the sails of the Act. This part of the note attempts to flag out some of the issues which solicit re-assessment, and to test the fidelity of certain provisions to the stated policy objectives of the Act.

A. *Technology Neutrality*

The technological scope of the Act is primarily restricted by the definition of "electronic message." The Act defines an "electronic message" to be a "message" sent to an "electronic address."[43] An electronic address is narrowly defined as either being

---

39 *Ibid*. s.7.

40 *Ibid*. Other jurisdictions such as Australia and Spain have also chosen to make their spam legislation applicable extraterritorially. See *supra* note 9 at s. 14 (Australia) and articles 4 and 8 of Law 34/2002, July 11, 2002 (as modified by Law 32/2003) (Spain).

41 *Supra* note 1, s. 7(2)(c) and (d).

42 *Ibid*. s. 7(3).

43 *Ibid*. s. 4.

an electronic mail address or a telephone number to which an electronic message can be sent.[44] The technological scope has been determined on the basis of the purported 'focus' of the Act as elucidated in the Second Consultation[45] and has been widened on an incremental basis between the inception of the consultation process and enactment of the legislation. The First Consultation sought to restrict the reach of the legislation to e-mail messages. The paper noted that the economics of mobile messaging (which unlike e-mail messages has a sizeable marginal cost) and technical architecture acted as a check on the spread of spam in mobile messaging.[46] However, the Second Consultation sang a different tune, bringing mobile messaging spam within the fold of the proposed enactment, citing its intrusive nature.[47] In its final form, the Act covers only e-mail messages, and text and multimedia messages sent to mobile phones. This is likely to blunt the impact of the Act, as the Act discriminates between various technologies or applications. Given that there have been significant developments in communication technology since the first anti-spam enactments,[48] the drafters of the Act should not have chosen to restrict its technological scope. Application of the concept of "technology neutrality"[49] to the Act would have guaranteed its vigour.

Sadly, this is absent from the Act. While the principle of technological neutrality has been used to ensure similar treatment to all electronic messages notwithstanding the means of access,[50] the definitions of "electronic message" and "electronic address"[51] are narrow and are not technology (or 'medium')-neutral. As a result, a number of applications and media such as facsimile transmissions, voice calls, instant messaging[52] and voice over Internet Protocol (VoIP) have been excluded from the reach of this Act. Technology neutrality is a very useful conceptual tool that means that different technologies and media offering similar functionality should be regulated in a similar manner.[53]

---

44 *Ibid*. s. 2.

45 Second Consultation, *supra* note 8 at para. 3.6.

46 Infocomm Development Authority of Singapore & the Attorney-General's Chambers, *Proposed Legislative Framework for the Control of E-Mail Spam* (25 May 2004) at para. 5.8, online: IDA Singapore <http://www.ida.gov.sg>. See too *supra* note 8.

47 *Supra* note 8 at para. 3.8.

48 *Liability of Persons Who Transmit Items of Electronic Mail that Include Advertisements*, Nev. Rev. Stat. §§ 41.705–735 (1997).

49 The term technological neutrality has been used in a loose manner. Typically, the principle of technological neutrality would apply to technologies (for example, GSM and CDMA in mobile phone technologies). However, here the term is used across mediums, technologies and applications.

50 See *supra* note 46 at para. 5.9.

51 *Supra* note 1, ss. 2 and 4.

52 *Supra* note 8 at para. 3.7.

53 For an explanation of the concept of "technology neutrality" in the traditional sense, see Information for Development Programme & International Telecommunication Union, *ICT Regulation Toolkit* at Module 7, para. 3.3.2, online: ICT Regulation Toolkit <http://www.ictregulationtoolkit.org>. See also *Code of Practice for Competition in the Provision of Telecommunication Services 2005*, (S. 87/2005 Sing.), section 1.5.5, which states that a key regulatory principle of the Telecom Competition Code 2005 is to ensure "technological neutrality" in regulation so as to reflect the "erosion of historic differences among various platforms" …. It is "functional equivalence" and not the way the various technologies work that must determine the scope of regulation. This principle has been profitably utilised by the UNCITRAL in the context of e-commerce, and the doctrine of "functional equivalence" now forms an integral part of regulation of electronic contracts. See *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment* (December 1996) at paras. 15-18, online: United Nations Commission on International Trade Law <http://www.uncitral.org>.

A technologically neutral approach has significant advantages. First, it provides regulatory flexibility by obviating the need to amend the laws repeatedly to keep pace with emerging technologies. It guarantees that the law cannot be circumvented by merely choosing a technology or medium that is not regulated. Second, (as a logical corollary) it provides a level playing field for every application or technology providing the same function.[54] As a result of this concept, the entire electronic communications market is regulated instead of the regulation of just specific communication technologies or applications.[55] It has been noted that regulation of the communications market in a technology or application neutral manner lessens the regulatory effort and allows the regulatory regime to be more robust in the face of emerging technologies and mediums.[56] The law will otherwise lag behind changes in technology. Using this principle, it is clear that spam regulation should cover not just e-mail, text and multimedia messages, but other variants of voice and data traffic as well, since they all serve the function of electronic communication. The reasons for excluding these technologies or media, even though several requests were made to include these technologies,[57] are not apparent.[58] Clearly, a voice-based telemarketing call (whether automated or not) to unsuspecting users can be as intrusive, if not more so, than a message sent to a mobile phone user. This problem is further amplified in Singapore since it, unlike other jurisdictions, lacks mechanisms such as a national "do-not call register"[59] or other legislation designed specifically to deal with such situations that are not covered by the Act.[60] Therefore, the definition of electronic messages should be worded so as to include any electronic medium or application that can be used for unsolicited communication. Those media or applications that are to be excluded (if so determined) may be incorporated as express exceptions to the technology-neutral definition. This will obviate the need for tinkering around with the definition of electronic messages to keep up with the ever-changing technology

