



Australian Government

Employee Records Privacy

**A discussion paper on information
privacy and employee records**

February 2004

**Attorney-General's Department
Department of Employment and Workplace Relations**

COMMENTS AND SUBMISSIONS

This discussion paper has been prepared for consultation purposes by the Attorney-General's Department and the Department of Employment and Workplace Relations. Comments and submissions on matters raised in this paper are welcome and should be sent to either of:

Ms Joan Sheedy
Assistant Secretary
Information Law Branch
Attorney-General's Department
Robert Garran Officers
National Circuit
BARTON ACT

Ph. (02) 6250 6211
Fax. (02) 6250 5939
Email: joan.sheedy@ag.gov.au

Ms Diane Merryfull
Assistant Secretary
Legal Policy Branch 2
Department of Employment
And Workplace Relations
GPO Box 9879
CANBERRA ACT 2601

Ph. (02) 6121 7883
Fax.(02) 6121 7798
Email: diane.merryfull@dewr.gov.au

The closing date for comments and submissions is 16 April 2004.

Contents

| | |
|---|-----------|
| Contents | 1 |
| Terms of Reference | 3 |
| Review of employee records privacy | 4 |
| Executive Summary | 4 |
| 1.Introduction | 7 |
| The nature of the employment relationship | 7 |
| Privacy..... | 7 |
| The Privacy Act..... | 8 |
| The Privacy Principles | 9 |
| Personal information | 9 |
| Genetic information | 10 |
| Small business exemption | 10 |
| The employee records exemption..... | 10 |
| Approved Privacy Codes..... | 11 |
| Industry privacy policies | 11 |
| 2.Employee records | 13 |
| Types of employment records | 13 |
| Union access to employee records..... | 13 |
| The employee records exemption | 13 |
| The exemption provision..... | 14 |
| ‘Directly related to’ | 14 |
| ‘Current or former employment relationship’ | 14 |
| ‘Employee records’ | 15 |
| Complaints handling | 16 |
| 3.Protection of employee privacy | 18 |
| Protection under the Privacy Act | 18 |
| Collection (NPPs 1 and 10)..... | 18 |
| Collection of sensitive information..... | 19 |
| Collection of genetic information..... | 19 |
| Collection of information from monitoring activities..... | 20 |
| Collection of information by prospective employers | 20 |
| Use and disclosure (NPP 2)..... | 21 |
| Disclosure to prospective employers | 21 |
| Data quality (NPP 3)..... | 22 |
| Security and retention (NPP 4)..... | 22 |
| Openness and privacy policies (NPP 5)..... | 22 |
| Access, alteration and correction (NPP 6)..... | 22 |
| Identifiers (NPP 7)..... | 23 |
| Anonymity (NPP 8) | 23 |
| Transborder data flows (NPP 9)..... | 23 |

| | |
|--|-----------|
| Privacy protection in Workplace Relations legislation | 24 |
| State legislation..... | 24 |
| Occupational health and safety legislation and workers' compensation legislation..... | 25 |
| State and Territory privacy legislation..... | 25 |
| Victorian privacy and health records legislation..... | 25 |
| New South Wales privacy and health records legislation..... | 25 |
| Australian Capital Territory health records legislation..... | 26 |
| Northern Territory privacy legislation..... | 26 |
| Queensland privacy regulation..... | 26 |
| South Australian privacy regulation..... | 26 |
| Tasmanian privacy regulation..... | 26 |
| Other protection for employees personal information | 26 |
| Privacy of employees' telecommunications..... | 27 |
| Privacy of child support information | 27 |
| Secrecy provisions | 27 |
| Common law..... | 27 |
| 4.Options for enhancing privacy protection of employee records..... | 28 |
| Issues | 28 |
| Sensitive information..... | 28 |
| Unfair collection practices..... | 28 |
| Access and correction rights..... | 28 |
| Union access to employee records..... | 28 |
| Transborder data flows..... | 29 |
| Compliance cost for business | 29 |
| International obligations..... | 29 |
| Options to increase privacy protection | 30 |
| Status Quo..... | 30 |
| Non-legislative measures | 30 |
| Education..... | 30 |
| Privacy Commissioner guidelines | 30 |
| Privacy policies and approved codes | 31 |
| Legislative Measures..... | 31 |
| Amend the Privacy Act..... | 31 |
| Delete the exemption..... | 31 |
| Narrow the exemption..... | 32 |
| Retain some of the NPPs for employee records..... | 32 |
| Enact specific employee records privacy principles | 33 |
| Enhancing protection of employee records in Workplace Relations legislation..... | 33 |
| Exclusive coverage in Workplace Relations legislation..... | 33 |
| Privacy provisions included in certified agreement or Australian workplace agreements | 34 |
| Comments and submissions | 34 |
| Attachments..... | 35 |
| Attachment A Information Privacy Principles..... | 35 |
| Attachment B National Privacy Principles..... | 39 |

Terms of Reference

To review the existing level of information privacy protection for employee records and consider whether further measures or new approaches are necessary to provide privacy protection for employee records.

2. The review will consider:
 - whether there is a need for additional measures to ensure privacy protection of employee records
 - whether additional measures would impose administrative and financial burdens on employers, and
 - the means by which additional measures, if any, should be implemented.

3. In examining these issues the review will have regard to:
 - the existing standards in the *Privacy Act 1988*, particularly the Information Privacy Principles and the National Privacy Principles that apply to the protection of personal information in Australia
 - the existing protection of employee records in Commonwealth and State workplace relations legislation
 - international obligations in relation to the protection of personal information
 - other protection for employees personal information
 - whether sensitive information in employee records requires any additional privacy protection, and
 - any other issues relevant to the privacy protection of personal information

4. In considering these issues the review will consult with relevant key stakeholders, including employer groups, employee groups, the Federal Privacy Commissioner and the States and Territories.

5. The review will report to the Attorney-General and the Minister for Employment and Workplace Relations on whether there is a need for additional measures to enhance privacy protection of employee records and, if so, options for implementing any additional measures.

Review of employee records privacy

Executive Summary

1. In November 2000 the Government announced that it would review existing Commonwealth, State and Territory laws to consider the extent of the privacy protection of employee records and whether there is a need for further measures.
2. The discussion paper examines the current level of privacy protection for employee records in privacy legislation and workplace relations legislation. It also examines some concerns raised about the privacy of employee records and suggests options for enhancing that privacy.
3. Employers and employees have various duties and responsibilities. There are common law, statutory and other obligations imposed under instruments such as certified agreements, Australian workplace agreements or awards. A large range of records are kept by employers. Many of these contain personal information about employees. Some records are required to be kept by legislation while other records are kept by employers as part of normal business practices.
4. Under Australian law an individual's claims to privacy are balanced against a range of competing community and public interests. Privacy protection provided by legislation focuses on information privacy. Information privacy is also referred to as 'data protection' or 'information protection'.
5. The Commonwealth *Privacy Act 1988* specifies standards for the collection and handling of personal information. The Information Privacy Principles (IPPs) apply to Commonwealth agencies and the National Privacy Principles (NPPs) apply to the private sector. There are a number of exemptions under the private sector provisions of the Act including the employee records exemption.
6. The employee records exemption means that the standards for the collection and handling of personal information in the Act do not apply to employee records of private organisations. The exemption operates where:
 - the employer is acting in its capacity as the employer or former employer of the individual

- the act or practice of the employer relates directly to that employment relationship with the individual, and
- the act or practice directly relates to an employee record.

7. Not all personal information about an employee will be regarded as an employee record. Personal information that is not an employee record is protected by the Privacy Act.

8. Sensitive personal information such as health information and genetic information is given greater protection under the Act when the information is handled by private organisations. This higher level of protection does not apply to employee records.

9. Commonwealth workplace relations legislation requires employers to keep records of certain employment matters. The legislation provides employees with rights to access and correct records but does not restrict disclosure or publication of those records. State workplace relations legislation also requires employers to keep records. Some State Acts prohibit unauthorised disclosure of that information.

10. Proposals for additional privacy protection of employee records will require careful consideration so as not to impose any unnecessary additional administrative and financial burdens on Australian employers.

11. A higher level of privacy protection for employee records would assist in addressing concerns raised by Australia's trading partners that employee records data being transferred to Australia be given appropriate protection.

12. One option to increase the privacy protection of employee records could be to modify the scope of the exemption. For example, the exemption could be revised to exclude sensitive or other types of personal information.

13. Another option would be to amend the Privacy Act so that the exemption only applied to low risk privacy principles. For example, the exemption could be amended so that employee records were not exempt from, say, the principles relating to data quality (NPP 3), security and retention (NPP 4), openness (NPP 5), access (NPP 6), transborder data flows (NPP 9) and sensitive information (NPP 10).

