2014

THE LEGISLATIVE ASSEMBLY
FOR THE AUSTRALIAN CAPITAL TERRITORY

INFORMATION PRIVACY BILL 2014

REVISED EXPLANATORY STATEMENT

Presented by
Simon Corbell MLA
Attorney-General

Information Privacy Bill 2014
Overview and Purpose

The main purpose of the Information Privacy Bill 2014 is to introduce ACT privacy legislation to regulate the handling of personal information (other than personal health information) by public sector agencies in the Territory.

Background

ACT privacy legislation

Previously the Commonwealth *Privacy Act 1988* (the Privacy Act), as enacted in 1994, applied to the ACT and was administered by the Privacy Commissioner on behalf of the ACT Government.

The Privacy Act applied to ACT public sector agencies by virtue of section 23 of the Commonwealth *Australian Capital Territory Government Service (Consequential Provisions) Act 1994*. The Privacy Act also applied to the private sector in the Territory, as it does in other Australian jurisdictions.

In addition to this, the ACT has its own legislation dealing with personal health information and workplace surveillance:

- the *Health Records (Privacy and Access) Act 1997* provides a for privacy and access rights to personal health information whether it is held in the public or the private sector;
- the *Workplace Privacy Act 2011*, modelled on NSW legislation, regulates when an employer may conduct surveillance on an employee.

In acknowledging the responsibilities of ACT self-governance, and in light of the Commonwealth privacy reforms, it is timely for the ACT to consider developing its own Privacy Act applying to public sector agencies in the Territory.

This would cease the operation of the Commonwealth law in relation to public sector agencies in the Territory, leaving the Commonwealth law to cover the private sector, an approach adopted in other Australian jurisdictions, including New South Wales and Victoria.

The introduction of an ACT Privacy Act was a 2012 ACT Labor election commitment.

ACT Labor's 2012 election commitment for a fair, just and equitable society included a commitment to the development of the ACT's own privacy legislation, and a commitment to introduce a statutory cause of action to protect against serious invasions of privacy. Separate privacy legislation for ACT public sector agencies meets this commitment. Additional policy work on evaluating the suitability of a statutory cause of action for a breach of privacy will continue after the Australian Law Reform Commission (ALRC) report into a statutory cause of action for serious invasions of privacy that will guide the second stage of the Commonwealth's privacy reforms is published in June 2014.

Commonwealth privacy review

The Information Privacy Bill will be introduced in a time when significant amendments to the *Privacy Act 1988* (Cth) enter into force.

In early 2006, the ALRC received Terms of Reference to inquire into the extent to which the Privacy Act continues to provide effective privacy protection in Australia.

The ALRC's Report 108 '*For Your Information – Australian Privacy Law and Practice*' was released on 11 August 2008 and 295 recommendations were made to improve privacy protection in Australia.

On 23 May 2012 the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 was introduced into the Commonwealth Parliament. The Bill is designed to implement the major legislative elements of the Government's first stage response to the Australian Law Reform Commission's recommendations on privacy reform. The first stage response addressed 197 of the ALRC's 295 recommendations.

<u>Offences in the Information Privacy Bill</u>

The Information Privacy Bill is concerned with regulating the information handling and privacy practices of ACT public sector agencies. There are two provisions (sections 53(1) & (2)) which create criminal offences for the unauthorised and reckless use or disclosure of protected information by a public sector officer or other person who has obtained the information through their role performing functions under the Information Privacy Bill.

It is a defence to the charge of use or disclosure of protected information if the use or disclosure is authorised by a Territory law, is in relation to the exercise of a function under a Territory law, is in a court proceeding or is used or disclosed with consent of the person to whom the information relates.

The maximum penalty for these offences is 50 penalty units, imprisonment for 6 months or both. These offences are in line with the principles set out in the JACS Guide to Framing Offences and are aimed at ensuring that personal information which can come into the possession of individual public sector officers by virtue of their position in a public sector agency is not misused. Creating offences to discourage the abuse of personal information is necessary to ensure trust in the ability of the Commissioner and other officials to responsibly manage information obtained or compelled from ACT residents by the operation of the Information Privacy Act.