---

54 This principle is also the cornerstone of the EU legislation against spam. See the Preamble to the EC Directive on the protection of privacy in the electronic communications sector. See *supra* note 13.

55 *Ibid*. For application of this concept in telecommunication regulations, see Peter Alexiadis & Miranda Cole, "The Concept of Technology Neutrality", online: Gibson, Dunn & Crutcher LLP <http://media.gibsondunn.com> (arguing for the adoption of a similar but not identical regulatory framework for telecommunication technologies under the electronic communications networks and services in Europe).

56 David E. Abrams *et al.*, "A Comparative Analysis of Spam Laws: The Quest for a Model Law" (Background Paper for the ITU WSIS Thematic Meeting on Cybersecurity, June 2005) at para 5.1, online: International Telecommunications Union <http://www.itu.int>.

57 Facsimile transmissions have been reported by some participants during the consultation process to be a real problem in Singapore. See *e.g*. Julinda Chia Siew Hong, "Response to Proposed Legislative Framework for the Control of E-mail Spam (Joint IDA-AGC Consultation Paper)", online: IDA Singapore <http://www.ida.gov.sg> (submitting that junk facsimile transmissions is a bigger menace than e-mail spam as the recipient incurs higher costs as a result of such unsolicited facsimile transmissions).

58 See First Consultation, *supra* note 46. As noted above, while the economic argument has subsequently (from the Second Consultation) been dropped, it is not clear as to why the same was not extended to voice calls and facsimile transmissions.

59 A "Do Not Call Register" is a register that allows telemarketers to vet their contact lists against the register containing those who do not wish to receive telemarketing calls. Telemarketers who fail to comply with this register may have to bear penalties. See Australia's *Do Not Call Register Act 2006* (Cth.), No. 88 of 2006.

60 The CAN-SPAM Act is not the only legislative tool against unsolicited communications in the United States. For example, the *Telephone Consumer Protection Act* prohibits using "any telephone facsimile machine, computer, or other device to send an unsolicited advertisement to a telephone facsimile machine": 47 U.S.C. § 227(b)(1)(C) (1991).

landscape. It will also ensure comprehensive coverage of known forms of intrusive technologies by the Act.[61]

B. *Trapped after Consent*

1. *Irrevocable consent?*

The Act prescribes a number of requirements for UCE messages, including the provision of an unsubscribe facility.[62] However, the electronic message will not be considered to be unsolicited if the recipient has earlier requested the same or has consented to the receipt of the message.[63] As a result, the sender does not have to provide such a recipient with an unsubscribe facility or even an accurate and functional electronic mail address or telephone number by which the sender can be readily contacted.[64] In such a scenario, it is not clear how the recipient can request the sender to cease sending electronic messages. Section 5 of the Act may provide us with a possible solution. Section 5(3) obliquely prohibits the sending of an electronic message to a person who may have previously requested or consented to receiving the same, but has subsequently made an unsubscribe request.[65] The requirement of the Act is that only UCE messages need to provide an unsubscribe facility or even contact details of the sender.[66] However, the text of the Act does not spell out the method by which a recipient, who had initially consented to or requested the receipt of an electronic message, may later submit an unsubscribe request.

The easiest way out of this vicious circle would be to prescribe the unsubscribe request requirement of the Second Schedule to the Act (which provides labelling and other requirements to be complied with) for all commercial electronic messages sent in bulk[67] rather than just mandating it for UCE messages. This would allow those who have previously consented or requested receipt of such commercial electronic messages to opt-out of receiving further communications at any time they wish. Situations where recipients no longer desire to receive such electronic messages are not inconceivable. The CAN-SPAM Act is an example of a legislation with an opt-out framework that mandates an unsubscribe mechanism for all "commercial electronic mail messages," thereby explicitly providing for an exit route for those who have previously consented to receipt of such communication.[68] The Singapore *Code of*

---

61 See the Schedule to the *Unsolicited Commercial Electronic Messages Act* 2007 (N.Z.) 2007/7.

62 *Supra* note 1, Second Schedule, para. 2.

63 *Ibid*. s. 5.

64 *Ibid*. Second Schedule, para. 3(1)(d).

65 An "unsubscribe request" is "a request by a recipient of an electronic message, requesting the sender to cease sending any further electronic messages to his electronic address": *supra* note 1, s. 2. See too *supra* note 30 and accompanying text.

