Does the Spam Act 'CAN-SPAM'?

Matthew Leung, Telstra Corporation

Matthew Leung is a lawyer with Telstra Corporation Limited in Melbourne.

Introduction

Spam is moving from a nuisance to a serious problem not only in Australia but globally.[1] Despite the good intentions of the Australian and United States governments to prevent the proliferation of spam, it is doubtful if their 'war on spam' is being won. In October 2003, about 50 per cent of email sent globally was spam, but in September 2005, this figure had risen to about 68 per cent.[2] Pornographic spam is particularly problematic. A survey conducted in 2004 found that 2.5 billion pornographic emails had been sent daily that year, and 91 per cent of the public rated pornographic email spam as the 'most annoying' type of spam.[3] In light of these statistics, this article will discuss how the Australian Spam Act 2003 (Cth) (as amended) ('Spam Act') and the United States Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003[4] ('CAN-SPAM Act') attempt to define spam, and the obligations they place on spammers to obtain the recipient's consent to receive spam. It will conclude that while the Spam Act forms an important overall strategy to combat spam, valuable lessons can be learnt from the CAN-SPAM Act and incorporated into the Spam Act to improve its effectiveness to regulate spam.

Spam legislation in Australia and the United States

The Australian Government's attempt to regulate spam culminated in the Spam Act, which came into effect on 11 April 2004. The Spam Act is enforced by the Australian Communications and Media Authority[5] ('ACMA') and aims to reduce Australia as a source of spam, to minimise spam for Australian end-users and to extend Australia's involvement in worldwide anti-spam initiatives.[6] One purpose of the Spam Act is to regulate the sending of 'commercial electronic messages'. A message is a 'commercial electronic message' if, having regard to its content, presentation, the content to which the message links and any contact information it contains, it would be concluded that the purpose of the message is, among other things, to offer to supply, provide, advertise or promote goods, services, land, business opportunities or investment opportunities.[7] The Spam Act provides for civil penalties including warnings, infringement notices and monetary penalties. ACMA can institute proceedings in the Federal Court against an individual who breaches the Spam Act to recover penalties of up to $44,000 for contraventions on a single day, while an organisation could be fined up to $220,000 in a day.[8] Infringers with a prior record will be penalised up to a maximum of $220,000 each day for individuals, and $1.1 million each day for organisations.[9]

In the United States, the CAN-SPAM Act came into effect on 1 January 2004. The CAN-SPAM Act pre-empts State anti-spam legislation and is enforced by the Federal Trade Commission ('FTC'). The CAN-SPAM Act establishes requirements for the sending of 'commercial electronic mail messages' which are defined as 'electronic mail message[s] the primary purpose of which [are] the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)'.[10] The CAN-SPAM Act provides civil and criminal penalties for those who breach these requirements, and gives the Department of Justice the authority to enforce its criminal sanctions. Other federal and state agencies can enforce the CAN-SPAM Act against organisations under their jurisdiction,[11] and internet service providers ('ISPs') may also bring actions against infringers.[12]

Characterising 'spam' in the Spam Act and the CAN-SPAM Act

A common feature of the Spam Act and the CAN-SPAM Act is that neither seek to define 'spam'. Although the Spam Act is an 'Act about spam', it regulates 'commercial electronic messages'. Similarly, the CAN-SPAM Act does not define 'spam', but rather regulates 'commercial electronic mail messages'. However, there are a number of differences between these laws, and this article will focus on two of these differences. First, the Spam Act is deliberately technologically neutral so that it applies to any form of commercial electronic messages, while the CAN-SPAM Act applies specifically to commercial email. Second, the Spam Act requires the sender to obtain the prior consent of the recipient before sending a 'commercial electronic message', while the CAN-SPAM Act permits a sender to send commercial email until the recipient indicates they no longer wish to receive such email.

