

Recent Developments in Australian Spam Law

By Jeremy Malcolm¹

Introduction

Spam is expected to account for approximately 40% of all Internet email delivered this year,² contributing about US\$2–3 of the average consumer's monthly Internet bill.³ The law, despite having a long (and undistinguished⁴) history with spam, has been caught short in its response to this unexpected and unwelcome phenomenon.

This paper begins by outlining the positions of some of the bodies involved in public debate on spam regulation, and goes on to provide an overview of the current state of legislation and case law in Australia as it concerns spam, along with an outline of the legal avenues that exist or are being developed to address the challenge that spam presents.

As a preliminary matter, it is necessary to define what constitutes spam. CAUBE–AU (the Coalition Against Unsolicited Bulk Email, Australia)⁵ defines spam very broadly as any electronic mail message that is:

- (a) transmitted to a large number of recipients; and
- (b) not explicitly and knowingly requested by some or all of those recipients.⁶

Other common definitions of spam also require that the messages be commercial in nature.⁷ For present purposes, spam can be defined as unsolicited bulk (and usually, but not necessarily, commercial) electronic mail. SMS⁸ and fax messaging will not be specifically considered in this paper.

The spam regulation framework

Government

Australia's National Office for the Information Economy (NOIE), an Executive Agency within the Department of Communications, Information Technology and the Arts, is currently undertaking a review of the spam problem at the request of its

-
- 1 Jeremy Malcolm is a Perth lawyer and a technology consultant, whose legal practice emphasises IT and communications law, commercial litigation, intellectual property and Trade Practices law. He is the President of the Western Australian Society for Computers and the Law Inc, an Executive Committee member of the Western Australian Internet Association, Secretary of the Australian Public Access Network Association Inc, a Director of the Internet Society of Australia and Vice Chairman of the Society of Linux Professionals (WA) Inc.
 - 2 Morrissey, B. "Spam Under the Tree", <http://www.internetnews.com/IAR/article.php/1561201>. URLs referenced in this article were last accessed on 1 February 2003.
 - 3 1998 Washington State Commercial Electronic Messages Select Task Force Report, <http://www.wa-state-resident.com/finalrpt.pdf>.
 - 4 What is commonly regarded as the first ever Usenet (Internet newsgroup) spam was sent in 1993 by an immigration law firm; see Campbell, K. "A Net Conspiracy So Immense", http://www.eff.org/Legal/Cases/Canter_Siegel/c-and-s_summary.article.
 - 5 CAUBE–AU is the Australian anti-spam lobby organisation, which has equivalents in the United States (CAUCE) and around the world (EuroCAUSE, CAUCE Canada, CAUCE India).
 - 6 <http://www.caube.org.au/whatis.htm>
 - 7 <http://www.cauce.org/about/faq.shtml>
 - 8 GSM Short Message Service.

Minister, Richard Alston. NOIE released its interim report⁹ in August 2002, and was due to present a final report in November 2002 (although that has yet to occur at the date of writing).

NOIE's interim report makes a number of draft recommendations, which are in summary:

- Before the problem can effectively be tackled, an agreed definition of spam must be settled upon. NOIE provides a draft definition, of approximately 300 words in length, that is much more specific and somewhat narrower than those of CAUBE-AU or CAUCE referenced above.
- It is suggested that industry bodies develop codes of conduct, guidelines and strategies on spam. Some, indeed, already have done so,¹⁰ and the response of Australia's Internet Industry Association will be described in more detail below.
- Consideration should be given to the compulsory use of caller line identification (CLI) to identify users of dial-up Internet accounts, potentially allowing known abusive customers to be refused a connection. Currently a number of Internet Service Providers (ISPs) do collect such information, but this practice has raised privacy concerns.¹¹ When collected by an ISP that is also a telecommunications company, from a telephone line on which CLI has been disabled (and for which the CLI information would therefore not be available if the ISP were not a telecommunications provider) the practice is even more controversial.¹²
- NOIE suggests that a self-regulated list of known spam senders be maintained, which could be used by ISPs or users to block suspected spam. Of course, there are many such so-called "blocklists" in current use, but the distinguishing feature of a government-sponsored blocklist is that it would, one hopes, offer some protection for its administrators from liability.
- NOIE proposes an improved programme of education of the community about mail filtering systems and tools. It separately proposes that a public information campaign about spam be developed.
- Authorities administering laws of general application, such as the Australian Competition and Consumer Commission (ACCC), the Australian Securities and Investments Commission (ASIC) and the Office of the Federal Privacy Commissioner (OFPC), should consider whether there is scope for greater enforcement of those laws against spammers.
- Australia should also work in partnership with International agencies, at operational and policy levels, in acting to counter the spam problem.
- The application of the National Privacy Principles to the operations of spam senders, such as the harvesting of email addresses, should be clarified.¹³
- Consideration should be given to the spam problem in the course of the next reviews of the Privacy Act in December 2003 and the Broadcasting Services Act in October 2002. (The recommendations of the Broadcasting Services Act

