be respected"[6] would be sufficient. It is likely that more detailed rules relating to privacy will be required.

Other provisions also recognise the important role of the media in facilitating the free flow of information to the public. Importantly, it is not an offence for a journalist to refuse to give information, answer a question or produce a document or record which he or she would otherwise be required to give under the Act (eg. to the Privacy Commissioner) where this would tend to reveal the journalist's confidential source.[7]

The legislation also recognises[8] that the public interest in the free flow of information to the public through the media may compete with the right to privacy. The Privacy Commissioner and approved privacy code adjudicators will be required to take these competing interests into account when considering complaints.[9]

CONCLUSION

The Act contains provisions designed to preserve the ability of the media to provide information to the public. The most important of these provisions is the journalism exemption. Like other provisions in the Act, the journalism exemption is general in its terms. This gives the Act the flexibility to accommodate technological and other developments, but also means that much will depend upon interpretation of it by the Commissioner and the courts.

Glen Sauer is a lawyer at the Sydney office of Blake Dawson Waldron.

[33] Attorney General Fact Sheet – Privacy and the Media, July 19 2001 http://law.gov.au/privacy/newfacts/Media.html.

[5] Office of the Federal Privacy Commissioner telephone hotline 7 January 2002.

[6] see, eg., clause 2.2(e) of the Commercial Radio Code of Practice ("In the preparation and presentation of current affairs programs, a licensee must ensure that respect is given to each person's legitimate right to protection from unjustified use of material which is obtained without an individual's consent or other unwarranted and intrusive invasions of privacy"), clause 9 of the Australian Journalists' Code of Ethics ("They shall respect private grief and personal privacy and shall have the right to resist compulsion to intrude on them"), clause 3 of the Australian Press Council Statement of Principles ("Readers of publications are entitled to have news and comment presented to them honestly and fairly, and with respect for the privacy and sensibility of individuals. However the right to privacy should not prevent publication of matters of public record or obvious or significant public interest") and the MEAA Code of Ethics (MEAA members commit themselves to "respect private grief and personal privacy").

[77] section 66 (1A)

[9] sub-section 29(a).

Spam – Is Enough Being Done?

Ben Kuffer and Rebecca Sharman take a hard look at spamming issues.

On 30 May 2002, the European Parliament voted to approve an opt-in system for email, faxes and automated calling systems. The result of this is that European businesses and individuals should give permission for receiving unsolicited electronic communications for marketing purposes. The formal adoption of the directive by member States makes it illegal to send unsolicited email, text messages or other advertisements to individuals with whom companies do not have a pre-existing relationship.

CAUBE believes this will turn Europe into a virtual "spam free zone" by the end of 2003. However, may European politicians and lawyers have voiced doubt over the effectiveness of the new anti-spam laws. As Michael Cashman, MEP and Member of the Citizen's Freedoms and Rights, Justice and Home Affairs Committee points out "spammers do not abide by the law and the expectation that they will be caught under this new directive is crazy". Furthermore, the directive does nothing to curb spam coming from outside Europe and it will take years to restructure EU member States IT systems which presently operate on an opt-out approach.

The Federal Government announced in February 2002 that, with the continuing expansion of Internet usage in Australia, it wishes to ensure that "spamming does not get out of hand". This article considers the problem of spamming, the effectiveness of the current legislative and self-regulatory measures to limit spamming and what can be done to improve the current deluge of emails that hit your inbox on a daily basis.

WHAT IS SPAM?

Unsolicited bulk email, commonly referred to as "spam", is any electronic mail message that is transmitted to a large number of recipients where some or all of those recipients have not explicitly and knowingly requested those messages. Spam is now recognised by government, industry and consumer groups in Australia and overseas as a significant problem requiring urgent management.

Spam raises many issues, including breaches of privacy, illicit content, misleading and deceptive trade practices and increased costs to consumers and businesses for internet service provider access. Spammers are in effect taking resources away from users of valuable resources and the suppliers of these resources without compensation and/or authorisation.