66 The Second Consultation claims that *s*. 5(3) of the Act addresses the concern that recipients may be unable to unsubscribe from solicited commercial electronic messages. See *supra* note 8 at para. 3.4. However, the present wording of the enactment is ambiguous and requires fine-tuning and consistency.

67 Currently the Second Schedule applies to all unsolicited commercial electronic messages *sent in bulk*. The need and efficacy of the *sent in bulk* requirements has been critiqued below. See Part III.D., below.

68 47 U.S.C. § 7704(a)(3) (2003). The Australian *Spam Act*, *supra* note 9, s. 18, provides that all commercial electronic messages need to provide the recipient with a functional unsubscribe facility. However, note that the Australian framework provides for an opt-in framework. Similarly, China,

Practice for Competition in the Provision of Telecommunication Services 2005,[69] though implementing an opt-in framework, is also very instructive with respect to an effective and rational consent framework. The Code lays down regulations with respect to the use of End User Service Information ("EUSI") by telecommunication licensees. The EUSI consists of all information that a licensee obtains in the course of providing telecommunication services to an end-user.[70] Licensees are prohibited from using the EUSI for any purpose other than those stated in the Code *unless the prior consent* of the licensee's end user is obtained.[71] Further, the end user has to be provided with a clear and easy means to withdraw such consent at any time.[72]

2. *Double standards for consent*

The Code also raises another interesting issue in connection with the Act. Though the Code and the Act are based on dissimilar conceptual frameworks regarding consent requirements, they may be applicable to the very same subject matter—for example, UCE messages to mobile devices.[73] While the Code deals with the use of EUSI, the Act governs the act of sending UCE messages. Telecommunication licensees have to be entitled to use the EUSI (for example, the mobile phone number of the end user) under the Code, in order to be legally eligible to send UCE messages to its end users. Once this consent is obtained, the commercial electronic message sent by the telecommunication licensee will not be considered unsolicited. As a result, the requirements under the Second Schedule to the Act will not apply. Consequently, telecommunication licensees will have to comply with differential standards for different users; a stricter standard (an opt-in system with a mechanism to revoke consent), based on the Code, for the licensee's own end-users, and a relatively diluted standard, as provided under the Act, for those who are not end users of the licensee.[74] The operation of provisions of the Code and the Act lead to some such peculiar circumstances. The Infocomm Development Authority may have to iron out some of these issues to ensure consistency across regulatory frameworks.

C. *Safe Harbour for Relationships Communications*

There are other anomalies with the architecture of consent in the Act. Of significance is the impervious definition of the term "unsolicited."[75] Right from the start, the

---

which has adopted an opt-in framework, also mandates that all commercial e-mails must provide the recipient with an unsubscribe facility even after the recipient has opted in. See *Regulations on Internet E-Mail Services*, online: Ministry of Information Industry of the People's Republic of China, <http://www.mii.gov.cn/art/2006/03/02/art_524_7341.html>.

69 S 87/2005 [the Code]. See too *supra* note 53.

70 *Ibid*. s. 3.2.6.1.

71 *Ibid*. s. 3.2.6.2 & 3.3.7.

72 *Ibid*. s. 3.3.7.

73 Other instances may include where telecommunication licensees send e-mail messages or voice calls to offer new products and services.

74 Assuming the mobile telephony market consists of two licensees, X and Y. X may send an unsolicited commercial electronic message to Y's end users but cannot send any such electronic message to its own end users.

75 S*upra* note 1, s. 5.

legislative process acknowledged that legitimate interests of the business community were important factors in determining the letter of the law. In this context it is surprising to note that the Act does not provide any leeway for situations in which communications are sent pursuant to a prior business relationship. As was highlighted by internet and online service providers (as participants) during the consultation process, communications are often sent to existing customers as part of the service being offered to the customer.[76] While such communications normally take the form of service messages, they also frequently inform customers about new product offerings or upgrades/updates. A number of spam laws across the world, whether under the opt-in or the opt-out framework, provide for a prior business relationship exception. Article 13 of the EU Directive[77] is an example of legislation that expressly recognizes the prior business relationship exception to the general rule under an opt-in framework.[78] In the context of an opt-out framework, the spam control regime in the United States of America also explicitly provides legitimacy to "transactional or relationship messages."[79]

Relationship and service messages are increasingly used to provide customers with better service. The submissions made by some of the participants in the consultation process and the detailed studies of various 'benchmark jurisdictions' undertaken by the Ministry of Information, Communication and the Arts[80] should have alerted the drafters to provide a 'safe harbour' for such communications. It is submitted that this would also have been in line with the avowed purpose of ensuring that legitimate business and consumer needs are not stifled unreasonably by the Act. The way forward for the Act should either be to add a proviso to the definition of "commercial electronic message," or amend the definition of "unsolicited" to exclude communications sent on the basis of a prior business relationship. The provision of an unsubscribe facility in all commercial messages (as suggested earlier in this note)[81] will ensure that, notwithstanding the prior business relationship, users can unsubscribe if they choose to do so.