14. Enacting specific employee records privacy principles would also increase privacy protection. However, this could be confusing for organisations which may be required to comply with different privacy principles for different types of personal information.
15. To address concerns raised about allowing authorised union representatives to access records of non-union members, the Workplace Relations Act (WR Act) could be amended to specify that access by union representatives is limited to members' records.
16. Further amendments to the WR Act could be made so that one piece of legislation governed general record-keeping obligations and privacy requirements in relation to employee records. This would simplify employer obligations and clarify employees' rights.
17. Another option would be to amend the WR Act to direct parties to consider, or compulsorily require, privacy provisions in certified agreements or Australian workplace agreements.
18. The review is being conducted by officers of the Attorney-General's Department and the Department of Employment and Workplace Relations. This discussion paper forms the basis of the consultation on the review. The paper will be distributed to employer groups, employee groups, the Federal Privacy Commissioner and the State and Territories seeking comments and submissions on the issues and options discussed in the paper. Comments are sought by 16 April 2004 (see page i).
19. Following this consultation, the review will make its report to the Attorney-General and the Minister for Employment and Workplace Relations.

1. Introduction

- 1.1 This paper examines the current level of privacy protection for employee records with a view to determining whether further measures or new approaches are necessary to ensure employee records are adequately protected. The paper only considers in detail the protection of personal information in employee records. The protection of personal information is often referred to as information privacy.
- 1.2 The discussion below looks at the nature of the employment relationship and the types of records created and kept in relation to employees. It also outlines the framework of the *Privacy Act 1988* which regulates the handling of personal information by Commonwealth Government agencies and the private sector.

The nature of the employment relationship

- 1.3 The common law characterises the relationship between employers and employees as one based on trust and mutual obligation. Employers and employees are expected to act respectfully, maintain confidentiality and sustain an atmosphere of trust.
- 1.4 These common law obligations are supplemented by various statutory obligations. For example, employers must terminate employment lawfully and fairly, and they are generally prohibited from discriminating on grounds related to race, sex and disability. Further obligations may be created by the particular instrument governing the work relationship, such as a certified agreement, Australian workplace agreement, contract of employment or an award.
- 1.5 Few other relationships have the same level of regulation from such varied sources as the employment relationship. There is the potential for an employer to create a large number of documents in complying with various rules and regulations.

Privacy

- 1.6 There is no absolute right to privacy in Australia.¹ Under Australian law an individual's legitimate claims to privacy are balanced against a range of competing community and public interests.
- 1.7 The law protects some aspects of privacy. Legal actions that touch on privacy matters are available in Australia. For example:
 - the laws of trespass and nuisance may provide remedies for physical intrusions and harassing behaviour
 - an action for breach of confidence may exist where a person's personal information was disclosed by someone who owed an obligation of confidence to that person, and

¹ A recent decision of the District Court of Queensland, *Grosse v Purvis*, held that there can be a civil action for damages based on the actionable right of an individual person to privacy. On 14 July 2003 an appeal against the decision was filed in the Queensland Supreme Court.

- the law of defamation addresses issues arising from publication of material that causes damage to a person's reputation.
- 1.8 However, in the absence of a common law or statutory right, there may be acts and practices that a person considers to be an invasion of their privacy for which the law provides no remedy.
- 1.9 Privacy protection by statute in Australia focuses on **information privacy**—the way in which an individual's personal information is collected, used and disclosed. It also covers access and correction—an individual's right to find out what information is held about him/her and the right to have it amended if appropriate. Information privacy is also sometimes referred to as 'data protection' or 'information protection'.

The Privacy Act

- 1.10 The Commonwealth *Privacy Act 1988* commenced operation in 1989. The provisions of the Privacy Act are designed to protect the interests of an individual in respect of his or her personal information by specifying standards for the collection and handling of personal information. The Act established rules of conduct for Commonwealth agencies called Information Privacy Principles (IPPs) (see **Attachment A**). The IPPs make provision for the collection, storage, access to, correction, use and disclosure of personal information. The Act does not attempt to make provision for physical privacy which is protected by other laws, such as trespass. Nor does it create a general or civil remedy for breaches of the Privacy Act. Part IIIA of the Act regulates credit providers and credit reporting agencies.
- 1.11 In December 2000 the *Privacy Amendment (Private Sector) Act 2000*, including the employee records exemption, was enacted amending the Privacy Act. The private sector privacy provisions came into force in December 2001. This Act established the National Privacy Principles (NPPs) (see **Attachment B**) as the minimum privacy standards for the private sector. The NPPs regulate the collection, storage, access to, correction, use and disclosure of personal information in the private sector.
- 1.12 The Privacy Act reflects a commitment to implement Australia's international obligations concerning information privacy into domestic legislation. The privacy principles in the Act are derived from the principles contained in the OECD Guidelines,² and acknowledge Australia's obligations under the *International Covenant on Civil and Political Rights* (ICCPR)³ and the *1948 United Nations Universal Declaration of Human Rights* (UDHR).⁴ Both the ICCPR and the OECD Guidelines are cited in the preamble to the Privacy Act.

² As an OECD member, Australia is committed to take the OECD's *Guidelines governing the protection of privacy and transborder flows of personal data* (1980) into account in domestic legislation. Those Guidelines form the basis of information privacy laws around the world.

³ Australia ratified the ICCPR on 13 August 1980. Article 17 of the ICCPR states:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

⁴ Article 12 of the UDHR states:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The Privacy Principles

- 1.13 The Privacy Act regulates the handling of personal information by most Commonwealth⁵ and ACT⁶ Government agencies ('agencies'). Agencies bound by the Privacy Act must comply with the IPPs (Attachment A) when collecting and handling all personal information, including personal information contained in employee records.
- 1.14 The privacy standards that apply in respect of private sector organisations are the NPPs (Attachment B). The 10 NPPs are similar, but not identical, to the IPPs. The NPPs provide the framework for private sector organisations in their handling of personal information. They regulate the collection, use and disclosure, and overseas transfer of personal information, and require organisations to ensure that the personal information they hold is accurate, up-to-date and complete, and secure. Organisations are also required to be open about how they manage personal information, provide access and correction rights to individuals and, if lawful and practicable, allow people to deal with them anonymously.
- 1.15 The Privacy Act also provides for private sector organisations to develop and implement their own privacy codes which contain equivalent obligations that equal or exceed the NPPs (see paras 1.26–1.28).

Personal information

- 1.16 The Privacy Act regulates the privacy of 'personal information', which is defined in subsection 6(1) of the Act as:
- 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.
- 'Individual' is defined in subsection 6(1) to mean a natural person.
- 1.17 Sensitive information is given greater protection under the Privacy Act when the information is handled by a private sector organisation. Sensitive information is defined in subsection 6(1) of the Act as:
- (a) information or an opinion about an individual's
- (i) racial or ethnic origin; or
 - (ii) political opinions; or
 - (iii) membership of a political association; or
 - (iv) religious beliefs or affiliations; or
 - (v) philosophical beliefs; or
 - (vi) membership of a professional or trade association; or
 - (vii) membership of a trade union; or

⁵ 'Agency' is defined in subsection 6(1) of the Privacy Act. Some agencies, such as Australia's intelligence agencies, are wholly exempt (ss7(1)(f),7(2)). In addition, some acts and practices of particular agencies are exempt. For example, while information about judicial functions of a federal court are exempt, acts and practices of a federal court of an administrative nature are not exempt (ss7(1)(a)(ii),(7)(1)(b)).

⁶ The provisions apply by virtue of section 23 of the *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* (Cwth).

- (viii) sexual preferences or practices; or
 - (ix) criminal record;
- that is also personal information; or
- (b) health information about an individual.

Information about employees could also be ‘sensitive information’.

Genetic information

- 1.18 The report of the joint Australian Law Reform Commission (ALRC) and the Australian Health Ethics Committee (AHEC) inquiry into the protection of human genetic information, *Essentially Yours: The Protection of Human Genetic Information in Australia*, was released in May 2003. The report makes 144 recommendations dealing with the ethical, legal and social implications of human genetic information.
- 1.19 The Report considers that genetic information about individuals derived from genetic samples and other sources falls within the Privacy Act’s definition of personal information. The Report recommends that the Privacy Act should be amended to ensure that employee records that contain health information or genetic information are subject to the protections of the Act (recommendations 34–1, 34–2⁷). The Australian Government has yet to determine its response to the report.

Small business exemption

- 1.20 There are a number of exemptions under the private sector provisions of the Act. One of these is the exemption for small business operators. This exemption recognises that most small businesses do not pose a threat to the privacy of people’s personal information.
- 1.21 A small business is defined as a business with an annual turnover of \$3 million or less— subsection 6D(1). A small business will be exempt from the operation of the legislation unless it engages in activities that represent a privacy risk. For example, a small business that is related to a large business will not be exempt, nor will a small business that holds health information and provides a health service, nor will a small business that trades in personal information.

The employee records exemption

- 1.22 The employee records exemption contained in subsection 7B(3), provides that the provisions of the Act, including the NPPs, do not apply to employee records of private sector organisations in certain circumstances. The exemption does not apply to Commonwealth agencies.

⁷ 34-1 The Commonwealth should amend the Privacy Act to ensure that employee records are subject to the protections of the Act, to the extent that they contain genetic information.