How Prevalent is Spam?

Spam is growing at a rapid rate. Statistics compiled by Brightmail Inc, a spam filtering service, state that in the last 12 months, spam constituted 20% of all email screened by them. The Coalition Against Unsolicited Bulk Email (CAUBE) found that the number of unsolicited bulk email received by Australian Internet users in 2001, was six times more than that received in 2000. America Online have stated that spam accounts for half of all electronic mail they process.

In 1999 CAUBE conducted a 12 month spam survey, where addresses were 'planted' at internet sites where spammers were known to have harvested addresses. CAUBE found that of the spammers utilising the 'planted' email addresses, Australian based organisations accounted for 16% of the spammers caught.

PROBLEMS ASSOCIATED WITH SPAM

A number of problems are associated with spamming. It has been said that, the Internet relies on the cooperative use of private resources and that the sending of an email is a privilege not a right. These issues are described below.

No cost to the sender means unlimited spam

Spam enables a sender to advertise

instantaneously to a huge number of people all around the world for negligible cost. The commercial viability of the marketing capacity of spam can not be matched by any traditional face-to-face methods. By simply participating in chat rooms, or discussion groups, or subscribing to online magazines or clubs, spammers have access to your email address. The emails obtained from these public sites are then sold and resold to spammers all around the world. For this reason, the possible sources from which a user will receive spam is potentially huge, and to some extent unlimited.

The recipient and Internet Service Providers (ISPs) pay for receiving spam – time & money

A recipient incurs numerous costs when receiving spam. Firstly, bills received by innocent users from ISPs will increase due to time spent on unnecessary downloads. The large number of downloads associated with spam ultimately impact on subscription fees across the industry. Furthermore, as ISPs cannot distinguish between spam and other types of emails, they have to process all messages, which results in slower internet speed. CAUBE reports that as much as 10% of ISP operating costs are related to processing spam.

The recipient also loses the time it takes to physically delete spam. This is particularly significant when the recipient is an employee, as this is effectively time and money lost by the company. Furthermore, hitting delete does nothing to control the scale of spam.

Spam reduces the Owners Control over their Mailbox

Spammers infiltrate mailboxes without the consent of the owner. This means that the owner has no say on what information they receive, even though they are the ones who pay for the mailbox.

The value of legitimate email is diminished by spam

It can be difficult to locate legitimate email amongst spam. As a result, legitimate email may not be read or may be accidentally deleted. Furthermore, the infiltration of inboxes by spam inevitably leads many users to simply stop using their email account.

Denial of Service (DoS) Attacks

It has been suggested that spam has been used deliberately in connection with DoS attacks.

Filters are Ineffective

Filters can only be used to bar spam after you have received the unsolicited email. Furthermore, as spammers continually change their emails, filters are ineffective at stopping spam from senders even if you have placed a block on them. CAUBE points out that even the existing 'qualitative' filters which supposedly detect and discard spam, are problematic in that they sometimes reject legitimate mail as mistakenly identified spam.

Spoofing

In his press release dated 9 April 2002, Senator the Hon Richard Alston identified "spoofing" as a potential spam related problem. Spoofing occurs when nuisance email is routed through an innocent firm so that it appears to have been sent by it. This has the potential to damage commercial reputations and divert resources from the firm to rectify the problem and deal with annoyed spam recipients.

WHAT IS BEING DONE?

In its Press Release of February 2002, the Federal Government stated that the National Office for the Information Economy will examine the effectiveness of the measures in place to counter spam. The findings of the review are to be made public by mid-year. Presently, there is a myriad of regulatory and self-regulatory schemes in place.

Self-Regulation

The Government's *E-Commerce Best Practice Model,* titled *"Building Consumer Sovereignty in Electronic Commerce"*, covers acceptable conduct for businesses dealing in e-commerce and serves as a guide for the various industry codes. The model states that spam sent by business to people with whom they have no relationship is unacceptable conduct.