---

76 See for example eBay Singapore, eBay's Response to the Joint IDA-AGC Consultation Paper entitled "Proposed Spam Control Bill"', online: IDA Singapore <http://www.ida.gov.sg> (pointing to the absence of an immunity to communication sent to the customer pursuant to a pre-existing business relationship). See also Microsoft, "Submission in Response to the Proposed Spam Control Bill", online: IDA Singapore <http://www.ida.gov> ['*Microsoft Submission*'].

77 EC Directive on the protection of privacy in the electronic communications sector, *supra* note 13 at art. 13, para. 2.

78 Schedule 2, c. 2 of the Australian *Spam Act*, *supra* note 9, defines consent to include what can be "reasonably inferred, from conduct and the business and other relationships of the individual or organization concerned."

79 The definition of "commercial electronic mail message" excludes "a transactional or relationship message." See 15 U.S.C. §7702 (2)(A) (2003). A "transactional or relationship message" has further been defined in 15 U.S.C. §7702 (17) in order to ensure that the same is not construed in a broad and ambiguous manner and is strictly used in furtherance of a prior business transaction or relationship with the recipient.

80 See Sing., *Parliamentary Debates*, vol. 83, col. 568 (12 April 2007). See also, Dr. Lee Boon Yang, "Second Reading of Speech on the Spam Control Bill 2007" at para. 5, online: http://stars.nhb.gov.sg/stars/public/viewPDF.jsp?pdf no=20070412982.pdf.[Second Reading]. See also *supra* note 46 at para 2.12.

81 See Part III.B.1, above.

D. *A Bright Line for Bulk*

Under the Act, only communications that are unsolicited, commercial in nature and sent in bulk need to comply with the requirements of Schedule 2.[82] As noted above, certain numerical thresholds, derived from the law of the United States, have been prescribed in order to ascertain whether a message has been sent in bulk or not.[83] While such thresholds provide certainty to senders of commercial electronic messages, they may also allow abusers to get away scot-free by sending unsolicited communications just short of the threshold numbers. The government agencies behind the formulation of the Act have acknowledged the problem in specifying a bulk requirement, especially the numerical threshold.[84] However, they believe that spammers will have no incentive to send messages which fall just below the numerical threshold, as it would not be commercially viable for them to do so.[85] There appear to be several conceptual flaws in the usage of the bulk requirement. Thus, the wisdom of the sending in bulk condition under the Act needs to be questioned.

First, abuse of telecommunications infrastructure (at a macro level) is not the only concern the Act is attempting to tackle. One of the primary objectives of the Act is to address the concern of end-users or the recipients of spam.[86] Typically, the concern of the end-user is either the content of or the inconvenience caused by such unsolicited communication, rather than the volume.[87] Second, the problem with the use of the bulk requirement gets heightened since the Act allows individuals (at least in theory) to pursue legal actions against those contravening the provisions of the Act. Should an individual recipient decide to take legal action against a spammer,[88] it would be practically impossible for him or her to prove that the thresholds for sending in bulk were satisfied by the spammer.[89]

Further, across other jurisdictions the issue of bulk has not been a critical factor in the general prohibition against unsolicited communication. In the United States, the volume of communications is only relevant to provisions connected with criminal offences—those dealing with "fraud and related activit[ies] in connection with electronic mail."[90] The volume requirement has no bearing on the other prohibitions

---

82 *Supra* note 1, s. 11.

83 *Supra* note 26. Thresholds obtained from United States legislation deal with "fraud and related activity in connection with electronic mail". Contraventions of these provisions invite criminal sanction. See 18 U.S.C. § 1037(b) (2003).

84 Second Consultation, *supra* note 8 at para 3.12.

85 *Ibid*.

86 *First Consultation*, *supra* note 46 at para 2.11.

87 See N.Z., Office of the Associate Minister of Information Technology, "Legislating against Unsolicited Electronic Messages Sent for Marketing or Promotional Purposes (SPAM)", online: Ministry of Economic Development, <http://www.med.govt.nz>.

88 There have been instances of successful claims maintained by individuals against spammers. See for example, *Gordon Dick v. Transcom Internet Services Ltd.*, January 30, 2007, (Edinburgh Sheriff Court, Scotland) SA1170/06, online: <http://www.scotchspam.org.uk>. These litigants did not have to prove the bulk requirement as the same in not mandated under EU spam laws.

89 See Australian Government, Department of Communications, Information Technology and the Arts, *Report on the Spam Act 2003 Review* (June 2006) at 33, online: Australian Government, Department of Communications, Information Technology and the Arts <http://www.dcita.gov.au> (arguing that the bulk requirement cannot be established by complainants).

90 See *supra* note 83.

imposed by the CAN-SPAM Act.[91] Australia has usefully adopted the communication volume as only an element to be factored in determining the penalty to be imposed on the spammer.[92] The civil penalty imposed on the spammer is increased substantially based on the number of contraventions committed.[93]

Another reason that has been cited by the regulators for incorporating the bulk requirement into the Act in Singapore is to protect personal or one-on-one communication.[94] However, this is necessitated only by the inflexible conception of consent under the Act, which does not provide for a subjective analysis of the consent requirement. It is submitted that the sending in bulk requirement is not necessary and does not coalesce well with other aspects of the Act. Given the present wording of the Act, the removal of the bulk requirement has to be accompanied by moving to a flexible framework of what constitutes unsolicited communications, such as recognising consent that can be reasonably inferred from the relationship of the parties.

