Canning the spam five years on: a comparison of spam regulation in Australia and the US

Kayleen Manwaring

Kayleen Manwaring

Kayleen Manwaring *previously practised in technology law in Australia and the United Kingdom, and now works in knowledge management at Blake Dawson. This article was written while the author was a student in the LLM program at the University of New South Wales. The views expressed are those of the author only*

1 Introduction

This note outlines the current regulation of spam in Australia. This regulation is compared to that of the United States, the jurisdiction from which the spam problem originated and which still dominates the worldwide spam landscape today.

This note also contains a brief introduction to issues of the effectiveness of spam regulation that need to be further considered in both the domestic and international spheres.

2 The current state of play

The National Office for the Information Economy delivered its seminal report on spam in Australia in 2003[1] (**NOIE Report**). In response, the Australian government enacted significant restrictions on the sending of "unsolicited commercial electronic messages", bringing the *Spam Act 2003* (Cth) (**Spam Act**) into effect on 10 April 2004.

Spam and e-marketing was not completely unregulated before the Spam Act, but the coverage was patchy and mostly untargeted.[2]

The passing of the Spam Act in Australia followed close upon the heels of federal legislation in the United States also dealing with commercial messages. *The Controlling the Assault of Non-Solicited Pornography and Marketing Act 2003* (**CAN-SPAM Act**) came into effect on 1 January 2004. However, the CAN-SPAM Act contains significant differences to the Spam Act, in particular in its choice of an opt-out model. It is pertinent to compare the two in detail as the US, despite the existence of the CAN-SPAM Act, still ranks as the world's No 1 in spam creation.

A comparison of the major provisions of the Spam Act and the CAN-SPAM Act is set out below in Table 1:

Table 1: Comparison of key provisions

Concept	Australia	USA
	(All references to Spam Act unless otherwise specified)	**(All references to CAN-SPAM Act unless otherwise specified)**
Coverage	"Spam" not defined. Act regulates "unsolicited commercial electronic messages" with an Australian link (**UCEM**). An **electronic message** is a message sent using an Internet carriage service or other listed carriage service to an electronic address connected to an account (s5(1)). "Electronic address" includes email addresses and telephone numbers. **Commercial** (s6(1)) Message designed to achieve one of a number of specified commercial purposes eg: • offering to supply/provide, advertising or promoting goods, services, land, business opportunities or investment opportunities; • advertising or promoting suppliers or prospective suppliers/providers of the above; and • assisting or enabling a person, by a deception, to dishonestly obtain a financial advantage or obtain a gain from another.	"Spam" not defined. Act regulates "commercial electronic mail messages" (**CEMM**). A **commercial electronic mail message** is "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service" (s3(2)). The definition excludes a "transactional or relationship message", messages sent as part of an existing transactions or business relationship (s3(17)).

