Privacy and Data Protection in Australia.

1. Overview of Privacy Legislation

1.1 The Privacy Act 1988 (Cth) (**legislation**) regulates the protection of personal information handled by Australian federal and ACT government agencies, large private sector organisations, all private sector health service providers, some small businesses, credit reporting agencies, credit providers and both individuals and organisations which use personal tax file numbers.

1.2 Personal information is defined as

> *'information or an opinion…about an individual whose identity is apparent, or can be reasonably be ascertained, from the information or opinion'*.

Obvious examples are the name, address, phone number and /or birth date of person but there are obviously less specific identifiers which are also caught by this definition.

1.3 Significant legislative changes were introduced in Australia in December 2001[1] which established a national scheme to regulate the handling of personal information by the private sector. The legislation was designed to bring Australia into line with international standards.

2. Office of the Federal Privacy Commissioner

2.1 The legislation is regulated by the Office of the Privacy Commissioner (**Commissioner**) established by the Federal Government. The Commissioner is responsible for investigating complaints from individuals about breaches of the legislation and also has the power to initiate own motion investigations regarding potential breaches of the legislation that do not relate to particular complaints.

2.2 Some of the additional roles of the Commissioner include reviewing and making submissions on proposed legislation.

[1] The *Privacy Amendment (Private Sector) Act 2000 (Cth)* amended the existing *Privacy Act 1988 (Cth)*. The amendments came into effect on 21 December 2001.

2.3 The Commissioner also has some regulatory functions under other legislation, including the *Telecommunications Act 1997 (Cth)*, *National Health Act 1953 (Cth)*, *Data Matching Program (Assistance and Tax) Act 1990 (Cth)* and the *Crimes Act 1914 (Cth)*.

3. Private Sector Business

Application

3.1 The private sector provisions of the legislation apply to individuals, bodies corporate, partnerships, trusts and unincorporated associations.

3.2 There are a number of exemptions to the legislation for private sector organisations which generally include media organisations, political parties, small businesses and employee records.

3.3 A business is deemed to be a small business if it has an annual turnover of $3,000,000 or less per annum except where the business:

(a) relates to the provision of a health service to another individual and

(b) holds any health information or discloses personal information about another individual to anyone else for a benefit, service or advantage (eg a credit reporting agency or a mailing list company).

National Privacy Principles

3.4 The legislation, insofar as it applies to the private sector, is based upon 10 legally binding National Privacy Principles (**NPPs**). The NPPs regulate how personal information may be collected, kept, used and disclosed. The following is a brief summary of each of the NPPs.

(a) *NPP 1 Collection*

Personal information must only be collected if it is necessary for one or more of its functions or activities and where such collection is lawful.

(b) *NPP 2 Use and disclosure*

An organisation must not use or disclose personal information for a purpose other than the purpose for which it was collected. There are some exceptions to this principal which include instances where the individual has consented to the use or disclosure or it is impractical for the organization to obtain the individual's consent.

(c) *NPP 3 Data quality*

An organisation must take reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

(d) *NPP 4 Data security*

An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorized access, modification or disclosure. The organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under NPP2.

(e) *NPP 5 Openess*

An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it. On request, an organisation must 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.

(f) *NPP 6 Access and correction of information*

Generally, an organisation must upon a request by an individual, provide them with access to their personal information. There are some limited exceptions to this requirement, for example, if such provision would be unlawful.

(g) *NPP 7 Identifiers*

An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by a government agency. (An identifier is a number used by a government agency to identify an individual, for example, a tax file number).

(h) *NPP 8 Anonymity*

Where it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

(i) *NPP 9 Transborder data flows*

An organisaiton is not generally permitted to transfer personal information to someone who is in a foreign country. There are some exceptions which include where the organisation reasonably believes a law, binding scheme or contract applies at the destination which effectively delivers privacy standards substantially similar to the NPPs or where the in individual consents to the transfer.

(j) *NPP 10 Sensitive information*

An organisation is generally not permitted to collect sensitive information about an individual.

*"**Sensitive information**"* is defined as information or an opinion about an individual's racial or ethnic origin, political opinions or associations, religious beliefs, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices or criminal record or health information about an individual.

There are a number of exceptions to organisations collecting sensitive information which include where: the individual has consented; the collection is required by law and the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual.

Private Codes

3.5 The legislation enables the private sector to create its own privacy codes which can be submitted to the Commmissioner for approval. Once approved they become binding for that organisation instead of the NPPs. To date, only a few of these codes have been approved.

