MONASH University

**Corporate Law and Accountability Research Group**

**September 2006**

**Working Paper No. 2**

# AUSTRALIA'S SPAM LEGISLATION: A MODERN-DAY KING CANUTE?

**Mark Robert Bender**

The Corporate Law and Accountability Research Group (CLARG) was established in the Department of Business Law and Taxation, Faculty of Business and Economics, Monash University, in November 2005.

CLARG invites the submission of papers for publication in its Working Paper Series.

Submissions on corporate law, corporate governance and corporate accountability issues as well as related topics such as corporate governance and labour law, and corporate environmental and social responsibility are welcomed. For details, go to: http://www.buseco.monash.edu.au/depts/blt/clarg/working_papers.php

# AUSTRALIA'S SPAM LEGISLATION: A MODERN-DAY KING CANUTE?

**MARK ROBERT BENDER**[1]

## ABSTRACT

This paper considers a number of aspects of Australia's recently introduced unsolicited commercial email (UCE or spam) legislation, the *Spam Act 2003* (Cth). The magnitude and nature of the harm caused by the spam problem is outlined, as are the key provisions of the legislation enacted in an attempt to reduce spam. Observations are made as to some of the perceived shortcomings of the Act, and of lawmakers' approaches in general in trying to legislate against spam. The fundamentals of Australia's legislative approach are contrasted with those of the corresponding US legislation and some key distinctions drawn, notably the 'Opt-In' / 'Opt-Out' dichotomy, Australia having used the former approach, while the US used the latter. Some alternative approaches and suggested enhancements to the Australian legislation are also considered, including proposals by Bill Gates and Lawrence Lessig. Finally there is a summary of and some limited comment on the first case brought under the Australian legislation.

## I INTRODUCTION

According to legend, King Canute was assured by his advisers that he had such great power that he could stop the incoming ocean tide. He made the point of demonstrating to his courtiers that even the power of the king had limits. This paper discusses lawmakers' responses to the growing tide of unsolicited email, considering the Australian and US legislative approaches and some potential additional approaches to combat the growing spam problem.

The internet generally has proved an extremely complex area for the law, challenging existing legal paradigms including evidence, privacy, contract, intellectual property,

[1] Legal Practitioner of the Supreme Court of the ACT, Barrister of the High Court of Australia, LLB (Hons), BBus (Bus Law), Department of Business Law and Taxation, Faculty of Business and Economics, Monash University; Member of the Corporate Law & Accountability Research Group. Contact: mark.bender@buseco.monash.edu.au

international law and jurisdictional issues. Many aspects of the law have struggled to deal with the rate of technological change that has typified developments in computing generally and the internet specifically.

Email has been frequently described as the 'killer application' of the internet. This term refers (somewhat paradoxically) to the compelling usefulness and application of the technology, rather than a measure of how lethal it may be. Email has proved to be of immense value and utility, but its efficiency is now being undermined by an insidious scourge, that of unsolicited commercial email (UCE) colloquially known as spam.

The consensus as to the etymology of the term spam seems to be that:

> it was derived from the widely popular Viking Spam skit from Monty Python…the couple in the cafe could not hold a conversation over the din of vikings yelling and singing "spam, spam, spam, spam". It seems quite analogous to the problem of having intelligent conversation on a newsgroup when there is a mass of unrelated trash to wade through.[2]

An alternate suggestion as to the term's origins suggests that it is analogous to throwing a chunk of spam (a brand of tinned meat[3]) at a fan. Interestingly, it has been reported that a law firm was one of the first spammers.[4]

This paper initially considers some general background issues relevant to the spam problem, and challenges facing lawmakers attempting to deal with the problem. The Australian legislative approach to spam is discussed, contrasted briefly with the US legislative approach, and some perceived shortcomings of the Australian legislative response are highlighted, as are some suggested alternative approaches. Australia's first (and only, at the time of writing) case under the anti-spam legislation is also discussed.

## II THE PROBLEM

The Second Reading Speech for the *Spam Act 2003* (Cth) (the Act) suggested that the volume of spam 'threaten(s) the effectiveness and efficiency of electronic communication and legitimate online business'[5]. Others have gone further, suggesting that spam is 'tearing at the very fabric' of the internet.[6]

There seems to be no shortage of evidence as to the magnitude of the problems attributable to UCE, or spam. While estimates vary, the National Office for the Information Economy (NOIE) cited data from the Gartner Group, a leading IT research and consulting firm, estimating that 50% of all inbound business email

---

[2] John W. Cobb, <http://english.ttu.edu/kairos/1.3/inbox/moo/cspam.html> at 29 April 2004; Brad Templeton, <http://www.templetons.com/brad/spamterm.html> at 28 July 2006.
[3] <http://www.spam.com?> at 5 March 2006.
[4] Brad Templeton, <http://www.templetons.com/brad/spamterm.html> at 28 February 2006.
[5] Commonwealth, *Parliamentary Debates*, House or Representatives, 18 September 2003, 20441 (Mr McGauran, Minister for Science).
[6] Peter Coroneos, 'Perceptions of Spam' (2003) 6(5) *Internet Law Bulletin*.

messages were spam in 2005.[7] Whether the exact metrics of this assessment are accurate seems moot. Anyone with an email account would acknowledge there is a significant and growing spam problem.

Once again, there is much data available detailing the extent and nature of the symptoms of this problem. Productivity loss, monetary loss at the hands of fraudulent spammers and children's exposure to offensive or inappropriate content are frequently cited as the consequences of spam. European and US studies (in 2001 and 2002)[8] cited by NOIE attempted to quantify some of these costs, suggesting costs to business in these regions alone exceed AUD$33 billion annually. In the Second Reading Speech for the Spam Bill 2003 (Cth), the cost of spam to business was cited as $900 per employee, per year.[9] According to Australian Bureau of Statistics (ABS) data, the total number of employees (both private and government) in 2002 – 2003 was 9,441,300[10]; if the government's figures are used, then the annual financial cost to Australia from spam is approximately AUD$8.5 billion.

There are broadly two general sub-segments of spammers, or people that send unsolicited commercial email: those that are driven by 'commercial' outcomes, including those that seek gain fraudulently or illegally; and those that are motivated by other factors, such as virus perpetrators. It is outside the scope of this present discussion to specifically consider the latter in any detail.

Consideration of the 'commercially' motivated spammers' position would seem relevant to assist in determining the appropriateness and likely effectiveness of countermeasures (legal and otherwise) that can be taken against them. The nature and magnitude of penalties would be expected to have some deterrent effect on some spammers who may refrain from the practice on risk/reward considerations. It is typically anticipated by lawmakers that the criminalisation of any given activity may be expected to reduce such activity in some measure. However the actual effect that criminalisation and associated penalties will have on the spam problem remains to be seen. Research on deterrent theory suggests that criminalization and penalization as means of reducing criminal behavior is far from conclusive, suggesting that criminalisation and associated penalties may not always lead to a marked reduction in undesired behavior[11]. Ultimately, the effectiveness or otherwise of external measures, such as the US legislation and international countermeasures, will likely be the key determinant of spam levels in Australia, given that most spam arriving in Australia

---

[7] Commonwealth, National Office of the Information Economy, *Spam; Final report of the NOIE review of the spam problem and how it can be countered* (2003) 9 <http://www.dcita.gov.au/__data/assets/pdf_file/21064/SPAMreport.pdf > at 30 August 2006.

