mark. In many cases celebrity merchandise carries images that are not used in order to indicate the origin of the goods but simply for their own innate appeal.

Some celebrities do use their persona as trade marks in the traditional sense, for example 'Elle Macpherson Intimates' underwear or 'Paul Newman's Own' range of condiments. These trade marks clearly give their owners more protection for their personality rights than they would otherwise have, especially as they may be able to establish that their names are well-known marks under the provisions of s120(3)(c). This protection however still suffers from the requirement that any offending use must be use as a trade mark.

Trade marks legislation suffers from the same weakness as the other areas of law already discussed, it is not designed to protect personality rights and is fundamentally ill-equipped to do so.

CONCLUSION

Although personality rights do not exist in Australia it is long overdue for such rights to be formally introduced. The courts have introduced a de-facto basis for making personality rights claims by extending and distorting the laws of passing off and defamation. The rationale for doing so, in nearly every case is that the public expects, perhaps out of some notion of fairness or natural justice, that such rights already exist. One of the many problems with this approach is that we are now left with a poorly equipped and inconsistent set of laws that try valiantly to enforce a set of rights that do not really exist. This not only results in difficulties for celebrities wishing to know their rights. It creates ludicrous inconsistencies such as the *Tracey Wickham* case and the *Kieren Perkins* case which tarnish one of the principle ideals of justice - consistency.

Clearly many courts in Australia feel that the law should protect against the misappropriation of one's personality and it is evident that the public assumes such rights already exist. Therefore the debate about whether they are necessary would already seem to be concluded. If we accept that such rights are necessary then surely it is better to enable them through properly drafted and well-thought through legislation than to continue with the present hodge-podge of inconsistent decisions and legal fictions.

David Bowman is a biomedical engineer and is currently a Masters of Intellectual Property student at the University of Technology Sydney.

1 *Pacific Dunlop v Hogan (1989) 32 FCR 314*

2 Heerey P "Character and Personality: Where to for Protection in the Intellectual Property Area?"(1999) *Intellectual Property Forum* 39 at 8

3 *Ibid*

4 McMullan J "Personality Rights in Australia" (1997) *Australian Intellectual Property Journal* 8 at 86

5 *Reddaway v Banham* (1896) AC 199

6 *Conagra Inc v McCain Foods (Aust) Pty Ltd* 23 IPR 193

7 *Radio Corp Pty Ltd v Henderson* (1960) 60 SR (NSW) 576

8 *Olivia Newton-John v Scholl-Plough (Aust) Ltd* (1986) ATPR 40, 697

9 *McIlhenny Co v Blue Yonder Holdings Pty Ltd* (1997) 30 IPR 187

10 op cit note 2 at p. 13

11 op cit note 4 at p. 87

12 *Talmax Pty Ltd v Telstra Corporation Ltd* 36 IPR 46

13 *Pacific Dunlop v Hogan* (1989) 23 FCR 553

14 *Wickham v Association of Pool Builders* (1988) 12 IPR 567

15 op cit note 12 at p 53

16 op cit note 2 at p 16

17 Slater A "Personality Rights in Australia" (2001) 20(1) *Communications Law Bulletin* 12 at 13

18 *Tolley v JS Fry & Sons Ltd* (1931) AC 533

19 (1991) 23 NSWLR 443

20 op cit note 2 at p 10

21 Weathered L "Trade Marking Celebrity Image: The Impact of Distinctiveness and use as a Trade Mark" <http:// www.bond.edu.au/law/blr/vol12-2/Weathered.doc>

The End of Spam?

Nick Abrahams and Colin Chang consider Australia's current approach to spam, and the proposals of a recent NOIE report.

Spam has become enemy number one in enterprise IT. A serious threat to security and productivity, spam is a real headache for networking pros.

Spam is no longer merely an annoyance. The widespread proliferation of spam in recent years now threatens the very viability of email as a communications medium. It has been estimated that as much as 55% of all email traffic now consists of spam[1]. According to Brightmail (a vendor of anti-spam solutions), the number of spam attacks detected on its network more than doubled from 2.7 million in the month of January 2002 to over 6 million in the month of January 2003[2].

Employers hate spam due to its impact on productivity whilst network providers hate spam due to the drain that it places on their limited resources. In a recent survey by Silicon.com, 82% of respondents reported spending as much as one and a half hours per week dealing with spam[3]. It is estimated that spam will cost companies more than US$20.5 billion this year and that this will blow out to more than US$198 billion within the next 5 years[4].