Concept	Australia	USA
Jurisdiction	**Australian link** (s7): • message originating in Australia; • sender or addressee physically in Australia or an organisation centrally managed and controlled in Australia; • message being accessed by a computer, server or device in Australia; • for a message sent to a non-existent address, it being reasonably likely that (if the address existed) the message would have been accessed using a computer, server or device in Australia.	No specific jurisdictional requirements, but extra-territoriality may be confined to foreign **businesses** sending email communications to a US recipient[3].
Who can bring an action?	Australian Communications & Media Authority (**ACMA**) (ss 26, 32, 38, 41). Anyone who has suffered loss or damage ("victims" may include both individuals and organisations) can bring a claim for compensation (s28), but this is dependent on a previous successful civil penalty claim by the ACMA (s28(1)(a)).	Federal Trade Commission (**FTC**) (s7(a), other federal agencies (s7(b)), state attorneys-general and state agencies (s7(f)). Affected ISPs (s7(g)). No right for individuals.
Opt-in / opt-out	Opt-in Consent must be obtained **before** sending UCEM (s16). Consent can be given **expressly** or it can be **reasonably inferred** from the conduct, business and other relationships of the recipient of the message. Consent **not** inferred from **mere publication** of the recipient's email address. Guidelines on inferring consent contained in Schedule 2 and further guidance given by the Federal Court in *Australian Communications and Media Authority v Clarity1 Pty Ltd* [2006] FCA 410.	Opt-out Prior consent need **not** be obtained before sending CEMM. Legislation merely "prohibit[s]...transmission of commercial electronic mail after objection" (s5(a)(4)).
Other basic rules	UCEM must: • include accurate sender information (s17); and • contain a functional unsubscribe facility (s18).	CEMM must: • not contain false or misleading sender information or subject lines (s5(a)(1)-(2)); • contain a clear notice allowing the recipient to opt-out by request to the sender (s5(a)(5)); • contain a functioning return email address or other way to contact the sender (s5(a)(3)), and provide physical contact details (s5(a)(5)(ii)); and • identify itself as an advertisement (s5(a)(5)(i)).
Exemptions	**Exempt messages** "Designated commercial electronic messages" (Sch 1): • factual information only (with or without comment) (cl 2(1), Sch 1), can include company name and logo, author's contact details and sponsor ID; or • the message is sent under a reasonable mistake of fact. Telemarketing (voice) calls (exempted under s5(5) - regulated under *Do Not Call Register Act 2006*) Faxes (exempted under s6(7) Spam Act and cl 2.1 *Spam Regulations 2004*). **Exempt senders** Government bodies, registered political parties, religious organisations, charities and educational institution are exempt from most of the provisions of the Spam Act (Sch 1). Innocent intermediaries: • providers of carriage service only (s9); • employees may be protected from personal liability for messages sent as part of their work (s8(1)).	CAN-SPAM Act only regulates **email** messages. It does not include SMS, MMS, voice calls or faxes (s3(2)). Voice calls are regulated under the *Do-Not-Call Implementation Act 2003*. Faxes are regulated under the *Telephone Consumer Protection Act and the Junk Fax Prevention Act 2005*.

Concept	Australia	USA
Address harvesting	Prohibited supply, use and acquisition of address-harvesting software, harvested-address lists, or rights to use them (ss20-22). **Exemptions** • Suppliers with no reason to suspect that the lists were to be used to send UCEM (s20(2)), or that the customer had a relevant Australian connection (s20(3)) (onus of proof on defendant (s20(4)). • Users or acquirers of lists who did not use or intend to use them to send UCEM (ss21(2) and 22(2)).	No outright prohibition. However, if a spammer violates another section using harvested addresses, the violation is an aggravated offence subject to increased punishment (s4(b)).
Penalties	Civil penalties (up to $220,000 per day), and up to AUD1,100,000 for repeat offender companies) (Pt IV) Injunctions (Pt V) Compensation orders for "victims" (s28) Enforceable undertakings (Pt VI) Formal warnings (s41) No criminal penalties	Civil penalties: up to $16,000 per violation (ss 5(l) and (m) of the *Federal Trade Commission Act 1914*)[4] State agencies and ISPs may bring actions for damages (including aggravated damages) and apply for injunctions (s7) Criminal penalties: up to 5 years' imprisonment (US Code Title 18 USC s1037)
Other relevant law	*Criminal Code Act 1995* (Cth) (amended in 2001 to include the following offences): • access/modification of computer data and impairment of electronic communications (s477.1) • unauthorised impairment of electronic communications (s477.3) *Trade Practices Act 1974* • misleading and deceptive conduct (s52). *Privacy Act 1988* *National Privacy Principle* 2.1(c): special rules on how personal information can be used for the secondary purpose of direct marketing	For fraudulent emails: *Computer Fraud and Abuse Act 1986* *Racketeer Influenced and Corrupt Organizations Act 1970* *Electronic Communications Privacy Act 1986* Common law: cases based on "trespass to electrons" have had some limited success[5]
Codes of Practice	*ADMA eMarketing Code of Practice* *Internet Industry Spam Code of Practice* (both compulsory codes registered under the *Telecommunications Act 1997* (Cth)	

3 Issues with anti-spam legislation

On its face, the Australian Spam Act provides more effective legal protection for spam recipients than the US CAN-SPAM Act, especially because of its requirement of prior consent ("opt-in" rather than "opt-out"). However, the legislation is not without its problems, some of which are discussed below.