[8] Commission of the European Communities, *Unsolicited Commercial Communications and Data Protection: Summary of Study Findings* (2001) 9 (Note: all currency conversions as at 31 January 2003) <http://www.csp.it/irisi/pdf/sum_SPAM.pdf> at 14 August 2006;
Ferris Research, *Spam Control: Problems and Opportunities* (2003) <http://www.ferris.com/view_content.php?o=Email&id=105&>; see also <http://www.internetnews.com/IAR/artcle.php/1564761>.

[9] Above n 5.

[10] Australian Bureau of Statistics, *Small Business in Australia*, 23 October 2002, <http://www.abs.gov.au/Ausstats/abs@.nsf/Lookup/598FB856F3D486B5CA256DEA00053A2E> at 30 April 2004.

[11] See for example Isaac Ehrlich, 'The Deterrent Effect of Criminal Law Enforcement' (1972) 1(2) *The Journal of Legal Studies* 259-276.

originates from offshore.

It has been suggested that one reason spam volumes will continue to increase will be the falling yields, or response rates, that spammers generate for a given number of messages they send, leading them to send more and more messages to generate the outcomes they have had in the past.[12] A purported key plank of the Australian government's approach is education, notionally resulting in better-informed, less susceptible, less responsive spam recipients, which is likely to lead to spammers having to send more spam. This situation highlights a particularly circular circumstance, one that would appear to be difficult, if not impossible to defeat with legislative approaches alone. This point obviously also applies to technical and other non-legal responses – the more successful they are, the more messages spammers will have to send to achieve their outcomes.

The costs of sending spam are very low, almost non-existent. Other intrusive forms of solicitation, 'such as the phone or even being accosted by beggars on the street have costs that put limits on their volume - spam lacks that limiting force'.[13] It is suggested that massive disincentives must be created as deterrents. Reducing yields through education and technological responses may make the spammers simply work harder and smarter and will probably have little deterrent effect.[14]

## III THE AUSTRALIAN LEGISLATIVE APPROACH

Although there are numerous alternative definitions of spam in use, it would seem prudent for the purposes of this paper to utilise those definitions adopted in the Commonwealth's *Spam Act*[15] ('the Act'). The Act defines spam as 'unsolicited commercial electronic messages'.[16] Some of the individual elements of this moniker are also given detailed statutory definitions under the Act.[17]

Commercial electronic messages that are covered by the Act include both internet-based messaging, such as email and instant messaging (iM) and mobile phone-based messaging, such as short message service (SMS) and multimedia message service (MMS). Voice-to-voice communication by telephone (including Voice over Internet Protocol or VOIP), messages sent by facsimile, non-electronic messages (such as ordinary mail and flyers) and internet advertising such as 'pop up' windows and 'banners' that appear on World Wide Web (WWW) sites are expressly excluded from the ambit of the Act. The Regulations provide for these definitions to be amended to accommodate new technology. One such new technology is text messaging to fixed

[12] Katya Culberg 'Regulating The Proliferation And Use Of Spam' (2002) 6(3) *Journal of Internet Law*.
[13] Brad Templeton, *Essays on Junk email (spam)* <http://www.templetons.com/brad/spam/> at 27 March 2004.
[14] Robert Lemos, *Spam could soon be majority of e-mail* <http://www.zdnet.com.au/news/business/0,39023166,20267797,00.htm> at 29 March 2004.
[15] *Spam Act 2003* (Cth).
[16] Above n 16, ss 4 - 6.
[17] Ibid.

line telephones.[18]

For the Act to apply, the message (or one of its purposes) must be commercial in nature. Commerciality under the Act is to be determined with regard to the purpose, content and presentation of the message itself, or content that can 'be located using the links, telephone numbers or contact information (if any) set out in the message'[19] - for example, the information displayed at a website that the message directs or links the reader to.

The Act defines messages as commercial, 'where … it would be concluded that the purpose, or one of the purposes, of the message is' to offer, advertise or promote goods, services, land or an interest in land, business or investment opportunities or a supplier, or prospective supplier, of such.[20] Presumably this characterisation is made by the administrative arm of government in determining the existence or otherwise of a breach in the first instance. Messages that assist or enable a person to dishonestly obtain property, a gain or financial advantage from another person by deception are also categorized as commercial messages under section 6. It is immaterial whether the goods, services, land, interest or opportunity exists, or whether it is lawful to acquire them. The definitions under section 6 seem not to be an exhaustive list, with section 6(1)(p) providing that any purpose specified in the regulations will also be covered.

Under the Act, there is no requirement that a message be sent or received in bulk; indeed, a single message can be considered spam. Lack of prior consent, either express or 'reasonably inferred' from conduct and business and other relationships[21] on the part of the recipient is also required for messages to be regarded as unsolicited under the Act. Generally (subject to some statutory exceptions) consent 'may not be inferred from the mere fact that the relevant electronic address has been published'.[22]

The Act provides for ancillary liability, which arises where parties authorise, aid, abet, counsel, procure, conspire, induce or are knowingly concerned with contravention.[23] Carriage service providers such as Internet Service Providers (ISPs), are generally expressly excluded from primary or ancillary liability under the Act when they have not been knowingly involved in a breach. Presumably, parties whose computers, accounts, networks and services are used by spammers without their knowledge or consent will also be free from liability. The practice of hijacking resources of innocent third parties, known as 'zombies', is somewhat common among spammers, leading many ISPs and corporations to implement technical solutions in attempts to prevent such abuses, such as firewalls, open relay blocking and other technical security measures.

Although innocent third parties whose assets have been hijacked are not likely to have any liability under the Act, it will be interesting to observe whether, over time, potential liability may lie in tort - for example, against parties that fail to take

[18] See for example *Telstras TalkingText*™ <http://www.telstra.com.au/talkingtext/index.htm> at 19 April 2004.
[19] Above n 16, s 6 (1)(c).
[20] Above n 16, s 6.
[21] Above n 16, Sch 2 Cl 2.
[22] Above n 16, Sch 2 Cl 4(1).
[23] Above n 16, s 16 (9).

adequate steps to prevent their facilities being used by spammers to cause damage to third parties.

The use of electronic address harvesting software, or lists generated using such software, is prohibited 'where it is intended to be used to send unsolicited commercial electronic messages in contravention of section 16'.[24]

According to a document jointly published by the Australian Communications Authority (ACA) and NOIE, harvesting software and harvested lists may still be used 'for legitimate purposes such as collecting data for research, marketing or maintaining websites'[25]. The suggestion that marketing is a legitimate purpose for the use of harvesting software and/or harvested list seems at odds with the purposes of the Act. This ACA/NOIE document also states that lists generated manually (for example by reviewing websites) are not prohibited. According to the Explanatory Memorandum[26], the prohibition on harvested lists extends to cover lists produced before the commencement of the Act.[27] A potential loophole seems to exist here, especially in relation to mobile phone numbers, many of which are listed in phone directories and therefore could relatively easily be extracted without the use of harvesting software.

