be reasonable to predict a shift in market power away from the established application and network providers and resellers to large ASPs which maintain and control strong client relationships, the positioning of such established providers themselves in the ASP market raises interesting questions regarding distribution channels, the control and development of client relationships and the sustainability of technology brands.

In addition, the infancy of the ASP model presents issues for ASPs and customers alike. Managing expectation gaps regarding service levels and the scope of services, the total cost of the ASP relationship, and integrating the provision of services from numerous ASPs will present challenges on both sides of the ASP model. Relationship management will become the all-important skill in the ASP model. IT personnel will now, more than ever before, need to work with their service providers to develop and manage ASP services which are suited to the needs of their organisation. Although ASPs offer certainty of IT expenditure as a selling point for their services, customers are only just beginning to realise the true cost of implementing ASP services. Although these issues may lead to some resistance and negativity in the ASP market, ASPs and customers must work through these if the underlying rationale for the ASP model can be applied within organisations.

This rationale, and perhaps the most exciting aspect of the ASP model, is a shift in emphasis away from the underlying technology to the business objectives which technology is used to facilitate. Over the years we have changed our focus away from technology as an end in itself and towards technology as a means to an end. In the same way that ecommerce is simply a facilitator of commerce, the development of the ASP model is clear evidence of a relisation in the market that technology is simply a tool to facilitate such commerce. The underlying technology and technology brands are of little interest to an organisation which has its focus on its core business.

Kim Gordon
Lawyer
Tel: +61 2 9367 8945
email: kgordon@gtlaw.com.au

Michael Robertson
Lawyer
Tel: + 61 2 9374 4871
email: mrobertson@gtlaw.com.au

Legal Requirements Relating to Privacy

Kiet Dang, Freehills

1. INTRODUCTION

Consumers' concern about the impact of new technologies on privacy has become one of the major issues confronted by business and government. A Roy Morgan survey, published in August 1999, found that, " the majority of Australians (56%) are worried about invasion of privacy issues created by new information technologies." [1] This trend is not confined to Australia. A report published by the US based Forrester Research in October 1999 found that ninety per cent of online consumers want the right to control how their personal information is used after it is collected and half are willing to call on the government to regulate privacy[2].

The consumers' perception about loss of privacy has been further reinforced by developments such as:

- the establishment of a joint venture between Acxiom RTC Inc., a US company, and Publishing and Broadcasting Limited to set up a data warehouse containing personal and financial details of almost every Australian;[3] and
- the assignment by RealNetworks Inc of globally unique identification numbers to its popular music listening software that can be used to track users without their knowledge[4].

In response to the public concern about how personal information is handled by private sector organisations, the Federal Government has put forward a bill to extend the application of the Privacy Act 1988 (Cth) to these organisations[5].

Consequently, it is important for businesses, especially online businesses, to be aware of, and comply with their, legal obligations relating to the collection and usage of personal information. The purpose of this paper is to outline the current legislative framework in relation to the handling of personal information and discuss the new bill proposed by the Federal Government.

2. CURRENT LEGISLATIVE FRAMEWORK

2.1 *What is meant by "privacy"?*

Privacy, for the purposes of this paper, means information privacy. This should be distinguished from other privacy issues such as:

(a) communications and surveillance privacy (listening devices, phone tapping or

interception, e-mail monitoring, video surveillance, calling number display);

(b) territorial privacy (unlawful entry into buildings and dwellings, home invasions); and

(c) personal privacy (which might include blood testing, whether of sports people or otherwise and fingerprint security systems sometimes called biometric identification systems).

The *Privacy Act 1988* (Cth) (Privacy Act) covers personal information which is defined in sec 6 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."

2.2 *No general right to privacy*

There is no common law right to privacy in Australia. The privacy right may, however, be enforced indirectly via other areas such as defamation (spread of personal information), copyright and confidential information. Consequently, while no right to privacy exists, it is sometimes possible to rely on other areas of the law to achieve similar results and restrain the distribution of personal information.

2.3 *Statutes generally*

The principal statute in relation to privacy is the Privacy Act. There are a number of other statutes conferring a limited degree of privacy in specific instances. These include the *Telecommunications Act 1997* (Cth) which governs the use of personal information by carriers and others and the Commonwealth Spent Convictions Scheme under the *Crimes Act 1914* (Cth) which provides protection against unauthorised use and disclosure of old criminal records after ten years (or five year in the case of juvenile offenders).

