Green eggs and SPAM – regulation of unsolicited email in Australia

Sophie Dawson, Blake Dawson and Waldron

Sophie is a senior associate of Blake Dawson and Waldron. She practises in the area of Media Law, and has experience in providing pre-publication advice and in running commercial, and particularly defamation, litigation. Pre-publication advice extends to contempt, listening devices, copyright and trade practices issues, as well as to statutory restrictions on publication that affect publishers.

1. Introduction

As most people now know, spam is a term used to describe unsolicited bulk email. Spam is now recognised by government, industry and consumer groups in Australia and overseas as being a problem requiring management. In addition to being a nuisance for the recipients, it can cost them time and money and can increase the costs of ISPs. It has also been associated here and in the US with misleading and even criminal conduct. Spam has been the subject of at least five cases in the United States and at least one in Australia.

That said, not all bulk email is bad. Email is a cheap means of communication which can be used by business to communicate effectively with consumers. For example, travel companies use bulk emails to tell their customers promptly about airfare and travel deals available, which many customers like to know. In most cases, such emails are solicited. That is, the customers have requested that available deals be emailed to them regularly. In addition, spam is environmentally friendly relative to traditional direct mail.

Moreover, just as some people are happy to receive their David Jones' brochure in the post each season, some keen shoppers are no doubt pleased to receive unsolicited email advertising.

The challenges which bulk email presents are therefore to ensure that it is sent only to those that wish to receive it and to ensure that it is not used in a misleading or criminal way.

A number of measures have been taken to manage bulk email in Australia. These include industry codes, anti-spamming measures taken by ISPs and, most recently, amendments to the *Privacy Act 1988* which extend to the private sector. In addition, sections 52 and 53 of the *Trade Practices Act 1974* and section 76E of the *Crimes Act 1914* (Cth) will sometimes apply to spammers. As discussed below, at least one spammer has now been convicted of an offence under the latter provision.

These measures are complemented by an increasing emphasis in the marketing industry on permission based marketing and respect for customer preference.

2. Why has spam got such a bad name?

In contrast to traditional direct mail, email can be sent to millions of people at almost no cost. Available technology allows spammers to "harvest" a very large number of email addresses from websites and news groups. The only cost associated with sending bulk emails is the cost of internet access, which is normally only about $20.00 per month.

When spam is sent to people that do not wish to receive it, it is wasteful for everybody involved. It takes time for recipients to identify and delete unsolicited email, particularly if there are video or other bulky attachments, and they must pay for internet access during that time. Many ISPs reportedly find that up to 50% of their email traffic is spam. This means that they have to provide staff and equipment sufficient to carry up to twice the number of emails that they would otherwise have to provide for. Again, this ends up costing the consumer by way of access fees. When such spam is sent for marketing purposes, it is also a waste for the businesses which send it, in that the spam is likely to annoy rather than ingratiate potential customers.

In addition to these problems, spam is often associated with misleading and even criminal conduct. This has been recently acknowledged by the Australian Competition and Consumer Commission[1], which has identified misleading, deceptive and fraudulent activity on the internet as an enforcement priority. The anonymity which the internet provides and the enforcement problems that this creates guarantee that this will be a continuing problem.

3. Spamming can be a Crime

Existing criminal laws, the *Corporations Law* and the *Trade Practices Act 1974* contain prohibitions which are likely to catch most of the common types of "dishonest" spam. That is, spam which is specifically designed to mislead, deceive or rob the unwary. The problem is one of enforcement rather than regulation.

For example, a commonly used way to prevent recipients of spam from identifying the sender is to send the message via third parties' servers and to make it look like it came from that server. A recent case[2] illustrates that this method may sometimes interfere with third parties' computers in such a way as to constitute a crime under part VIA of the *Crimes Act* 1914 (Cth). The same case illustrates the way in which other criminal laws can catch dishonest spammers.

On 30 October 2000, Steven George Hourmouzis was sentenced to two years imprisonment in relation to each of three crimes which he pleaded guilty to having committed by sending a fraudulent email to millions of people in Australia and overseas. Of the 2 year sentence, he was required to serve 3 months with a good behaviour bond for the remainder of the term.

The convictions resulted from spam sent by Mr Hourmouzis and an associate and from bulletin board messages posted by them which were designed to inflate the price of a NASDAQ listed corporation called Rentech Inc in which they had purchased shares. In May 1999, they sent in excess of three million emails messages to addresses in Australia, the United States and elsewhere. The messages were sent through an ISP from which Mr Hourmouzis had anonymously purchased internet access kits. He used Telstra telephone lines to connect with the ISP.

So as to avoid detection, Mr Hourmouzis relayed the messages through nine third party servers, which made the messages look to recipients as though they had emanated from those servers. Use of the third party mail servers in this way did not damage them, but required them to be shut down in order to clear them of the messages. The businesses that used the servers also became concerned about the effect on their reputation as a result of the spam and that somebody had gained access to the servers.