3.1 Opt-in versus opt-out

Australia's opt-in requirement has been generally hailed[6] (although not universally[7]) as the preferred model for anti-spam laws.

This model appears to be quite effective. A review of the Spam Act, conducted in 2006, noted a decrease in spam **originating** in Australia since its commencement[8]. By 2007, Australia had dropped from 10th to 37th on Sophos' list of spam-creating nations,[9] and has not reappeared in its top 12 list.

The US, with its opt-out model, continues to be No 1 on this list.[10] Spam has effectively been legalised by the opt-out provisions of the CAN-SPAM Act. In addition, the FTC's decision not to adopt a Do-Not-Email Registry[11] means that US recipients must still send an opt-out request to each individual organisation's CEMM, a heavy time and cost burden for both consumers and ISPs.

Effectiveness aside, the ideology behind a strict opt-in model such as that contained in the Spam Act is not unquestioned. The US opt-out model has been defended for protecting freedom of speech.[12] Even in Australia, the minority on the Senate Committee reviewing the Spam Act advanced an argument that not all unsolicited commercial messages are unwanted and that single emails to genuinely interested recipients ought to be permitted.[13] As some people respond to spam, the first part of that argument may have some validity.

3.2 Right to bring an action

Under the Spam Act, any "victim" of spam (including individuals and ISPs) may claim compensation, a right not available to individuals under the CAN-SPAM Act. However, that right is dependent on the ACMA bringing a successful civil penalty action. ISPs may bring actions for damages under the CAN-SPAM Act without similar restriction.

As a result, Microsoft alone has brought at least 92 lawsuits against spammers under the CAN-SPAM Act[14], while no ISP or individual court actions are reported in Australia.

The ACMA does appear to have been fairly active in enforcing the Spam Act[15]. However, some privately funded enforcement is to be preferred, and therefore a lifting of the Spam Act restriction should be considered.

3.3 The need for international cooperation

Unfortunately, despite its domestic effect, it appears that the Spam Act has not reduced the amount of spam actually received by Australians[16]. In fact, one report cites Australia as the fourth most-spammed country in the world for the month of March 2009, with a spam rate of 86.4%[17].

Worldwide, the story is equally as sombre. Despite a number of countries passing spam legislation in the 21st century[18], spam rates have escalated to a rate somewhere between 70-90%[19], and it appears that "[a]lthough domestic regulations have had some domestic impact, their effect has been negligible on a global scale".[20]

This outcome is not completely unexpected. It was acknowledged both in the NOIE Report[21] and in the CAN-SPAM Act[22] that domestic legislation could not be the only solution, considering that spam is by its nature and the practice of ISPs mostly unfettered by geographical boundaries. Two key recommendations in the NOIE Report encouraged engagement in international harmonisation and cooperation efforts[23].

Australia has been active in the area of international cooperation. Australian agencies and departments are signatories to a number of bilateral and multilateral anti-spam arrangements, and Australia has been involved with the International Telecommunications Union's (**ITU**) World Summit on the Information Society, the OECD Spam Task Force[24] and APEC's 2005 Lima Declaration on spam.[25]

Despite the high rates of current spam generation, some concrete results have already been achieved as a result of international cooperation. Nigeria was notorious in the 1990s as a safe haven for spam, but due to "diplomatic encouragement and pressure", the Nigerian government passed laws in 2002 requiring ISPs to filter all outbound email. It has been reported that spam email originating in Nigeria has been reduced as a result[26]. More recently, the ACMA's cooperation with an FTC investigation resulted in the freezing of assets of a New Zealander allegedly running a large Australian-based spam operation.[27]

However, concern exists that most, if not all of the international activity in which Australia has been involved are designed merely to promote cooperation between domestic enforcement agencies, and do not attempt to reach agreement on consistent regulation[28]. This creates problems where agencies wish to enforce a prohibition under their domestic legislation that is legal in the spammer's jurisdiction. For example, the tripartite arrangement signed between the US, UK and Australia only applies to conduct that is substantially similar to conduct which is illegal under the other signatories' spam laws.[29] The ACMA may well find it impossible to get US cooperation in enforcing the opt-in provisions of the Spam Act against a US spammer sending spam to Australian recipients.