At the same time, the bill provides that officials cannot be held civilly liable for an act or omission done honestly and without recklessness in the exercise of a function under the Information Privacy legislation.

Human rights considerations

Right to privacy – section 12 Human Rights Act 2004

Privacy is a quality that emphasises human desire for personal autonomy, dignity and freedom from arbitrary or unreasonable or oppressive interference and intrusion into an individual's personal sphere.

The right to privacy and reputation is set out in section 12 of the *Human Rights Act 2004*. That section states that -

Everyone has the right—

(a) not to have his or her privacy, family, home or correspondence interfered with unlawfully or arbitrarily; and

(b) not to have his or her reputation unlawfully attacked.

The right to privacy in the Human Rights Act is based on the right to privacy set out in Article 17 of the International Covenant on Civil and Political Rights ('ICCPR'). The UN Human Rights Committee ('UNHRC'), commenting on the right to privacy, noted that 'as all persons live in society, the protection of privacy is necessarily relative. However, the competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society...'[1]

The UNHRC has stated that unlawful, in the context of the right to privacy set out in Article 17, "means that no interference can take place except in cases envisaged by the law. Interference can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant".[2]

The protection from arbitrary interference with privacy means that the State cannot randomly or capriciously interfere with an individual's privacy in a manner that is unrestrained or not based on demonstrable evidence. The UNHRC has stated that an interference that is lawful can be arbitrary if it is unreasonable in the circumstances.[3] Reasonableness implies that any interference with privacy must be proportionate to the end sought and must be necessary in the circumstances of any given case.[4]

[1] UN Human Rights Committee, *General Comment 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art 17*), UN Doc CCPR General Comment 16 (1988), para.7
[2] Ibid, para.3
[3] Ibid, para.4
[4] Toonen v Australia, Communication 4888/1992, UN Doc CCPR/C/50/D/488/1992 (1994), para 8.3.

The Information Privacy Bill supports and enhances the right to privacy by ensuring that there is a clear framework setting out how ACT public sector agencies collect, use, disclose and otherwise manage personal information.

Ensuring there is a comprehensive and clearly identifiable privacy regime in the ACT means that individuals are protected from arbitrary or unlawful breaches of an individual's right to privacy. If breaches do occur, the Information Privacy Bill establishes mechanisms for the independent investigation and resolution of complaints and an avenue for redress through the courts.

Arguably, part 4 of the Act may impose a limitation on the right to privacy by exempting some public sector agencies from the operation of the Act. The right to privacy is not absolute and may be reasonably limited by laws which can be demonstrably justified in a free and democratic society.

Under section 24 an exemption for certain public sector agencies is limited in application to three non-permanent investigative bodies, plus entities prescribed by regulation, that can be established to perform important functions of inquiry, according to law.

These include:

(a) a board of inquiry under the *Inquiries Act 1991*;

(b) a judicial commission under the *Judicial Commissions Act 1994*;

(c) a royal commission under the *Royal Commissions Act 1991*; and

(d) an agency prescribed by regulation.

Section 17 of the *Inquiries Act 1991;* s 28 of the *Judicial Commissions Act 1994* and s 20 of the *Royal Commissions Act 1991* all create criminal offences for the unlawful and unauthorised collection, use or disclosure of information obtained by virtue of a person's involvement with the inquiry or commission. These protections are stricter than those set out in the Information Privacy Bill 2014, but also appropriately tailored to the special nature and conduct of such investigations.