The spam and bulletin board messages achieved Mr Hourmouzis's objective. Trading in the shares of Rentech Inc on the day following that on which the emails were sent was ten times the average daily trading volume. The share price doubled before trading was halted pending an announcement to be made by the Company. Rentech Inc issued a press release denying the statements in the email and bulletin board messages. Its share price then fell to below the price at which it had started.

The first two counts to which Mr Hourmouzis pleaded guilty were of making statements or disseminating information that was:

1. false in a material particular; and
2. materially misleading and likely to induce the purchase of securities by other persons contrary to the Corporations Law.

The maximum penalty for these offences is a $20,000 fine or imprisonment for five years or both.

The third count to which he pleaded guilty is one which is of more general relevance to spammers. It was of committing an offence under sub-section 76E(c) of the Crimes Act 1914, which relevantly provides that:

"a person who, by means of a facility operated or provided by the Commonwealth or by a carrier, intentionally and without authority or lawful excuse....interferes with, interrupts or obstructs the lawful use of a computer....is guilty of an offence.

Penalty: Imprisonment for 10 years".

A bulk emailer that uses third party computer facilities to send very large quantities of unsolicited bulk email, knowing that to do so will cause an interruption to those facilities, risks being charged with an offence under section 76E.

The sentence in the Hourmouzis case demonstrates that the penalties may be harsh. In that case, a custodial sentence was imposed notwithstanding that Mr Hourmouzis had cooperated with police, had pleaded guilty and had no prior convictions. That said, he was not helped by an email that he had sent to his associate which said:

"This is illegal but I like it. Just don't mention anything to anyone about anything until we purchase the stock and always keep our true identity very concealed."

Of course, the *Corporations Law* and the Commonwealth *Crimes Act* are not the only pieces of legislation which can be used against bulk emailers who engage in misleading, deceptive or fraudulent conduct. Such people and organisations may also find themselves being the subject of civil or criminal proceedings commenced pursuant to the *Trade Practices Act* (1974) (Cth), State Crimes Acts or Fair Trading Acts or, for example, be sued for passing off. There have been a number of cases in the US which have relied upon similar laws, particularly in relation to companies which have sent out emails which have been made to appear to emanate from a different source.[3]

4. The Privacy Amendment (Private Sector) Act 2000

4.1 Introduction

At present, self regulation and ISP contracts are the only constraints on honest spamming activity in Australia. This will soon change quite dramatically with the commencement of the private sector amendments to the *Privacy Act 1988* (the "Act"[4]). The Act will subject bulk email to substantial restrictions and requirements. The amendments commence on 21 December 2001, or in the case of most small businesses to which the Act applies, 21 December 2002 .

As with most new legislation, there is much doubt as to how the Act will apply. Draft Guidelines released by the Privacy Commissioner on 7 May 2001[5] (the "Draft Guidelines") reveal how the Commissioner is likely to approach the legislation, including the way in which he considers ambiguities should be resolved.

If the Act is interpreted by the courts consistently with the Draft Guidelines, then it will limit the means by which Australian bulk emailers can collect email addresses and the sources from which they can obtain them. It will also limit use of email addresses collected by spammers after 21 December 2001 to those belonging to individuals who have consented to receive spam.

Whether or not the Act will be interpreted in accordance with the Draft Guidelines remains to be seen. There appears to be at least one key difference between it and the Explanatory Memorandum which deals with the private sector amendments to the Act.[6] The Explanatory Memorandum has greater importance as extrinsic material which can be taken into account by a court interpreting ambiguous provisions of the Act.

From a business perspective, however, the Draft Guidelines count. The Act endows the Privacy Commissioner with power to investigate and make determinations in relation to interference with the privacy of an individual.[7] Even if ultimately overturned by a court, a determination by the Commissioner that an organisation has interfered with the privacy of an individual is likely to have a substantial negative impact on that organisation's reputation.

Under the Act, an act or practice of an organisation will be an interference

with privacy if it breaches a privacy code which binds that organisation and has been approved by the Privacy Commissioner or, in the absence of a code, breaches a National Privacy Principle. Codes will not be approved by the Commissioner until 21 December 2001. The National Privacy Principles are contained in schedule 3 of the Act.

4.2 "Personal Information" and "Organisations"

The National Privacy Principles apply to "organisations". That term is defined to include individuals as well as companies, partnerships, unincorporated associations and trusts.[8] Small Business Operators and political parties and State and Territory government bodies are excluded from the definition.

The requirements of the National Privacy Principles relate to "personal information", which is defined to mean:

"information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion".

It appears from the Draft Guidelines that the Privacy Commissioner takes the view that all email addresses are, without more, "personal information". Many spammers will not have any other information about the individuals to whom they send emails. Whether or not an email address constitutes personal information may depend upon its form. My email address, "sophie.dawson@bdw.com.au", clearly falls within the definition. Others, such as "guesswho@yahoo.com" arguably would not. Alternatively, all email addresses could be personal information on the basis that, by sending an email to an address, it will often be possible to find out the identity of the individual that uses it.