It will probably come as a surprise to many that 2003 marks the 25th anniversary of spam. The earliest recorded case of spam dates back to 1978 when Gary Thuerk, a sales representative with DEC, sent an email to every person with an ARPAnet (the precursor to today's Internet) address on the western seaboard of the United States advertising DEC's latest products[5]. The result was, not surprisingly, a huge groundswell of complaints from within the ARPAnet community.

From these early beginnings, spam has grown to become one of the largest issues facing Internet users today. The attraction of spam to mass marketers is that, unlike traditional mail, it costs no more to send 1 million messages than it does to send a single message. Even if a spammer only receives a positive responses from 1% of recipients, the number of response in absolute terms can prove highly lucrative. In recent years, a whole industry has arisen to combat the increasing spam problem. It has been estimated that

revenues for anti-spam vendors will total US$653 million this year and increase to over US$2.4 billion in 5 years time[6].

The call for governments to take action has grown louder as industry and users alike have struggled to cope with the increasing flood of unsolicited emails. Even direct marketing groups have joined in the call for legislation as fears grow that spammers will threaten the viability of legitimate bulk email as well. In the United States, twenty-six states have introduced legislation in various degrees to fight the spam epidemic. The European Union has recently joined suit[7].

CURRENT SPAM REGULATION IN AUSTRALIA

Australia does not presently have any legislation in place which directly addresses spam. This deficiency was recently highlighted in a case in which a man sought to extract revenge against a former girlfriend as well as her flatmate by sending emails to thousands of addresses telling the recipients that they were the owner of an unclaimed bank account or the beneficiary under a deceased estate, and including a number to call - a number which belonged to the workplaces of the former girlfriend and her flatmate. The result was a flood of incoming calls to these two workplaces and interfering with the normal flow of business operations. At the time of writing, the spammer had yet to be charged as the police struggled to find an appropriate charge to lay against the spammer[8].

Whilst legislation such as the *Privacy Act* 1988 and the *Crimes Act* 1914 have some application to spam, they were not drafted with the issue of spam in mind and hence their effectiveness in combating spam is far from ideal.

NOIE REPORT

In April 2003, the National Office for the Information Economy (**NOIE**) released a report titled "*The Spam Problem and How It Can Be Countered.*" In it, NOIE called for a multifaceted approach in tackling spam which consisted of:

- **Legislation** – Existing legislation would be amended to handle spam. The crux of such amendments would be the prohibition of commercial electronic messaging without the consent of the end user (except where there was an existing business relationship), thus introducing an "opt-in" mechanism. Furthermore, each email would be required to include the sender's correct contact details. This approach is based loosely upon the European model.
- **Industry Assistance** – Bodies such as the Internet Industry Association (**IIA**) and the Australian Information Industries Association (**AIIA**) would be asked to encourage their members to take steps to establish both technical as well as contractual barriers to the transmission of spam.
- **International Cooperation** – Australia should cooperate with both multilateral bodies (such as the OECD and APEC) as well as partner country agencies to develop international guidelines and mechanisms in a joint bid to reduce the spam problem.
- **Partner Agency Cooperation** – Where appropriate, government agencies such as the ACCC, ASIC and the Office of the Federal Privacy Commissioner should ensure that the legislation are enforced against spammers.
- **Information and Education** – Educating the public on the nature of spam and providing resources to assist in the reduction of such spam.

It is interesting to contrast the recommendations contained in NOIE's final report against those contained in the interim report that it published in August 2002. The interim report did not favour a legislative route and stated that legislation would

> ... *"not eradicate or minimise spam, given the difficulties in identifying spammers, the global nature of the Internet and the competing enforcement priorities faced by regulatory agencies."*

This approach was widely criticised by a number of stakeholders. The author of the interim report, Allan LeBusque, was replaced by Lyndsay Barton who subsequently rewrote the report from scratch[9]. There has been much speculation as to the reasons for the turnaround in NOIE's position[10], but the fact remains that the legislative approach advocated by the final report will provide another useful weapon in the fight against spam.