The Act has ostensibly adopted an 'Opt-In' approach: that is, as a general proposition, consent of the receiver must be obtained prior to sending a message to them. The alternate model, 'Opt-Out'(adopted in the US Federal legislation), does not require consent of the recipient of a message, but requires that a recipient specifically request removal and that such requests are acted upon by the sender by refraining from sending messages in the future.

## IV ISSUES ARISING FROM THE AUSTRALIAN LEGISLATIVE APPROACH

### A *Spam largely originates outside Australia*

Then Attorney General, Daryl Williams, succinctly highlighted a critical (and what may well prove to be ultimately fatal) shortcoming of the Government's approach: 'Enforcement of the new law against overseas-based spammers will be dependent on the cooperation of other jurisdictions.'[28]

The deficiency of relying on domestic legislation alone (even if coupled with other 'soft' measures, such as education), and indeed any unilateral legislative-only approach taken by other national governments, is obvious, as the spam problem is a global problem with the vast majority of spam originating from outside Australia.

---

[24] Above n 16, Part 3.

[25] National Office of the Information Economy, *Spam Act 2003: A practical guide for business* (2004) <http://www.dcita.gov.au/__data/assets/pdf_file/20455/Spam-4-Business-Web-4-2.pdf> at 10 August 2006.

[26] Explanatory Memorandum, Spam Bill 2003 (Cth). <http://www.scaleplus.law.gov.au/html/ems/0/2003/0/2003092501.htm> at 24 June 2006.

[27] Ibid.

[28] Daryl Williams, 'Spam Act Becomes Law' (Press Release, 19 December 2003) <www.darylwilliams.dcita.gov.au/Article/0,,0_7-2_4011-4_117569,00.html> at 6 March 2006.

Peter Coroneos, Chief Executive of the Internet Industry Association in Australia, stated clearly where the geographic sources of the spam problem lie:

> It needs to be acknowledged that only a small proportion of spam, probably under 2 per cent, originates in Australia. The vast majority comes via servers in the US, Russia, China, Korea and South America.[29]

There are two factors that may contribute to the geographic sources of spam shifting in the future. The US anti-spam legislation that came in to force at the beginning of 2003, and the actions brought against US spammers under its provisions, are likely to have some limited positive impact in the US, although many of the points raised in this document questioning the effectiveness of the Australian legislation are similarly applicable to the US Act. Another trend that will likely affect where spam originates from (and spam volumes) is the increasing growth in key Asian economies, notably China[30] and India.

The expected continued economic growth in these regions will naturally give rise to continued massive increases in internet usage in these nations. China had an estimated 33.7 millions users in 2002;[31] this number had grown to an estimated 103 million internet users in 2005.[32] India had an estimated 38.5 million users in 2005[33] up from an estimated 9 million users in 2002.[34]

The explosion of the spam problem in the US seems, from anecdotal observation, to have been directly related to the growth of internet use in that country. It could be assumed that this principle will hold for China and India: the more internet users, the more individuals are likely to contemplate spamming and the more attractive spamming will become to existing spammers.

Although the government in China already regulates the internet very heavily, it remains to be seen what its response to spam will be. It seemed a long, slow journey for the government there to develop legislative protection of intellectual property

---

[29] Above n 6.

[30] Peter Weigang Lu, *Internet Development in China; An Analysis of the CNNIC Survey Reports* <www.chinaonline.com/commentary_analysis/internet/currentnews/secure/c000316OInternetAnalysis.pdf> at 1 May 2004. See also China Internet Network Information Center, *15th Statistical Survey Report on the Internet Development in China* (January 2005) <http://www.cnnic.net.cn/download/2005/2005012701.pdf> at 1 March 2006.

[31] China Internet Network Information Center, *9th Statistical Survey Report on the Internet Development in China* (January 2002) <http://cnnic.cn/download/manual/en-reports/9.pdf> at 7 March 2006.

[32] China Internet Network Information Center, *16th Statistical Survey Report on the Internet Development in China* (July 2005) <http://www.cnnic.net.cn/download/2005/2005072601.pdf> at 7 March 2006.

[33] Unknown author, 'Indian Internet Users to Reach 100 Million', *Internet and Mobile Association of India* (India), 13 February 2006 <http://www.iamai.in/section.php3?secid=16&press_id=822&mon=2> at 10 March 2006.

[34] Peter Wolcott, *The Provision of Internet Services in India* (University of Nebraska at Omaha) <http://mosaic.unomaha.edu/India_2005.pdf> at 12 March 2006.

considered necessary by the US and other nations prior to considering China for admission to the WTO, for example.

### B *Adequacy of penalties to act as effective deterrent*

The escalating penalty provisions under the Australian *Spam Act* begin with infringement notices, potentially leading (if subsequent breaches can be shown) to applications for injunctions and civil penalty provisions and seizure of equipment.[35] Whether this compliance regime will be effective as a deterrent remains to be seen.

The Australian Computer Emergency Response Team (AusCERT), in its submission to the Government's 2006 review of the *Spam Act 2003*, put the view that spam levels had continued to increase significantly. As of March 2006 only 13 fines had been issued to five
companies and individuals and one successful prosecution had been carried out under the Act.[36]

While the Federal Government suggests that 'it has been reported that the percentage of worldwide spam originating from Australia has decreased since the enactment of the Spam Act', MessageLabs figures released in July 2006,[37] suggest a 3.2% fall in spam levels in Australia. However, the report suggests that 48% of email in Australia is spam, with other sources estimating spam levels to be as high as 80%. This discrepancy highlights the immense difficulty in estimating spam levels, making any meaningful measurement of the legislation's effectiveness equally problematic.

Would harsher penalties act as more powerful deterrents? In some jurisdictions, notably Italy[38] and the US,[39] imprisonment is provided for in anti-spam legislation. Given the global nature of the problem, any deterrent effect is likely to simply shift the sending of spam. Sophos, a leading anti-spam software provider, suggests that the effect of the US spam legislation has been merely to drive spammers to other jurisdictions in many instances.[40]

### C *Exceptions provided for by the Act*

---

[35] Above n 16, ss 23 – 27.

[36] Department of Communications, Information Technology and
the Arts, *Report on the Spam Act 2003 Review 2006* (2006) <http://www.dcita.gov.au/__data/assets/pdf_file/40220/Report_on_the_Spam_Act_2003_Review-June_2006.pdf> at 7 August 2006.

[37] MessageLabs, *Intelligence Report* (2006) <http://www.messagelabs.com/publishedcontent/publish/threat_watch_dotcom_en/intelligence_reports/july_2006/DA_155200.chp.html> at 12 August 2006.

[38] *Personal Data Protection Code* Legislative Decree no. 196 of 30 June 2003 entered into force 1 January 2004, s 168.