Increasingly, organisations which send bulk emails for marketing purposes are likely to hold more information about individuals to whom they send emails than just their email addresses so that they can target email campaigns. Such organisations will certainly carry out "personal information" collection, use and disclosure, which is regulated by the legislation.

4.3 Commencement

National Privacy Principles which deal with collection, use and disclosure of personal information will apply only to information collected after the commencement of the Act. Thus, use and disclosure of personal information already held by organisations will be unaffected unless and until that information is updated after 21 December 2001, or 21 December 2002 in the case of most small businesses that are not exempt from the legislation.

Other National Privacy Principles which regulate matters including data quality and security, privacy policies and openness, access and correction, anonymity and transborder data flows commence on 21 December 2001, or 21 December 2002 for most small businesses, regardless of the date on which the information was collected.

4.4 Collection of Personal Information

The Act includes principles relating to collection of personal information which are designed to ensure that individuals know who holds information about them and what they are likely to do with that information. These principles apply so long as personal information is collected for inclusion in a record or generally available publication. [9] They apply regardless of whether the information is from a publicly available source or not.

The first of the collection principles is National Privacy Principle ("NPP") 1.1, which prohibits collection of information by an organisation unless the information is necessary for one or more of the organisation's functions or activities. This provision is likely to have a limited impact on bulk emailers, as an organisation which includes bulk emailing amongst its functions and activities would be justified in collecting information necessary for that purpose. An interesting question arises, as to whether information that is desirable, but not necessary, for bulk emailing purposes, such as demographic information useful to target an email campaign, can be collected in accordance with NPP 1.1. The Draft Guidelines do not deal directly with this issue, though they do state that "necessary" will be interpreted in a "practical but narrow" sense.

Perhaps the most important effect of the Act will be to prohibit spammers' from using cheap methods to collect email addresses from the internet. NPP 1.2 provides that an organisation must collect personal information only by lawful and fair means. The Draft guidelines state that[10]:

"An organisation that collects personal information without telling an individual (for example, via a banner on a website or using software that trawls the net for email addresses) for the purpose of sending Spam will be engaging in unfair collection in breach of NPP 1.2 unless it gives individuals proper notice".

In practice it is likely NPP 1.2 will require organisations that collect email addresses from the internet to ensure that appropriate disclosures have been made on the sites from which they are collected.[11] This ties in with the obligations in NPPs 1.3, 1.4 and 1.5.

NPP 1.3 governs disclosures to be made when personal information is collected from individuals. It provides that, at or before the time (or, if that is not practicable, as soon as practicable thereafter) an organisation collects personal information about an individual from the individual, it must take reasonable steps to ensure that the individual is aware of:

(a) the identity of the organisation and how to contact it;

(b) the fact that he or she is able to gain access to the information;

(c) the purposes for which the information is collected;

(d) the organisations (or types of organisations) to which the organisation usually discloses information of that kind;

(e) any law that requires particular information to be collected; and

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

The Commissioner takes the view that, in the case of information collected via the internet, it will almost always be necessary to notify individuals of the matters in NPP 1.3 before the information is collected. The Draft Guidelines state that "it will be practicable to notify at or before the time of collection in almost all conceivable circumstances where an organisation is using information and communications technology, such as phone-in call centres, wired networks such as the internet, or wireless networks or interactive television services to collect information."[12]

NPP 1.4 requires that, if reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual. The Draft Guidelines indicate that the circumstances in which it is impracticable to collect information directly from an individual will be rare. However, a more liberal approach will be taken to the question of whether it is unreasonable to require collection directly from the individual. Where collection of personal information is accepted practice, such as where it is obtained from the White Pages or from a list rental organisation, this will seemingly weigh in favour of it being acceptable to collect information from third parties.

In cases where information is collected from third parties, NPP 1.5 will apply. This principle provides that, if an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in NPP 1.3, unless to do so would pose a serious threat to the life or health of the individual.

The Draft Guidelines acknowledge that it will in many cases be sufficient for the purposes of NPP 1.5 to ensure that the relevant information has been provided by the organisation that collected information from the individual or , for example, to use advertising in the local media as a "reasonable step".

The Draft Guidelines sensibly acknowledge that it will be perfectly reasonable to take no steps at all for the purposes of NPP 1.3 and NPP 1.5 where information is obvious. This is to be applauded since it presumably means that it will not be necessary to tell individuals each time an organisation collects a new copy of the White Pages and its employees include information from it in business contact records. It should be obvious to most members of the general public that information in the White Pages is used in that way.

Collection of "Sensitive Information" is separately dealt with in the Act. "Sensitive Information" includes, for example, information about individuals' health, race, sexual preferences, criminal record and political beliefs. Its collection is generally prohibited subject to exceptions such as where the individual's consent is obtained.[13] Email addresses would not constitute sensitive information in the usual case.

4.5 Use and Disclosure of Personal Information

The Draft Guidelines indicate that the Commissioner will take the same tough approach to spam in enforcing use and disclosure rules as will be taken in enforcing the collection provisions.