1 Spam: a technologically neutral definition

It is important to settle on a clear and agreed definition of spam so that anti-spam legislation is effective,[13] and so that ISPs and regulatory authorities are reasonably confident of this definition before they enforce their terms and conditions or any regulations or laws against spammers.[14] The Spam Act prohibits the sending of a 'commercial electronic message' with an Australian link without the prior consent of the recipient, unless it is a designated commercial electronic message.[15] The legislature was careful to ensure that the definition of 'commercial electronic message' is technologically neutral in order to account for the convergence of technologies and media (for example, SMS, MMS and 3G applications) and their potential for

future spam growth.[16] However, such an exhaustive definition of spam could be problematic as it is unclear whether this definition covers all methods of commercial transactions,[17] and litigation is likely to be necessary to determine whether a transaction falls within this definition.[18] An inclusive definition that provides examples of what would, and would not, be considered a commercial electronic message would be preferable in order to overcome such uncertainty.[19]

In contrast, the CAN-SPAM Act regulates 'commercial electronic mail messages',[20] and is therefore capable of targeting spamming activities specifically related to email more effectively than the Spam Act. A technique widely used by spammers to conceal the origin of email is to forge the header information by relaying the email through other people's open or non-secure email servers without permission. The CAN-SPAM Act regulates such activity by prohibiting false or misleading email header information, such that a person who sends an email is in breach if they '[use] another...computer to relay or retransmit the message for purposes of disguising its origin'.[21] Therefore, the CAN-SPAM Act specifically prohibits spammers from using another person's email or computer account to send email spam. The Spam Act, however, because of its technological neutrality, is unable to target spamming activities specifically related to email as effectively as the CAN-SPAM Act, in ways such as prohibiting false and misleading header information. A consequence of this shortcoming is that Australian ISPs need to pay for more bandwidth than their customers would require as spammers can continue to take advantage of open relays, and inevitably, such costs are passed on to consumers. While ISPs may use filters to delete email spam as a service to their customers, ISPs nevertheless would be required to acquire extra bandwidth to receive every item of email and scan them for spam-like features.[22]

Further, the CAN-SPAM Act specifically requires the subject lines of unsolicited commercial email to be clearly identified as solicitations or advertisements for products and services.[23] The Spam Act, however, is unable to impose a similar requirement as its technologically neutral approach means it must be able to regulate any form of commercial transaction, not all of which feature a subject line – for example, SMS and MMS messages do not feature a specific subject line. However, a limitation of the CAN-SPAM Act is that it does not prescribe the words which must be used in the subject line. Rather, the sender is permitted to choose the words that constitute the subject line. This impedes the ability of email software to automatically delete or redirect email according to specific words in the subject line. Therefore, a subject line that contains words such as 'We've got a fantastic offer for you – read now!' could be sufficient to satisfy the requirement that the subject line must identify the content of the email as a solicitation or advertisement for products and services. If specific characters such as 'ADV:' were prescribed, this would assist spam filtering software to recognise and deal with advertorial email. Unfortunately, this is not the opinion of the FTC, which found that subject line labelling requirements in relation to advertorial email are not an effective means of reducing spam through more efficient sorting or filtering.[24]

However, the CAN-SPAM Act does require specific words to be in the subject lines of pornographic email spam. The CAN-SPAM Act requires any email 'that includes sexually oriented material' to contain the words 'SEXUALLY-EXPLICIT:' in the subject line.[25] This wording, which was prescribed by the FTC and came into effect on 19 May 2004, enables recipients who do not wish to view such material to program their email software to automatically filter email containing the words 'SEXUALLY-EXPLICIT:' in the subject line so that the email will be deleted automatically or redirected outside the recipient's ordinary view. The seriousness with which the FTC treats a breach of this rule was demonstrated in a widely publicised case where the FTC charged a network of corporations and individuals with using spam to sell access to online pornography on the basis that they sent email containing sexually-explicit content without the prescribed wording in the subject lines of the email.[26] Admittedly, the effectiveness of this rule relies on the willingness of the sender to comply – a survey conducted soon after this rule came into effect found that only one in six unsolicited pornographic emails complied with this FTC rule regarding labelling of pornographic email.[27] This rule also offers little comfort to the recipient who manually sorts email and will still see pornographic material even though the subject line contains the prescribed words, or if the recipient's email software automatically displays a preview of incoming email, including email containing the pornographic material.[28]