The Internet Industry Association (IIA) Code of Practice provides that IIA members and subscribers to the code must not engage in sending spam and must not encourage spam. The exception to this is if they have a pre-existing relationship with the recipient. In this case IIA members must provide recipients with the opportunity of opting-out.

The Australian Direct Marketing Association (ADMA) Code of Practice sets out specific standards for organisations involved in direct marketing to consumers. The code binds all ADMA members and all employees, agents, subcontractors and suppliers of ADMA members. The ADMA code reflects the NPPs.

Regulation by codes of practice has numerous limitations in relation to the current proliferation of spammers. In particular, compliance with a code is reliant upon the participant's desire to comply, its fear of legislation and/or its need for protection. It comes as no surprise that spammers do not necessarily have any desire to voluntarily adopt codes that restrict their conduct. Typically spammers have no interest or investment that they wish to be protected and only stand to lose a portion of their monthly ISP access fee if they are cut off from their ISP. Spammers usually receive no protection from codes and have no desire or incentive to comply with their provisions

Privacy Act

On 21 December 2001, the provisions under the *Privacy Amendment (Private Sector) Act* 2000 (Cth) came into force. The Act gave legislative force to 10 National Privacy Principles (NPPs) with which certain private sector organisations must comply. Under NPP 2.1, private sector organisations must not use or disclose personal information about their customers, for example using their email address to send spam, for a purpose other than the primary purpose for which the information was collected, unless they have the consent from their customers to do so. If the spam is being sent for the purposes of direct marketing, permission must be sought prior to use of the information, unless it is impracticable to do so.

Furthermore, private sector organisations must give their customers the chance of opting out of future emails. However, providing an opt-out scheme does not save an organisation from being in violation of the provisions requiring consent. CAUBE have expressed concern over the success of opt-out schemes. They point out that a 'list that is operated by spammers is fundamentally untrustworthy. It is not in the spammer's interest to remove addresses – it is only in their interest to add them'. Furthermore, contacting every individual spammer and requesting that you do not receive any further communication, may take longer than just hitting delete.

If an organisation fails to comply with the NPPs, the Privacy Commissioner can investigate the complaint and make determinations including; requiring the

corporation to apologise to the complainant, that the complainant be compensated for their loss and that the corporation change their procedures and practices. These orders, if made by the Privacy Commissioner are not binding. If a corporation fails to comply with the determinations, the Privacy Commissioner or a complainant can commence proceedings in the Federal Court to have them enforced. The effectiveness of these sanctions against spammers are questionable.

The Online Content Scheme (OCS)

The OCS, created pursuant to the *Broadcasting Act* 1992 (Cth) , is a joint effort involving the Internet Industry, the Australian Broadcasting Authority (ABA) and the Office of Film and Literature Classification (OFLC). The scheme, which monitors and investigates offensive content on the internet, is administered by the ABA. As spam can contain offensive or illegal material, it may be caught by the OCS.

Any member of the public can make a complaint to the ABA about offensive content they have viewed on online. The ABA must then investigate the complaint and determine whether the material falls within one of the prohibited classification categories within the OCS as established by the OFLC. If the material is potentially prohibited, and is hosted within Australia, the ABA will issue the internet content host (ICH) with a notice to take down the content. The ICH faces potential penalties for non-compliance with such a notice. If the offensive material is hosted outside Australia, the ABA will inform ISPs and the makers of internet content filters. The specific content of emails is not subject to OCS scrutiny. Where the email directs the recipient to a web page, this material will be within the scope of the OCS.