(a) Application of Use and Disclosure Rules

The Act contains restrictions on the use and disclosure of personal information which, together with the other principles that regulate personal information after it has been collected by an organisation, apply only if the relevant personal information is held by an organisation in a "record".[14]

The effect of this restriction is to relieve organisations of the need to comply with use and disclosure rules in relation to use and disclosure of items such as generally available publications. It means that it is not necessary to make sure that a relevant consent is in place before using or disclosing a copy of the White Pages or Who's Who.

(b) Restrictions on Use and Disclosure

NPP 2.1 prohibits an organisation from using or disclosing personal information about an individual for a purpose (the "secondary purpose") other than "the *primary purpose of collection*" unless one of a number of exceptions apply.

The key issue for the purpose of this provision is the definition of "primary purpose of collection." This raises two questions. First, whose purpose is referred to? And second, what is the scope of the purpose? That is, should purpose be broadly or narrowly defined.

With respect to the question of whose purpose it is, there are at least two possibilities:

1. the purpose of collection is that of the individual that first discloses the information; or
2. the purpose of collection is that of the organisation that most recently received the information and wishes to use or disclose it.

These purposes are likely to differ in most circumstances. For example, the individual's purpose in providing information on an application form might be to join a club, and the purpose of an organisation which obtains the application form information from the club might be to conduct a direct marketing campaign.

The Explanatory Memorandum appears to support the latter view. It states that:

"NPP 2 sets out the general rule that personal information must only be used or disclosed for the primary purpose for which it was *collected*...

.....Where the information is not collected from the individual, the organisation usually uses the information soon after it collects it and this is a guide to the primary purpose of collection. For example, if an insurance company consults an insurance reference service in the course of considering an applicant, it seems clear that the primary purpose of collection is to decide whether or not to insure the individual." [15]

In contrast, the Draft Guidelines quite clearly state that the question of purpose is to be judged from the perspective of the individual and not that of the using or disclosing

organisation.[16] For example, the Draft Guidelines state that:[17]

"The primary purpose is determined mainly by looking at it from the point of view of the individual whose information it is. Although it is a little more difficult, an organisation should take this perspective even if it collects information from someone other than the individual."

The Draft Guidlines also indicate that the Commissioner will be supporting extremely narrow interpretations of primary purposes. For example, when an individual provides information to obtain a home contents insurance policy, the Draft Guidelines state that the primary purpose is to provide home contents insurance policy, not "providing insurance products".[18]

This issue of interpretation will have a fundamental impact on the extent to which the Act restricts use and disclosure of information, not only by bulk emailers, but generally. If the primary purpose is taken to be that of the organisation wishing to use or disclose the information, then NPP 2's impact on bulk emailers will be limited. In the case of a bulk emailer who collects email addresses of individuals for a single direct marketing campaign, for example, it is likely that campaign will be the primary purpose of collection, in which case the use and disclosure restrictions in NPP 2.1 will not apply.

If the purpose is that of the individual disclosing the information, then bulk emailers may be much more constrained by NPP 2. This is particularly the case where information is obtained by bulk emailers from third parties, who will often have collected the information for a distinct purpose. In most cases, the purpose for which the individual gave the information is unlikely to coincide with that of the bulk emailer. A bulk emailer would thus normally have to fall within one of the exceptions to the prohibition, discussed below, to be able to use or disclose personal information.

Three exceptions to the prohibition on use and disclosure[19] of personal information for secondary purposes likely to be relevant to organisations which use bulk email will be dealt with briefly in turn.

(i) Consent

NPP 2.1(b) allows an organisation to use or disclose personal information if the individual has consented to the use or disclosure. This is likely to be by far the most useful exception to the prohibition on use and disclosure and the one most frequently relied upon by bulk emailers and other marketing organisations.

The benefit of consent from a direct marketer's perspective is twofold. In addition to enabling use and disclosure of information under the Act, it indicates that an individual is receptive to direct marketing communications. These considerations are likely to lead to a significant premium being placed upon personal information obtained from individuals who have consented to its use and disclosure for marketing purposes, particularly after commencement of the Act.

Consent may be express or implied. The issue of when consent may be implied reveals further tension between the Draft Guidelines and the Explanatory Memorandum. The Explanatory Memorandum states that:

"consent to the use or disclosure may be express or implied. Implied consent would be acceptable in some circumstances. Implied consent could legitimately be inferred from the individual's failure to object to a proposed use or disclosure (that is, a failure to opt out), provided that the option to opt out was clearly and prominently presented and easy to take up."[20]

In many cases, this could enable bulk emailers to rely upon consent rather than upon the direct marketing exception to the prohibition below after their first communication with an individual.

However, the Draft Guidelines indicate that the Commissioner will be slow to imply consent. They emphasise that consent must be voluntary, must be informed, must be given by a competent person and should ordinarily be express. They state that:

"Except in the most limited circumstances it is questionable whether implied consent can be inferred from a failure to opt out, or an individual's objection to a proposal."[21]

The Commissioner indicates that he is likely to imply consent from failure to opt out only where a further 9 conditions are met (and even then, not in all circumstances). The Commissioner has invited submissions on the issue of whether the opt-out approach can constitute valid consent.