[39] *Controlling the Assault of Non-Solicited Pornography and Marketing Act*, 15 USC 7701 (2003), s 4(a).

[40] Sophos, *The Sophos spam dirty dozen - Podcast*, <http://podcasts.sophos.com/en/sophos-podcasts-003.mp3> at 14 August 2006.

The Act provides for certain exemptions from its prohibitions. The first class of exemptions are Designated Commercial Electronic Messages (DCEMs). Exempted DCEMs include messages from charities, political parties, governments and religious groups.[41] Also exempt are factual messages that include the logo and address of the sender, if such messages would not have been commercial in nature if they did not contain the logo and address.[42] This was apparently intended to provide for newsletters[43] and the like, but it is suggested that this provision, at worst, could permit spam from many commercial senders and at best will remain an unclear provision, giving rise to much difficulty in distinguishing between exempt factual DCEMs and prohibited commercial messages. This view has also been expressed by commentators in the field.[44]

Certain provisions of the Act seem to severely undermine the Opt-In principle, notably the conspicuous publication provision, which effectively deems consent for messages relevant to work-related business, functions or duties of an employee, if the address (this could included a phone number) has been conspicuously published and:

> (d) the publication is not accompanied by:
>
> (i) a statement to the effect that the relevant electronic account holder does not want to receive unsolicited commercial electronic messages at that electronic address; or
>
> (ii) a statement to similar effect …[45]

For example, spammers frequently make tantalising offers of career enhancing academic qualifications without any classes, lectures, assignments, theses and the like. Under this loophole of deemed consent, any recipient whose functions or duties could be enhanced by a bogus doctorate or masters degree, and who had not appended a no-spam disclaimer when their address appears on their employer's website, would be fair game for spammers. Clearly this is a completely unsatisfactory situation and presumably provides some indication of the power of the pro-marketing lobby group during the consultation process that preceded the drafting of this Act. The relevance of the message to the recipient again seems to introduce a murky test that will presumably require clarification by the courts.

### D *No grounds for civil action under the Act*

Another key shortcoming of the Act is its failure to provide grounds for civil action by individuals or corporations against spammers. The Australian Communication and Media Authority (ACMA) is the only party with such standing. Civil causes of action may lie under other legislation, such as the *Trade Practices Act* 1974 (Cth), and other government bodies may also have standing, such as the Australian Consumer and Competition Commission (ACCC). This is a criticism that has also been levelled against the US legislation.

---

[41] Above n 16, s 16(1)(b).
[42] Above n 16, Sch 1 cl 2, esp cl 2 (1)(b).
[43] Above n 27.
[44] David Vaile, Spam canned? New electronic message laws for Australia, *Internet Law Bulletin*, 2004 (6) 9.
[45] Above n 16, s 4(2)(d).

### E *Inadequate resources to support the Act*

The ACMA (previously the Australian Communications Authority or ACA) has been charged with administering the Act. It is suggested that the funding allocated to the ACA to administer the Act has been manifestly inadequate. According to the ACA's 2002/2003 Annual Report, the average number of ACA employees for the financial year 2002/2003 was 395. Employee related expenses for the same period were $28,434,000, so, as a rough interpolation, this suggests an average cost per ACA employee of $71,985.

The ACA's total expenditure (FY 02/03) was $51,443,000. Employee related expenses therefore accounted for 55.3% of the total expenditure. Assuming this proportioning of funding allocation remains, that is, of the additional funding provided under the Act, 55.3% will be allocated to additional staffing resources, then the $300,000 allocated for FY03/04 would have enabled the ACA to hire 2.3 more staff. The staffing for the ACA for the following period (FY04/05) could have been increased by an additional 9.2 staff members with one more additional staff member hired in FY05/06, based on the funding provided for under the Act.

So, an entirely new legislative regime, enacted to deal with an exponentially growing problem, costing businesses, government and consumers in Australia many billions of dollars annually was (in effect) allocated less than a dozen new public servants to enforce it.

In the Second Reading Speech, immediately after stating that spam costs $900 per employee per year (as previously stated, equating to $8.5 billion given the 2002/2003 Australian workforce of 9,441,300), the Minister said 'this bill shows the Government is serious about addressing the problem'.[46] However, $300,000 allocated in the first year of the Act to combat an $8.5 billion dollar pandemic, seems manifestly inadequate.

These estimates are however, based on an assumption that is almost certainly incorrect, that all the funding provided for under the Act (and consequential amending legislation) will be provided to the ACA. The fact that other government bodies have been tasked with elements of the Government's approach to spam, such as NOIE's educative role, would almost certainly mean that they will require some of this funding, further reducing the resources and staff available to the ACA in its efforts to administer the Act.

It is somewhat surprising that, given the practically universal nature of the problem, in that spam directly affects almost every computer user in the country, there seems to be no cohesive lobby group with enough political leverage to raise the profile of this issue in lawmakers' minds to secure greater levels of funding for enforcement of the anti-spam legislation.

[46] Above n 5.

### F *No obligations on the ISP industry*

The consultative process leading up to the Act's drafting, including the Spam Law Implementation Forum jointly hosted by the ACA and the Department of Communications, Information Technology and the Arts (DCITA) on 27 February 2003, included heavy involvement by internet industry groups, notably the Internet Industry Association (IIA). The question might be asked if this group, with an understandable reluctance for tighter legislative regulation, had significant lobbying power, which may have contributed to the Government's decision to not place requirements on ISPs to do more to counter spam.

The Act also fails to make Internet Service Providers (ISPs) accountable for reducing spam levels. Most spam that reaches an individual computer user's email in-box comes via that user's ISP. This obviously results in significant cost burdens to ISPs (a point covered in extensive detail in the NOIE report),[47] providing at least an indirect financial and operational incentive for ISP to undertake aggressive counter-measures. Following the 2006 review of the Act, DCITA's recommendation is that obligations not be placed on ISP's to do more to combat spam under the Act.[48]

The United Nations International Telecommunication Union Head of Regulatory Reform, Doreen Bogdan, stated in March 2006: 'So far, existing anti-spam laws have had little effect as most laws target spammers, not the ISPs that carry spam …'. This suggests that the time may be ripe for governments to work with ISPs who can be instrumental in fighting spam. One proposal made was 'the establishment of enforceable codes of conduct that would require ISPs to prohibit their customers from using ISPs as a source of spam.'[49]

Cynics may also point out that with most major ISPs offering access plans typified by low monthly access fees, with low download allocations and data traffic-based (per Mb etc) additional fees, ISPs could possibly stand to gain from additional traffic that their users download, even if some of this traffic was made up of spam. Whilst the Federal Government remains the majority owner of the nation's largest ISP (Telstra) and wholesale supplier to much of the ISP industry, it may also be seen by some as having a vested interest in reducing potentially costly obligations, that may negatively affect any likely subsequent sale price or create potentially legal exposure for any non-compliance that might occur.

## V THE UNITED STATES' LEGISLATIVE APPROACH

Anti-spam legislation has also been enacted in a number of the jurisdictions around the world. The US position will now be briefly considered, in order to highlight some of the differing approaches that have been adopted.