A flaw in the CAN-SPAM Act is that it does not apply to commercial email that merely provides a hyperlink to the website of, or a reference by name to, a commercial entity if the primary purpose of the email is not a commercial purpose.[29] Thus, an email that merely contains a link to a pornographic website would be exempt from the requirements of the CAN-SPAM Act. This exception hinders the ability of email spam filters to delete or redirect pornographic email effectively. If Congress was serious about combating pornographic email spam, the requirement for the subject line to contain the prescribed words should apply regardless of whether the email contains pornographic images or merely a hyperlink to a pornographic website. In contrast, an email that contains only a hyperlink is not excluded from the Spam Act, which regulates any electronic message that contains a link to a website that is commercial in nature.[30] Nevertheless, there is no requirement in the Spam Act that the subject line of pornographic email must contain suitable identifying words, which inhibits the effectiveness of email filters to deal with such material. This is ironic as a report on spam published by the National Office of the Information Economy was particularly concerned about minors receiving email containing indecent material.[31] Nevertheless, it is often difficult for the law to provide a solution to the problem of minors accessing pornographic material online,[32] and there can be no substitute for parental supervision in their child's use of

email.[33] Parents who allow their children to access online resources may need to accept the risk that their children could engage in online activities that involve dangerous or objectionable content,[34] and if parents trust their children to use online resources, then parents may need to deem their children sufficiently responsible to know how to deal with pornographic email spam.[35]

While the Spam Act should be regarded as a part of an overall strategy to combat email spam, its attempt to characterise spam in a technologically neutral manner restricts its effectiveness to target specific forms of spam, such as email spam. In particular, its regulation of pornographic email spam can be improved by requiring specific words in subject lines in order to assist email filtering software and to alert recipients to the pornographic content contained within the email.

2 Consent: an opt-in regime

The Spam Act and the CAN-SPAM Act place different obligations on a spammer in respect of the time that they must obtain the consent of a person to receive their material. The Spam Act adopts an 'opt-in' regime, such that sending unsolicited commercial electronic messages is prohibited unless the recipient has opted-in to receive such messages by giving prior consent.[36] In contrast, the CAN-SPAM Act adopts an 'opt-out' regime, such that people can receive unsolicited commercial email without first having provided their consent. Thus, the CAN-SPAM Act allows businesses to send email advertisements to potential customers even where these recipients have not given prior consent to receive such messages and where the sender does not have a pre-existing or current business relationship with the recipient. Instead, the sender must stop sending them only after the recipient so requests,[37] which means the CAN-SPAM Act effectively gives each advertiser in the United States one free shot at each consumer's email inbox.[38] One reason that the United States chose an opt-out regime was to avoid violating the First Amendment of the United States Constitution, which contains a right of free speech.[39]

The opt-in regime of the Spam Act is preferable over the opt-out regime of the CAN-SPAM Act for a number of reasons. First, the Organisation for Economic Co-operation and Development ('OECD') considers that online consumers should be afforded transparent and effective protection that is not less than the protection afforded in other forms of commerce.[40] In the offline world, people can protect themselves from receiving unsolicited postal mail by placing a 'No Junk Mail' or equivalent sign to their letter box to avoid receiving unsolicited mail,[41] which is equivalent to first having to consent to receive the material in an opt-in regime. In the offline world it is also common etiquette to request permission before speaking by words such as, 'Excuse me, may I speak with you?'. The person approached would then be given an opportunity to refuse by replying, 'No, you may not speak to me'. Likewise, in the online world, a person should not be forced to read a spammer's communication – the recipient of the communication should be allowed to ignore the spammer's request to send the communication until they wish to receive it. Accordingly, an opt-out regime does not provide consumers with the same level of protection in the online environment than they enjoy offline.