Under section 25 the Information Privacy Bill will not apply to the following acts and practices:

(a) for a Minister—an act done, or a practice engaged in, by the Minister other than an act done, or a practice engaged in, by the Minister in relation to the affairs of a public sector agency administered by the Minister;

(b) for an ACT court—an act done, or a practice engaged in, by the ACT court other than an act done, or a practice engaged in, by the ACT court in relation to a matter of an administrative nature;

(c) for the Office of the Legislative Assembly—an act done, or a practice engaged in, by the Office other than an act done, or a practice engaged in, by the Office in exercising a function in relation to a proceeding of the Legislative Assembly;

(d) for officers of the Assembly—an act done, or a practice engaged in, by the officer of the Assembly other than an act done, or a practice engaged in, by the officer in relation to a matter of an administrative nature;

(e) for an FOI exempt agency—an act done, or a practice engaged in, by the agency in relation to a document in relation to which the agency is exempt from the operation of the FOI Act;

(f) for an agency prescribed by regulation—an act done, or a practice engaged in, by the agency in relation to a matter prescribed by regulation.

Section 28 of the Human Rights Act states that rights can be subjected to reasonable limitations set by laws that can be demonstrably justified in a free and democratic society.

These exemptions for the listed specific acts and practices are necessary for the effective operation and independence of those specified entities. The exemptions continue existing privileges for Government and the Legislative Assembly and maintain the independence of the Courts. FOI exempt agencies have been identified as appropriately exempted from other information handling and release rules because they relate to commercial–in-confidence information or relate to personal health information.

Entities exempted from the Information Privacy Act in relation to their non-administrative functions are subject to other forms of accountability and oversight which offer equivalent privacy protections in manner that is suitably adapted to allow certain public officials in specific agencies, officers and members of the Assembly and the judiciary to perform their important functions.

These limitations are already extant under the Commonwealth Privacy Act as it applies in a modified form in the ACT. They are clearly defined and the boundaries within which practices are exempted are proportionate to the importance of supporting the functions of the exempted entities. There are no blanket exceptions for these entities, and their administrative functions still fall within the scope of the Act. There are no less restrictive means reasonably available to achieve the purpose of these exemptions.

Right to freedom of expression – section 16 Human Rights Act 2004

By regulating the collection, use and disclosure of information, the Information Privacy Act 2014 will necessarily limit the right to freedom of expression in section16 of the Human Rights Act.

Freedom of expression

1) Everyone has the right to hold opinions without interference.
2) Everyone has the right to freedom of expression. This right includes the freedom to seek, receive and impart information and ideas of all kinds, regardless of borders, whether orally, in writing or in print, by way of art, or in another way chosen by him or her.

While the right to freedom of expression is a fundamental right, the Information Privacy Act balances the need for communication of information with the right to privacy by setting out different categories of information and imposing additional requirements for the handling of personal information and sensitive information. Other forms of information can be collected and stored without restriction, subject to other Territory or Commonwealth laws. The limitations set out in requiring public sector officials to observe the Territory Privacy Principles (TPPs) in the Act, aim to limit unauthorised use or disclosure of personal information obtained by ACT public sector agencies. These limitations are both justified and proportionate to ensure that this information, collection of which is necessary for the proper functioning of governance, is handled in accordance with clear procedures and practices that recognise the importance of personal information to the person to which it relates.

In the landmark UK case *McKennitt v Ash* Eady J considered the tension between freedom of expression and the privacy rights of an individual. He stated that -

> It is clear that [in the United Kingdom] there is a significant shift taking place as between, on the one hand, freedom of expression for the media and the corresponding interest of the public to receive information, and, on the other hand, the legitimate expectation of citizens to have their private lives protected … Even where there is a genuine public interest, alongside a commercial interest in the media in publishing articles or photographs, sometimes such interests would have to yield to the individual citizen's right to the effective protection of private life.[5]

It is desirable that the broad powers of agencies to require and compel, on threat of penalty, a wide range of personal information, are restrained by a general system of checks on the fair and reasonable use and disclosure of that information. The limitations in the TPPs are not absolute. Personal information can be used or disclosed within circumstances prescribed by the Act or other Territory laws. There are protections for use or disclosure done honestly and without recklessness by an officer in the course of performing functions under the Act. The Act establishes mechanisms for investigating and resolving alleged breaches of privacy and as part of such investigation may determine that a an act or practice was not an interference with the privacy of the individual or was authorised by law.