---

[47] Commonwealth, National Office of the Information Economy, *Spam; Final report of the NOIE review of the spam problem and how it can be countered* (2003).
[48] Above n 37.
[49] International Telecommunications Union, 'Call to connect the unconnected by 2015' (Press Release, 7 March 2006) <http://www.itu.int/newsroom/press_releases/2006/02.html> at 12 August 2006.

Leading up to the passing of the current legislation, a number of bills in the US were vying for the support of law makers, including a proposal for much more severe jail penalties, (for example, the bill sponsored by Senator Orrin Hatch, Chairman of the Senate Judiciary Committee).[50] There were also unsuccessful calls for the establishment of a central, government-overseen, 'do not email' register, as has been adopted in relation to telemarketing and direct mail in the US.

The US legislation, showcasing that nation's penchant for carefully constructed acronyms, is the *Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)* and came into force on 1 January 2004, just a few months before the Australian Act. The fundamental bases of these two pieces of legislation are diametrically opposed. The US has decided to adopt an 'Opt-Out' approach, effectively making it *legal* to send unsolicited commercial email if its source and nature are not disguised, resources were not misappropriated to send it, and consumers have a meaningful way to avoid receiving future mailings.[51]

It is suggested that the US adoption of an 'Opt-Out' model, whilst clearly providing less protection for consumers, ISPs and other victims of spam, was probably dictated by the constitutionally protected freedom of speech principle that could provide serious grounds for challenging an 'Opt-In' based regime.

The first of the three requirements in the US legislation outlaws spammers using false or misleading headers in the messages they send.[52] These headers can be used to trace the path that messages have taken on their journey, ultimately disclosing the unique IP address of the originating machine, so a law mandating accurate header information will be able to greatly assist identifying those that breach the other key provisions of the US Act.

The Australian Act takes a different approach, requiring clear and accurate identification of and contact details for the individual or organisation that authorises the sending of a message. This differs significantly from the US provisions in that there is no explicit obligation to provide accurate header information (typically not readily visible to recipients, but essential to locate originating servers), but just human readable contact details. This could potentially hinder cooperation with other jurisdictions, especially the US which require the more useful header information to be accurate.

The US Act also places (perhaps somewhat vague) requirements on what spammers must include in the subject heading of messages: 'subject headings must not be likely to mislead a recipient … regarding the contents or subject matter' of a message.[53] This outcome was well short of many calls by legislators in the US for mandatory labelling with a prescribed prefix (for example 'ADV:') indicating the nature of the message, as is the case in some state legislation in the US (e.g. California has such a

[50] *Criminal Spam Act of 2003,* 108th Congress, 1st Session (2003).
[51] Dan Fingerman, 'Spam Canned Throughout the Land? Summary of the CAN-SPAM Act' (2004) 7(8) *Journal of Internet Law*, 1.
[52] *Controlling the Assault of Non-Solicited Pornography and Marketing Act,* 15 USC 7701 (2003), s 5(a)(1).
[53] *Controlling the Assault of Non-Solicited Pornography and Marketing Act,* 15 USC 7701 (2003), s 5(a)(2).

provision).[54] The CAN-SPAM Act expressly pre-empts some pre-existing US state laws, some of which had adopted an Opt-In approach, with a clearly stated intention to cover the field to the exclusion of the states. With regard to email, states do remain free to legislate in ancillary areas such as torts, trespass and computer fraud.[55]

Pornographic messages under the US Act are, however, required to carry a prescribed identifier in the subject line.[56] It has been suggested that this provision may be susceptible to constitutional challenge, based on first amendment free speech rights mentioned above.[57]

US courts have developed a doctrine, not presently accepted in Australia, in relation to spam and related computer infringements, known as trespass to chattels. The CAN-SPAM Act provisions dealing with misappropriation of resources are underpinned by this principle. This doctrine can provide redress for conduct where unauthorized interference or use of property occurs, if such action results in actual injury.

Two prominent cases in the US have considered this principle. In the *CompuServe case*[58], an ISP obtained a preliminary injunction based on the trespass to chattels doctrine, against the sending of spam to its subscribers. It was held that the spammers uninvited and intrusive actions had led to physical and non-physical economic harm on CompuServe's network, draining storage space and processing capability that should have been used to serve customers. The court found that 'injury aside from the physical impact of defendants' messages,' such as harm to business reputation and goodwill, was an equally viable basis for a trespass to chattels claim.[59]

This principle was again considered, in the case of *Intel v Hamidi*[60], which involved a disgruntled ex-employee of Intel, who had been made redundant, sending unsolicited messages to his former employer's staff. The court considered what extent of damage was necessary to establish trespass to chattels. Intel had relied largely upon harm to employee productivity as grounds for liability. Under Australian law, criminal liability or other remedies may arise under the *Criminal Code Act* 1995 (Cth), where spammers misappropriate another's resources for spamming. Interestingly, in one of the early actions commenced by the Federal Telecommunications Commission under the US CAN-SPAM Act, the defendant was an Australian company, Global Web Promotions Pty Ltd.[61] This proceeding culminated in a default judgement against the defendants with monetary relief of over US$2.2 million ordered.[62]

---

[54] *Business & Professions Code*, § 17538.4, California (1998).
[55] *Controlling the Assault of Non-Solicited Pornography and Marketing Act*, 15 USC 7701 (2003), s 8.
[56] *Controlling the Assault of Non-Solicited Pornography and Marketing Act*, 15 USC 7701 (2003), s 5(d)(1)(a).
[57] Dan Fingerman, 'Spam Canned Throughout the Land? Summary of the CAN-SPAM Act' (2004) 7(8) *Journal of Internet Law*, 12.
[58] *CompuServe Inc. v. Cyber Promotions, Inc* 962 F.Supp. 1015 (1997).
[59] Ibid, 1022-1023.
[60] [1999] WL 450944 (unpublished, Cal. App Super, April 28 1999): Tentative ruling granting Intel's summary judgment motion; not officially published.
[61] Federal Trade Commission, 'FTC Announces First Can-Spam Act Cases' (Press Release, 29 April 2004) <http://www.ftc.gov/opa/2004/03/040429canspam.htm> at 30 August 2006.
[62] Federal Trade Commission v Global Web Promotions Pty Ltd, FTC File No. 042-3086, Civil Action No.: 04C 3022 (N. D. Ill. filed April 28, 2004) <http://www.ftc.gov/os/caselist/0423086/050920defjudg0423086.pdf> at 21 August 2006.

# VI ALTERNATIVE APPROACHES TO THE SPAM PROBLEM

It has been observed in relation to the spam problem, that;

> A domestic legal solution is necessary but will be an insufficient response and must form part of a broader strategy which also incorporates technological and educational approaches.[63]

This seems a reasonably accurate summation of the situation, but as discussed above legal and other measures must be adequately resourced if they are to have meaningful impact. Prior to the enactment of the Australian legislation, there were numerous though somewhat disparate legislative provisions to deal with spam. Indeed, the Explanatory Memorandum stated that 'despite the breadth of measures theoretically available they are rarely used to prosecute spammers'[64]. These measures include the *Privacy Act 1998* (Cth), in particular the National Privacy Principles that could be clarified and/or strengthened to better regulate spammers.