34-2 The Commonwealth Attorney-General’s Department and the Department of Employment and Workplace Relations, in their pending inter-departmental review of the employee records exemption, should consider whether the Privacy Act should be amended to ensure that employee records are subject to the protections of the Act, to the extent that they contain health information other than genetic information.

- 1.23 The exemption operates where:
- the employer organisation is acting in its capacity as the employer or former employer of the individual
 - the act or practice of the employer relates directly to that employment relationship with the individual, and
 - the act or practice must relate directly to an employee record as defined by the Privacy Act.
- 1.24 The employee records exemption is discussed in greater detail in paras 2.4-2.17.
- 1.25 In November 2000 the Government announced that it would review existing Commonwealth, State and Territory laws to consider the extent of privacy protection for employee records and whether there is a need for further measures. At that time the Government expressed the view that while employee records are deserving of privacy protection, such protection is more properly a matter for workplace relations legislation.

Approved Privacy Codes

- 1.26 Section 18BB of the Privacy Act permits organisations or broader industry sectors to develop their own privacy codes. Such codes must incorporate obligations that either equal or exceed the NPPs and must be approved by the Federal Privacy Commissioner. Once approved, the standards in a privacy code will be binding on organisations that agree to be bound by the code. Organisations not bound by an approved code must comply with the default provisions of the NPPs.
- 1.27 Privacy codes give organisations the flexibility to tailor privacy standards to their own needs. To assist organisations in the development of appropriate privacy the OFPC issued *Guidelines on Privacy Code Development* in September 2001.⁸
- 1.28 At present there is some uncertainty whether special rules concerning employee records, or other exempt records, can be legally incorporated into a privacy code. The Government has introduced an amendment to the Privacy Act to expressly provide that a privacy code can include records, such as employee records, that would otherwise be exempt under the Act⁹.

Industry privacy policies

- 1.29 As well as privacy obligations imposed by legislation (including provisions contained in privacy codes approved under the Privacy Act), private sector organisations are increasingly adopting voluntary privacy protection measures. Some organisations have adopted best practice privacy policies providing some privacy protection for customers and employees that do not rely on legislation for enforcement and compliance. The adoption of such measures is viewed by these organisations as being in their own business interests.

⁸ The guidelines are located at <<http://www.privacy.gov.au/business/guidelines/index.html#3.1>>.

⁹ Privacy Amendment Bill 2003, Part 3 Item 6. This Bill was introduced in Parliament on 3 December 2003.

1.30 In addition, more and more private sector employers are placing their privacy policies, including references to information privacy issues in the employment and recruitment context, prominently on their internet sites.¹⁰

¹⁰ For example see the privacy policy for Coles Myer which is located at <http://www.colesmyer.com/privacy_shopping.asp>.

2. Employee records

Types of employment records

- 2.1 The combination of different forms of regulation under Commonwealth and State legislation results in a diverse range of records which may contain personal information. There are personnel records, which may contain anything from administrative information—such as details of next of kin, addresses, birthdates, banking information, workplace diversity matters and records of absences—to qualitative information—such as curriculum vitae with qualifications, previous work history and details of activities outside the workplace, performance assessments and disciplinary matters.
- 2.2 Apart from records required to be kept under legislation, many other records kept by employers, as part of normal business practices, may contain information about employees. For example, many businesses keep records of email and computer use by employees (see paras 3.14-3.17).

Union access to employee records

- 2.3 Section 285B of the *Workplace Relations Act 1996* (WR Act) allows an authorised union representative to enter a workplace (with 24 hours notice) where relevant members work for the purpose of investigating suspected breaches of the WR Act. The authorised representative may inspect and copy time sheets, pay sheets or other documents relevant to the suspected breach and is not limited to inspecting records of union members.

The employee records exemption

- 2.4 The private sector provisions in the Privacy Act apply to organisations. ‘Organisation’ is defined widely by section 6C of the Act to include an individual, a body corporate, a partnership, any other incorporated association, or a trust. Commonwealth, State and Territory agencies, public schools and hospitals, registered political parties and ‘small business operators’ are not included in the definition of an organisation for the purposes of the Act.
- 2.5 The Act regulates the ‘acts and practices’ of organisations when collecting and handling personal information, regardless of the means by which the information is collected or stored, for example, electronically or face-to-face.
- 2.6 The Act does not apply unless the personal information is intended to be, or has been, recorded in some form, such as in a document or a database.¹¹ Once the personal information has been recorded, whether on an electronic database or in a paper file, the Act

¹¹ A ‘record’ of personal information could include making a pictorial representation of an individual, for example a picture or video recording.

will generally regulate the handling of that information, including the way it is stored, used and disclosed.¹²

The exemption provision

2.7 The employee records exemption as set out in subsection 7B of the Privacy Act is in the following terms:

Employee records

(3) An act done, or practice engaged in, by an organisation that is or was an employer of an individual, is **exempt** ... if the act or practice is directly related to:

- (a) a current or former employment relationship between the employer and the individual; and
- (b) an employee record held by the organisation and relating to the individual.

2.8 The first limb of the provision significantly limits the application of the exemption. The exemption applies only to acts and practices of organisations that are ‘directly related to’ a ‘current or former employment relationship’ between the employer and the individual.

‘Directly related to’

2.9 An individual’s personal information in an employee record will only be exempt if the employer deals with that information as part of an act or practice that is directly related to the employment relationship. If the act or practice is not directly related, the Privacy Act will apply and any personal information about employees that is collected or handled by the organisation will be regulated. For example, any use of employee records for a commercial purpose would be subject to the existing Privacy Act requirements.

2.10 For instance, an organisation that is normally regulated by the Privacy Act may hold the personal address of its employees on file. If a law enforcement agency requests access to that information to assist with an investigation that is not related to the individual’s employment by the organisation, the organisation will not be able to rely on the employee records exemption in order to disclose the information. Such a disclosure would be regulated by NPP 2.¹³

‘Current or former employment relationship’

2.11 The requirement that the information collected relates to a ‘current or former employment relationship’ should be distinguished from the relationship between a job applicant and a prospective employer.

¹² An exception to this general rule is that where the personal information is intended for inclusion, or has been included in a magazine, book, newspaper or other publication that is or will be generally available to the public, the Privacy Act only regulates the collection of the information. See the definitions of ‘generally available publication’ and ‘record’ in subsection 6(1).

¹³ Note that this does not mean the organisation could never lawfully disclose the personal address or other relevant personal information of an employee to a law enforcement body. Such disclosure may be permissible depending on the circumstances. See discussion of NPP 2 at paras 3.20-25.

2.12 The Office of the Federal Privacy Commissioner (OFPC) makes the following observations in *Information Sheet 12-2001 Coverage of and Exemptions from the Private Sector Provisions*:

The act or practice must also be directly related to a current or former employment relationship. This does not cover future employment relationships. This means that personal information collected from prospective employees who are subsequently not employed by an organisation, such as unsuccessful job applicants, will not be covered by the employee records exemption.

2.13 This interpretation has been discussed in academic reports¹⁴ and adopted by some private sector employers. If those views are adopted by courts, whether or not a current or former employer is technically regulated by the Privacy Act, a prospective employer will be required to comply with the NPPs when collecting information directly from the applicant, when subjecting the applicant to intelligence, psychological, genetic, drug or alcohol tests, and when seeking to obtain information from the individual's current or former employer.

2.14 The application of the provisions of the Privacy Act to the employment application process is further discussed in the context of NPPs 1, 2 and 10, at paras 3.18-19 and 3.26.

'Employee records'

2.15 Personal information that an employer might hold about an employee can be broadly categorised as either personal information about employees (such as pay slip information and health records) and personal information created by employees or as a by-product of their activities (such as email and records of internet usage). Not all personal information about an employee will be regarded as an 'employee record' under the Privacy Act.

2.16 A 'record' is defined by the Act to mean a document,¹⁵ a database, or a photograph or other pictorial representation of a person.¹⁶

2.17 The Act defines employee record as personal information relating to the employment of the employee. Rather than providing a restrictive or exclusive list, the Act then provides examples of the types of personal information that could be characterised as an employee record. The definition of employee record is set out in subsection 6(1) of the Privacy Act in the following terms:

employee record, in relation to an employee, means a record of personal information relating to the employment of the employee. Examples of personal information relating to the employment of the employee are health information about the employee and personal information about all or any of the following:

- (a) the engagement, training, disciplining or resignation of the employee;
- (b) the termination of the employment of the employee;

¹⁴ For example see M Otlowski, 'Employment Sector By-passed by the Privacy Amendments' (2001) 14(2) *Australian Journal of Labour Law* 169.

¹⁵ 'Document' is defined in Section 25 of the *Acts Interpretation Act 1901* to include any paper or other material on which there is writing, marks, figures, symbols or perforations and also includes any article or material from which sounds, images or writings are capable of being reproduced with or without the aid of any other article or device.

¹⁶ The definition also includes a list of items that are not considered records for the purposes of the Privacy Act.