Voluntary application

3.6 Private sector organisations which are not bound by the legislation can elect to be bound by the legislation.

4. Government

4.1 The NPPs do not affect the federal public sector. Commonwealth agencies (**agencies**) must comply with eleven Information Privacy Principles (**IPPs**) set out in

the legislation. The IPPs are based on the 1980 OECD guidelines governing the protection of privacy and transborder flows of personal data.

4.2 The agencies must also comply with the tax file number guidelines identified in the legislation and guidelines issued by the Privacy Commissioner under the legislation to govern the conduct of data-matching using tax file numbers.

4.3 Each year, the agencies must also maintain a record setting out the nature and the various types of records of personal information kept by the agency and related details in Personal Information Digests.

4.4 Where actions by these agencies breach the Privacy Act, but it is in the public interest for these actions to occur, the agencies may apply to the privacy Commissioner for public interest determinations.

IPPs

4.5 In summary, the IPPs ensure that the agencies:

(a) only collect personal information for lawful purposes and by lawful and fair means;

(b) inform individuals when personal information is being collected and disclose the purpose for which the information is being collected;

(c) take reasonable steps to ensure that the personal information is relevant to the purpose for which it was collected and is up to date and complete;

(d) employ security safeguards to protect personal information against loss, unauthorised access, misuse etc.

(e) use and disclose personal information only for the purposes for which it was collected

4.6 In addition to compliance with the IPPs, the agencies must also ensure that any contracts that it enters into with its contractors impose upon those contractors the same obligations as the agencies would have under the IPPs.

5. Health Service Providers

5.1 The legislation does not bind Commonwealth, State and Territory public sector health service providers. It does bind private sector or non-government organisations that provide health services.

5.2 The definition of '***health service'*** in the legislation is broad and includes hospitals, pharmacists, general practitioners, gyms and weight loss clinics.

5.3 Health providers must comply with the NPPs but are also subject to higher standards. Health information has special protection under the legislation as sensitive information. More stringent privacy standards apply to the handling of sensitive information than personal information. In addition, the small business exemption does not apply to health providers.

5.4 Health Providers also have the opportunity to create their own privacy codes which can be submitted to the Commissioner for approval. Once approved they become binding for that organisation instead of the NPPs. To date a few codes have been approved.

6. Credit Providers

6.1 Commercial credit information only is regulated by the NPPs where a credit reporting agency is bound by them.

6.2 As a general rule only credit providers can obtain credit reports or report payment defaults to a credit reporting agency. Credit providers include not only to additional lenders such as banks and finance companies but also retailers who provide payment terms. In the context of these restrictions we are only talking about consumer credit ie credit obtained by an individual for domestic, household or family purposes. The NPPs however apply to both consumer and commercial credit. An example of the restrictions in relation to credit reports are as follows:-

(a) only defaults of at least 60 days overdue and recovery action has commenced, can be reported;

(b) only cheques over $100 dishonoured time can be reported;

(c) defaults and dishonoured cheques must be removed from the credit reporters records after 5 years;

(d) information on bankruptcies must be removed after 7 years;

(e) the credit reporting agency must obtain the customer's consent if it is disclosing information to a credit provider for the purposes of the credit provider assessing an application for credit;

(f) customers can obtain access to their records on request.

7. International use of information

7.1 One of the aims of the legislation was to reduce barriers to international trade encountered as a consequence of Australia's absence of compliance with international standards.

7.2 The legislation applies to activities engaged in outside of Australia by an organisation if the activity relates to personal information about an Australian citizen or resident and the organisation has a link with Australia.[2] The organisation will have a link with Australia if there is an "organisational link" under the act or where an organisation carries on business in Australia and the organisation collects or holds personal information in Australia. The definition of organisational link includes an Australian citizen, a company incorporated in Australia, a resident, a partnership formed in Australia.

7.3 Where an organisation performs an act outside Australia which would be in breach of the legislation but is required the act is required by the law of a foreign country, it does not interference with the

7.4 NPP9 (identified in paragraph 3.4(i)) relates to the transborder flow of data. It prohibits the transfer of personal information to other countries unless certain criteria are met.