9 http://www.noie.gov.au/projects/confidence/Improving/Spam/Interim_Report/contents.htm.

10 The Western Australian Internet Association's code is found at <http://www.waia.asn.au/info/spamcode.shtml>.

11 See <http://www.efa.org.au/Issues/Privacy/cndnomand.html>.

12 Fitzsimmonds, Caitlin. "Privacy Battle over CLI", http://www.news.com.au/common/story_page/0,4057,5389026%255E15306,00.html.

13 CAUBE-AU provides guidelines to businesses on ethical email marketing in compliance with the National Privacy Principles on its Web site: <http://www.caube.org.au>.

review, which has since taken place, are yet to be finalised.)

- The introduction of specific anti-spam legislation should be considered. Whether to prohibit spam outright, or whether to restrict the scope of the legislation to misleading spam (which is already to some extent covered by existing legislation such as the Trade Practices Act) is a question left open by NOIE. A third alternative proposed by ASIC is the introduction of a new Commonwealth offence of using an electronic carriage service to commit any other Commonwealth offence.
- NOIE observes that the spam problem and the technical counter-measures that are available should continue to be monitored by government, in order to ensure the continuing appropriateness of the measures to be taken.

Prior to NOIE's interest in this issue, in May 2000, a set of Electronic Commerce Guidelines were prepared by the Expert Group on E-Commerce advising the Commonwealth Treasury Department.¹⁴ These Guidelines recommend that an "opt-in" standard be adopted by business for promotional email communications. The Guidelines do, however, concede that "acquaintance spam", or promotional email directed to persons with whom the sender has a pre-existing business relationship, may be sent on an "opt-out" basis, possibly in concession to the interests of marketing stakeholders such as the Australian Direct Marketing Association.¹⁵

¹⁴ <http://www.ecommerce.treasury.gov.au/publications/BuildingConsumerSovereigntyInElectronicCommerce--ABestPracticeModelForBusiness/index.htm>.

¹⁵ The Australian Direct Marketing Association refers consumers to the American Direct Marketing Association's Web site at <http://www.e-mps.org> which allows consumers to add their email addresses to a database of those who have chosen not to receive spam. This database is reportedly used to "cleanse" members' email lists, although since most spam senders are not members of the American Direct Marketing Association the effectiveness of this approach is limited.

Industry

The Internet Industry Association (IIA) is a national industry association for Australian ISPs, dominated by larger industry participants. Early versions of its Code of Practice for the Internet industry were somewhat lax in their application to spam.¹⁶ In response to criticism on this count, the relevant clauses were eventually excised from the Code and replaced by stronger provisions.¹⁷ However even in their strengthened form, IIA's response fell short of the standard expected by some user organisations, including CAUBE-AU which is critical of any policy which condones the sending of acquaintance spam.

Since 2000, IIA has divided its code of conduct into several more specific codes, including a draft Privacy Code¹⁸ which is based on the National Privacy Principles.¹⁹ It is intended that this code will be registered with the Privacy Commissioner and thereby effectively replace the National Privacy Principles for code signatories.²⁰

Clause 6.9 of the draft code provides "For the purposes of section 6.8(c)(i), it shall in all circumstances be deemed practicable for a Code Subscriber to seek the individual's prior express consent to use Personal Information for the secondary purpose of direct marketing in an online environment." Apart from this clause, the National Privacy Principles could allow a company to send spam to an individual whose personal details had previously been lawfully obtained for another purpose, if it was impractical to seek the individual's consent to the use of those details for the receipt of spam.