[5] *McKennitt v Ash* [2005] EMLR 10, [57].

Climate change impacts

Climate change impacts have been considered and no impacts have been identified.

Clause Notes

Part 1 Preliminary

Clause 1 Name of Act

This clause provides that the title of this Act is the *Information Privacy Act 2014*.

Clause 2 Commencement

This clause provides that the Act will come into operation on a day fixed by the Minister by written notice. Notes included in the clause refer to certain commencement provisions in the *Legislation Act 2001* which are relevant to this commencement provision.

This clause also fixes a day for the purposes of the *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* (Cth) to end the application of the *Privacy Act 1988* (Cth) to public sector agencies in the ACT.

Clause 3 Dictionary

This clause clarifies that the dictionary at the end of the Act is part of the Act and that definitions in the dictionary apply also to the local application provisions of the Act.

Clause 4 Notes

This clause clarifies that a note included in the local provisions of this Act is explanatory and not part of those provisions.

Clause 5 Offences against Act –application of Criminal Code etc

This clause clarifies that the Criminal Code and other legislation apply in relation to offences against this Act.

Clause 6 Relationship with other laws

This provision sets out that the Information Privacy Act does not modify the operation or existing obligations in other territory laws relating to personal information and record keeping.

Part 2 Objects and important concepts

Clause 7 Objects of Act

The objects clause outlines the underlying purpose of the Act and provides assistance with interpretation. There are four objects:

1. promote the protection of the privacy of individuals;
2. recognise that the protection of the privacy of individuals is balanced with the interests of public sector agencies in carrying out their functions or activities;
3. promote responsible and transparent handling of personal information by public sector agencies and contracted service providers; and
4. provide a way for individuals to complain about an alleged interference with their privacy.

Clause 8 Meaning of *personal information*

This clause defines which information is considered to be personal information for the purposes of this act. Personal information is any information that is -

'*information or an opinion about an identified individual, or an individual who is reasonably identifiable—*

a) whether the information or opinion is true or not; and
b) whether the information or opinion is recorded in a material form or not'.

The definition has been adopted from Commonwealth *Privacy Act 1988* incorporating amendments by the Commonwealth Privacy Amendment (Enhancing Privacy Protection) Bill 2012.

The amendments to the definition do not significantly change the scope of what is considered to be personal information. The definition continues to be based on factors which are relevant to the context and circumstances in which personal information is collected and held.

The definition continues to be sufficiently flexible and technology-neutral to encompass changes in the way that information that identifies an individual is collected and handled.

The definition of ***personal information*** in the Act specifically excludes personal health information. The ACT's existing *Health Records (Privacy and Access) Act 1997* will continue to regulate privacy and access rights to personal health information held in the public or the private sector.

Clause 9 Meaning of *public sector agency*

This clause defines which entities are considered to be a public sector agency for the purposes of this Act.

Public sector agency is defined to mean:

- a Minister – defined in the *Legislation Act 2001* to mean the Chief Minister or a Minister appointed under section 41 of the Self-Government Act;

- an administrative unit – defined in the Legislation Act to mean an administrative unit for the time being established under section 13(1) of the *Public Sector Management Act 1994*. Administrative units are currently listed in schedule 1, column 3 of Administrative Arrangements 2013 (No 1) NI2013-244[6]. An example is the Justice and Community Safety Directorate;

- a statutory office-holder and the staff assisting the statutory office-holder – statutory office-holder is defined in the Legislation Act to mean a person occupying a position under an Act or statutory instrument (other than a position in the public service). An example is the Director of Public Prosecutions, appointed under section 22 of the *Director of Public Prosecutions Act 1990*;

- a territory authority – defined in the Legislation Act to mean a body established for a public purpose under an Act, other than a body declared by regulation not to be territory authority. An example of a body established for a public purpose is the Legal Aid Commission (ACT);