In view of this reluctance on the part of the Commissioner to imply consent, it is likely that most organisations will use clear language to obtain it. It is also likely that, notwithstanding a caution in the Draft Guidelines to the contrary,[22] broad consents will be sought and obtained so as to maximise the value of personal information.

(ii) Direct Marketing

Prior to release of the Draft Guidelines, it was thought that NPP 2.1(c) would be the exception of most importance to organisations which use bulk email for marketing purposes. It provides an exception to the prohibition on use and disclosure of personal information which applies:

(A) if the information is not sensitive information and the *use* of the information is for the secondary purpose of direct marketing; and

(B) it is impracticable for the organisation to seek the individual's consent before that particular use; and

(C) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and

(D) the individual has not made a request to the organisation not to receive direct marketing communications; and

(E) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and

(F) each written direct marketing communication by the organisation with the individual

(up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically.

The intention of this exception appears to be to provide a balance between the interests of organisations wishing to send marketing material to individuals who may not have had contact with them or their products before and those of individuals who wish to be able to control the flow of direct marketing communications. The Explanatory Memorandum states that:

"This sub-principle allows personal information, other than sensitive information, to be used in order to establish initial contact with an individual, provided that the individual is given the chance to opt out of any further approaches."

It appears from an early media release, entitled "Privacy and the Electronic Environment"[23] that this was intended to apply to use by organisations of personal information to send bulk email for direct marketing purposes. The release states that:

"The legislation allows the use of personal information for direct marketing purposes, provided the individual is given the opportunity to opt out of receiving any further direct marketing. This will regulate spamming – the unwanted bombardment of junk emails – from Australian private sector organisations".

However, the Commissioner's position appears to be different. The Draft Guidelines indicate that this exception will never be available in respect of spam. They state at page 77 that:

"The Commissioner takes the view that it will never be impracticable to seek the individual's consent where an organisation engages in direct marketing online and so such techniques as Spam cannot rely on NPP 2.1(c) to direct market. This means the organisation will need to seek the individual's consent and in most cases, the Commissioner will require that consent to be explicit consent".

They add the following cautionary note to spammers:

"Direct marketers who want to collect personal information for the primary purpose of direct marketing by Spam will need to abide very carefully by their notice obligations under NPP 1 and their obligations under the other NPPs."

(iii) Related to Primary Purpose

NPP 2.1(a) provides an exception to the prohibition on use and disclosure for secondary purposes where both of the following apply:

(A) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection; and

(B) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose.

The operation of this exception depends upon the resolution of the primary purpose issue described above.

If the primary purpose is that of the individual at the time of original collection, then this exception is only likely to be useful to the organisation that originally collects the information from the individual. So, for example, if an organisation collects an individual's email address on an application for insurance, it can probably use it under this exception for the purpose of issuing and administering the insurance policy and for email marketing of related products. However, if the organisation provides the email address to another organisation, for example, a direct marketing company, the direct marketing company would be unlikely to be able to rely upon this exception because its purposes are unrelated to the original application for insurance.

In contrast, if the primary purpose is that of the organisation which holds the information and wishes to use or disclose it, then in the example above the direct marketing company could rely upon this exception for purposes related to its purpose of collection. If its purpose for collecting the email address was to send the individual spam, then purposes related to that purpose would fall within the exception. It could rely upon the exception so long as disclosures made to the individual were sufficient for the individual to reasonably expect the email address to be used for direct marketing purposes.

Predictably, the Draft Guidelines take the view that NPP 2.1(a) must be viewed from the perspective of the individual. The test is objective. It is necessary to show that the ordinary person in the street who has no special knowledge would expect the information to be used or disclosed for the other purpose. It is not necessary to show that a particular individual had that expectation. Factors to be taken into account include the closeness of the relationship between the primary purpose and the relevant secondary purpose, standard industry practices and public awareness of them, the sensitivity of the information, NPP 1.3 and 1.5 disclosures, the context in which the information was collected and the demographics of the organisation's customer base.

If this exception is interpreted in accordance with the Draft Guidelines, it is likely that it will rarely be relied upon by bulk emailers.

It therefore appears that consent, and *express* consent, may be the only basis upon which bulk email can be sent after the commencement of the private sector provisions. That is, it may be an interference of privacy to send spam after 21 December 2001 (or 21 December 2002 in the case of most small businesses).

4.6 Other Requirements Imposed by the Privacy Act

The Act contains a number of further requirements that will apply to all organisations that hold personal information, including organisations which use bulk email.

This paper will not deal with them in detail. However, they include:

(A) NPP 3, which requires an organisation to take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date;

(B) NPP 4, which requires an organisation to take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure and to permanently de-identify personal information which is no longer needed for any purpose for which it may be used or disclosed under NPP 2;

(C) NPP 5, which requires organisations to set out in a document clearly expressed policies on their management of personal information and to make that document available to anybody who asks for it. On request by a person, an organisation must also take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes and how it collects, holds uses and discloses that information;

(D) NPP 6 which, subject to limited exceptions, requires an organisation which holds personal information about an individual to provide the individual with access to the information on request by the individual and requires the organisation to take reasonable steps to correct any information which the individual is able to establish is not accurate, complete or up to date;

(E) NPP 8, which requires that, where it is lawful and practicable, individuals musts have the option of not identifying themselves when entering transactions with an organisation; and

(F) NPP 9, which restricts transfer by an organisation of personal information to someone (other than the individual or the organisation) in a foreign country.