In New South Wales there is the *Privacy and Personal Information Protection Act 1998* (NSW) which applies principally to public sector agencies in NSW. This Act is only likely to apply to a private sector entity if the entity provides personal information data management services to a NSW public sector agency.

3. PRIVACY ACT

3.1 *Limited application to private sector*

The Privacy Act contains 11 Information Privacy Principles (**IPPs**) which set out obligations in relation to the management of personal information. The IPPs apply principally to Federal and ACT Government departments and agencies.

The private sector is subject to the Privacy Act in the following ways:

(a) credit providers[6] and credit reporting agencies must comply with the credit reporting rules in the Act (and in a legally binding Code of Conduct) for the handling of credit worthiness information about individuals; and

(b) all persons who hold and use tax file number information must comply with tax file number guidelines issued by the Privacy Commissioner under section 17 of the Privacy Act.

3.2 *Credit providers*

Section 11B of the Privacy Act defines a credit provider as, among others:

(a) a bank; or

(b) a corporation:

i that is a building society; or

ii that is a credit union; or

iii a substantial part of whose business or undertaking is the provision of loans (including the provision of loans by issuing credit cards); or

iv that carries on a retail business in the course of which it issues credit cards to members of the public in connection with the sale of goods, or the supply of services, by the corporation; or

v that:

A carries on a business or undertaking involving the provision of loans (including the provision of loans by issuing credit cards); and

B is included in a class of corporations determined by the Commissioner to be credit providers for the purposes of this Act.

For the purpose of section 11B(1)(b)(v)(B), the Privacy Commissioner has made a determination[7] that all corporations belonging to the following classes are to be regarded as credit providers:

- a corporation that is considering providing, or has provided, a loan in respect of the provision of goods or services on terms which allow the deferral of payment for at least 7 days. A business would therefore be regarded as providing a loan if it allowed customers to obtain goods or services and defer payment for seven days or more; or
- a corporation engaged in the hiring, leasing or renting of goods for at least seven days wherean amount less than the value of the goods is paid as deposit for return of the goods. Examples of hire arrangements include most car or equipment rentals and the hiring of videos and games, even if the hire fee is paid in advance.

Given such a broad scope of the definition of credit provider, most businesses that allow deferred payment for their goods and/or services would fall within the definition of a credit provider.

3.3 *Legal obligations of the credit providers*

Part IIIA of the Privacy Act governs the handling of credit worthiness information about individuals by credit reporting agencies and credit providers. The Privacy Act ensures that the use of this information is restricted to assessing applications for credit lodged with a credit provider and other legitimate activities involved with giving credit.

The key requirements of Part IIIA include:

(a) generally only credit providers may obtain access to a credit file of an individual held by a credit reporting agency and only for specified purposes. In addition, real estate agents, debt collectors, employers, general insurers are barred from obtaining access;

(b) limits on the purposes for which a credit provider can use a credit report obtained from a credit reporting agency. These include:

- to assess an application for consumer credit or commercial credit;
- to assess whether to accept a person as guarantor for a loan applied for by someone else; and
- to collect overdue payments.

(c) prohibition on disclosure by credit providers of credit worthiness information about an individual, including a credit report received from a credit reporting agency, except in specified circumstances. These include:

- where the disclosure is to another credit provider and the individual has given consent;
- to a mortgage insurer;
- to a debt collector (but credit providers can only give limited information contained in or derived from a credit report issued by a credit reporting agency);

(d) rights of access and correction for individuals in relation to their own personal information contained in credit reports held by credit reporting agencies and credit providers;

(e) rights of access and correction for individuals in relation to their own personal information contained in credit reports held by credit reporting agencies and credit providers.

In addition, under section 18A of the Privacy Act, the Privacy Commissioner has issued a Code of Conduct which is legally binding and complements the provisions of Part IIIA.

3.4 *Credit Reporting Code of Conduct*

The Code of Conduct supplements Part IIIA of the Privacy Act on matters of detail not addressed by the Act. Among other things, it requires credit providers and credit reporting agencies to:

(a) deal promptly with individual requests for access and amendment of personal credit information;

(b) ensure that only permitted and accurate information is included in an individual's credit information file;

(c) keep adequate records in regard to any disclosure of personal credit information;

(d) adopt specific procedures in settling credit reporting disputes; and

(e) provide staff training on the requirements of the Privacy Act.