E. *The Clasp of the Enactment*

1. *Bite of criminal sanctions*

Conceptual inconsistencies exist in the area of legal remedies and sanctions provided under the Act. Given that the majority of spam emanates from outside Singapore, the Act's primary objective is, admittedly,[95] to act as a deterrent. However, a conscious choice has been made not to include criminal sanctions for a variety of reasons. The framers of the Act have concluded that spammers normally do not act with malicious intent.[96] Further, the Ministry of Information, Communications and the Arts found no other instance of the act of spamming *per se* being criminalised in other jurisdictions.[97]

The issue of whether criminal provisions should be made a part of the Act never figured as a question during the consultation process.[98] The First Consultation observes

---

91 See *e.g.* 15 U.S.C. §7704 (2003).

92 *Supra* note 9 at s. 25(1). See also Yahoo!, "Yahoo!'s Response to the Joint IDA-AGC Consultation Paper Titled "Proposed Legislative Framework for the Control of E-Mail Spam"" at 2, online: IDA Singapore <http://www.ida.gov.sg> (arguing that the bulk requirement should only be used for the purpose of determining criminal penalties).

93 *Supra* note 9 at ss. 25(3)(b), (4)(b), (5)(b) and (6)(b). See also *Australian Communications and Media Authority v. Clarity1 Pty Ltd* [2006] FCA 1399. The case is the first successful prosecution under the Australian *Spam Act*.

94 Second Consultation, *supra* note 8 at para. 3.10.

95 Second Reading, *supra* note 80 at para. 12.

96 *Ibid*., at para. 23. This conclusion is at odds with the experience of enforcement agencies in some jurisdictions. It has been found that more than two-thirds of spam contained clear falsity and less than one-fifth of spam did not sell illegitimate products or services. See Hugh Stevenson, "U.S. Federal Trade Commission International Law Enforcement against Spam", online: International Telecommunications Union <http://www.itu.int> (detailing the challenges and important factors in improving cross-border anti-spam enforcement).

97 *Ibid*.

98 However, some entities that participated in the consultation process have nevertheless voiced the need for criminal provisions. See CompTIA, "Comments of the Computing Technology Industry Association (CompTIA) For Consideration of the Singapore Government Anti Spam Legislation" at 13, online: IDA Singapore, <http://www.ida.gov.sg> (arguing that harsh penalties and criminal remedies may

that a number of existing Acts, including the *Penal Code*,[99] the *Computer Misuse Act*[100] and the *Consumer Protection (Fair Trading) Act*,[101] already cover certain actions of spammers that may involve malicious intent. If this is to be accepted then what is the need for sub-sections (x) to (xii) in Section 3(1) of the Act? These deal with instances in which messages are used to dishonestly obtain gain, property or financial advantage from another person. What is being achieved by including such messages within the definition of commercial electronic message? The paradox is obvious when one compares Section 3(1)(x)-(xii) read with Section 11 (mandating that all UCE messages comply with the requirements of Schedule 2 to the Act) on the one hand and the *Penal Code* on the other. An unsolicited message that assists or enables a person, by deception, to dishonestly obtain property from another person can be sent as long as it provides an unsubscribe mechanism and complies with the labelling requirements mentioned under Schedule 2 to the Act. However, attempting to dishonestly obtain property from another person may constitute a criminal offence under the relevant provisions of the *Penal Code*.[102] Surely, Parliament would not have intended to permit sending a message that could lead to a criminal offence, just because it complies with labelling and other such requirements under the Act.

Further it may not be proper to rely on the position in other jurisdictions, with respect to criminal offences under spam legislation, as the legal environment may materially differ between jurisdictions.[103] The definition of commercial electronic message in the Act has been derived from the Australian *Spam Act*. In deriving and applying legislation from another jurisdiction, the legal context must be kept in mind and cannot be severed. The Australian *Criminal Code Act* contains provisions that are suitably worded to tackle online frauds. It may therefore not have been necessary for the Australian *Spam Act* to stipulate a criminal offence.[104] The situation in Singapore differs materially. Enactments such as the *Computer Misuse Act* and the *Consumer Protection (Fair Trading) Act* do not explicitly cover issues such as online fraud. By providing for criminal sanction against actions that have been committed dishonestly,

---

aid in making the enactment more effective.). See also Bryan Tan & Siew Kum Hong, "Response to Consultation Paper on Proposed Spam Control Bill," online: IDA Singapore <http://www.ida.gov.sg> (arguing that criminal provisions should be included in the enactment as the cost of civil action and the uncertainty surrounding the recovery of damages might dampen efforts to press civil action).

99 Cap. 224, 1985 Rev. Ed. Sing.

100 Cap. 50A, 2007 Rev. Ed. Sing.

101 Cap. 52A, 2004 Rev. Ed. Sing.

102 See the *Penal Code*, supra note 99 s. 420, which states: "Whoever cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment for a term which may extend to 7 years, and shall also be liable to fine."