- a territory instrumentality – defined in the Legislation Act to mean a corporation that is established under an Act or statutory instrument, or under the Corporations Act, and is a territory instrumentality under the *Public Sector Management Act 1994* (is comprised of people, or has a governing body comprised of people, a majority of whom are appointed by a Minister or an agency or instrumentality of the Territory, or is subject to control or direction by a Minister, or is declared under the Act to be a territory instrumentality). An example is the ACT Professional Standards Council established under the *Civil Law (Wrongs) Act 2002*;

- a territory-owned corporation or a subsidiary of a territory-owned corporation – defined in the Legislation Act to mean a Territory owned corporation under the *Territory-owned Corporations Act 1990*. An example is ACTEW;

- an ACT court-defined in the dictionary to mean the Supreme Court, Magistrates Court, Coroner's Court or a tribunal, and include a judge, magistrate, tribunal member and any other person exercising a function of the court or tribunal in relation to the hearing or determination of a matter before it.

[6] This instrument can be located on the ACT Legislation Register at http://www.legislation.act.gov.au/ni/2013-244/default.asp

In addition to the categories above, this clause also includes a power to prescribe by regulation an entity to be treated as a public sector agency for the purposes of this act.

Clause 10 Reference to *act* or *practice* of a public sector agency etc

This clause specifies that references to act or practice of a public sector agency or a contracted service provider is taken to mean an act done or practice engaged in by the public sector agency or contracted service provider.

This clause specifies that a reference to doing an act means both doing an act in accordance with a practice and failing to do an act.

Clause 11 Meaning of *interference* with individual's privacy

This clause sets out a definition of ***interference*** for the purposes of this Act. It outlines the circumstances that will result in an interference with the privacy of an individual.

An act or practice of a public sector agency will be an interference with the privacy of an individual where it breaches a Territory privacy principle in relation to personal information about the individual, or breaches a TPP code that binds the agency in relation to personal information about the individual.

An act or practice of a contracted service provider under a government contract will be an interference with the privacy of an individual if the act or practice breaches a TPP or TPP code binding the agency which entered into the contract.

Clause 12 Meaning of *breach* a TPP etc

This clause sets out a definition of ***breach*** for the purposes of this Act. This clause outlines the circumstances that will result in a breach of Territory privacy principles, or a TPP code.

An act or practice breaches a Territory privacy principle, or approved TPP code, only if it is contrary to, or inconsistent with, the principle or code.

An act or practice would not breach a Territory privacy principle, or approved TPP code, if it was done, or engaged in, outside the ACT, and is required by a law of another jurisdiction or a foreign country.

Part 3 Territory privacy principles

Division 3.1 Important concepts – Territory privacy principles

Clause 13 Territory privacy principles

This clause establishes the Territory privacy principles as the principles set out in schedule 1 of the Act (see below for an explanation of the principles).

Clause 14 Definitions--sch 1

This clause provides definitions of some important concepts that are used in the Territory privacy principles, including ***Australian law***, ***court or tribunal order***, ***enforcement body***, ***enforcement related activity***, ***related body corporate***, ***sensitive information***, ***territory record*** and ***collects***, ***holds***, ***solicits*** and ***de-identified*** personal information.

Clause 15 Meaning of *collects* personal information – sch 1

This clause defines collection of personal information as the collection of information for inclusion in a record or generally available publication. This means that use of information generally, for example by a public sector officer reading newspaper, is not collection of personal information if this information is not to be recorded or re-published. If an agency does collect information by recording it, even where that information exists in the public domain, that collection must be in accordance with the TPPS.

Clause 16 Meaning of *holds* personal information – sch 1

This clause defines the circumstances in which an agency will be taken to hold personal information. An agency is taken to hold personal information if the agency has possession or control of that information.

Clause 17 Meaning of *solicits* personal information – sch 1

This clause defines the circumstances in which an agency will be taken to solicit personal information. An agency is taken to solicit personal information if the agency requests another entity to provide personal information of an individual, or some other information from which personal information can be obtained.