Interactive Gambling Act 2001 (Cth)

It is an offence under the *Interactive Gambling Act* 2001 to broadcast, datacast or publish an advertisement in Australia regarding certain interactive gambling services. The Act covers advertisements in the form of emails, such as spam. Complaints about prohibited gambling content online can be made to the ABA by both members of the public and Australian businesses. If the content is hosted within Australia, then the ABA must not investigate the complaint, but refer the matter to the Australian Federal Police. If the content is hosted outside Australia, the ABA will notify the markers of internet content filters and ISPs so that they can update the filter lists to include the new content.

Criminal Provisions

Section 85ZE of the *Crimes Act* 1914 (Cth) provides that it is a criminal offence to use an internet carriage service to harass or menace another person. This provision does not apply to internet content per se. However, email and spam, which uses a carriage service would come within the scope of the provision.

Under s76E of the *Crimes Act* (now repealed) it was an offence to interfere with the lawful use of a computer using a carrier. Spamming may fall within this category. New offences under the *Cybercrime Act* 2001 (Cth) provide that any unauthorised impairment of electronic communication to or from a computer is an offence. To be held liable, a person must know that the impairment is unauthorised and intend, or is reckless as to the impairment. The Explanatory Memorandum to the Act states that this offence is designed to target denial of service attacks by way of spamming, where an email address is overloaded with a large volume of unwanted messages thus overloading the computer and disrupting, impeding or preventing it from functioning.

Trade Practices Act/State Fair Trading Legislation

It is not uncommon for spammers to make misleading and deceptive representations, engage in bait advertising or promote illegal schemes, such as pyramid selling. This conduct is in breach of the *Trade Practices Act* (TPA) and State Fair Trading legislation. The TPA is enforced by the Australian Competition and Consumer Commission (ACCC). The ACCC can initiate legal proceedings against a company whom they believe is in breach of the TPA. Penalties for breaching the TPA include damages, injunctions and ancillary orders. Of course, the TPA is only effective if the spammer can be identified and has assets in the jurisdiction.

Trespass

In the recent US case *Intel v Hamidi*, the Court granted an injunction preventing an aggrieved ex-employee from sending spam to Intel employees. The court reasoned that the sending of spam constituted a trespass to the company's server, as Intel's email system was internal, proprietary and for employee use only. The ex-employees argument that the emails were Internet based and did not originate on Intel property and were not sent to Intel property was rejected by the court. As this is a US case, it is difficult to predict how an Australian court will deal with this issue.

PROPOSED SOLUTIONS

Despite the Federal Government's stated intentions of addressing the prevalence of spam, it was reported on 6 June 2002, that the Australian Government web site 'The Source' sent out spam emails promoting free movie tickets to people. This incident raises serious questions regarding the sincereness of the Federal Government's intentions and is being investigated by the Federal Privacy Commissioner. As stated by Senator Kate Lundy, Shadow Minister for Information Technology and Sport in a press release, '.. the Coalition is not leading by example.' Senator Lundy quite rightly called for a directive from the Ministers office to all departments and agencies with an interactive online presence to ensure that this does not happen again.

An alternative to the European model, proposed by CAUBE, is the introduction of direct legislation. Such legislation should make spam an offence, prohibit the sale and advertising of spamming tools, and provide an independent cause of action on behalf of the recipient to recover damages from the spammer. It is suggested that a private cause of action is necessary as requiring the action to be commenced by the government places strain on federal revenue.

With the increasing prevalence of spam it is pertinent to note the requirement of the European Parliament that "a review of the Spam Directive occur within 3 years of its application". It would be appropriate for the Australian Federal Government to ensure a similar review occurs.

It remains to be seen whether or not the Federal Government is genuinely prepared to get tough on spammers. If this is the case, then one has to question the tools it currently has at its disposal. Perhaps the CAUBE model suggesting direct legislative pronouncement would be more effective in curbing this annoyance.

The views expressed in this article are those of the authors and not necessarily those of the firm or its clients.

Ben Kuffer, is an Associate, and Rebecca Sharman is a Law Graduate in the Information, Communications & Technology Group at PricewaterhouseCoopers Legal, Sydney.