- (c) the terms and conditions of employment of the employee;
- (d) the employee's personal and emergency contact details;
- (e) the employee's performance or conduct;
- (f) the employee's hours of employment;
- (g) the employee's salary or wages;
- (h) the employee's membership of a professional or trade association;
- (i) the employee's trade union membership;
- (j) the employee's recreation, long service, sick, personal, maternity, paternity or other leave;
- (k) the employee's taxation, banking or superannuation affairs.

Complaints handling

- 2.18 Complaints or enquiries about employee records are received by both the OFPC and the Department of Employment and Workplace Relations (DEWR) in writing, by telephone or email. Both organisations deal with legislation that covers different, but related, aspects of employee records and both have powers to investigate breaches of provisions of the respective legislation.
- 2.19 The WR Act and Regulations require employers to observe the terms of certified agreements, awards and other industrial instruments under the WR Act. Inspectors are appointed under the WR Act and are employed by either DEWR or contracted State Governments, to investigate claims about breaches of the WR Act, awards and agreements.
- 2.20 The Privacy Act gives the Federal Privacy Commissioner the power to investigate breaches of the Act. The OFPC deals with most of the enquiries about employee records. In the period between 21 December 2001 and 30 May 2003 the OFPC received 36,731 enquiries of which 1458 related to the employee records exemption. In the same period 1544 formal complaints were received of which 16 related to employee records. These 16 complaints were not investigated because of the employee records exemption under the Act.
- 2.21 The employee records enquiries received by OFPC in this period dealt with a wide range of concerns including:
- transborder and within Australia outsourcing of payroll and HR functions
 - privacy and security of email and other computer records
 - privacy of confidential complaints about workplace harassment
 - access to private employee information through computer networks
 - disclosure to third parties of sensitive medical information held by employers
 - whether an employer can use sensitive medical information gained through OH&S monitoring for other purposes without employee's consent
 - rights of access to employee records and pay information in relation to unfair dismissal claims
 - rights of unions to access employee records
 - publication of photographs of staff on websites

- whether an employer could disclose employee records to a potential buyer of the business, and
- payslips
 - too much information being printed e.g. bank account details, and
 - privacy and security of emailed payslips.

2.22 Many enquiries to the OFPC concern the introduction of new practices involving employee records, including changes to the management, storage, disclosure and security of information. In particular, there were concerns about the security of emailed payslips and access by other employees to names and addresses, in the absence of any business need. Concerns have also been raised with the OFPC about excessive personal information, particularly financial information such as bank account details, being included on payslips. Related to this, individual employees have also expressed concerns about employers failing to modify off-the-shelf software packages, with the result being that more, and possibly too much, information was printed on payslips.

2.23 Loss or theft of documents, such as payslips, is a concern to employees. Sometimes disclosure of a small amount of personal information such as a person's full name led to concerns about privacy and personal security as this information could be combined with information from public sources such as telephone directories and employer websites. Employees also complain about insecure computer systems which permit wide access and dissemination of personal information stored in employee records.

3. Protection of employee privacy

Protection under the Privacy Act

- 3.1 The NPPs (Attachment B) regulate an organisation's dealings with an employee's personal information. The general operation of each of the NPPs is briefly summarised below. Some examples of personal information about employees that is not captured by the employee records exemption and is therefore protected by the Privacy Act are also discussed.

Collection (NPPs 1 and 10)

- 3.2 NPP 1 concerns the collection of personal information by a private sector organisation. The Privacy Act regulates the collection of personal information whether collection occurs face-to-face, or by mail, telephone or the internet. NPP 10 concerns the collection of personal information that is also 'sensitive information'.¹⁷ NPP 10 prohibits collection of sensitive information except in a number of specific circumstances. One such circumstance is where the individual consents to the collection.
- 3.3 NPP 1.2 prohibits an organisation from collecting personal information except by 'lawful and fair means' and not in an unreasonably intrusive way. This requirement is fundamental to information privacy laws worldwide.¹⁸
- 3.4 The requirement for lawful collection of personal information means that personal information must not be collected in a manner that is against the law. As employee records are exempt from the operation of the Act, where an employer collects such information by unfair or unlawful means, there will be no breach of NPP 1.2. In such cases the employee may have remedies under other legislation. Where the information was unlawfully collected, there would be clear remedies (eg where listening devices have been illegally used to intercept telephone calls).
- 3.5 Only personal information about an employee that is directly related to the employment relationship, including information that is required to be collected under workplace relations legislation, is subject to the employee records exemption. Therefore, where an employer collects bank account information about an employee for the purpose of paying a salary to that employee, the employee records exemption in relation to that information will normally apply and the employer will not be bound by the Act.
- 3.6 Although 'personal and emergency contact details' is included in the definition of employee records, the collection of information about an employee's family will normally be regulated by the Act, and not captured by the employee records exemption. In order to come within the exemption, the employer must show that the information about an

¹⁷ That is, information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices or health information about an individual—subsection 6(1) of the Privacy Act.

¹⁸ See clause 7 of the OECD *Guidelines governing the protection of privacy and transborder flows of personal data* (1980).

employee's family is directly related to the employment relationship with the employee. This is because the exemption only operates with respect to information relating to a current or former employee—not to a relative of such a person.

- 3.7 If an employer collects an employee's personal information that is neither directly related to the employment relationship nor required under workplace relations legislation, that collection will be regulated by NPP 1 (and, in the case of 'sensitive information', NPP 10).

Collection of sensitive information

- 3.8 Health information falls within the definition of sensitive information in the Privacy Act. The employee records exemption would permit an employer to obtain information to confirm that an employee's absence from work on medical grounds was legitimate. However the Act does not provide guidance on how much detail an employer may collect.
- 3.9 It is not certain whether the exemption effectively permits the collection of detailed information to ensure that the employee's medical condition is not exacerbated on his or her return to work, or to prevent further occurrences of the condition. Similarly, whether the exemption effectively permits employers to collect detailed information about medical absences to prevent excessive and unnecessary absences from work is not certain.
- 3.10 The situation is clearer where an employee is seeking compensation for an injury sustained at work. Employees are generally required to provide consent forms to permit claims to be evaluated. There is also a direct relationship between the medical information and the employment relationship. These factors would normally permit an employer to collect information about an employee's condition for the purposes of evaluating the claim.

Collection of genetic information

- 3.11 The use of genetic testing in the work context has increased in recent years. Such testing has information privacy implications in relation to the results of those tests, which contain information not only about the employee, but also about the genetic relatives of the employee.
- 3.12 The use of genetic testing as part of the recruitment or employment screening process is subject to the Privacy Act because the collection of information is not related to a 'current' or 'former' employment relationship.
- 3.13 The ALRC/AHEC report on genetic information recommended that employers should not collect or use genetic information in relation to job applicants or employees, except in limited circumstances where this is consistent with privacy, anti-discrimination, and occupational health and safety legislation.¹⁹ The Australian Government is considering its response to the report.

¹⁹ See chapters 30-34 of the ALRC/AHEC report *Essentially Yours: The Protection of Human Genetic Information in Australia*.

Collection of information from monitoring activities

- 3.14 Employers can now monitor employees' computer use and email correspondence, and issue electronic passes or install video cameras which provide details about the physical location and behaviour of an employee whilst at work.
- 3.15 The same rules about collection of personal information apply to records of employee's internet use and emails. Therefore, unless the information can be shown to be an employee record, and that record is directly related to the employment relationship, records of internet usage or email messages (which contain personal information) will attract the protection of the Privacy Act.
- 3.16 The OFPC's *Guidelines on Workplace Email, Web Browsing and Privacy*²⁰ were developed in response to concerns about the privacy of these activities. The Guidelines are directed at organisations in both the public and private sector and are based on the important privacy principle of openness. That is, individuals should be informed about how their personal information is collected, used and disclosed. As owners of the computer equipment used by employees in the workplace, employers can specify acceptable use of email and other networks. The OFPC guidelines encourage organisations to devise clear email and web browsing policies which are widely known and understood by their staff.
- 3.17 A related issue is that of monitoring employees' activities through video surveillance devices and telephone intercepts. The Commonwealth *Telecommunications (Interception) Act 1979* limits an organisation's ability to monitor their employees' telephone conversations or make copies of their personal or business-related e-mail messages. State and Territory legislation may also provide some protection by restricting an organisation's ability to undertake surveillance of its employees.²¹ While the Privacy Act regulates the records created by these activities, this will not be the case where the record comes within the employee records exemption.

Collection of information by prospective employers

- 3.18 When an individual applies for employment with an organisation, there is certain information that the prospective employer generally seeks in order to make a decision about whether to engage that individual. This might include references and performance-related information requested from former or current employers of the employee, as well as information obtained from the applicant.
- 3.19 Prospective employers are required to comply with the NPPs when collecting information from applicants. The collection of information could include information about applicants obtained through the administration of intelligence, psychological, genetic, drug or alcohol tests, as well as information from the individual's current or former employer.

²⁰ The guidelines are available on the OFPC's website at <www.privacy.gov.au>.