Second, an opt-out regime gives spam undeserved legitimacy. The legitimisation of some spam could defeat one of the main purposes of anti-spam legislation, which is to decrease the costs and burdens associated with preventing the increase in spam. An opt-out regime would encourage people and organisations to persist in their spamming activities legitimately.[42] This is demonstrated in South Korea, where the announcement of proposed opt-out anti-spam legislation was interpreted by some residents as legitimising all spam provided it was opt-out based. This resulted in a sudden increase in South Korean spam volumes.[43] Indeed, the Coalition Against Unsolicited Commercial Email has announced that 'the [CAN-SPAM Act] fails the most fundamental test of any anti-spam law, in that it neglects to actually tell any marketers not to spam.'[44]

Third, an opt-out regime forces consumers to take action to block subsequent messages,[45] which contradicts email common sense. It is common for email users not to respond to spammers, not even in response to requests to unsubscribe. In fact, ACMA advises consumers that it is generally unwise to open or reply to any email that appears to be from a spammer, because this confirms to the spammer that the email address is 'live', which will be an incentive for the spammer to continue sending spam to that email address.[46] Thus, an opt-out regime is likely to be ineffective given that most email users adopt the pragmatic approach of never responding to unsolicited email.[47]

However, an opt-out regime is not without merit. Consider a situation where Ruth wishes to purchase an iPod. She receives an unsolicited commercial email from a reputable retailer with which she has never transacted. In its email, the retailer offers to sell the iPod to Ruth for half the price offered by any other retailer she has contacted previously. If this email had been sent to Ruth who had no intention of purchasing an iPod, the email would be considered to be spam. However, Ruth may wish to receive such email as it would enable her to purchase the iPod at a lower price and save time so that she would not be required to undertake additional shopping. This scenario demonstrates that while some people may consider spam messages to be helpful and relevant, an opt-in regime will prevent them from receiving the benefit of these messages.[48] Moreover, an unsolicited commercial electronic message may be extremely relevant to some people, mildly relevant to others and absolutely irrelevant to the rest. In fact, one writer believes that spam not only enables transactions to take place which would otherwise not occur as a result of prohibitive search costs or lack of consumer awareness about products which satisfy their needs, but also is able to fill gaps left by other advertising media, and therefore can contribute to market economies.[49] An opt-in regime could even stifle the development and expression of ideas on the internet.[50]

Further, in the offline world, consumers regularly tolerate irrelevant advertisements in other media, such as

on billboards and television, with less annoyance than they feel toward unsolicited commercial electronic messages,[51] and so the need for a recipient to consent to receiving irrelevant spam would be incompatible with the absence of needing consent to view irrelevant advertisements in other media. It is interesting to note that the Australian Government's concerns about the exponential growth of spam and its threat to the effectiveness and efficiency of electronic communications, and indeed, anything that affects the functionality of email as a viable tool for online commerce,[52] has led it to choose an opt-in regime at the expense of the benefits of an opt-out regime discussed previously. This suggests that the Australian Government could be more concerned about the detrimental effects of spam on commercial and network efficiency than other issues such as the content of spam messages or their social impact.

Some commentators, however, believe that whether consent is opt-in or opt-out is not the main issue. Rather, they argue that the crucial point is that an unsolicited electronic message should be permitted to be sent only where a valid pre-existing relationship exists between the sender and the recipient.[53] In this regard, the Spam Act provides that the recipient's consent may be reasonably inferred from the conduct of the recipient or business or other relationship with the sender, or if the electronic address of the recipient has been published according to certain criteria.[54] However, the CAN-SPAM Act only provides a narrow range of 'transactional or relationship messages' which can be sent on the basis of inferred consent, which includes messages sent to facilitate an ongoing transaction or relationship to, among other things, provide information about an employment relationship or related benefit plans, account balances, upgrades, product recalls, warranties, product safety and subscriptions.[55] The failure of the CAN-SPAM Act to provide a broad range of messages which can be sent on the basis of inferred consent, such as messages to consumers with whom the sender has a pre-existing or current business relationship, is in contrast with the Spam Act which permits organisations to contact past and present clients without having to obtain their express consent. The Spam Act therefore encourages businesses to communicate electronically with consumers, and promotes online commerce in accordance with the goals of the Australian Government.