The *Interactive Gambling Act 2001*(Cth) and the *Therapeutic Goods Act 1989* (Cth) only deal with content hosted in Australia, but could potentially be amended to catch spam and the overseas sites linked by spam. Internet content is regulated by the *Broadcasting Services Act 1992* (Cth). Schedule 5 of this Act could also apply to sites to which spammers link and could be extended to cover spam messages themselves. The *Trade Practices Act 1974* consumer protection provisions prohibit false and misleading claims about goods and services, a feature of many spam messages. It may also apply to falsified headers and false opt-out measures. Under the *Crimes Act 1914* (Cth)[65] it is an offence to use email that is menacing, harassing or offensive; this could cover pornographic spam and as mentioned above, the *Criminal Code Act 1995* (Cth) may also be applicable in cases where spammers hijack innocent parties' computing facilities to send spam.

Amongst the non-legal technical approaches to the problem, there are numerous spam blocking services.[66] Often these are 'self help', non commercial organisations that maintain registers of known spammers' IP addresses and block traffic from such sources. These efforts undoubtedly deliver some positive effects but face legal challenges as well as the technical challenges that have beset them as spammers get 'smarter'. In addition to US cases, there has been one case of a spammer in Australia bringing an (unsuccessful) action against an individual who listed the spammer on an anti-spam service.[67] The plaintiff spammer here alleged unlawful interference with trade or business interests, a tort not as yet recognised in Australia.

Some of these approaches also suffer from resource constraints and may be unlikely to scale adequately over time to effectively impact on the explosive increase in the volume of spam. Most of the non-legal initiatives against spam are undertaken by

[63] Above n 6.
[64] Above n 27.
[65] See especially s 85ZE.
[66] For example Spam Prevention Early Warning System (SPEWS) http://www.spews.org, accessed 12 March 2006, this site also contains an extensive list of other anti-spam services.
[67] *Which Co Pty Ltd t/as T3 Direct v McNicol* [2002] WADC 217; (2002) 29 SR (WA) 17.

non-government organisations, either voluntary groups such as SpamHaus[68] and Open Relay Databases[69] or commercial operations such as Sophos.[70]

Another non-legal approach to the spam problem that has been suggested on numerous occasions, including by Microsoft founder, Bill Gates,[71] is the notion of some form of tax on email. Such an approach is an attempt to address the free transmission that is at the heart of what makes spam so attractive. There would be many, probably insurmountable, obstacles to any such proposals that undermine the fundamental notions of the freedom and independence of the internet, not the least of which will be the added scepticism such proposals may receive now that they have been voiced by the planet's wealthiest individual, whose company has been regularly challenged by competition regulators over its domination of many aspects of computing.

One of the more thought provoking alternate approaches to combating spam has come from Lawrence Lessig,[72] noted US cyber-law academic, and was adopted by some US politicians in bills that were prepared as alternatives to the current US spam legislation. The concept is that a bounty is offered for individuals or corporations who are able to identify, locate and collect sufficient evidence to convict spammers. Proceeds from successful legal action (brought by government regulators) would be used to fund the bounty payments and thus the programme could theoretically be self funding. Given that current funding levels by the Australian government will largely limit the effectiveness of the *Spam Act 2003*, approaches such as this may have some merit. The other challenge faced by governments may also be an inability to attract staff with the requisite technical expertise to combat the ever-increasing expertise of the spammers. Lessig's approach would possibly incentivate some of the best anti-spam minds to take up the cause. Critics might suggest this smacks f vigilantism, but rewards are currently offered for enforcement against other crimes including intellectual property breaches, such as software piracy[73].

Almost all spam messages contain a hyperlink to a website, along with a message encouraging the recipient to click on the link and be taken to a page on the world wide web. Frequently these websites are unscrupulous, deceptive or pornographic and may not even be maintained by the spammers themselves. The website operators often are running affiliate programs as a tool for generating traffic to their sites. Spammers sign up as affiliates with the website operators and are paid for every visitor that they generate to the site. Given this model is at the heart of the revenue potential for many spammers, it may contribute substantially to the problem. There would undoubtedly be higher barriers to entry for would- be spammers if they had to set up websites, produce and/or procure bogus products, establish payment facilities etc, rather than just needing to get recipients to click on a website link with the lure of free pornography, miracle health products or low interest rates.

---

[68] <http://www.spamhaus.com> at 12 March 2006.
[69] <http://www.ordb.org> at 12 March 2006.
[70] <http://www.sophos.com> at 12 March 2006.
[71] Bill Gates, 'United Nations Development Program Press Conference' (Speech delivered at the World Economic Forum, Davos, Switzerland, January 2004) <http://www.microsoft.com/billgates/speeches/2004/01-23undp.asp> at 27 August 2006.
[72] <http://www.lessig.org> at 19 February 2006.
[73] See for example, <http://www.bsaa.com.au> at 12 March 2006.

Affiliate programs are obviously a legitimate business tool in many instances, but given their use by site operators that effectively use such structures to encourage, aid and abet spammers, consideration should be given to how liability might arise for such operators who engage affiliates that are or become spammers.

# VII THE FIRST AUSTRALIAN CASE

The ACMA's 'enforcement activities in the initial phase of the Spam Act's administration have been focussed on the prosecution of global professional spammers - those who send out messages in very large numbers to strangers, often using tactics designed to hide their identity and to bypass spam filters'.[74] The first case brought against such an organisation was commenced in June 2005[75].The ACMA alleged that Clarity1 Pty Ltd (trading under the names Business Seminars Australia and the Maverick Partnership) and its sole director and shareholder had:

- obtained email addresses through the use of address harvesting software;
- sent Commercial Electronic Messages to these email addresses;
- not obtained the consent of the email address account holders for such messages.

The ACMA led evidence from expert forensic examiners, who apparently had access to Clarity1's computer systems; a record of interview with Mr Mansfield, Clarity1's director; and a number of affidavits from recipients of email messages from Mansfield. Mansfield represented himself in the case and raised many of the defences available under the Act, though there seems to have been no merit on the facts to any of the defences raised.

*Use of harvesting software prior to Act's introduction*

The respondent attempted to argue, inter alia, that they had not used address harvesting software since the Act came into force. The court held that this was not relevant as the Act clearly proscribes the use of harvested addresses, including addresses harvested prior to the Act coming into effect.[76]

*Messages from Charities exemption*

The respondents contended that they had been 'contracted to provide services to registered charities so that the electronic messages were not 'commercial' and would therefore fall under the relevant exemptions in the Act.[77] The respondent failed to adduce evidence to support this claim or to identify which, if any, of the messages came within this alleged exception.[78] The facts indicate that there were certainly adequate volumes of messages that clearly had no relation to charities. The fact that

[74] Australian Communications and Media Authority, *Submission to the Spam Act review* (2006) 7.
[75] *Australian Communications and Media Authority v Clarity1 Pty Ltd* [2006] FCA 410.
[76] Above n 16, s 22.
[77] Above n 16, Sch 1 Cl 3(a)(iv).
[78] Above n 76, [69].

some messages may have been sent on behalf of charities could therefore not be effective as a defence.