Legislation on spam

Trade Practices Act

As noted by NOIE in its draft review, there is some existing Australian legislation that bears upon the spam problem. If the spammer is located within Australia, this legislation can be used as a weapon against spam. Section 52 of the Trade Practices Act in particular has obvious application in combatting spam that is misleading or deceptive, either in its body or in its headers.²¹ Although no authority is known of in which the Act has been applied against spam or spammers in Australia, the Federal Trade Commission has applied equivalent

¹⁶ See <http://www.iaa.net.au/Code4.html>.

¹⁷ Amongst other refinements, version 5 of the Code prohibits its members from sending or encouraging the sending of spam (except for "acquaintance spam"), and does not allow prohibited content to be included in spam under any circumstances (this includes material that would be classified with an R rating or would be refused classification by the Office of Film and Literature Classification). IIA members are required to have an Acceptable Use Policy (AUP) and to take action against spammers for breaches of that policy, which may involve the termination of their services. Members must also have an "abuse" email address to receive complaints about spam, and should not allow open relay mail servers on their networks (these are mail servers that are vulnerable to being used by spammers from anywhere on the Internet as a transmission point for spam).

¹⁸ <http://www.iaa.net.au/privacycode.html>.

¹⁹ Privacy Amendment (Private Sector) Act 2000 (Cwlth).

²⁰ Mackenzie, Kate. "Privacy delays cybercrime code", AustralianIT, 6 December 2002, <http://australianit.news.com.au/articles/0%2C7204%2C5628313%5E15319%5E%5Enbv%5E15306%2C00.html>.

²¹ Headers are for example the "From" and "To" line of an email message, but there are also many hidden headers containing information such as the path that the message has taken between sender and recipient.

legislation against United States spammers.²²

Corporations Law

ASIC has taken action against spam that promotes unlicensed investment schemes contrary to the Corporations Law. In *R v Hourmouzis*²³ the defendant pleaded guilty to interfering with, interrupting or obstructing the lawful use of a computer contrary to s.76E of the Crimes Act 1914 (for sending the spam through open relay mail servers), and to making statements or disseminating information that was false in a material particular or materially misleading and likely to induce the purchase of securities by other persons, contrary to section 999 of the Corporations Law. The United States Securities Exchange Commission also obtained judgment against him in the District Court of Colorado for about US\$ 15,800 under broadly equivalent legislation.²⁴

Privacy Act

The intended effect of the Privacy Act in its current form is to preclude spammers from harvesting email addresses without the consent of their owners. This must in general be consent to the use of the address for spam, as a person who has consented to the collection of their email address for a particular purpose does not thereby consent to it being used for other purposes.

As indicated above however, spammers may be entitled consistently with the National Privacy Principles to send spam to email addresses that were collected for a different purpose if it is impracticable to obtain the recipient's consent to the use of their address for spam. Even if it will always be practical to obtain the recipient's consent, the prospect that spammers might seek such consent by email somewhat defeats the purpose of using the Privacy Act to combat unwanted email.

Furthermore, spammers may argue that unless an email address is able to be used to individually identify its owner, it is not personal information at all, or alternatively that those who publish their email address publicly, for example on a Web site, implicitly consent to its collection.

The Office of the Federal Privacy Commissioner's submission to the NOIE spam review²⁵ touches on these issues, but concludes that "[i]t is not yet clear the extent to which the Privacy Act does provide an effective remedy for people who want to take action about [spam]".

This has not prevented the OFPC from receiving complaints about spam. In accordance with the Office's procedures, if a complaint relates to a spammer who is bound by and found to be in breach of the Act, the spammer can be requested to remedy its breach. In the event that the spammer fails or refuses to comply, the complaint can be elevated to the Privacy Commissioner for an enforceable determination to be made. The failure to comply with an enforceable determination is actionable in the Federal Court.²⁶ To date, no complaint about spam has reached this point.