Clause 18 Meaning of *de-identified* personal information – sch 1

This clause defines the circumstances in which personal information is considered to be de-identified. Information is de-identified for the purposes of this act if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.

De-identified personal information is not considered to be personal information for the purposes of this Act.

This means that if an agency can effectively remove a reasonable possibility of information being traced back to or linked with a specific individual then the information is no longer treated as personal information. Such de-identified information will not be subject to the protections and controls under this Act.

The APP Guidelines produced by the Office of the Australian Information Commissioner state that when determining if information is 'reasonably identifiable' an agency may have regard to the cost, difficulty, practicality and likelihood of the information being linked with a specific individual.

Clause 19 Meaning of *permitted general situation* in relation to the collection, use or disclosure of personal information - sch 1

This clause defines permitted general situation for the purposes of this Act.

There are a number of exceptions in the TPPs where the collection, use or disclosure by a public sector agency of personal information about an individual will not be a breach of the principles. One of these exceptions is referred to as a ***permitted general situation***. ***Permitted general situation*** is defined in this part in the following manner -

<u>Prevention of serious threat to life, health or safety</u>
The first condition of this exception is that it is unreasonable and impracticable to obtain the individual's consent to the collection, use or disclosure and the officer has a reasonable belief that the use of the personal information is necessary to lessen or prevent a serious threat to life, or to the health and safety of an individual or of the public. For the purposes of this exception, whether it is 'reasonable' to seek consent would include whether it is realistic or practicable to seek consent. This might include where it could be reasonably anticipated that the individual would withhold consent (such as where the individual has threatened to do something to create the serious risk). It would also likely be unreasonable to seek consent if there is an element of urgency that requires quick action.

Seeking consent would not be 'practicable' in a range of contexts. These could include when the individual's location is unknown or they cannot be contacted. If seeking consent would impose a substantial burden then it may not be practicable. It may also not be practicable to seek consent if the use or disclosure relates to the personal information of a very large number of individuals.

In assessing whether it is 'reasonable or practicable' to seek consent, agencies could also take into account the potential consequences and nature of the serious threat.

Secondly, the act or practice will be permitted where the collection, use or disclosure of personal information is necessary to lessen or prevent a serious threat to the life, health or safety of any individual or to public health or safety.

Unlawful activity

This exception will apply where the public sector agency has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to an agency's functions or activities has been, is being or may be engaged in, and the agency reasonably believes that the collection, use or disclosure of personal information is necessary in order for the entity to take appropriate action in relation to the matter.

The provision, by specifying that the unlawful activity or serious misconduct must relate to an entity's functions or activities, intends that the exception will apply to an agency's internal investigations. Examples of 'appropriate action' in this context may include collection of personal information for an internal investigation in relation to a breach of the *Public Sector Management Act 1994*.

Missing people

This exception will apply where the agency reasonably believes that the collection, use or disclosure of personal information is reasonably necessary to assist a public sector agency to locate a person who has been reported as missing, and the collection, use or disclosure complies with rules made by the Information Privacy Commissioner.

Legal or equitable claim

This exception will allow a public sector agency to collect, use or disclose personal information where it is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim.

Confidential alternative dispute resolution

This exception will allow a public sector agency to collect, use or disclose personal information where it is reasonably necessary for the purposes of a confidential alternative dispute resolution process.

The confidentiality safeguard included in the provision will limit the scope of the alternative dispute resolution exception and so ensure an additional protection for personal information.

Division 3.2 Compliance with TPPs

Clause 20 Public sector agencies must comply with TPPs

This clause sets out the general requirement that a public sector agency must act in accordance with this Act. A public sector agency must not do any act, or engage in a practice, that breaches a TPP.

A breach of the TPPs will be an interference with privacy by the public sector agency and can be subject to investigation by the Information Privacy Commissioner under part 6 of the Act.