4.7 Conclusion as to Act

The Draft Guidelines make it clear that the Privacy Commissioner will construe the Act strictly against spamming when the amendments commence. If the interpretation in the Draft Guidelines is upheld by the Courts, then it will effectively outlaw spamming. It will only be possible to use or disclose personal information in accordance with the Act for bulk email purposes if express consent is obtained from individuals. In addition, the Act will require organisations to be open about their use of information for email and other purposes.

From a public policy perspective, this may be a positive outcome. Individuals will be better informed and have greater control over use and disclosure of their personal information. From industry's perspective, the emphasis on the requirement for consent is in many respects positive. People that consent to receive direct marketing are most likely to respond positively to it.

If too strictly construed, however, there is potential for the Act to add unduly to the costs involved in obtaining and using information, which could come back to consumers in the form of higher prices. Whether or not this is the case will to a large extent depend upon the Commissioner's and the court's approach to mechanisms which are designed to maximise efficient use of information, such as list rental, and to requirements such as NPP 1.5, which could impose costs even where consents are obtained. Likewise, there is a risk that, if the Commissioner more strictly construes the Act in relation to spam than in relation to more traditional forms of marketing, such as direct mail, this will cause inefficiency by forcing organisations to favour a more expensive means of communicating with customers. Such an approach would also have environmental consequences in that the impact of bulk email appears likely to be much more slight than that of other forms of communication. These considerations should lead the Commissioner to take a pragmatic approach to, for example, organisations obtaining broad consents. An individual should be allowed to consent to receiving a broad range of marketing communications and organisations should not be discouraged from obtaining such consents. Otherwise, organisations and individuals will be required to waste time and resources obtaining or giving multiple consents.

5. Industry Codes and Commonwealth Best Practice Model

Up until the announcement of the private sector provisions of the Act, self regulation was the main restriction on use of spam in Australia. Industry codes which deal with spam specifically require an opt-in or an opt-out approach to be taken. In addition, the Federal Government has released a Best Practice Model (see part 6) which advocates a similar approach and which may ultimately become a code.

Even after the commencement of the new provisions, these codes will play an important role. Some may become enforceable codes under the Act. And more generally, they convey a message that certain types of spam are considered unacceptable amongst reputable business people.

5.1 ADMA Code

The Australian Direct Marketing Association ("ADMA") has over five hundred corporate members accounting, according to its website, for over 80% of direct marketing advertising spending in Australia.

As a condition of membership, ADMA requires its members to agree to comply with the ADMA Direct Marketing Code of Practice (the "Code"). In addition to repeating the National Privacy Principles, the Code provides for a "do not mail/do not call" and email preference service administered by ADMA. This allows individuals to send a single request to ADMA not to receive direct marketing which all of ADMA's members are required, subject to limited exceptions, to comply with.

The Code contains the following clauses which apply to use of email by its members for direct marketing purposes:

33 A direct marketer must use the Do Not Mail/Do Not Call and Email Preference services of ADMA when conducting a direct marketing campaign, in order to remove the name of any consumer, other than a current customer, who has requested that they not receive direct marketing offers. For the purposes of this clause a "current customer" is any customer who has made a purchase within the last six months or during a normal selling cycle.

34 A direct marketer must remove a consumer' name from all internal marketing list or lists for transfer to a third party at the request of the consumer.

35 A direct marketer must inform a customer, on request, of the source of the individual's personal information.

Clause 36 of the Code sets out the protocol for the Do Not Mail/Do Not Call/ Email Preference Service ("e-MPS"), which works as follows:

(a) consumers are offered the opportunity to inform ADMA via postage paid reply mail and ADMA's website that they do not wish to receive marketing communications from ADMA members;

(b) ADMA registers the name of consumers exercising this preference and makes the registry available to its members electronically or on a computer disk;

(c) ADMA members who utilise unsolicited e-mail to market goods or services must use the e-MPS service to remove from their marketing list the names of consumers who have registered not to receive such offers; and

(d) ADMA Members are required to keep the names of consumers that register on the e-MPS service suppressed for at least two years from the date on which they receive the registration.

The benefit of this system is that it enables individuals to communicate their preferences once only to ADMA rather than receiving and responding to numerous disclosures and requests for consents from organisations. This saves the time and money of the individual and of the organisations.

The Code contains a complaints mechanism whereby, if a member is found to be in breach of the Code, the ADMA Code Authority may impose such sanctions as it considers appropriate, including requiring a formal apology, corrective advertising, correction or deletion of relevant records and requiring a member to give an undertaking that the breach will not be repeated and recommending that membership be revoked. According to the Code, the board of ADMA may order the payment of money, suspend or cancel the membership of a member or issue any public admonition of a member.