²¹ Examples of legislation regulating the use of video surveillance devices include the *Surveillance Devices Act 1998 (WA)*, *Surveillance Devices Act 1999 (Vic)*, *Workplace Video Surveillance Act 1998 (NSW)*, *Workplace Video Surveillance Regulations 1999 (NSW)*. The protection afforded by these Acts is limited to situations where employees have not consented to the surveillance, and where the activity being monitored is inherently private.

Use and disclosure (NPP 2)

- 3.20 An organisation should only use or disclose personal information for the primary purpose for which it was collected unless one of the exceptions in NPP 2.1 applies. In general, there should only be one primary purpose for collecting personal information.
- 3.21 Personal information can be used for another (secondary) purpose if the individual has given consent to its use for that other purpose²² or if the individual has a reasonable expectation that the information will be used for that other purpose.²³ Generally, in order to show that an employee would have reasonably expected the information to be used or disclosed for that purpose, an organisation would have to show that the individual had been advised of the secondary purpose in writing.
- 3.22 If an employer wishes to use or disclose the employee's information for a purpose that is not directly related to the employment relationship, the employer will need to obtain the employee's consent or establish that the secondary use or disclosure is related to the primary purpose for which the information was collected, and the employee would have reasonably expected the information to be used or disclosed for that purpose.
- 3.23 Regardless of whether an employee record is exempt from the Privacy Act when being used or disclosed by an individual's employer, an employee record which has been disclosed to a third party such as a union, superannuation provider, insurer or compensation body will not be exempt in the hands of that third party.²⁴
- 3.24 Medical and genetic information, once obtained by an employer, could affect an employee's relationships with others to whom results are disclosed, for example, insurers. In this context, it is important to remember that any disclosure of such information by an employer that is not directly related to the employment relationship will be regulated by the Act.
- 3.25 If an employer sought to use or disclose an employee's personal and emergency contact details or other information about an employee's family or personal life for a purpose other than that for which it was collected, for example, to contact a specified person in case of an emergency, such use or disclosure would be regulated by the Act, and the NPPs would prevent such a use or disclosure.

Disclosure to prospective employers

- 3.26 The limits on what can properly be regarded as an act or practice related to the employment relationship have yet to be tested in the context of disclosing information to potential employers. For example, if information that an employer was administering a garnishee order on an employee's wages was regarded as directly related to the employment relationship, that financial information could be disclosed to a prospective employer.

²² NPP 2.1(b).

²³ NPP 2.1(a).

²⁴ This will be subject to the normal exceptions for small business operators and other organisations exempted from the operation of the Privacy Act.

Data quality (NPP 3)

- 3.27 NPP 3 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.
- 3.28 Provided the information collected, used or disclosed is directly related to the current or former employment relationship, and the other requirements in the exemption are satisfied, employees have no right under the Privacy Act to access or correct their own employee records. However, employees have rights to access and correct information required to be kept under workplace relations legislation (see paras 3.45-3.46).

Security and retention (NPP 4)

- 3.29 NPP 4 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. It also requires an organisation to take reasonable steps to destroy or permanently de-identify personal information that is no longer needed for any purpose for which it may be used or disclosed under NPP 2.
- 3.30 Provided the information stored by an employer is directly related to the employment relationship, and the other requirements in the exemption are satisfied, employers are not obliged to take reasonable steps to destroy or permanently de-identify personal information that is no longer needed for any purpose for which it may be used or disclosed. Nor are they required to take reasonable steps to protect the personal information they hold from misuse and loss and from unauthorised access, modification or disclosure.

Openness and privacy policies (NPP 5)

- 3.31 NPP 5 requires organisations to have clearly expressed policies on their management of personal information that must be made available to anyone who asks for it. The presence of a privacy policy on a web site or advertising material assists consumers to know whether a particular organisation is subject to the Privacy Act.
- 3.32 Employers are not required to maintain privacy policies regarding personal information in employee records.

Access, alteration and correction (NPP 6)

- 3.33 NPP 6 enables individuals to access information held about them by an organisation. Access is not an unlimited right and there are circumstances where access can be refused. The right to access one's own personal information is supported by the provision for correction of the information. If an individual establishes that the information an organisation holds about them is not accurate, complete and up to date, then there is an obligation on the organisation to take reasonable steps to correct it. Where the individual and organisation disagree on the issue, there is provision for a statement setting out the individual's view to be associated with the information.

- 3.34 Only records that are not directly related to the employment relationship will be subject to the access, alteration and correction requirements in the Privacy Act.²⁵ There is a risk that information collected by an employer about employees in employee records may be inaccurate and subsequently used or disclosed to a third party to the detriment of the employee.

Identifiers (NPP 7)

- 3.35 NPP 7 regulates the adoption, use and disclosure of an identifier of an individual that has been allocated by a Commonwealth government agency.
- 3.36 Employers are not prevented from adopting, using or disclosing Commonwealth identifiers if that adoption, use or disclosure is done as part of an act or practice that is otherwise exempt by virtue of the employee records exemption. This could include the use or disclosure of an employee's tax file number for administrative purposes associated with preparing the tax returns of the organisation.
- 3.37 Employers are not permitted to use or disclose identifiers unless the employee records exemption applies. Therefore employers cannot use identifiers for non-employment related purposes.
- 3.38 Where an employer legitimately discloses an identifier to a third party, that record will no longer be exempt, and the third party will need to consider whether it is entitled to adopt, use or disclose that identifier.

Anonymity (NPP 8)

- 3.39 According to NPP 8, individuals have the option of remaining anonymous in their dealings with organisations, where it is lawful and practical to do so.
- 3.40 Organisations are not required to give their employees this option in the context of transactions directly related to the employment relationship. In any case, both practical considerations and statutory requirements mean employees are not able to remain anonymous in their transactions with their employers.
- 3.41 Employees retain the right to remain anonymous in dealings with their employers that are not directly related to the employment relationship. For example, where an employee purchases goods or service from his or her employer, if practical and lawful, the employee is not required to provide identifying information to the organisation.

Transborder data flows (NPP 9)

- 3.42 NPP 9 places restrictions on the transfer of personal information outside Australia. It prevents an organisation from transferring an individual's personal information to someone in another country that is not bound by an information privacy regime that upholds privacy standards comparable to the NPPs, unless the individual consents or other limited circumstances apply.

²⁵ Other legislation or the common law may impose obligations on employers to maintain accurate records and permit employees to access those records—see paras 3.44–3.50.

- 3.43 Where an employer transfers employee records outside Australia as part of an act or practice that is directly related to the employment relationship, the employer is not required to take steps to ensure that overseas entity is subject to an information privacy regime that upholds privacy standards comparable to the NPPs in their country.

Privacy protection in Workplace Relations legislation

- 3.44 The Commonwealth *Workplace Relations Regulations 1996* (the WR Regulations) enacted under the WR Act require employers to keep records of employment matters. These requirements apply to employees covered by a certified agreement (CA), Australian workplace agreement (AWA), or a federal award under the Act.
- 3.45 The WR Regulations require employers to keep records for employees in relation to overtime, remuneration, leave, superannuation and termination. Details are also required to be recorded concerning the classification of the employee, their date of birth, any leave taken, gross and net pay, other deductions, and the industrial instrument that applies to their employment. Employers must ensure that such records are maintained in a condition that allows an inspector or an authorised officer in the case of an AWA to determine whether the conditions of a CA, AWA or an award have been complied with. These records can also be inspected by authorised union representatives for the purposes of investigating suspected breaches of the WR Act (see para 2.3).
- 3.46 The WR Regulations provide employees with rights of access to, and correction of, records required to be maintained about them. The Regulations do not restrict an employer, union representative or inspector from publishing that information or disclosing it to a third party. However, the publication or disclosure to a third party of information contained in an employee record by a union representative or inspector may be regulated by the Privacy Act. The regulations do not provide employees with rights of access to, and correction of, other records.
- 3.47 AWAs, as individual agreements, are the only industrial instruments under the WR Act that have confidentiality provisions. The WR Act gives an authorised inspector access to AWA records to investigate alleged breaches. However, unauthorised disclosure of ‘protected information’ relating to an AWA is subject to a penalty under section 170WHB of the WR Act. The terms of and the name of an employee party to an AWA is, as a consequence, afforded more privacy protection than other employee records.

State legislation

- 3.48 State workplace relations legislation also contains provisions requiring employers to maintain certain employee records. The aim of these provisions is to ensure that certain specified employment information is documented, and available for official inspection to ensure compliance with statutory requirements. Some State Acts provide a right of access and correction by an employee to their records. However, only Queensland, South Australia and Tasmanian workplace relations legislation prohibit unauthorised disclosure of information acquired by persons in the course of performing their functions or exercising powers under those respective Acts.