With spam rates so high, and domestic legislation leading to no appreciable fall in the spam rate, it seems that mere cooperation, while critical for tracking down spam offenders, is not enough. Actual harmonisation of laws by means of an international treaty must be considered if the spam problem is to be properly addressed, and that some countries do not become or continue to be safe havens for spammers.[30] It has been suggested that the work done by the ITU, which has suggested the framework for a model law, may act as a good basis on which to build such an international instrument.[31]

3.4 ISPs and technological fixes

Technological fixes such as filtering and improved network security solutions are generally seen as much more effective than legislation in stopping spam. They "are not constrained by jurisdictional boundaries, or constitutional limitations[32]", and ISP level filtering systems have claimed success levels as high as 99.6%[33].

ISPs generally have far superior tools and knowledge to implement technological fixes than individuals. However, since fixes cost money, and many ISPs receive a commercial benefit from their spamming customers, it is difficult to ensure that technology is introduced when it should be.

One suggestion is that the law should be changed to hold ISPs accountable for inadequate technological fixes[34]. It has also been suggested that ISPs also need some clear legal protection against those who object to being blacklisted[35], as this has previously been used as a tool against anti-spam organisations[36].

Australia has gone part of the way with its enforceable code of practice governing ISPs[37], but this does not go far enough, as it does not go so far as to require ISPs to implement anti-spam technologies.

4 Conclusion

Australia has strong legislation regulating spam and limiting unsolicited e-marketing, and this has been effective in reducing the amount of spam created domestically. Australian domestic regulation compares well to the United States, although enforcement could be improved and the legislation's effect on free speech is somewhat questionable.

However, as contemplated when the legislation was passed, domestic legislation is insufficient to eliminate spam, or even reduce it to an acceptable level. International law enforcement cooperation efforts cannot solve the problems of conflicting obligations in a cross-jurisdictional problem. Legislative support must also be given to support worldwide legislative harmonisation and effective technological solutions.

[1] National Office for the Information Economy, *Spam: Final Report of the NOIE Review of the Spam Problem and How it can be Countered*, Canberra, 2003

[2] See "Other Relevant Law" row in Table 1

[3] Hladjk, J, "Effective EU and US approaches to spam? Moves towards a co-ordinated technical and legal response – Part I", *Communications Law*, Vol 10, No 3, 2005 at 76-77

[4] Adjusted for inflation on 2 February 2009 as part of new Federal Trade Commission Rules, FTC 16 CFR Part 1

[5] See Lawrence, A, *The law of ecommerce*, LexisNexis, 2003 (loose leaf) at [110,230] and [30,470] for more detail

[6] Eg Schryen, G, "Anti-spam legislation: an analysis of laws and their effectiveness", *Information & Communications Technology Law 2007*, 16(1) at 26; Linford, S, "Follow Australia!", 19/7/04, http://www.spamhaus.org/news.lasso?article=154; and Boone-Lutz, S, "Just say yes: drug trafficking treaties as a model for an anti-spam convention", 39 *George Washington International Law Review* 367 (2007) at 393

[7] See the discussion in Bolin, R, "Opting out of spam: a domain level Do-Not-Spam registry", 24 *Yale Law & Policy Review* 399 (2006)

[8] Australian Government Department of Communications, Information and the Acts, "Report on the *Spam Act 2003* Review", June 2006, at 14

[9] http://www.acma.gov.au/WEB/STANDARD/pc=PC_310314

[10] Sophos Plc, "Security threat report: 2009", available at http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf. See also Spamhaus' current top 10 list, see http://www.spamhaus.org/statistics/countries.lasso, accessed on 13 April 2009

[11] Federal Trade Commission, "National Do Not Email Registry: A Report to Congress", June 2004