7.5 Personal information may be transferred overseas where:

(a) the organisation reasonably believes that an equivalent law, binding scheme or contract which would provide substantially similar privacy standards to the NPPs exists at the destination;

(b) the individual consents to the transfer;

(c) the transfer is for the benefit of the individual and it is impractical to obtain that individual's consent. It must be likely that consent would be given by the individual;

(d) the transfer is required by a contract between the individual and the organisation;

(e) the organisation has taken reasonable steps to ensure that the information will not be held, used or disclosed by its recipient inconsistently with the NPPs.

[2] Section 5B

8. Sanctions

8.1 Commissioner can:

(a) order reimbursement for expenses in bringing a complaint;

(b) make a declaration that an organisation has breached the NPPs;

(c) order compensation for loss or damage suffered by a complainant;

(d) order correction of any record;

(e) issue up to $30,000 for individuals and $150,000 for companies.

9. Spam

9.1 I have dealt with the Privacy Act in this presentation which is the central legislation in Australia governing privacy of personal information however it is perhaps worth mentioning in passing that in April 2004 the Spam Act was introduced. The key factors of this Act are as follows:-

(a) opt in regime (based on consent) for commercial electronic messaging (spam);

(b) spam must contain a functioning unsubscribe facility;

(c) there is a prohibition on electronic address harvesting.

10. Criticisms of the legislation

10.1 In 2001, the Data Protection Working Party of the European Union (**Party**) expressed many reservations about the legislation and suggested that it did not meet with the EU's minimum standards. The concerns held by the Party included:

(a) Some exemptions to the legislation were too broad for example, employee records (which records can include health information, contact details, salary, performance and conduct etc), media organisations and small businesses.

(b) Low standards of protection in some areas, for example the legislation allows organisations to collect personal information for secondary purposes where it is not "practicable" to obtain that individual's consent. The organisation merely has to provide that individual with the opportunity to opt out of further direct marketing communications.

(c) The legislation regulates the collection but not use or disclosure of sensitive information except for health information.

(d) The legislation allows the transfer of information to countries with inadequate privacy laws.

10.2 The Australian Attorney General rejected the Working Party's findings and considered that the Committee's comments displayed an ignorance about Australia's law and practice and did not go to the substance of whether Australia the legislation was fundamentally adequate from a trading point of view. He stated that Australia would only look at options that did not impose unnecessary burdens on Australian business.

11. **Freedom of Information Acts (FOIA).**

11.1 The Federal Government, all six States and the two Territories have enacted FOIAs .

11.2 The object of these Act sis to extend as far as possible the right of the Australian community to access to information in the possession of the Government of the Commonwealth by creating a general right of access to information in documentary form in the possession of Ministers, departments and public authorities, limited only by exceptions and exemptions necessary for the protection of essential public interests and the private and business affairs of persons in respect of whom information is collected and held by departments and public authorities[3].

11.3 An unsuccessful applicant can appeal to the courts for review.

11.4 Following on from 11.2, for example, the Minister can issue a certificate that the matter inquired after relates to the deliberative processes of government and that disclosure is contrary to the public interest. If based on reasonable grounds this defeats an application. This was upheld recently in the highest court in Australia – the High Court - by majority of 3:2 [4] In this case the national newspaper, the Australian, had applied for Government Treasury documents dealing with its approach to income tax brackets and the tendency for more and more tax payers to be pushed to higher brackets s their wages increased with inflation.

[3] See the High Court 's decision in McKinnon v Secretary, Department of Treasury [2006] HCA 45 (6 September 2006) in the judgement of Callianan and Heydon JJ and the Objects of he legislation defined in the Comonwealth FOIA.

[4] "There is a "general right of access to **information** limited only by exceptions and exemptions necessary for the protection of essential public interests [and other matters not presently material]" (s 3(1)(b)). That is the context in which a Minister makes a decision under s 36(3), and in which such a decision is reviewed under s 58(5" –(Gleason CJ and KirbyJ)

11.5 This has excited much debate as it is seen as too easy for a Minister to issue a certificate on grounds he can argue are' reasonable' and that this is contrary to the intent and purpose of he Act.

12. **Hot Topics.**

12.1 The issue raised in 11.2 and 11.4 is being debated in Australia at present with ` strong view form outside government being put that the reasonable grounds needs tightening

12.2 As well just this week, with a number of major corporate entities in Australia announcing that either they are about to outsource, or are considering the outsourcing, to other countries functions such as calls centres, data management and IT , the Government has called for assurance that the Privacy Principles will be adhered to and reminded these companies they are open to prosecution if they do not.

Simon Ward

Piper Alderman

www.piper-alderman.com.au

11 October 2006.