103 It is not uncommon for spam legislation to contain criminal sanctions where the actions extend beyond mere non-compliance with the labelling or identification stipulations. See *e.g.* art. 32 of Japan's *Act on Regulation of Transmission of Specified Electronic Mail*), Act No. 26 of April 17, 2002, online: Ministry of Internal Affairs and Communications <http://www.soumu.go.jp>.

104 See *e.g. supra* note 22 at s. 474.14 (dealing with using a telecommunications network with intention to commit a serious offence). As noted earlier, the United States also imposes criminal penalties for certain fraudulent activities involving electronic mail including imprisonment where an offence under the CAN-SPAM Act is committed in "furtherance of any felony under the laws of the United States or of any State." See 18 U.S.C. § 1037 (2003).

the Act could have taken the first few steps in stemming online fraud—an escalating problem in Singapore.[105]

2. *The enforcement abyss*

A typical piece of modern legislation may be divided into two portions—one which is constructed *a priori* and the other that is fashioned subsequent to deliberation of issues amongst stakeholders. The 'terms of reference' of the consultation exercise, and the manner in which the issues are framed, etch the divide between the two portions. Such a division becomes apparent when reflecting on the topic of enforcement (and criminal sanction) under the Act. No powers have been specifically reserved with the government or sectoral regulators to enforce provisions of the Act.[106] The question was never raised or considered in either the First or Second Consultations.[107] Submissions were made by various participants, even as late as the Second Consultation, urging the Government to assume the mantle of enforcing the Act.[108] Providing remedies to individuals and entities (including ISPs) that have suffered loss or damage as a result of contravention of the Act is undoubtedly important.[109] However, one should not forget that it will be virtually impossible for individuals to successfully carry out any such action given various enforcement difficulties, including the insurmountable evidentiary burden. In this scenario, only fairly large commercial enterprises and entities, and internet service providers, would be in a position to lead the charge against spammers. It would further the goals of the Act to allow the State to wield its big-stick against contraventions. Jurisdictions that provide State regulators with enforcement powers have been most robust in the fight against spam.[110] It

---

[105] In 2006, a multi-jurisdictional enforcement action against spammers involved in furthering fraud schemes was carried out. The operation resulted in the conviction of 80 people in North America alone and an estimated loss of $1 billion to the victims. See "Fact Sheet: Operation Global Con" (23 May 2006), online: United States Department of Justice <http://www.usdoj.gov>.

[106] The enactment only contemplates a statutory right to sue for "any person" (civil action). See above, Part II.E.1. Under the CAN-SPAM Act, 2003, the Federal Trade Commission (FTC) and other sectoral regulators such as the Securities and Exchanges Commission have been bestowed with powers to ensure compliance with the provisions of the Act. See 15 U.S.C. § 7706 (2003).

[107] The first consultation paper centred on whether internet service providers should be vested with a statutory right to commence legal action against those responsible for 'unlawful spam'. See First Consultation, *supra* note 46 at paras. 5.30-5.34. The Second Consultation considered whether the statutory right to commence action should be open to, not just internet service providers but also others who may have suffered loss or damage as a result of contravention of the enactment. See Second Consultation, *supra* note 8 at paras. 3.39-3.41.

[108] See *Microsoft Submission*, *supra* note 76 at para. 7; and Singapore Telecommunications Limited, "Submission to IDA and AGC on Proposed Legislative Framework for the Control of E-Mail Spam" at paras. 4.37 & 4.43, online: IDA Singapore <http://www.ida.gov.sg>.

[109] The provision of a statutory remedy forms a sound basis for individuals and entities to initiate action against spammers. Without such a basis, individual and entities in other parts of the world have had to arduously establish their claims under the law of trespass or on the basis of principles of contract (arising from the breach of the terms of service imposed by the service provider on the spammer). See *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015 (S.D. Ohio 1997); *Hotmail Corp. v. Van$ Money Pie Inc.*, 1998 U.S. Dist. LEXIS 10729 (N.D. Cal. 1998).

[110] *Supra* note 89 at 29 (providing details of the enforcement activities carried out by the Australian Communications and Media Authority between April 2004 and October 2005, which includes over 360 anti-spam actions).

is pivotal to allow for the most realistic enforcement mechanism, since deterrence is a crucial aspect of the Act.[111]

The absence of state enforcement against spammers may also relegate Singapore to the sidelines of the international campaign against spam. The efficacy of cross-border enforcement cooperation agreements, including the OECD Recommendation[112] and the London Action Plan,[113] is premised on the ability of governmental authorities to receive and act on complaints.[114] Without enforcement powers, no State body in Singapore will be able to effectively contribute to such trans-national efforts. Further, no provision in the Act enables any governmental agency to extend cooperation to, or seek assistance from, enforcement authorities in other jurisdictions. We need to look no further than the *Competition Act* of 2004[115] for an example of such a provision, the presence of which is vital to tackle problems that often have cross-border implications. The *Competition Act* allows the Competition Commission of Singapore to enter into arrangements with "foreign competition bodies."[116] A similar provision should be replicated in the Act to facilitate meaningful exchanges across borders. In the absence of state enforcement powers and an enabling provision that allows participation in cross-border cooperation, the Act will remain a 'paper tiger.'