²² See eg. *People v Lipsitz*, 663 N Y S 2d 468, 468 (Sup Ct 1997).

²³ Unreported, 30 October 2000, Victorian County Court.

²⁴ Compare *SEC v Tribble*, No 98-8699 (RVX) (C D Cal filed 27 October 1998) in which case the perpetrator of a spam stock promotion was fined by the United States Securities Exchange Commission.

²⁵ http://www.noie.gov.au/projects/confidence/Improving/Spam/Interim_Report/OFPC_Sub.PDF.

²⁶ Section 55A of the Privacy Act 1998 (Cwlth).

Criminal Code Act

As noted above, many spammers exploit open relay mail servers, in an endeavour to mask their real locations, and also to cast the cost of delivery of the spam onto the owner of the misconfigured server.

This practice may now be in breach of section 478.1 of the Criminal Code Act 1995 (Cwlth).²⁷ It is likely that, by virtue of section 476.3 of the Criminal Code Act, it is even in breach of that provision if the mail server that is abused is overseas (which is very common, as there are many old and misconfigured mail servers in the third world). In simplified terms, liability will attach if the offender institutes or assists in the institution of an unauthorised connection to an open relay server, provided that the connection is either initiated in Australia, or if results of the abuse occur in Australia, or if the offender is an Australian citizen.

Although the legislation is not unambiguous and these provisions have not been tested, it is certainly arguable that the mere sending to an Australian recipient of spam through a compromised open relay server overseas would constitute an offence by the sender, even if the sender had no other connection with Australia. The reverse, namely an Australian spammer sending to overseas addresses through an open relay, is even more likely to be caught by these provisions.

Broadcasting Services Act

As noted above, the Department of Communications Information Technology and the Arts has recently undertaken a review of the provisions of the Broadcasting Services Act, which regulates Australian Internet content by reference to the classification scheme applicable to motion pictures. Included in its terms of reference was the question of whether any extension to the Internet content regulation regime should be made in respect of spam, which generally falls outside the scope of the legislation at present due to the transitory nature of email communications.

Although the results of the review have not been finalised at the date of writing, even in its present form the Act does have some existing application to spam, in that clause 60 of Schedule 5 specifies that an industry code and/or industry standard should be drafted to deal with the procedures to be followed upon receipt of a complaint about spam that promotes offensive material on the Web.²⁸

Overseas comparisons

The United States has progressed some way further than Australia in developing a legislative response to the spam problem. However, this response has generally been State-based, and is consequently fragmented and inconsistent.²⁹

Approximately 25 States now have Acts regulating spam, and these range from an outright prohibition on spam as in Delaware,³⁰ to legislation that simply requires a series of letters such as "ADV" to be prepended to promotional email, as in Utah³¹

27 Under United States law, compare the cases cited in David E. Sorkin, Technical and Legal Approaches to Unsolicited Electronic Mail (2001) 35 USF L Rev 325, 361.

28 Advertising of interactive gambling services through spam or other means is also constrained: Interactive Gambling Act 2001 (Cwlth) s.61CA.

29 See generally <http://www.spamlaws.com>.

30 Del Code tit 11, §§931(12)-(17), 937, 938. Acquaintance spam is excepted.

31 Utah Code tit 13, Chapter 36, applied in *Terry Gillman v Sprint Communications*, an unreported case against Sprint Communications noted at <http://www.adlawbyrequest.com/inthecourts/SprintSpam081202.shtml>.

and California,³² or that requires removal instructions to be included in each mailing as in California and Nevada.³³

California's anti-spam legislation also allows ISPs in that State to sue spammers who violate the ISP's anti-spam policy, so long as the spammer has actual notice of the policy. This legislation has been constitutionally upheld.³⁴

Washington's anti-spam law³⁵ has also been upheld.³⁶ It attacks the problem from a different angle by prohibiting the sending of email that uses a third party's domain name without permission, or has a false or invalid return address, or contains a false or misleading header. It also permits ISPs to block messages which it believes are in violation of the law, and permits an individual to recover up to \$500 damages for any spam message received in violation of the law.