[12] Rogers, KM, "Viagra, viruses and virgins: a pan-Atlantic comparative analysis on the vanquishing of spam", *Computer Law & Security Report* 2006, 22(3) at 234

[13] Senate Environment, Communications, Information Technology and the Arts Legislation Committee, "Provisions of the Spam Bill 2003 and the Spam (Consequential Amendments) Bill 2003", October 2003 at 26

[14] Microsoft Trustworthy Computing, " Microsoft: Can-Spam and Global Efforts to Combat Cyber Crime", March 2008, available at http://download.microsoft.com/download/2/2/D/22DFC1E7-0260-4AF7-8B81-D3D17ADA5A05/Support_for_CAN_SPAM_Mar08.doc

[15] http://www.acma.gov.au/WEB/STANDARD/pc=PC_310314

[16] Boone-Lutz, S, "Just say yes: drug trafficking treaties as a model for an anti-spam convention", 39 *George Washington International Law Review* 367 (2007) at n 153

[17] http://www.messagelabs.com.au/mlireport/MLIReport_2009.03_Mar_FINAL.pdf

[18] Eg the US, the UK and other EU countries, China, Australia, Japan, (http://www.oecd-antispam.org/countrylaws.php3), New Zealand, Israel, Pakistan, Singapore (http://en.wikipedia.org/wiki/E-mail_spam_legislation_by_country)

[19] The NOIE Report in 2003 (at 2.4) cited an estimate of worldwide spam rates at 20% for all email, and 35% for business email. More recently, MessageLabs reported worldwide rates based on spam caught by its filtering agencies at: 86.2% (2006), 84.6% (2007), 81.2% (2008), 74.5% (Q1 2009) – see annual (2006-2008) and monthly (Jan, Feb, Mar 2009) reports at http://www.messagelabs.com.au/intelligence.aspx. Spamhaus currently estimates a rate of 90%: http://www.spamhaus.org/effective_filtering.html

[20] Boone-Lutz, S, "Just say yes: drug trafficking treaties as a model for an anti-spam convention", 39 *George Washington International Law Review* 367 (2007) at 386-7

[21] National Office for the Information Economy, *Spam: Final Report of the NOIE Review of the Spam Problem and How it can be Countered*, Canberra, 2003 at 1.2

[22] S2(12)

[23] National Office for the Information Economy, *Spam: Final Report of the NOIE Review of the Spam Problem and How it can be Countered*, Canberra, 2003, Recommendations 4 and 5, at 1.3

[24] http://www.acma.gov.au/WEB/STANDARD/pc=PC_310313

[25] The sixth APEC ministerial meeting on the telecommunications and information industry (TELMIN6) (1-3 June, 2005 Lima, Peru), Lima Declaration, available at http://www.apec.org/apec/ministerial_statements/sectoral_ministerial/telecommunications/2005/annex_e.html#guideline

[26] Soma, J, Singer, P, Hurd, J, "Spam Still Pays: The Failure of the CAN-SPAM Act of 2003 and Proposed Legal Solutions", 45 *Harvard Journal on Legislation* 165 (2008) at 195

[27] Moses, A, "World's largest spam bust linked to Australia", *Sydney Morning Herald*, 15/10/08, available at http://www.smh.com.au/news/technology/biztech/usfreezes-assets-of-spam-king/2008/10/15/1223750102617.html?page=fullpage#contentSwap1

[28] Boone-Lutz, S, "Just say yes: drug trafficking treaties as a model for an anti-spam convention", 39 *George Washington International Law Review* 367 (2007) at 386

[29] Memorandum of Understanding on mutual enforcement assistance in commercial email matters, cl 1(H), definition of "Spam Violations", available at http://www.acma.gov.au/webwr/consumer_info/spam/spam_mou-aus_uk_usa.pdf

[30] Boone-Lutz, S, "Just say yes: drug trafficking treaties as a model for an anti-spam convention", 39 *George Washington International Law Review* 367 (2007) at 386-393

[31] Schryen, G, "Anti-spam legislation: an analysis of laws and their effectiveness", *Information & Communications Technology Law* 2007, 16(1) at 28