F. *Compliance Woes*

The Second Schedule to the Act is in essence the compliance manual for the transmission of UCE messages and provides certain objective standards that need to be adhered to. Some of these issues relating to compliance will be raised and discussed below.

1. *Labelling: a counterproductive requirement*

A seemingly innocuous component of the Second Schedule is the fixed format labelling requirement for all UCE messages. Every unsolicited commercial

---

111 While prosecutions and civil actions have not stemmed the flow of spam, they bolster the technological crusade against spam. There have been a number of successful prosecutions recently. See Sharon Gaudin, "Brooklyn Man Pleads Guilty To Spamming 1.2 Million AOL Users," *Information Week* (12 June 2007), online: Information Week <http://www.informationweek.com>; Ian Kehoe, "Data Commissioner to Proceed with Spam Case", *The Post*, (11 April 2004), online: The Sunday Business Post Online <http://archives.tcm.ie/businesspost>.

112 See *OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam* (13 April 2006), online: OECD Task Force on Spam <http://www.oecd-antispam.org> (which provides for a cooperation framework amongst "national public bodies" "with enforcement authority for laws connected with spam").

113 *The London Action Plan on International Spam Enforcement Cooperation* (11 October 2004), online: <http://www.londonactionplan.org>.

114 See *Cooperation Procedure Concerning the Transmission of Complaint Information and Intelligence Relevant to the Enforcement of Article 13 of the Privacy and Electronic Communication Directive 2002/58/EC, or any other Applicable National Law Pertaining to the Use of Unsolicited Electronic Communications* (1 December 2004), online: Europe's Information Society Thematic Portal, <http://ec.europa.eu/information_society>.

115 Cap. 50B, 2006 Rev. Ed. Sing.

116 *Ibid*. s. 88.

electronic message needs to contain "<ADV>" in either the subject line or the first line of the message (where no subject field exists).[117] A number of countries, including Japan[118] and South Korea,[119] have incorporated fixed format labelling requirements.[120] Fixed format labelling in these jurisdictions has not proven to be particularly useful. While some jurisdictions have had to repeatedly modify the requirement[121] to play catch up with spammers, others have found that even legitimate marketers often fail to comply with such requirements.[122]

Fixed format labelling is supposed to provide network service providers and end-users with a straightforward method to separate the wheat from the chaff (*i.e.* genuine messages from UCE messages).[123] Given that, for the most part, spam is not generated by law abiding entities, a sizeable number of UCE messages are unlikely to carry any labels to tip-off the end-users or the ISPs. As a result, end-users may believe that messages without the fixed label are genuine while legitimate messages may be filtered out by filters that are calibrated to block <ADV> labelled messages.[124] Thus, fixed format labelling may actually be counterproductive from the perspective of end-users since it may provide false comfort to end-users regarding the nature of e-mail received by them.

Further, the fixed format label requirement must be reviewed since it is likely to increase compliance costs for businesses that have a regional or international presence. Since the labelling format differs from country to country, senders will have to ensure compliance with each of these regimes[125]—for example, sieving out Singapore-based recipients to ensure that the <ADV> label is employed for them.[126]

Most regulations admittedly increase the costs of compliance and operation for legitimate businesses. Therefore, regulations attempt to set the cost of

---

117 S*upra* note 1 at Second Schedule, para. 3.

118 See *supra* note 103.

119 The relevant law in South Korea is Article 50 of the Ordinance of the Ministry of Information and Communication of the Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001, [2005] PrivLRes 2 as amended Act No. 7812 (30 December 2005).

120 See also *Subject Line Labelling as a Weapon against Spam: A CAN-SPAM Act Report to Congress* (June 2005) at 7-9, online: Federal Trade Commission <http://www.ftc.gov> (arguing that subject line labelling should not be made a mandatory requirement under the CAN-SPAM Act).

121 See Xingan Li, E-marketing, "Unsolicited Commercial E-mail, and Legal Solutions," 3(1) *Webology* (Article 23), online: Webology <http://www.webology.ir>. See also Pacific Internet, "Comments on Joint IDA-AGC Consultation Paper" at 3, online: IDA Singapore <http://www.ida.gov.sg> (calling for a flexible labelling requirement in order to "meet the demands of the prevailing circumstances").

122 See *"Spam", A Report of the All Party Internet Group* (October 2003) at 9, online: All Party Internet Group, <http://www.apcomms.org.uk>, quoted *supra* note 120.

123 The fixed labeling requirement does not appear to vastly improve technological measures such as blocking or filtering in any significant manner. See *Microsoft Submission*, *supra* note 76 at para 6.2 (noting that labels are no longer critical for filtering technology).

124 See *supra* note 120 at 13 (discussing the detrimental effect of the labelling requirement in cases where internet service providers employ filters on the basis of a label).

125 It is useful to note that major jurisdictions including Australia, the United States of America and the EU, do not currently mandate a fixed label requirement.