Occupational health and safety legislation and workers' compensation legislation

- 3.49 Various provisions in federal, State and Territory occupational health and safety legislation allow for the appointment of inspectors who can inspect and copy any document at a workplace including an employee record for the purpose of monitoring or enforcing compliance with the relevant Act.
- 3.50 There are also some provisions in State and Territory workers' compensation legislation which impose record-keeping obligations on employers. Provisions of workers' compensation legislation in New South Wales, Victoria, Queensland, South Australia, Tasmania, and the Australian Capital Territory prohibit the unauthorised disclosure of that information.

State and Territory privacy legislation

- 3.51 Section 3 of the Privacy Act allows State or Territory laws that regulate the handling of personal information by private sector organisations to continue to operate to the extent that those provisions are not directly inconsistent with the Privacy Act.

Victorian privacy and health records legislation

- 3.52 The Victorian *Information Privacy Act 2000* regulates the handling of personal information held by Victorian public sector agencies, including personal information about Victorian public sector employees. Personal information about private sector employees is not regulated.
- 3.53 Victoria has also enacted legislation regulating the handling of health records: *Health Records Act 2001*. That Act applies to health information held by public hospitals, public sector agencies, private sector health service providers, and other organisations that collect, use or handle health information. The Health Records Act does not include an exemption for health information contained in private sector employee records.²⁶

New South Wales privacy and health records legislation

- 3.54 The New South Wales *Privacy and Personal Information Protection Act 1998* regulates the NSW public sector. Like the Victorian Act, it does not regulate personal information about private sector employees held by their employers.
- 3.55 The *Health Records and Information Privacy Act 2002* will regulate the privacy of health information in the private and public sectors when it commences operation.²⁷ The definition of personal information in the Act expressly excludes employee records as defined by the Commonwealth Privacy Act.²⁸ Personal health information about employees held by their private sector employers will not be regulated by the Act.

²⁶ This appears to conflict with the Commonwealth Privacy Act.

²⁷ The Act will commence on proclamation.

²⁸ According to subsection 5(3) of the NSW Act:

Australian Capital Territory health records legislation

- 3.56 Australian Capital Territory government agencies are subject to the Commonwealth Privacy Act.²⁹ In addition, the ACT's *Health Records (Privacy and Access) Act 1997* regulates the privacy of health records held by both the public and private sectors. The Act does not include an exemption for health information contained in private sector employee records.³⁰

Northern Territory privacy legislation

- 3.57 The Northern Territory *Information Act 2002* commenced on 1 July 2003. It regulates the handling of personal information by Northern Territory public sector agencies. The NPPs in the Commonwealth Privacy Act apply to private sector agencies in the Northern Territory.

Queensland privacy regulation

- 3.58 Queensland has an administrative scheme that adopts the Commonwealth IPPs. The scheme regulates personal information handled by Queensland Government agencies. In addition Queensland Health participates in the national privacy scheme for the private sector and is governed by the NPPs. The NPPs in the Commonwealth Privacy Act apply to private sector agencies in Queensland.

South Australian privacy regulation

- 3.59 In South Australia, an administrative scheme based on the Commonwealth IPPs regulates the handling of personal information by South Australian public sector agencies. The NPPs in the Commonwealth Privacy Act apply to private sector agencies in South Australia.

Tasmanian privacy regulation

- 3.60 Public sector agencies in Tasmania are bound administratively by Information Privacy Principles based on those in the Commonwealth Privacy Act. The NPPs in the Commonwealth Privacy Act apply to private sector agencies in Tasmania.

Other protection for employees personal information

- 3.61 Some additional regulation of personal information is provided by other Commonwealth legislation as well as in privacy codes under the Privacy Act and in privacy policies adopted by organisations.

Personal information does not include any of the following:

(n) information about an individual that forms part of an employee record (within the meaning of the *Privacy Act 1988* of the Commonwealth) about the individual held by a private sector person

²⁹ The provisions of the Privacy Act apply in modified form to the ACT.

³⁰ As with the Victorian Health Records Act, this appears to conflict with the Commonwealth Privacy Act.

Privacy of employees' telecommunications

- 3.62 The *Telecommunications (Interception) Act 1979* (TI Act) is one of several pieces of Commonwealth legislation with the central aim of protecting the privacy of users of the Australian telecommunications system. The TI Act prohibits employers from monitoring employees' telephone conversations without the knowledge of all parties to the communications. The TI Act also regulates monitoring and copying of employees' personal or business-related e-mail messages.

Privacy of child support information

- 3.63 Section 58 of the *Child Support (Registration and Collection) Act 1988* restricts employers and their agents from disclosing information about child support matters. The privacy protection afforded by this provision is limited as other persons who lawfully obtain such information are not specifically prohibited from disclosing that information.

Secrecy provisions

- 3.64 Secrecy provisions in legislation administered by particular agencies may apply in relation to information obtained from employee records. For example, section 130 of the *Health Insurance Act 1973*, and sections 201-210 of the *Social Security (Administration) Act 1999* impose specific confidentiality provisions. There are many other examples of secrecy and confidentiality provisions in Commonwealth legislation. They are generally designed to prohibit individuals from disclosing information obtained in the course of their employment unless such disclosure is authorised or required by the employment.

Common law

- 3.65 Contractual and equitable principles may be relevant for maintaining confidentiality and protecting employees' rights and interests. However, it has been argued that the costs and difficulty in establishing a breach through the courts renders any protection with respect to such remedies unsatisfactory.³¹
- 3.66 While this paper aims to examine and evaluate existing privacy protection for employee records, an examination of aspects of the common law which relate to privacy is beyond the scope of this paper.

³¹ For example see M Otlowski, 'Employment Sector By-passed by the Privacy Amendments' (2001) 14(2) *Australian Journal of Labour Law* 169.

4. Options for enhancing privacy protection of employee records

Issues

Sensitive information

- 4.1 Sensitive information such as health information is given more protection than other types of personal information under the private sector provisions of the Privacy Act. This higher level of protection does not apply where the employee records exemption applies.
- 4.2 The inherently private nature of health, genetic, and other 'sensitive information' that may be included in an employee record, may need additional protection to alleviate concerns about the collection and handling of such information. (See discussion of sensitive information at paras 1.17 and 3.8-3.10).

Unfair collection practices

- 4.3 There may be instances where collection of personal information about an employee is directly related to the employment relationship, and therefore protected by the exemption, but that collection is unfair (see para 3.4). The fact that employers are not required to advise employees about information collected means that there is no way of assessing whether the collection of information is unfair.
- 4.4 Additional measures could be introduced to ensure that the collection of personal information about employees by their employers is fair, and that employees are advised when their personal information is collected for inclusion in an employee record.

Access and correction rights

- 4.5 Additional measures could be introduced to ensure organisations maintain accurate records, and to provide employees with rights to access and correct or annotate inaccurate or misleading records. See discussion of access and collection at paras 3.33-3.34.

Union access to employee records

- 4.6 As discussed in para 2.3 an authorised union representative may enter a workplace to inspect records. Employers are concerned about allowing access to records of non-members without the knowledge or consent of the employee. Employees may feel it is inappropriate and an invasion of their privacy that a representative from an organisation of which they are not a member can view their personal information. However, any use of personal information obtained by an authorised representative for purposes other than investigating suspected breaches of the WR Act would be subject to the provisions of the Privacy Act.

Transborder data flows

- 4.7 Where an organisation legitimately transfers an employee record overseas to an entity that is not subject to privacy regulation, that entity may engage in conduct that breaches the employee's privacy. Additional measures requiring organisations to ensure entities to which they transfer employee records are regulated by a suitable privacy regime would reassure employees that their privacy was being protected. See discussion of transborder data flows at paras 3.42-3.43.

Compliance cost for business

- 4.8 While of particular concern to small businesses—although most are currently exempt from the Privacy Act—issues of regulatory burden are important for businesses of all sizes. Any proposals for additional employee records privacy provisions, regardless of the form those proposals would take, require careful consideration so as not to impose any unnecessary additional administrative and financial burdens on Australian employers.
- 4.9 Different types of information may require different levels of protection. However, trying to regulate all records maintained by employers is not feasible due to monitoring and compliance costs. It should be noted that appropriate remedies may already exist. For example, if health information contained in a document is misused to terminate an employee, or is the basis for a decision not to grant a promotion, then workplace relations and discrimination legislation may provide remedies.

International obligations

- 4.10 In recent years Australia's trading partners have increasingly sought assurances that information disclosed will be given appropriate protection. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* ('the Directive') came into force in October 1998. The Directive restricts the transfer of personal information from member countries to other countries unless those countries have adequate privacy safeguards. During the development of the private sector privacy provisions the Directive was consulted to ensure the provisions would satisfy Australia's trading partners.
- 4.11 In *Opinion 3/2001 of the European Commission Data Protection Working Party*³² ('the EC Working Party'), the EC Working Party considered that the private sector amendments represented a significant step towards the fulfilment of Australia's commitment to abide by the 1980 OECD guidelines and recognised the "innovative value of the co-regulatory scheme". However, the opinion recommended that additional safeguards such as contractual clauses be used to protect employee records data being exported to Australia. The opinion also noted, in the conclusion, that such information might also be covered by approved industry codes.