Federal anti-spam legislation has been introduced to the United States Senate on a number of occasions, but has on each occasion lapsed. The only spam-related bill before the current session of Congress is the Wireless Telephone Spam Protection Act³⁷ which, if passed, would prohibit SMS spam.

Turning to Europe, the European Union Parliament's E.Privacy Directive which was passed in 2002 makes a much stronger statement against spam, prohibiting it outright in the absence of prior "opt-in" consent.³⁸ In the Asian region, Japan has the strongest position on spam, prohibiting its transmission unless an opt-out facility is provided.³⁹

Case law on spam

Clearly, the legislative regime that currently exists is at best a piecemeal solution to the spam problem, and the institution of a new *sui generis* regime is likely to be necessary in order to achieve real progress in the battle against spam. Until then, the application of existing common law rights and remedies will be of greater utility in this campaign.

Property law

Since the devices (usually computers) on which email is received are generally the property of the recipient, some indignant recipients of spam have attempted to call property law in aid of the protection of their inboxes.

There are a number of difficulties with this approach. First, even assuming that an electronic, rather than a physical, incursion into personal property is legally actionable in any circumstances, there is clearly a licence granted by the owner of an email address to (at least some) people who wish to send email to that address.

In an off-line context, a home owner grants a licence to the general public to come to the front door and knock,⁴⁰ even if the licensee has no previous

32 Cal Bus & Prof Code ss.17511.1 and 17538.45 and Cal. Penal Code s.502.

33 Nevada Revised Statutes ss.41.705 – 41.735.

34 *Ferguson v Friendfinder, Inc*, 94 Cal.App.4th 1255, 115 Cal.Rptr.2d 258 (Cal.App.1st Dist. 2002).

35 Wash. Rev. Code tit 19, Chapter 190.

36 *State v Heckel*, 143 Wash 2d 824, 24 P.3d 404 (2001).

37 HR 122.

38 Directive on Privacy and Electronic Communications (Directive 2002/58/EC),

<http://register.consilium.eu.int/pdf/en/02/st03/03636en2.pdf>.

39 See <http://www.japantoday.com/e/?content=news&cat=2&id=221054>.

40 *Holden v White* [1982] QB 679.

relationship with the resident but is visiting for promotional purposes.⁴¹ This implied licence can naturally be revoked, by means of a "no hawkers" sign on the door or a "no junk mail" sign on the letterbox, or any other method that is adequate to communicate the revocation of the licence to the licensee. Once this has been done, the licensee becomes a trespasser if he has not departed after a reasonable time.⁴²

Is the same implied licence granted by the owner of an email address to those who would send email to it? There does not seem to be any reason in principle why not, except possibly in a case where the email address has never been made public.

What, then, is the electronic equivalent of a "no hawkers" sign? Responding to an "opt-out" procedure, if available, is no doubt sufficient, but this does not provide a mechanism to prevent the original spam from being sent in the first place. One proposal for such a mechanism is known as "SMTP banner notification". During the process of sending email, an automated conversation takes place between email software of the sender and recipient, following the Internet email sending protocol (SMTP). It is possible for a "no spam" message to be transmitted by the recipient's software to the sender's during this automated exchange.⁴³

Should SMTP banner notification be regarded as sufficient to bring the termination of the implied licence to the sender's attention? It could well be argued that it should not, since in most cases the sender will never actually see the message, as the SMTP conversation is typically invisible to the human sender and recipient. What about a message on the recipient's Web site or in his email signature? Again, in the absence of statutory intervention, it is difficult to contend that the sender's implied licence to send email should be rescinded unless on the balance of probabilities the sender either saw the "no spam" message or was willfully blind to it.