While the opt-in regime adopted by the Spam Act has advantages over an opt-out regime, these advantages should be balanced against the potential disadvantages of an opt-in approach. One benefit of an opt-in regime is its obligation on the sender to obtain the recipient's prior consent to receive spam. However, an opt-in regime may also prevent a recipient from receiving spam which may be relevant to them. Given the Australian government's strong aim to reduce Australia as a source of spam and to minimise spam for Australian end-users,[56] an opt-in approach would appear to be the most effective solution to achieve this mandate.

Conclusion

This article has discussed the differences between the Spam Act and the CAN-SPAM Act in relation to their characterisation of spam, and their obligations on spammers to obtain the consent of the recipient to receive spam. It has found that the Spam Act's technologically neutral expression of spam limits its ability to regulate specific forms of spam, especially advertorial and pornographic email spam, and that its ability to regulate email spam could be improved by adopting certain principles contained in the CAN-SPAM Act. This article has also found that the Spam Act's opt-in regime is an effective method to protect consumers from unwanted spam in order to bring benefits in terms of improved efficacy of electronic communications and direct online marketing.[57]

The opinions expressed in this article are the author's own.

---

1 The National Office of the Information Economy, *Spam: Final report of the NOIE review of the spam problem and how it can be countered* (2003) 2.

2 'Average global ratio of spam in email scanned by MessageLabs' <http://www.messagelabs.com/publishedcontent/publish/threat_watch_dotcom_en/threat_statistics/spam_intercepts/DA_114633.chp.html> at 23 November 2005.

3 Don Evett, 'Spam Statistics 2004' <http://spam-filter-review.toptenreviews.com/spam-statistics.html> at 23 November 2005.

4 Pub L No 108-187, 117 Stat 2699 (2004).

5 On 1 July 2005, the Australian Broadcasting Authority and the Australian Communications Authority merged to become the Australian Communications and Media Authority.

6 Commonwealth, *Spam Bill 2003 Explanatory Memorandum*, 2002-2003, 1.

7 Spam Act s 6.

8 Spam Act s 25.

9 Ibid.

10 CAN-SPAM Act § 3(2)(A).

11 CAN-SPAM Act § 7(f)(1)(B)(i).

12 CAN-SPAM Act § 7(g)(1)(B)(i).

13 Commonwealth, above n 6, 5.

14 Ibid 5.

15 Spam Act s 16.

16 Commonwealth, above n 6, 5.

17 Bradley Holland, 'Spam: The end of the unsolicited era?' (10 March 2004) *CommsWorld* 4.

18 Ibid.

19 Ibid.

20 Emphasis added.

21 CAN-SPAM Act § 5(a)(1)(C).

22 Dan Fingerman, 'Spam Canned Throughout the Land? Summary of the CAN-SPAM Act With Commentary' (2004) 7(8) *Journal of Internet Law*, 4.

23 CAN-SPAM Act § 5(a)(5)(A).

24 US Federal Trade Commission, 'Subject Line Labeling As A Weapon Against Spam – A Report to Congress' (June 2005), i.

25 CAN-SPAM Act § 5(d)(1)(A).

26 US Federal Trade Commission, 'Court Stops Spammers from Circulating Unwanted Sexually-Explicit Emails' (11 January 2005) <http://www.ftc.gov/opa/2005/01/globalnetsolutions.htm> at 21 November 2004.

27 Report by MX Logic, Inc (9 June 2004) <http://www.mxlogic.com/news_events/6_09_04.html> at 15 November 2004.

28 Eric Goldman, 'Where's the Beef? Dissecting Spam's Purported Harms' (forthcoming) *John Marshall Journal of Computer & Information Law* 15.

29 CAN-SPAM Act § 3(2)(D).

30 Commonwealth, above n 6, 54.

31 Above n 1, 4.

32 Above n 22, 17.

33 Ibid.

34 Ibid.

35 Ibid.

36 Spam Act s 16.

37 CAN-SPAM Act § 5(a)(4).

38 Coalition Against Unsolicited Commercial Email, 'Statement on House Spam Bill Vote' (22 November 2003) <http://www.cauce.org/news>.