126 See Hewlett Packard Company, "HP Comment on Proposed Spam Control Bill," online: IDA Singapore <http://www.ida.gov.sg> (noting the practical difficulties in having a fixed labelling requirement for a multinational enterprise). See also *supra* note 122 at para. 104 (recommending that fixed format labels not be used until universally accepted rules are formulated).

non-compliance at a level that disincentivises non-compliance.[127] However, regulations cannot be justified if, while increasing the costs of compliance for legitimate businesses, they effectively prevent the business from carrying out the regulated activity. In this case, while legitimate businesses have to bear increased compliance costs by way of the fixed format labelling requirement, this requirement may in effect nullify their marketing efforts (as discussed above). It is submitted that the other legal requirements (namely the option to unsubscribe and the identification requirement) along with technological measures will be more efficacious in controlling spam than fixed format labelling.

2. *Compliance for senders*

The term "sender" has been broadly defined in the Act to mean the person or entity that sends, causes or authorises the message to be sent.[128] This could cause uncertainty with regard to the stipulation in the Second Schedule that prevents the sender of UCE messages from sending any further UCE messages after ten days of receiving an unsubscribe request from the concerned recipient.[129] Marketing services and telecommunication companies act as intermediaries to companies that seek to reach out to end-users. These intermediaries generally send out UCE messages to end-users on behalf of a variety of entities. Thus, such intermediaries are likely to send UCE messages on behalf of more than one entity to the same recipient. Where the recipient sends an unsubscribe request, would the intermediary have to cease sending UCE messages to the recipient altogether? Consider a situation where a recipient sends an unsubscribe request for UCE messages sent on behalf of Company A to the intermediary. The intermediary also sends UCE messages on behalf of Company B. Can the intermediary continue to send UCE messages to the recipient on behalf of Company B? The all-encompassing definition of "sender" seems to suggest that the intermediary cannot do so, since both, the "entity that sends" the message and the entity that "causes or authorises the message to be sent" are considered senders. The drafters of the Act may have not intended such an outcome. Further, a consumer may not want to receive commercial communications regarding a certain product but may care for UCE messages for another product or service. Clarification or guidance on this issue would be valuable, as it would provide legal certainty to intermediaries.

IV. Conclusion

While Singapore's legislative response to spam was still being conceived, other jurisdictions were already testing their anti-spam legislation in the courts.[130] Drawing from the operational and enforcement experiences of other jurisdictions, the Act had the potential to be a 'state of the art' legislative tool against spam. However, in its final form, it falls short of being a comprehensive rejoinder to the scourge of spam. The Act contains a number of provisions that are not in step with the stated policy

---

127 Stephen Breyer, *Regulation and its Reform* (Massachusetts: Harvard University Press, 1982) at 271-284.

128 *Supra* note 1.

129 *Supra* note 29 at Second Schedule, para. 2(7).

130 Just as Singapore, New Zealand has also only recently passed an anti-spam legislation. It comes into effect from 5th September 2007. See *supra* note 61.

approach[131] or with the basic principles outlined during the consultation process.[132] First, provisions of the Act could have been inspired by existing regulations in Singapore, like the *Code* and the *Competition Act*. This would have ensured consistency under domestic regulation and would have allowed for a more enlightened approach in areas such as international cooperation. Further, while the legislature intended to be sensitive to the needs of the business community, it could have gone beyond just choosing the opt-out framework. For example, the recognition of prior business relationships and a more practical labelling requirement would have aided businesses without prejudicing the force of the Act. There exist other clefts in the Act, like the narrow conception of electronic messages and the incongruous consent framework. These need to be remedied at the earliest opportunity.

At a time when fraudulent spam and scams are attracting heightened enforcement efforts, criminal provisions are proving to be a potent enforcement tool.[133] On the other hand, legislation (like the Act) without the bite of criminal sanctions will only incentivise spamming. Also, expecting private individuals and entities to actively enforce the provisions of the Act is unrealistic and may render the legislative effort nugatory. The enormous evidentiary burden on the plaintiff, the significant cross-border element, and the exacting enforcement timelines which are normally features of such actions warrant the involvement of state agencies.[134] Therefore, in addition to introducing criminal sanctions under the Act, the legislature must mull over appointing an authority (for example, the IDA) to receive and act on spam complaints. The measures suggested above will aid the process of achieving a robust anti-spam regime which effectively balances the various interests involved, and will position Singapore as a key actor in the global effort against spam.

---

131 See *supra* note 46.

132 See *e.g.* First Consultation, *supra* note 6 at para. 2.12.

133 U.S. Department of Justice, Press Release, "Seattle Spammer Indicted for Mail and Wire Fraud, Aggravated Identity Theft and Money Laundering" (31 May 2007), online: United States Department of Justice <http://www.usdoj.gov> (providing details of the arrest of Robert Soloway who is allegedly responsible for sending out millions of junk e-mail and defrauding consumers).

134 OECD Task Force on Spam, *Anti-Spam Regulatory Approaches* (November 2005), online: OECD Task Force on Spam <http://www.oecd-antispam.org>.