In any case, an assumption has been made above that deserves closer investigation, namely that a trespass to goods can be committed by a non-physical interference with it. The law as it stands does not appear to support this assumption. In *Penfolds Wines v Elliot*,⁴⁴ Latham CJ (citing Halsbury's Laws of England) stated:

Trespass to goods is any direct infringement of the possession by another of corporeal personal chattels by means of an asportation or other physical invasion...⁴⁵

Although spam is a new phenomenon, non-physical incursions into personal property are not, and no suggestion that these are actionable can be found in case law. For example, it would be surprising if the owner of an unlisted telephone number had a proprietary right of action against cold callers for causing a non-physical interference with his telephone.

It could be argued that spam is somewhat different because it is usual that spam will be physically recorded (even if only temporarily) in a storage unit of the receiving device. However, would it make any difference to the example above if the telephone was connected to an answering machine, which recorded the

41 *Evans v Forsyth* (1979) 90 DLR 3d 155.

42 *Robson v Hallett* [1967] 2 QB 939.

43 See <http://www.cauce.org/proposal>.

44 (1946) 74 CLR 204.

45 *Ibid.* 217.

message onto a tape? If not, it seems difficult to contend that spam should be treated differently.

Although one commentator has argued that trespass to goods arising out of the receipt of spam is actionable in Australia,⁴⁶ and has in fact commenced proceedings in Western Australia on that basis (which however were dismissed on procedural grounds), the prospect of such proceedings succeeding could fairly be described as a speculative. It is likely that only the High Court could extend the law of trespass (or perhaps the law of nuisance, which now only protects real property) to provide a cause of action for the recipient of spam against its sender.

Even if such a cause of action does already exist, in most cases there will be no damage caused to a device that receives spam from a single sender (although one can certainly envision the case where an ISP or large company could have its systems brought down by a large volume of spam). Whilst trespass to goods is still actionable in the absence of damage, an award of nominal damages is the most that ordinary users could expect to be awarded against a spammer for such a trespass.

Contract

If a tortious claim for infringement of the recipient's proprietary rights does not exist, the obvious alternative is a contractual claim. Indeed, many spam recipients have endeavoured to make out the existence of contractual relationships with spam senders for the receipt of spam by the recipient for reward, in order to bring a claim for breach of contract when spam is received without payment of the agreed sum. This is usually done by means of a message directed to the spammer following the receipt of a spam message, offering to receive further spam messages at a cost of (say) \$1000 each. The offer can also be placed in the recipient's email signature or on his Web page.

The difficulty in enforcing such agreements is that there is rarely a voluntary acceptance by the spammer of the recipient's offer to receive spam for reward, since spammers almost invariably harvest and use email addresses by automatic means. Without a meeting of minds between spammer and spam recipient, the enforcement of an agreement to receive spam will only ever be possible in default of defence by the spammer.

Intentional interference with trade or business interests

The most celebrated recent case concerning spam in Australia (and the only such case to have proceeded to a judicial determination), is that of *The Which Company Pty Ltd v McNicol*.⁴⁷ Turning the tables for a moment, this is a case instituted by a spammer against a spam recipient, but is nonetheless worth reviewing for the applicability of the principles involved to future spam-related litigation.

The plaintiff in this case, a Western Australian marketing company trading as T3 Direct, claimed that the defendant, an Internet user named Joseph McNicol, had caused to be sent to an organisation named Spam Prevention Early Warning System (SPEWS) an unfounded complaint that the plaintiff had been sending Unsolicited Bulk Email.

In consequence of this alleged complaint, it was claimed by T3 Direct that SPEWS

46 Rollo T, "Liability for spam through trespass to goods" (2001) 8 PLPR 77.

47 [2002] WADC 217 (unreported). The author acted for the defendant in these proceedings.

had added its details to a spam blocklist published by SPEWS, which had resulted in a disruption to T3 Direct's business, including the termination by its ISPs of their contracts with T3 Direct (although there was an issue as to whether the ISPs were entitled to do so by reason that T3 Direct had breached their AUPs, or whether the terminations were wrongfully committed in order to avoid reprisals from anti-spam activists).

Although McNicol denied that he had sent any complaint to SPEWS, he admitted publishing a Web page complaining about T3 Direct's activities and discussing those activities on an Internet newsgroup. It was common ground that SPEWS had in fact added T3 Direct to their blocking list, and that in doing so they published a reference to the newsgroup in which McNicol had discussed T3 Direct's activities and to McNicol's Web site.