[32] Isreb, S, "Can the Spam Act 2003 independently protect the public against spam, or are additional legally sanctioned technology solutions required?", (2006) 11 *Media Arts & Law Review* 272 at 296

[33] The Spamhaus Project, "Effective Filtering", http://www.spamhaus.org/effective_filtering.html

[34] Soma, J, Singer, P, Hurd, J, "Spam Still Pays: The Failure of the CAN-SPAM Act of 2003 and Proposed Legal Solutions", 45 *Harvard Journal on Legislation* 165 (2008) 186

[35] Isreb, S, "Can the Spam Act 2003 independently protect the public against spam, or are additional legally sanctioned technology solutions required?", (2006) 11 *Media Arts & Law Review* 272

[36] See eg cases brought by e360Insight (who had been blacklisted) against anti-spam organisation The Spamhaus Project and the ISP Comcast, http://www.spamhaus.org/legal/answer.lasso?ref=3

[37] Internet Industry Association, Spam Code, 16 July 2006, available at http://www.iia.net.au/index.php/codes-of-practice/spam/spam-code.html

Bibliography

Australian Communications & Media Authority, www.acma.gov.au

Australian Government Department of Communications, Information and the Acts, "Report on the *Spam Act 2003* Review", June 2006

Australian Senate, Environment, Communications, Information Technology and the Arts Legislation Committee, "Provisions of the Spam Bill 2003 and the Spam (Consequential Amendments) Bill 2003", October 2003

Bolin, R, "Opting out of spam: a domain level Do-Not-Spam registry", 24 *Yale Law & Policy Review* 399 (2006)

Boone-Lutz, S, "Just say yes: drug trafficking treaties as a model for an anti-spam convention", 39 *George Washington International Law Review* 367 (2007)

Federal Trade Commission (US), www.ftc.gov

Hladjk, J, "Effective EU and US approaches to spam? Moves towards a co-ordinated technical and legal response – Part I", *Communications Law*, Vol 10, No 3, 2005 at 71

Internet Industry Association, Spam Code, 16 July 2006, available at http://www.iia.net.au/index.php/codes-of-practice/spam/spam-code.html

Isreb, S, "Can the Spam Act 2003 independently protect the public against spam, or are additional legally sanctioned technology solutions required?", (2006) 11 *Media Arts & Law Review* 272

Lawrence, A, *The law of e-commerce*, LexisNexis, 2003 (loose leaf)

Linford, S, "Follow Australia!", 19/7/04, available at http://www.spamhaus.org/news.lasso?article=154

MessageLabs Ltd, www.messagelabs.com

Microsoft Trustworthy Computing, "Microsoft: Can-Spam and Global Efforts to Combat Cyber Crime", March 2008, available at http://download.microsoft.com/download/2/2/D/22DFC1E7-0260-4AF7-8B81-D3D17ADA5A05/Support_for_CAN_SPAM_Mar08.doc

Moses, A, "World's largest spam bust linked to Australia", Sydney Morning Herald, 15/10/08, available at http://www.smh.com.au/news/technology/biztech/us-freezes-assets-of-spam-king/2008/10/15/1223750102617.html?page=fullpage#contentSwap1

National Office for the Information Economy, *Spam: Final Report of the NOIE Review of the Spam Problem and How it can be Countered*, Canberra, 2003, available at http://www.security.iia.net.au/downloads/spamreport.pdf

Rogers, KM, "Viagra, viruses and virgins: a pan-Atlantic comparative analysis on the vanquishing of spam", *Computer Law & Security Report* 2006, 22(3), 228-240

Schryen, G, "Anti-spam legislation: an analysis of laws and their effectiveness", *Information & Communications Technology Law* 2007, 16(1), 17-32

Soma, J, Singer, P, Hurd, J, "Spam Still Pays: The Failure of the CAN-SPAM Act of 2003 and Proposed Legal Solutions", 45 *Harvard Journal on Legislation* 165 (2008)

Sophos Plc, www.sophos.com

The Spamhaus Project, www.spamhaus.org

Season Greetings and Happy New Year to all and thank you to everyone who contributed to the Journal in the last year.