³² The opinion is located on the EC website at http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp40en.pdf.

- 4.12 The EC Working Party considered that the employee records exemption would permit “information about previous employers (sic) to be collected and disclosed to a third party (eg a future employer) without the employee being informed.” It also considered that NPP 10 that deals with sensitive information should also apply to sensitive information contained in employee records.
- 4.13 The European Commission lodged a submission with the House of Representatives Standing Committee on Legal and Constitutional Affairs inquiry into the Privacy Amendment (Private Sector) Bill 2000 on 13 June 2000, in which it expressed concern about the scope of the exemption for employee records.
- 4.14 A higher level of privacy protection for employee records would assist in addressing the EC Working Party’s concern.

Options to increase privacy protection

Status Quo

- 4.15 There are competing interests between the privacy rights of employees and the lawful rights of employers to take steps to ensure the safety, performance and productivity of their employees. In striving to achieve a balance between these competing interests it is necessary to consider both the individual’s interests in personal privacy and whether additional measures, if any, justify imposing additional administrative and financial burdens on employers. Some may consider that additional burdens placed on employers by any proposed changes would outweigh the privacy rights of employees.
- 4.16 There is no consistency in the privacy protection of employee records in State and Territory legislation. Some State and Territory privacy legislation includes an exemption for employee records while others do not (see paras 3.51-3.60). Some State and Territory workplace relations legislation prohibits disclosure of information obtained under the respective legislation (see para 3.48). An undesirable consequence of maintaining the status quo is that it may lead to further regulation by the State and Territories and thus increase the inconsistencies.

Non-legislative measures

Education

- 4.17 Privacy infringements are often caused by a lack of knowledge about privacy by organisations and agencies and their staff. Education and guidance would assist them to understand their legal obligations and the general concerns that individuals have about issues concerning collection, use and disclosure of their personal information.

Privacy Commissioner guidelines

- 4.18 The Federal Privacy Commissioner’s guidelines provide information and ‘best practice’ tips to assist agencies and organisations to comply with their obligations under the Privacy

Act. The publication of specific guidelines dealing with employee information would assist both employees and employers.³³

4.19 The guidelines could, for example:

- clarify the operation of the exemption
- encourage organisations to engage in fair collection practices
- encourage organisations to provide employees with access to their records
- suggest how much information an organisations is entitled to collect, and
- express a view on the interpretation of the terms ‘directly related’ and ‘employment relationship’.

4.20 Guidelines issued by the Privacy Commissioner are not legally binding. Therefore, the adoption of the guidelines as best practice benchmarks for the protection of employee records is unlikely to be successful unless the guidelines have the approval of key employer (and employee) organisations.

Privacy policies and approved codes

4.21 Organisations could be encouraged to develop privacy codes dealing with employee records and submit them for approval under the Privacy Act (see para 1.26). This approach gives organisations a leading role in developing privacy protection for employee records.

4.22 A less resource intensive alternative would be for organisations to develop and implement best practice voluntary privacy policies (see para 1.29). For example, an organisation could adopt a privacy policy granting access and correction rights to employees; and advising employees about the extent of monitoring they undertake.

4.23 Voluntary privacy policies, like approved privacy codes, rely on positive action by organisations.

Legislative Measures

Amend the Privacy Act

4.24 The Privacy Act could be amended to address some or all of the issues discussed above.

Delete the exemption

4.25 The exemption was inserted to balance competing interests and achieve the appropriate level of regulation at the time of the amendments. Deleting the exemption fundamentally changes the balance that has been achieved. While deletion would ensure employee records were treated in the same way as other personal information, it fails to take into account the special character of employee records and the needs of organisations that

³³ As noted in para 3.16 the OFPC has produced guidelines on workplace email, web browsing and privacy. The OFPC also an information sheet on exemptions from the private sector provisions of the Act which discusses the employee records exemption (Information Sheet 12-2001) (see para 2.12).

handle employee information on a daily basis. In addition, it could create significant compliance costs for organisations.

Narrow the exemption

- 4.26 The scope of the exemption could be narrowed. There are a number of ways in which the application of the exemption could be restricted. For instance, introducing a new definition for ‘exempt employee records’ and making acts and practices related to these records exempt could narrow the exemption. For example, the definition of ‘employee records’ could be narrowed to exclude sensitive or other specified types of information.
- 4.27 Narrowing the application of the exemption in this way would mean organisations would be regulated by the Privacy Act, including the NPPs, with respect to some personal information about employees, such as sensitive information which includes health information and genetic information. This would be consistent with the recommendations of the ALRC/AHEC report (see paras 1.18-1.19).
- 4.28 The exemption would continue to operate with respect to other personal information about employees, such as wages and time records, or records that are required to be kept by or under workplace relations legislation, and information relating to the engagement, training, disciplining, resignation or termination of the employee; and the employee’s performance and conduct.

Retain some of the NPPs for employee records

- 4.29 Another alternative would be to amend the Privacy Act so that the exemption only applied to those NPPs that have been or are identified as low risk for privacy breaches in the context of employee records.
- 4.30 For example, the exemption could be changed so that employee records were not exempt from, say, the operation of NPPs 3, 4, 5, 6, 9 and 10. This would mean organisations would be required to comply with those NPPs with respect to all personal information, including employee records.
- 4.31 Under this option, organisations would be required to:
- ensure that employee records were accurate, complete and up-to-date (NPP 3)
 - keep those records secure from interference and dispose of records once they were no longer required (NPP 4)
 - inform individuals about the information they hold (NPP 5)
 - permit employees to access their own records and correct or annotate records containing inaccurate information (NPP6)
 - comply with the requirements of the Privacy Act prior to transferring employee records overseas (NPP 9), and
 - comply with provisions relating to sensitive information about their employees (NPP 10).

Enact specific employee records privacy principles

- 4.32 Alternatively, the Commonwealth could enact specific employee records privacy principles. Such provisions could be included in the Privacy Act or other legislation, such as the Workplace Relations Act, or in a new Act.
- 4.33 One advantage of this option is that it would result in the enactment of specific privacy principles which acknowledge the special character of employee records and the practical needs of the organisations which handle them, while at the same time ensuring the privacy protection of employees' personal information.
- 4.34 However, the development of another set of privacy principles could be confusing for organisations which may be required to comply with different principles for different types of personal information. While the need for separate privacy principles for certain types of information, such as health information, could be justified on the basis of the sensitive nature of the information, information contained in employee records may not justify specific legislation.

Enhancing protection of employee records in Workplace Relations legislation

- 4.35 Limited privacy protection could be introduced by building on the existing obligations in the WR Act and Regulations. Additional provisions could impose obligations on employers not to disclose the information in records to third parties without the consent of the employees, subject to specific exemptions such as:
- to provide for access by inspectors, as presently provided under the Act, consistent with the enforceability of entitlements under the Act
 - where an employer needs to provide information for the purposes of the business, eg payroll processing, and
 - where required or authorised by law.
- 4.36 As noted in para 4.6 employers have raised concerns about allowing authorised union representatives to access records of non-members. To address this concern the WR Act and Regulations could be amended to specify that access by union representatives was limited to members' records.
- 4.37 The disadvantage of this option is that other employment records, kept by the employer but not required under workplace relations legislation, would remain unprotected. Those employment records could be protected by the Privacy Act. However, this would mean that employers would be required to comply with two legislative requirements.

Exclusive coverage in Workplace Relations legislation

- 4.38 Further amendments could be made to the WR Act so that one piece of legislation governed general record-keeping obligations and privacy requirements in relation to employee records. Additional provisions could provide access and correction rights to employees for records maintained additional to those that are required to be kept by the employer under workplace relations legislation. Provisions concerning collection of information, use of or access to information to persons other than the employee or other prescribed individuals, and security of information held by the employer could also be included.

- 4.39 Having one piece of legislation dealing with employee records and privacy protection of those records would simplify employer obligations and clarify employees' rights. This could also provide an opportunity to develop privacy standards, consistent with the NPPs, that recognise the particular needs of employers and employees.

Privacy provisions included in certified agreements or Australian workplace agreements

- 4.40 Although it is not a common practice, employees may negotiate provisions that protect their privacy, for inclusion in CAs or AWAs.
- 4.41 The WR Act could be amended to either direct the parties to consider, or even compulsorily require, privacy provisions in CAs or AWAs. This would be similar to the current requirement in the WR Act that AWAs contain provisions relating to discrimination.

Comments and submissions

- 4.42 This discussion paper has been prepared for consultation purposes. Comments and submissions on the options for enhancing privacy protection, or any other matters raised in this paper, are welcome. Comments should be sent to either of the addresses listed at page i. The closing date for comments and submissions is 16 April 2004.

Attachments

Attachment A Information Privacy Principles

Principle 1

Manner and purpose of collection of personal information

1. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:
 - (a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and
 - (b) the collection of the information is necessary for or directly related to that purpose.
2. Personal information shall not be collected by a collector by unlawful or unfair means.