4. TELECOMMUNICATIONS ACT 1997

The *Telecommunications Act 1997* (Cth) contains a number of provisions dealing with the privacy of personal information held by carriers, carriage service providers and others.

Part 6 of the *Telecommunications Act* provides for the development of industry codes and standards in a range of consumer protection and privacy areas. The Privacy Commissioner must be consulted on any privacy codes. The codes are voluntary in the first instance but are enforceable by the Australian Communications Authority.

Part 13 sets out strict rules for carriers, carriage service providers and others in their use and disclosure of personal information. Under this part, carriers, carriage service providers, number-database operators, emergency call persons and their respective associates must protect the confidentiality of information that relates to:

(a) the contents of communications that have been, or are being, carried by carriers or carriage service providers; and

(b) carriage services supplied by carriers and carriage service providers; and

(c) the affairs or personal particulars of other persons.

The disclosure or use of protected information is authorised in limited circumstances (for example, disclosure or use for purposes relating to the enforcement of criminal law). In addition, certain record-keeping requirements are imposed in relation to authorised disclosure or uses of information.

The Privacy Commissioner has the role under the Act of monitoring compliance with Part 13, Division 5 of the Act. This part of the Act obliges carriers and carriage service providers to make records of all disclosures of personal information (with only a few exceptions).

5. THE PROPOSED PRIVACY SCHEME FOR THE PRIVATE SECTOR

5.1 *Amendments to the Privacy Act 1988*

On 15 December 1998, the Commonwealth Government announced that it would develop a light touch legislative regime to

support and strengthen self-regulatory privacy protection in the private sector. The legislation will be based on the IPPs. The Federal Attorney-General is co-ordinating the development of the legislation.

On 12 April 2000, the Attorney General released the *Privacy Amendment (Private Sector) Bill 2000* **(Bill)**.

5.2 *Application of the proposed privacy scheme under the Bill*

The proposed scheme will apply to acts and practices of "organisations". Section 19 of the Bill defines an organisation as an individual, a body corporate, a partnership, any other unincorporated association and a trust. Consequently, the privacy scheme, will apply to all entities other than State instrumentalities or governmental agencies.

The proposed scheme provides for the following exemptions:

- acts done or practice engaged in by an organisation in the course of journalism;
- exemption in respect of employee records; and
- exemption for small business with an annual turnover of $1 million or less.

5.3 *Approved privacy codes and the National Privacy Principles*

The Bill sets out the National Privacy Principles (**NPPs**) which specify standards relating to collection, security, storage, use and disclosure of personal information. The NPPs serve as a basis for private organisations to develop their own codes of practice, which will have to be approved by the Privacy Commissioner. A code will only be approved by the Privacy Commissioner if it provides at least as much protection as the NPPs. If a private organisation does not develop its own code, these NPPs will provide a default framework for the protection of personal information.

The NPPs cover, among other things, the following areas:

(a) *collection*: an organisation must not collect personal information unless the information is necessary for one or more of its functions or activities;

(b) *use and disclosure*: an organisation must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection;

(c) *data quality*: an organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date;

(d) *data security*: an organisation must take reasonable steps to protect the personal information it holds. It must destroy or permanently de-identify personal information if it is no longer needed for any purpose;

(e) *openness*: an organisation must set out clearly its policies on management of personal information. It must also 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;

(f) *access and correction*: an organisation must allow individuals access to the personal information on request. It must correct the information if it is not accurate, complete or up-to-date;

(g) *identifiers*: an organisation must not adopt, as its own identifier, identifiers used by government agencies (for example, pension numbers or Medicare numbers);

(h) *anonymity*: where it is lawful and practicable, individuals must have the option of not identifying themselves when entering into transactions with an organisation;

(i) *transborder data flows*: there are only limited circumstances in which an organisation may transfer personal information to someone (other than the organisation or the individual) who is in a foreign country;

(j) *sensitive information*: an organisation must not collect sensitive personal information except in certain situations. Sensitive information includes information about race, political opinion, membership of certain associations, criminal records, etc.