T3 Direct argued that McNicol must have intended his communications to be received by SPEWS, because although SPEWS (deliberately) had no public contact details, McNicol should have had reason to believe that they would find his complaint and act on it by adding T3 Direct to the SPEWS blocklist. T3 Direct further argued that McNicol must have known that this would cause it to suffer loss, and that his complaint thereby intentionally interfered with T3 Direct's trade or business interests.

In response, McNicol argued that he had not communicated with SPEWS in any relevant sense, but that even if he had, there was nothing wrongful in what he said, since T3 Direct had in fact admitted sending spam, by an affidavit sworn by its managing director. In any case, McNicol challenged the existence of any cause of action in Australia for an intentional interference with trade or business interests,⁴⁸ and denied that T3 Direct had suffered any loss (since on its own admission it was continuing to send spam).

On an application for summary judgment by McNicol, the court was prepared to assume that the tort of unlawful interference with trade or business interests exists in Australia. However, it would be an element of any such tort that the method of interference be an independently unlawful act, such as for example defamation or an interference with contractual relations.⁴⁹ McNicol's actions were found not to be independently unlawful, as the statements he made were admittedly true; T3 Direct did send spam.

The court also found in any case that McNicol had not communicated with SPEWS simply by publishing a public Web page and discussing T3 Direct's activities in public newsgroups. The court decided that it was not appropriate to allow the case to proceed in the hope that additional evidence would be found by discovery or interrogatories, and awarded judgment along with indemnity costs to the defendant. An appeal was instituted by T3 Direct, but discontinued.

The publicity generated by the case has perhaps been disproportionate to the importance of the principles involved, which are largely confined to the case's particular facts. Further, the authority of a decision of a Registrar of the District Court of Western Australia on a summary judgment application is necessarily limited. However, for what it is worth, the case can be said to provide authority for the following principles:

1. It will be open to a court on particular facts to find that there is nothing unlawful

⁴⁸ *Sanders v Snell* (1998) 196 CLR 329.

⁴⁹ *Ibid.*, para 31 per Gleeson CJ, Gaudron, Kirby and Hayne JJ.

in the publication of a true but unqualified statement that a person is a spammer, in circumstances where that person also conducts activities other than spamming such as permission-based online marketing.

2. It will be open to a court to find on particular facts that a person's publication of a Web page or posting of articles to an Internet (or Usenet) newsgroup is not sufficiently causally related to a third party's reliance on the information so published that the person can be deemed to have communicated the information to that third party.⁵⁰

It is notable that in this case the plaintiff had admitted on oath that it sent spam. In a case in which the evidence of the spamming activities of the plaintiff did not come up to the civil standard of proof, a statement that it had done so made in a public forum might on particular facts be defamatory, or if made to a particular contractual partner of the plaintiff might amount to an intentional interference with contractual relations.

Such torts, apart from being independently actionable, could constitute an unlawful act such as is necessary to ground an action for intentional interference with trade or business interests. It is submitted that such an intentional interference might well be made out even in the absence of a communication from the defendant to a spam-blocking service, if the action taken by the spam-blocking service was nonetheless a foreseeable outcome of the defendant's independently tortious conduct.

Liability of spam blocking services

McNicol's case says nothing of the liability of spam-blocking services themselves, or of Internet Service Providers who subscribe to such services, at the suit of those who are listed in them. It might be speculated however that so long as a spam blocking service accurately represents the listing criteria that apply to its service, or adequately disclaims any undertaking to adhere to such a policy, there is unlikely to be a plausible claim that could be raised against it.⁵¹

Internet Service Providers are likely to be in a similar position, on the further provisos that it cannot be alleged against them that they are blocking email from competitor ISPs for an anti-competitive purpose (which might amount to a secondary boycott contrary to section 45D of the Trade Practices Act), and that they in breach of no contractual obligation to the sender to receive or deliver its email.