Principle 2

Solicitation of personal information from individual concerned

Where:

- (a) a collector collects personal information for inclusion in a record or in a generally available publication; and
- (b) the information is solicited by the collector from the individual concerned;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware of:

- (c) the purpose for which the information is being collected;
- (d) if the collection of the information is authorised or required by or under law—the fact that the collection of the information is so authorised or required; and
- (e) any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first-mentioned person, body or agency to pass on that information.

Principle 3

Solicitation of personal information generally

Where:

- (a) a collector collects personal information for inclusion in a record or in a generally available publication; and
- (b) the information is solicited by the collector;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:

- (c) the information collected is relevant to that purpose and is up to date and complete; and
- (d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 4

Storage and security of personal information

A record-keeper who has possession or control of a record that contains personal information shall ensure:

- (a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and
- (b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

Principle 5

Information relating to records kept by record-keeper

1. A record-keeper who has possession or control of records that contain personal information shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:
 - (a) whether the record-keeper has possession or control of any records that contain personal information; and
 - (b) if the record-keeper has possession or control of a record that contains such information:
 - (i) the nature of that information;
 - (ii) the main purposes for which that information is used; and
 - (iii) the steps that the person should take if the person wishes to obtain access to the record.
2. A record-keeper is not required under clause 1 of this Principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.
3. A record-keeper shall maintain a record setting out:
 - (a) the nature of the records of personal information kept by or on behalf of the record-keeper;
 - (b) the purpose for which each type of record is kept;
 - (c) the classes of individuals about whom records are kept;
 - (d) the period for which each type of record is kept;
 - (e) the persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and
 - (f) the steps that should be taken by persons wishing to obtain access to that information.
4. A record-keeper shall:
 - (a) make the record maintained under clause 3 of this Principle available for inspection by members of the public; and
 - (b) give the Commissioner, in the month of June in each year, a copy of the record so maintained.

Principle 6

Access to records containing personal information

Where a record-keeper has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

Principle 7

Alteration of records containing personal information

1. A record-keeper who has possession or control of a record that contains personal information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:
 - (a) is accurate; and
 - (b) is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.
2. The obligation imposed on a record-keeper by clause 1 is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents.
3. Where:
 - (a) the record-keeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and
 - (b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth;the record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

Principle 8

Record-keeper to check accuracy etc. of personal information before use

A record-keeper who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.

Principle 9

Personal information to be used only for relevant purposes

A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.

Principle 10

Limits on use of personal information

1. A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:
 - (a) the individual concerned has consented to use of the information for that other purpose;
 - (b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;
 - (c) use of the information for that other purpose is required or authorised by or under law;
 - (d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or
 - (e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.
2. Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.

Principle 11

Limits on disclosure of personal information

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:
 - (a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;
 - (b) the individual concerned has consented to the disclosure;
 - (c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;
 - (d) the disclosure is required or authorised by or under law; or
 - (e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.
2. Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.
3. A person, body or agency to whom personal information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.

Attachment B National Privacy Principles

Principle 1 Collection

- 1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.
- 1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.
- 1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:
 - (a) the identity of the organisation and how to contact it; and
 - (b) the fact that he or she is able to gain access to the information; and
 - (c) the purposes for which the information is collected; and
 - (d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and
 - (e) any law that requires the 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.
- 1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.
- 1.5 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 subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

Principle 2 Use and disclosure

- 2.1 An organisation must not use or disclose personal information about an individual for a purpose (the *secondary purpose*) other than the primary purpose of collection unless:
 - (a) both of the following apply:
 - (i) 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;
 - (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or
 - (b) the individual has consented to the use or disclosure; or
 - (c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:
 - (i) it is impracticable for the organisation to seek the individual's consent before that particular use; and

- (ii) 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
 - (iii) the individual has not made a request to the organisation not to receive direct marketing communications; and
 - (iv) 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
 - (v) 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; or
- (d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:
- (i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and
 - (ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and
 - (iii) in the case of disclosure—the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or
- (e) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:
- (i) a serious and imminent threat to an individual's life, health or safety; or
 - (ii) a serious threat to public health or public safety; or
- (f) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
- (g) the use or disclosure is required or authorised by or under law; or
- (h) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:
- (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
 - (ii) the enforcement of laws relating to the confiscation of the proceeds of crime;
 - (iii) the protection of the public revenue;
 - (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;
 - (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: It is not intended to deter organisations from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

- 2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.
- 2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.
- 2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:
- (a) the individual:
 - (i) is physically or legally incapable of giving consent to the disclosure; or
 - (ii) physically cannot communicate consent to the disclosure; and
 - (b) a natural person (the *carer*) providing the health service for the organisation is satisfied that either:
 - (i) the disclosure is necessary to provide appropriate care or treatment of the individual; or
 - (ii) the disclosure is made for compassionate reasons; and
 - (c) the disclosure is not contrary to any wish:
 - (i) expressed by the individual before the individual became unable to give or communicate consent; and
 - (ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and
 - (d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).
- 2.5 For the purposes of subclause 2.4, a person is *responsible* for an individual if the person is:
- (a) a parent of the individual; or
 - (b) a child or sibling of the individual and at least 18 years old; or
 - (c) a spouse or de facto spouse of the individual; or
 - (d) a relative of the individual, at least 18 years old and a member of the individual's household; or
 - (e) a guardian of the individual; or
 - (f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or
 - (g) a person who has an intimate personal relationship with the individual; or
 - (h) a person nominated by the individual to be contacted in case of emergency.
- 2.6 In subclause 2.5:
- child* of an individual includes an adopted child, a step-child and a foster-child, of the individual.
- parent* of an individual includes a step-parent, adoptive parent and a foster-parent, of the individual.
- relative* of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.

sibling of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.

Principle 3

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.

Principle 4

Data security

- 4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.
- 4.2 An 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 National Privacy Principle 2.

Principle 5

Openness

- 5.1 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.
- 5.2 On request by a person, 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.

Principle 6

Access and correction

- 6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:
 - (a) in the case of personal information other than health information—providing access would pose a serious and imminent threat to the life or health of any individual; or
 - (b) in the case of health information—providing access would pose a serious threat to the life or health of any individual; or
 - (c) providing access would have an unreasonable impact upon the privacy of other individuals; or
 - (d) the request for access is frivolous or vexatious; or
 - (e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or
 - (f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
 - (g) providing access would be unlawful; or

- (h) denying access is required or authorised by or under law; or
- (i) providing access would be likely to prejudice an investigation of possible unlawful activity; or
- (j) providing access would be likely to prejudice:
 - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or
 - (ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or
 - (iii) the protection of the public revenue; or
 - (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
 - (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;
 by or on behalf of an enforcement body; or
- (k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: An organisation breaches subclause 6.1 if it relies on subclause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where subclause 6.2 does not apply.

- 6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.
- 6.4 If an organisation charges for providing access to personal information, those charges:
- (a) must not be excessive; and
 - (b) must not apply to lodging a request for access.
- 6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up-to-date.
- 6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up-to-date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to do so.
- 6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

Principle 7

Identifiers

- 7.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:
- (a) an agency; or
 - (b) an agent of an agency acting in its capacity as agent; or
 - (c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

- 7.1A However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2).

- 7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:
- (a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or
 - (b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or
 - (c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before the matters mentioned in paragraph(c) are prescribed: see subsection 100(2).

- 7.3 In this clause:

identifier includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the *A New Tax System (Australian Business Number) Act 1999*) is not an *identifier*.

Principle 8

Anonymity

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

Principle 9

Transborder data flows

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

- (a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or
- (b) the individual consents to the transfer; or

- (c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or
- (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or
- (e) all of the following apply:
 - (i) the transfer is for the benefit of the individual;
 - (ii) it is impracticable to obtain the consent of the individual to that transfer;
 - (iii) if it were practicable to obtain such consent, the individual would be likely to give it;
 or
- (f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

Principle 10

Sensitive information

- 10.1 An organisation must not collect sensitive information about an individual unless:
- (a) the individual has consented; or
 - (b) the collection is required by law; or
 - (c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:
 - (i) is physically or legally incapable of giving consent to the collection; or
 - (ii) physically cannot communicate consent to the collection; or
 - (d) if the information is collected in the course of the activities of a non-profit organisation—the following conditions are satisfied:
 - (i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;
 - (ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or
 - (e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.
- 10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:
- (a) the information is necessary to provide a health service to the individual; and
 - (b) the information is collected:
 - (i) as required by law (other than this Act); or
 - (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.
- 10.3 Despite subclause 10.1, an organisation may collect health information about an individual if:
- (a) the collection is necessary for any of the following purposes:
 - (i) research relevant to public health or public safety;
 - (ii) the compilation or analysis of statistics relevant to public health or public safety;
 - (iii) the management, funding or monitoring of a health service; and

- (b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and
- (c) it is impracticable for the organisation to seek the individual's consent to the collection; and
- (d) the information is collected:
 - (i) as required by law (other than this Act); or
 - (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or
 - (iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

10.5 In this clause:

non-profit organisation means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.