*Messages from Educational Institutions exemption*

The respondents further contended that all the messages they had sent 'related to business education in the form of seminars and manuals'[79] and would therefore fall under those exemptions in the Act.[80] Clause 4 makes it patently clear that the education exemption was not relevant to Clarity1's case, as it only applies to educational institutions sending messages to current or former students relating to services the institution has or is supplying.

*Consent Generally*

The respondents also claimed that they had received consent from recipients, based on a number of arguments. The first of these was the recipients' failure to unsubscribe, which it was said entitled the respondent to reasonably infer consent.

The Act has clearly adopted an 'opt-in' model, as discussed above, and does 'not either expressly or by implication support an inference that a failure to use the unsubscribe facility implies consent.'[81] Despite this there was some extended consideration by the judge on the argument that consent could be inferred from failure to opt-out from previous spam messages, as discussed below.

*Inferred Consent*

The respondent raised statements contained by the Office of the Federal Privacy Commissioner in 'Guidelines to the National Privacy Principles' issued in September 2001 that 'it may be possible to infer consent from the individual's failure to opt out provided that the option to opt out was clearly and prominently presented and easy to take up'.[82] The court held that this statement needed to be considered in the context of the entire document it was extracted from, which subsequently concluded:

> It is unlikely that consent to receive marketing material on-line could be implied from a failure to object to it. This is because it is usually difficult to conclude that the message has been read and it is generally difficult to take up the option of opting out as it is commonly considered that there are adverse consequences to an individual from opening or replying to email marketing – such as confirming the individual's address exists.[83]

The court also held that whilst 'such publications cannot control the interpretation of an Act of Parliament' and that the 'words of the Act must speak for themselves and be interpreted according to the normal rules of statutory construction',[84] it may be

[79] Above n 76, [70].
[80] Above n 16, Sch 1 Cl 4.
[81] Above n 76, [74].
[82] See Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (September 2001) 37-38.
[83] Ibid.
[84] Above n 76, [76].

'appropriate to have regard to what the [respondent] relied upon as having shaped their approach to the Spam Act'.[85]

In a potentially ominous sign for the opt-in nature of the Act being upheld in future cases, the court further observed: 'If, as the respondents assert, there is to be an inference drawn of consent from the fact of a failure to reply to a CEM, the foundations for it must be found in the circumstances.'[86] While it was found that 'from that factual foundation, no such inference is logically open'[87] in the Clarity1 case, this statement by the Court could be seen to be suggesting that there may be circumstances in other cases where failure to respond to a message by a recipient may be considered sufficient to imply consent.

Such an inference of consent from failure to opt out was even less 'likely to be open where the entire relationship between Clarity1 and the recipient is constituted in the absence of bilateral communication'.[88] In the circumstances of this case, the court held that:

> Many inferences are open to speculation and none are logically dictated by the circumstances. There are a variety of methods available to recipients to deal with unwanted CEMs. These include simply deleting the CEM without reading it and so being unaware of the unsubscribe facility; ignoring the CEM and/or reporting it to the applicant; utilising a filtering or blocking technique. The sender, in this case Clarity1, would have no way of knowing whether the CEM has been opened or read; it is equally open to inference that it may not have been so that the unsubscribe facility was unknown to the recipient.[89]

It is possible when sending emails to enable a function that notifies the sender when a message is opened and read by the recipient. One wonders if a spammer was to prove that they had only sent messages to recipients who had opened the spammers' previous messages, this would have changed the facts sufficiently to successfully support a claim of reasonably implied consent, based on the statement above from the Clarity1 case.

Practically, however, in this case and presumably most, if not all, subsequent cases, the sheer volume of messages sent 'makes it improbable that the respondents could have been aware that consent was in place prior to the sending of the CEMs'.[90] The court then considered the business relationship arguments raised by the respondent. Some points to note from the judgment are set out below.

The court held that the burden of proof rests with the respondent to prove they had consent from the recipients. The court considered it 'relevant to have regard to the Principles in connection with the issue of consent because the applicant's own publication makes such Principles relevant to the understanding of existing

[85] Ibid.
[86] Above n 76, [77].
[87] Above n 76, [78].
[88] Above n 76, [79].
[89] Above n 76, [80].
[90] Above n 76, [85].

relationships'.[91]

In this case, each message had 'contained provision of a procedure stating what was required to remove the electronic address from the Lists'[92] and 'during the period from March 2001 to the hearing date, some 166,000 requests were made for removal from the Lists, all of which were acted upon'[93]. From March 2001 to the hearing date, 79 complaints were made to the ACMA concerning messages from Clarity1; there had been no complaints related to a failure by the respondent to remove any address from their database. [94]

*Consent inferred from Business Relationship*

The respondents argued that they could reasonably infer consent from the business relationships which Clarity1 had with the recipients of the messages, based on recipients' 'acceptance' of messages from the respondent over an extended period (over a year in many cases). The court held that:

> The reference to 'business relationships' in cl 2 of Sch 2 of the Spam Act must be understood in its immediate and surrounding context. The immediate context is one which conjoins the conduct of the individual or organisation who sent the CEM to the relationships as the factual foundation from which the inference may be drawn. It is not the business relationships alone which ground the inference. Additionally, the relevant relationships are not only business relationships; other relationships are equally relevant.[95]

> ''Business' is defined in s 4 of the Spam Act, subject to appearance of contrary intention to include 'a venture or concern in trade or commerce, whether or not conducted on a regular, repetitive or continuous basis'.[96]

The court held that the totally unilateral sending of a message could not 'properly come within the description of a 'business or other relationship'. There is no relationship when the communication is one sided. A relationship of the type referred to in Sch 2 implies a connection arising from mutuality. Communication from only one to another with no response from the other cannot properly be found to be a relationship, particularly in the context.'[97]

The respondent claimed that consent could be inferred for recipients whose details were gleaned from 'commercially available lists purchased, swapped or otherwise acquired prior to the implementation of the *Spam Act* in 2003'.[98] The court

[91] Above n 76, [57].
[92] Above n 76, [67].
[93] Ibid.
[94] Ibid.
[95] Above n 76, [87].
[96] Above n 76, [88].
[97] Above n 76, [92].
[98] Above n 76, [93].

summarily dismissed these arguments, stating that '[t]he circumstances of the acquisition of lists so described is itself antithetical to the drawing of any inference that the lists were obtained with consent'.[99]

The respondent claimed that there could be instances where recipients had handed business cards containing their email address to a business and this action had led to this information's inclusion in commercially available lists, subsequently acquired by the respondent. There was no consideration by the court as to whether these circumstances would be sufficient to be considered consent, as 'no evidence had been brought to support a finding that such an occurrence affected the collection of any of the electronic addresses in issue'.[100]

Whether the requisite consent would exist in circumstances where recipients 'by the action of entering a competition or a request for information website maintained by the respondent or associated joint venture entities who displayed relevant Terms and conditions statements that allowed the use of the email address for promotional purposes',[101] was also not considered as the respondent had not led evidence to support claims that addresses they used had been obtained in these circumstances.