Regardless of the above, spam blocking services have in fact been sued⁵² and even shut down altogether⁵³ by litigious spammers. As a result, some spam blocking services have adopted a policy of strict anonymity (SPEWS being a notable example), and others have deliberately avoided some of the techniques that had been used in the past to gather information for their blocking lists, such as testing mail servers for vulnerability to abuse (which could in itself be interpreted as a form

⁵⁰ The Registrar's comments in this regard are however obiter, and do not expressly avert to the relevance of the degree of foreseeability that the third party would receive the information published.

⁵¹ As an example of the latter tactic on the part of a spam-blocking service, the Dorkslayers service unequivocally (if disingenuously) states at <http://www.dorkslayers.com/intentions.html>, "The results from these queries should not be interpreted in any manner whatsoever. Do so at your own peril. In particular, the use of this list to block or tag email is NOT RECOMMENDED".

⁵² Media3 Technologies's lawsuit against prominent blacklist Mail Abuse Prevention System, LLC was settled on undisclosed terms; see <http://mail-abuse.org/pressreleases/2001-08-30.html>.

⁵³ http://www.internetnews.com/dev-news/article.php/10_995251.

of network abuse).⁵⁴

Intellectual property

One of the more creative proposals that has been developed to counter the spam problem is a patent-pending system developed by Habeas, Inc, whereby the company offers email senders a licence for the use of its trademark and a short haiku poem to be inserted into the headers of email messages. Habeas has undertaken to sue for infringement of its copyright and trademark rights, and to add to its own blacklist, any spammer who sends a message containing the Habeas headers.

Overseas comparison

United States case law on spam has been as inconsistent as the legislation from that country. Amongst the most common grounds upon which judgment has been obtained against spammers have been passing off (for email sent with forged or misleading headers),⁵⁵ and trespass against goods.⁵⁶

There are a number of isolated cases from around the world, although typically not cases of high authority. In the United Kingdom Virgin Net settled a suit against a spammer who had broken Virgin's Acceptable Use Policy.⁵⁷ A Dutch court recently ordered a spamming computer seller to stop harvesting e-mail addresses from an online address guide, and to delete the addresses already collected.⁵⁸ A German court has also granted an interim injunction against a spammer.⁵⁹ It is difficult however to draw a pattern from the few cases from outside the United States that have been reported to date.

Conclusion

This article has endeavoured to provide an overview of the state of Australian law concerning spam, as undeveloped as it is, and to make brief reference to some current proposals for regulation of this unique problem. It is difficult to resist the conclusion that the law as it stands is ill-equipped to respond to the challenge of spam, and that law reform of some nature will be required.

Some commentators have demonstrated a reticent, if not a defeatist attitude towards the reform of spam law, due to the inherent difficulties of regulating conduct online.⁶⁰ Similar considerations have not however precluded the reform of copyright law in the digital environment,⁶¹ nor the passage of "Cybercrime" legislation,⁶² or (more controversially) the implementation of an online content classification regime.⁶³

In the writer's submission, there is much to be said for the establishment of an industry-based co-regulatory framework on spam, focused on domestic offenders.

54 See <http://dsbl.org/faq-listed.html> under the heading "Are you testing servers?".

55 Cf. the cases cited in Sorkin, D. op. cit. 361.

56 See the cases collected in Sorkin, D. op. cit. 359.

57 See <http://www.vnunet.com/news/83928>.

58 See <http://www.idg.net/go.cgi?id=776096>.

59 LG Berlin 16 O 320/98 (unreported), 13 October 1998, <http://www.online-recht.de/vorent.html?LGBerlin981013>.

60 See Sorkin, D. op. cit. 383-384.

61 Copyright Amendment (Digital Agenda) Act 2000 (Cwlth).

62 Cybercrime Act 2001 (Cwlth).

63 Broadcasting Services Amendment (Online Services) Act 1999.

Even for foreign offenders against whom enforcement is more problematic, the making of a strong legislative position statement on spam will create an ideological footing for the future implementation of leading-edge technical measures against spam, perhaps beginning with an approved schedule of industry-maintained blacklists. Such steps will not eliminate the problem, but they are at least a first line of defence against Internet marketers who would treat our email inboxes as public property.