It should be noted that a legislative approach will not, in itself, eradicate the spam problem. Much of the spam

transmitted today originates from countries outside of Australia – countries in which Australian law has no jurisdiction. It has been estimated that as little as 16% of all spam sent globally originates from Australia[11]. Furthermore, legislation is only likely to prove effective against legitimate marketers. Unscrupulous marketers are unlikely to take note and the majority of those who do will simply shift their activities to those jurisdictions which are more tolerant of such actions.

CONCLUSION

It is clear that the only way that spam can be controlled is for a united approach to be taken by government, industry and users alike. Further, such an approach must be adopted not only in Australia, but also by governments in other jurisdictions as well. The fight against spam still has a long way to go. However, with the increased attention being given to the problem by governments worldwide, there is hope yet that we may eventually see a marked reduction, though not eradication, of spam in our everyday lives.

Nick Abrahams is a partner and Colin Chang is a lawyer in the Digital Industries Group at Deacons.

1 www.smh.com.au/articles/2003/06/02/1054406110138.htmlwww.messagelabs.com/viruseye/threats/

2www.brightmail.com/press/state_of_spam.pdf

3 www.silicon.com/news/165-500001/1/4618.html

4 www.vnunet.com/News/1141508

5 www.templetons.com/brad/spamreact.html

6 www.vnunet.com/News/1141508

7www.brightmail.com/press/state_of_spam.pdf For more details about spam laws, visit David E Sorkin's web site: www.spamlaws.com/

8 www.smh.com.au/articles/2003/06/09/1055010929990.html

9 See "Choking on Spam" by Garth Montgomery in *Australian Personal Computer*, June 2003

10 See "Choking on Spam" by Garth Montgomery in *Australian Personal Computer*, June 2003

11 www.caube.org.au/australia.htm

Update: Cybercrime Code of Practice for ISPs

Elizabeth Levinson and Natalie Ceola provide an update on the Internet Industry Associations Cybercrime Code of Practice.

Following 18 months of development the Australian Internet Industry Association (**IIA**) released a draft Cybercrime Code of Practice (**Code**) in relation to cybercrime on Monday, 21 July 2003.

THE PROBLEM

While the Internet can deliver enormous efficiencies for business, cybercrime is proving to be an escalating cost for Internet Service Providers (**ISPs**), government and businesses. Crime involving computers and electronic communications is a big challenge facing organisations as crimes such as internet based fraud, hacking, card skimming and electronic money laundering are difficult to detect.

The *2003 Computer Crime and Security* Survey, run in conjunction with the Australian Federal Police, Queensland Police, Western Australia Police and South Australia Police highlighted the extent of electronic crimes. This survey found that:

- total losses for organisations surveyed in 2003 were estimated at $12 million, more than double the losses for 2002
- 42 per cent of organisations experienced one or more computer attacks which harmed network data or systems
- financial fraud, laptop theft and virus, worm and Trojan infections were the largest source of losses.

CYBERCRIME CODE OF PRACTICE

Improving the safety and security of the Internet depends on early detection of criminal activity. The Code attempts to balance differing concerns including the law enforcement agencies' need to identify, investigate and prosecute offences, the privacy of end users and costs to the industry in complying with the Code.

The objectives of the Code are to:

- facilitate cooperation between ISPs and law enforcement agencies and establish clear policies and procedures for investigations;
- provide transparent mechanism for the handling of law enforcement agency's investigations for the Internet industry and ensure both ISPs and law enforcement agencies understand the procedures;
- promote positive relationships between law enforcement agencies and the Internet industry; and
- ensure that the privacy of users of the Internet will be protected from unlawful intrusion by law enforcement agencies.

The Code stipulates that customer information collected by ISPs, must be retained for six or 12 months, depending on the type of information. Personal information such as a customer's name, username, email address, phone number, credit card details and address details, must be retained for the greater of six months from the date a customer ceases to be a customer or 12 months after the creation of the record. Operational data, such as dynamic IP allocations records, dates and time of log-ins and the total data transferred, must be retained for six months from the date of creation. ISPs, however, are not required to capture subscriber's phone numbers via caller line identification.

The Code was delayed in its release due to privacy concerns. However, after consultation with the Privacy Commissioner it was determined that ISPs were not bound by the *National Privacy Principles* which were introduced on 21 December 2001 under the *Privacy Act* 1988 (Cth) (**Privacy Act**).

However, the Code requires all ISPs wishing to be a party to the Code to be bound by the Privacy Act. This means