5.4 *Effect of the NPPs on pre-existing information*

The Bill states that only the following NPPs will apply to personal information collected before the NPPs come into effect:

(a) data quality;

(b) data security;

(c) openness; and

(d) transborder data flows.

6. POTENTIAL APPLICATION OF THE PRIVACY SCHEME TO ONLINE BUSINESSES

It is not uncommon for online businesses to obtain personal information about potential users of their websites before allowing them to gain access to certain webpages or services. An example of this is the Easymail service offered by Telstra. In order to obtain this free email service, the potential users must disclose certain personal information such as date of birth, home address, gender, etc. as part of the registration process.

Given such a broad definition of "organisation", it appears that most, if not all, online businesses will fall within the scope of this privacy scheme. It is therefore imperative for these organisations to understand and comply with the scheme. To illustrate its operation, this paper outlines below some of the obligations imposed on businesses by Principles 1 (collection) and 2 (use and disclosure) of the scheme.

6.1 *Principle 1—Collection*

Clause 1.1 of the Bill states that an organisation must not collect personal information unless the information is

necessary for one or more of its functions or activities. The word "necessary" will be interpreted in a practical, not a theoretical or in-principle, sense.[8] That is, if an organisation cannot in practice effectively pursue a legitimate function or activity without collecting personal information, then that personal information would be regarded as necessary for that function or activity.

Principle 1 also requires organisations to collect personal information only by lawful and fair means and not in an unreasonably intrusive way. "Fair" for this purpose means without intimidation or deception.

Under Principle 1, organisations need not obtain the consent of individuals whose personal information is collected. Organisations must, however, disclose the following matters at or before the time of collection (or, if that is not practicable, as soon as practicable after):

- the identity or the organisation and how to contact it;
- the fact that he or she is able to gain access to the information;
- the purposes for which the information is collected;
- to whom the organisation usually discloses information of that kind;
- any law that requires the particular information to be collected; and
- the main consequences (if any) for the individual if all or part of the information is not provided.

Under clause 1.5 of the Bill, 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 above.

6.2 *Principle 2—Use and disclosure*

Although clause 2.1 of the Bill prohibits an organisation from use or disclosure of personal information for a purpose other than the primary purpose of collection, it does provide a number of exceptions. One exception of particular interest allows the use or disclosure of personal information for the secondary purpose of direct marketing without the consent of the relevant individuals, if:

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

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

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

(iv) the organisation gives the individual the express opportunity, at the time of first contact, not to receive any further direct marketing communications.

This exception uses the "opt-out" mechanism whereby the individuals must explicitly request the organisations not to send to them direct marketing communications.

7. CONCLUSION

In the online world, it seems that personal information is becoming increasingly valuable in its own right. Yet, at the same time consumers have become less willing to provide information about themselves. Accordingly, to win the trust and confidence of consumers, online businesses should not take any shortcuts in their preparation for compliance with the NPPs. This does not only protect businesses from legal risks, but also provides a mechanism for retaining competitive advantage in the environment where competitors are only a 'mouse-click away' and customer loyalty is built on trust.

1 *"Big Brother"; Bothers Most Australians*,Finding No. 3221, *Bulletin*, cover date 30 August 1999, http://www.roymorgan.com/polls/1999/3221/ on 1 February 2000.
2 Quoted in Miller, L and Weise, E, "FTC" studies Web site 'profiling'", USA TODAY at http://www.usatoday.com/life/cyber/tech/review/crg570.htm on 31 January 2000.
3 Grayson, I, "Packer sets up Big Brother data store", *The Australian*, 30 November 1999.
4 Macavinta, C, "RealNetworks faced with second privacy suit", *CNET News.com*, 10 November 1999 at http://news.cnet.com/news/0-1005-200-1435099.htm?tag=st.ne.1002 on 1 February 2000.
5 "Release of key provisions of National Privacy Legislation", Media Release of the Federal Attorney-General dated 14 December 1999 at http://law.gov.au/aghome/agnews/1999newsag/669_99.htm on 1 February 2000.
6 It appears that the definition of credit provider is broad enough to include any business that allows deferred payment for goods or services it provides.
7 Credit Reporting Determination 1996published on 13 June 1996 at http://www.privacy.gov.au/publications/pg3pubs.html#41 on 31 January 2000.
8 *National Principles for the Fair Handling of Personal Information*, Revised edition, January 1999, Office of the Privacy Commissioner at p.11.