39 Elizabeth Alongi, 'Has the US Canned Spam?' 46 *Arizona Law Review* 263, 275, 287.

40 See <http://www.ftc.gov/opa/1999/12/oecdguide.htm>.

41 Sebastian Hughes, 'Avoiding the Toothless Tiger' – Effective Anti-Spam Legislation for Hong Kong' (2004) 58 *Intellectual Property Forum* 38, 41.

42 Jacquelyn Trussell, 'Is the CAN-SPAM Act the Answer to the Growing Problem of Spam?' (2004) 16 *Loyola Consumer Law Review* 175, 187.

43 John Corker, 'Scams and legal approaches to spam' (2002) 5(6) *Internet Law Bulletin* 61, 67.

44 Above n 38.

45 Trussell, above n 42, 183.

46 Australian Communications and Media Authority, 'Consumer Information: Anti Spam - Reporting, Complaints, Enquiries' <http://www.acma.gov.au/ACMAINTER.65690:STANDARD:836464639:pc=PC_1970 > at 21 November 2005.

47 Hughes, above n 41, 42.

48 Goldman, above n 28, 5.

49 Ibid.

50 Ibid.

51 Ibid.

52 Commonwealth, above n 6, 1.

53 Hong Kong Internet Service Providers Association, 'HKISPA Response to the Consultation Paper on the Proposals to Contain the Problem of Unsolicited Electronic Messages' (25 October 2004) 6.

54 Spam Act sch 2 ss 2, 4(2).

55 CAN-SPAM Act § 3(17).

56 Commonwealth, above n 6, 1.

57 Commonwealth, above n 6, 22.

Please give me a Privacy Card

Andrew Perry, legal.consult Pty Limited

Andrew Perry is a Director, Legal & Technology for legal.consult Pty Limited. He is also the President of the Committee for the New South Wales Society for Computers & Law.

The issue of an Australia Card briefly raised its head again this year, following the London terrorist bombings committed by British citizens.

There is no question that times have changed since the Australia Card debate swept Australia in the early 80's. Australians, like the citizens of many other western countries, are far more willing to trust their government with powers that impinge civil liberties generally, and privacy in particular.

On 10 May 2005, the Attorney General and Minister for Justice and Customs announced the allocation of $5.9 million over two years in the 2005-6 budget, "to initiate the development of a national identity security framework that is strong, comprehensive, consistent and interoperable".[1]

While the amount of funding is relatively small, the purpose of this funding is significant. The funding will be used for two pilot projects that will have clear implications for privacy in Australia.

The first project is known as the on-line document verifications service (**DVS**) pilot. The DVS pilot involves the development of a prototype system that can be used by the Department of Immigration and Multicultural and Indigenous Affairs (**DIMIA**) and the Department of Foreign Affairs and Trade (**DFAT**) to check the accuracy of government documents presented to them against existing government databases including DIMIA, DFAT, drivers licence and births, deaths and marriages (**BDM**) databases.[2]

The stated goal of the DVS pilot is to test the effectiveness of online, real-time document verification in reducing the time and improving the accuracy of validating identity documents.[3] It is proposed as part of the Government's strategy for "A Safer Australia."

The Minister and Attorney General have sought to reduce concerns regarding the privacy implications of the DVS with an assurance that the system will:

(a) only validate with a "yes" or "no" the information contained in the document provided by the individual;

(b) not allocate an identifying number; and

(c) not store personal details on a database.[4]

These reassurances reflect the outcry in the 80's over the prospect of government agencies using a common identifier such as an Australia Card number to identify individuals and thereby create a large intelligence database using data matching.

Ironically, despite the apparent recognition of the Australia Card debate in the DVS pilot, the second project being funded from the 2005-6 Budget is the "Accuracy of data on an Australian Government database pilot" (**Data Matching Pilot**).[5]

The Data Matching Pilot will test the accuracy of 25,000 Australian Tax Office records through cross-agency data matching against DIMIA, DFAT, BDM, Health Insurance Commission, Australian Electoral Commission, Centrelink and drivers licence databases.[6]