There was some general discussion of what constitutes consent. In the Explanatory Memorandum, 'it is said that consent will not always be inferred where there is a pre-existing relationship between a person and a business'.[102] On this point, the court found that: 'The Memorandum accepts that the issue of consent is a question of fact to be considered according to each particular set of circumstances.'[103] The court further indicated that:

> What is required by cl 2 of Sch 2 of the Act is that consent can reasonably be inferred from both the conduct and 'the business and other relationships' of the individual or organisation concerned. Prima facie, the conclusion of a contract of purchase by an email order by an individual or organisation constitutes a 'business relationship' between the vendor and purchaser. In the absence of evidence to the contrary, it can be reasonably inferred that … a person having displayed interest in the wares of the vendor on one occasion, wishes to be kept in touch with future opportunities for purchase of products marketed by the same vendor.[104]

There was very little of evidence of prior purchase in this case: only 182 instances of prior purchases out of an alleged 213 million messages sent. There were held to be no breaches of the Act in relation to messages sent to the addresses of these previous customers, as the court inferred consent for the purposes of s 16(1).[105]

---

[99] Ibid.
[100] Above n 76, [94].
[101] Above n 76, [95].
[102] Above n 27, 115.
[103] Above n 76, [96].
[104] Above n 76, [97].
[105] Ibid.

*Conspicuous Publication of address as implied consent*

Conspicuous publication[106] was raised as a defence by the respondent. The court found that for this exception to apply, the following elements must be established:

> First, there must be a particular electronic address enabling the public, or a section of the public, to send electronic messages to the person or holders of particular offices, positions, functions or roles specified in cl 4(2)(a)(i) to (vii) of Sch 2 of the Spam Act. Secondly, the address must have been 'conspicuously published': cl 4(2)(b). Thirdly, it must be 'reasonable to assume' that the publication occurred with the agreement of the person or organisation concerned: cl 4(2)(c). Fourthly, it must be established that the publication was not accompanied by a statement to the effect that the relevant electronic account-holder does not want to receive unsolicited CEMs at that electronic address, or words to similar effect: cl 4(2)(d). Fifthly, it must also be established that the CEM is relevant to the work-related business, functions or duties of the employee, director, officer, partner, office-holder or self-employed individual concerned; the office or position concerned; or the function or role concerned: cl 4(2)(e)–(g)[107].

Again, these provisions were not examined in any detail by the court as there was not adequate evidence led by the respondent that this defence would apply.[108] There was in fact, evidence from recipients that messages had been sent that would indicate that the required elements above had not been met. The messages did not relate to the circumstances in which addresses were displayed, and recipients' addresses were only placed in 'limited non-conspicuous circumstances',[109] not published at all or published with a disclaimer.

*Conclusion*

The first case to be brought under the new *Spam Act* has been in all fundamental respects a somewhat straightforward case, with breaches of the key provisions of the Act being clearly evident. Of all the defences raised, none had any prima facie relevance to the facts in this case. The conduct in this matter seemed somewhat blatant, and did not result in any in-depth discussion of the nuances of the Act's provisions.

There was however some instructive discussion on the nature of consent and how it might be inferred under the provisions of the Act, particularly in relation to the business relationship provisions. The practical implications for businesses wishing to engage in email marketing activity that are underscored by this case are that by following the ACMA published guide for business, there will be little risk of infringing the Act. It is hoped that the civil penalty awarded against the respondent in

[106] Above n 16, Sch 2 Cl 4.
[107] Above n 76, [100].
[108] Above n 76, [107].
[109] Above n 76, [108].

this case will be of sufficient magnitude to act as a meaningful deterrent to other would be spammers. As at the date of writing, the Federal Court had not yet made a determination as to penalties in the Clarity1 case.

# VIII CONCLUSION

The Explanatory Memorandum to the *Spam Act 2003* (Cth) suggested that 'reduction of spam in Australia from other sources' will take place 'progressively and gradually' . It is suggested that a progressive and gradual response will, like King Canute, be unable to stem the exponentially growing tide of spam. International co-operation, resourcing commensurate with the problem and aggressive alternative measures, are necessary if domestic legislation is to be of any meaningful effect against the scourge of spam. It is suggested that further research in this area should focus on the following issues.

*Ensuring 'Opt In' really means 'Opt-in'*

Australia's legislative model, ostensibly requiring recipients to opt-in before messages can be sent to them is an appropriate model, but both the practical effect and legal certainty are undermined by the conspicuous publication and inferred consent provisions of the Australian legislation. Unfortunately, the 2006 review of the legislation did not take the opportunity to address these two issues.

*Measurement*

In order to ascertain the effectiveness of any anti-spam measures, be they legal, educative, technical or otherwise, some consistent and meaningful measurement approaches must be adopted. It is suggested that this is an area where ISPs could be required to collect and report data. The significant discrepancies between estimates of spam levels from various sources at present are so great as to render any attempts at measuring the effectiveness of counter-measures of little practical value.

*Global responses*

To date Australia has some anti-spam agreements with a number of nations. It is suggested that international treaties that require governments to take more aggressive measures will be required. Given the global nature of the problem, any nations that have poor legislation or inadequate resources, willingness or abilities to enforce their anti-spam legislation remain potential havens for spammers fleeing tougher regimes elsewhere, which results in no meaningful impact on spam levels globally. The challenges in developing effective international treaties are difficult to overcome, with

consensus required on the contents of such treaties and the development of means of supporting developing nations, technically and financially, to ensure they enact effective counter-measures. The OECD[110] and the UN[111] have both been attempting to developing strategies to deal with spam.

*Resourcing issues*

This paper has highlighted the limited funding available to deal with the spam problem. It is suggested that further research needs to be undertaken to ascertain what approaches will have the best chance of developing the political will to provide additional funding for anti-spam measures in Australia. Alternatively, consideratio needs to be given to how the legislation can be more effectively enforced. Options that have been suggested and could be investigated further include placing obligations on ISPs to have more involvement in spam prevention, and providing for technical investigations to be undertaken by highly skilled technical specialists, with a bounty system to reward them for successful prosecutions.

*Remedies and penalties*

Questions as to the deterrent effect of penalties, in the specific context of spam, require further consideration. This issue could be considered in conjunction with the resourcing issues raised above. Furthermore, the issue of whether those harmed by spammers may have some standing to seek remedies directly, rather than relying on a prosecution by a statutory authority, could be further explored. Consideration could also be given to the way penalties recovered from spammers are used, potentially including the establishment of a 'fighting fund' supported by penalties to further the development of technical and other counter-measures.

[110] See generally, <http://www.oecd.org/department/0,2688,en_2649_22555297_1_1_1_1_1,00.html> at 12 August 2006.
[111] UN Non-Governmental Liaison Service, *WSIS-related thematic meetings on Countering Spam* (2004) <http://www.un-ngls.org/site/article.php3?id_article=108> at 12 August 2006.