It is likely that the ADMA Code will be submitted to the Privacy Commission for approval when the Act commences. If it is approved, ADMA members that fail to comply with the Code will by virtue of section 16A(1) of the Act, be in breach of the Act and will, by virtue of section 13A(1)(a), have engaged in interference with the privacy of individuals concerned.

5.2 Internet Industry Association Code of Practice

The Internet Industry Association (IIA) released a Code of Practice in 1999 (the "IIA Code") which provided for a qualified opt in regime with respect to spamming. That is, one which prohibited members from sending unsolicited email unless they had pre-existing business dealings with the recipient or the recipient's consent. It also required members to provide recipients of unsolicited email with an option to opt out from further communications.

Due to requirements of the Australian Broadcasting Authority[24] and amendments to the *Privacy Act*, the spamming provisions have been removed from the new version of the IIA Code. The Internet Industry Association intends to reintroduce spamming provisions in 2001, unless the Commonwealth undertakes to subsume its work into its Best Practice Model for electronic commerce, in which case members will be directed by the IIA to comply with that model.[25]

6. Commonwealth Best Practice Model for Electronic Commerce

In May 2000, the Minister for Financial Services and Regulation released "Building Consumer Sovereignty in Electronic Commerce, a Best Practice Model for Business" (the "Best Practice Model"), which deals with internet issues including spam. Clause 23 of the Best Practice Model provides that businesses should not send commercial email except to people with whom they have an existing relationship or have already said they want to receive commercial email. It also provides that businesses should have simple procedures so that consumers can let them know that they do not want to receive commercial emails.

The Best Practice Model does not have any legal effect, but sends a strong message to businesses as to when spam should be considered inappropriate. If, as foreshadowed by the Internet Industry Association, it becomes an approved code for the purposes of the Privacy Act, it will also be possible to enforce it using the mechanisms in that Act in respect of businesses that agree to be bound by it.

7. ISP Anti-Spamming Measures

ISPs in Australia and overseas are increasingly taking measures to restrict use of their facilities for spamming.

First, and most importantly, most ISPs now include in their contracts with customers a term which entitles them to terminate internet access to any customer which uses their facilities for certain types of spam. Like the Internet Industry Association Code of Practice and the Government's Best Practice Model, many of these distinguish between spam sent to strangers and spam sent to acquaintances. For example, the terms of Telstra Big Pond Direct's contract prohibits spam being sent to strangers

but allows acquaintance spam so long as the recipients are given an opt out opportunity. Telstra Big Pond also prohibits various fraudulent, misleading and other undesirable practices using the Big Pond direct network.

Second, many ISPs keep a "blacklist" of domain names from which spam emails have previously been sent and block messages sent from those domain names to their customers.

A third measure taken by most ISPs is to educate their customers about measures their customers can take to combat spam. These are usually on ISPs internet sites. The measures generally recommended include:

- not including your email address in any message sent to a news group or mailing list;
- giving an email address you don't use to businesses; and
- giving an altered email address which cannot recognised by programs that harvest email addresses from the internet site as being incorrect, but that people would recognise as incorrect, such as: "jane.removethisbit@example.com .au"

Many also seek to educate their customers about why they should not use spam. For an example of this, see the Highlands Internet site at www.hinet.net.au.

8. Permission Based Marketing

One of the most important changes which appears to be taking place in Australia is that businesses are increasingly appreciating that failure to respect customer preferences with respect to communications, including email, damages goodwill. Increasingly, the rhetoric amongst marketers in Australia favours permission based marketing, which is premised on respect for consumer preferences.

This has no doubt resulted in part from the media focus on privacy issues, which has increased over recent years. Businesses that fail to respect customer's preferences with respect to use and disclosure of their personal information sometimes find themselves being the subject of bad publicity. It may also have resulted in part from businesses focussing on privacy issues for the purpose of ensuring compliance with the new legislation. There is little doubt, however, that good consumer relations plays a major part.

When the Act commences, regardless of its legal effect, consumers are likely to expect a high degree of control over what businesses do with their personal information and over what is sent to them. This will increase the incentive for businesses to make sure that they and their marketing contractors have their privacy houses in order.

9. Conclusion

The picture emerging is that most Australian businesses that use bulk email for marketing purposes are increasingly giving individuals choices as to whether to receive bulk email and other marketing communications. After 21 December 2001, as businesses seek to ensure they fall within exceptions to prohibitions on use and disclosure under the Act, this choice is more likely to take the form of an express request for consent to use personal information for purposes such as direct marketing. In many cases, this will be complemented by an "opt in" or an "opt out" approach or some combination of the two in direct marketing communications. It is also likely they will carefully target spam so that it is limited to people likely to be interested in their products or services. These changes are likely to result as much from changes in marketing philosophies, ISP contracts and industry initiatives as from legislation.

The anonymity which the internet provides is, however, likely to mean that there will always be some level of unwelcome spamming activity including spam which breaches the law. Such spam will continue to provide an enforcement, rather than regulatory, challenge.

---

1 See ACCC Update issue 6, May 2000 at page 12

2 The Queen v Steven George Harmouzis, Victorian County Court, 30 October 2000 (unreported)

3 See for example *Word Systems Corporation v CyberPromotions, Inc ; Compuserve Inc v CyberPromotions* (CS No. C2-96-1070). See also *CyberPromotions Inc v America Online Inc* (CA No. 96-2486), in which CyberPromotions argued unsuccessfully that it had a first amendment right to send mail to AOL customers.

4 "Act" is used in this paper to mean the Privacy Act 1988 as it will apply after the private sector amendments commence.

5 Available at www.privacy.gov.au. Submissions on the Guidelines have been sought by the Privacy Commissioner and are due on 6 July 2001.

6 Privacy Amendment (Private Sector) Bill 2000 Revised Explanatory Memorandum.

7 See Part V of the Act. Orders can be sought from the Federal Magistrate's Court or the Federal Court to enforce a determination. Those Courts will proceed by way of a hearing de novo: section 55A. A certificate from the Privacy Commissioner setting out his or her findings constitutes prima facie evidence of the facts found, but not of breach of a National Privacy Principle: section 55B.

8 Section 6C.

9 See section 16B of the Act.

10 At page 53.

11 Note that the Explanatory memorandum states that "fair" means "without intimidate or deception": paragraph 130. However, it also states that NPP 1.2 prevents covert collection of information, which is consistent with the Guidelines.

12 At page 55.

13 NPP 10.

14 Section 6 defines "record" to mean:

(a) A document; or

(b) a database (however kept); or

(c) a photograph or other pictorial representation of a person;

but does not include:

(d) a generally available publication, defined to mean "a magazine, book, newspaper or other publication (however published) that is or will be generally available to members of the public." 14

(e) anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition; or

(f) certain records dealt with in the *Archives Act 1983* and *Australian War Memorial Act* 1980; or

(g) letter or other articles in the course of transmission by post.

15 Revised Explanatory Memorandum, paragraphs 339 to 341.

16 At page 67.

17 At page 68.

18 At page 67.

19 The Act distinguishes between "use" and "disclosure" of information by an organisation. "Disclosure" is not defined in the Act. However, "use" is defined as follows:

"Use, in relation to information, does not include mere disclosure of the information, but does include the inclusion of the information in a publication."

"Publication" is not defined, but would presumably include a "generally available publication", above.

The Guidelines define "use" and "disclosure" as follows:

"Use of personal information refers to handling personal information within the organisation.

Examples of uses of information are:

- Adding information to a database;
- forming an opinion about information collected and noting it on a file; and
- assessing an application."

"An organisation discloses personal information when it releases information outside the organisation.

Examples of disclosure are:

- when an organisation gives another organisation information under contract to carry out a function or activity;
- selling information to another organisation; and
- sending an email list to people outside an organisation."

It appears from the above that inclusion of information in a publication which is released outside an organisation may be both a "use" and a "disclosure". This may cause confusion when it comes to the direct marketing exception, discussed below, which is expressed to extend only to "use".

20 At paragraph 344, page 135.

21 Page 40.

22 Page 38.

23 22 December 2000

24 Which has approved the revised Code pursuant to Schedule 5 of the *Broadcasting Services Act* (1992)

25 See the Internet Industry Association website at www.iia.net.au

Conference Announcements

Fall 2001 International Information Technology Law Conference

11 –12 October, 2001
Lisbon, Portugal

This conference will gather luminaries from legal practice, government, and academia to address cutting-edge legal issues ranging from new regulation of intellectual property rights on the Internet to the increased importance of specific IT contract clauses in today's uncertain economic environment. The conference combines in-depth analysis of new legal issues; updates on developing doctrines, case law, and regulatory action; and an overview of existing legal constructs that have new importance in a changing business climate. The conference will compare and contrast developments in Europe with those in North America and provide context for understanding the inter-relationships among the various new bodies of law that are emerging worldwide.

Advanced Topics in Emerging Technologies and Law Conference:
How Emerging Technologies Affect the Law, and How the Law May Affect the Development and Future of Technology

25-26, October, 2001
Monterey, California

The conference will explain such new technologies as new wireless broadband, optical, and other networking technologies; digital rights management; peer-to-peer architectures; network security; XML and related software development methodologies; device integration; nanomachinery and molecular computing; and data mining and mapping.

The IT Business in the Americas: An Update Toward Year 2002

November 29-30, 2001,Hotel Alvear Palace of Buenos Aires
Buenos Aires, Argentina

This conference will be unique in providing attendees with an opportunity to learn, in a single event, crucial information about the different business environments pertinent to information technology law from the Arctic Circle down to Tierra del Fuego. National panels will present country-specific information of importance to information technology business and law, following which in-depth presentations will cover corresponding legal issues that are developing for 2002 in e-commerce, digital data distribution, and general Internet areas.

Please visit http://www.cla.org/conferences.htm for more details

The briefs describing the conferences above have been reproduced with permission from:
http://www.cla.org/conferences.htm