Clause 21 Privacy protection requirements for government contracts

A public sector agency will be required to take appropriate measures for all future government contracts to ensure that a contracted service provider and any subcontractor does not do an act, or engage in a practice, that would breach a TPP, or a TPP code that binds the agency (see explanation about TPP codes below).

A public sector agency will be required to take appropriate measures for all future government contracts to ensure the contract does not authorise a contracted service provider, or any subcontractor to do a contravening act or breach of the Act.

However, failure by the public sector agency to comply with this section does not affect any obligations of the agency, the contractor or subcontractor to perform and fulfil the contract.

This clause defines 'subcontractor' as any person engaged by a contracted service provider under the government contract, or any subcontracting arrangement, to provide the services specified in that contract.

Division 3.3 Other privacy compliance matters

Clause 22 Deemed breach in relation to acts and practices of overseas recipients of personal information

This clause provides that a public sector agency will be taken to have breached the TPPs if:

a) the agency discloses personal information about an individual to an overseas recipient; and

b) TPP 8.1 (cross border disclosure of personal information) applies to that disclosure; and

c) the TPPs do not apply under the Act to acts done, or practices engaged in, by the overseas recipient in relation to the information; and

d) the overseas recipient does something that would be a breach of the TPPs if the TPPs had applied to those acts or practices.

The provision complements TPP 8.1, which contains key aspects of the accountability approach in the Act. Under TPP 8.1, there is a positive requirement on public sector agencies to take reasonable steps to ensure the overseas recipient will protect the information to a standard which is equivalent and consistent with the TPPs. The reasonable steps must be taken by the agency prior to any cross-border transfer of personal information occurring.

Clause 23 Commonwealth APPs apply to certain public sector agencies engaged in commercial activities

This clause provides that the Commonwealth APPs which entered into force on 12 March 2014 will apply to the acts and practices of certain ACT public sector agencies as if the agency were a private sector entity, only in relation to the agency's commercial activities.

Specific ACT public sector agencies to which the APPs will apply in relation to the agency's commercial activities are listed in the *Freedom of Information Regulation 1991* and may be varied or added to by amendment of that regulation. At present the only agency which falls within the scope of the provision is ACTTAB Limited in relation to documents in relation to its competitive commercial activities.

Other agencies listed in the Freedom of Information Regulation are not listed in relation to documents that relate to the performance of commercial activities mentioned. Clause 23 provides that additional agencies may be prescribed by regulation.

Part 4 Exemptions from application of Act
Clause 24 Exempt public sector agencies

This clause provides specific exemptions for certain public sector agencies whose functions are of an investigative nature from the operation and obligations set out in the Act.

The Act does not apply to:

- a board of inquiry under the *Inquiries Act 1991*;
- a judicial commission under the *Judicial Commissions Act 1994*;
- a royal commission under the *Royal Commissions Act 1991*;
- an agency prescribed by regulation.

As discussed in the human rights analysis above, section 17 of the *Inquiries Act 1991;* s 28 of the *Judicial Commissions Act 1994* and s 20 of the *Royal Commissions Act 1991* all create criminal offences for the unlawful and unauthorised collection, use or disclosure of information obtained by virtue of a person's involvement with the inquiry or commission. These protections are stricter than those set out in the Bill, but also appropriately tailored to the special nature and conduct of such investigations.

Clause 25 Exempt acts or practices of certain public sector agencies

This clause provides that the Act does not apply to the acts and practices of:

(a) for a Minister—an act done, or a practice engaged in, by the Minister other than an act done, or a practice engaged in, by the Minister in relation to the affairs of a public sector agency administered by the Minister;

(b) for an ACT court—an act done, or a practice engaged in, by the ACT court other than an act done, or a practice engaged in, by the ACT court in relation to a matter of an administrative nature;

(c) for the Office of the Legislative Assembly—an act done, or a practice engaged in, by the Office other than an act done, or a practice engaged in, by the Office in exercising a function in relation to a proceeding of the Legislative Assembly;

(d) for officers of the Assembly—an act done, or a practice engaged in, by the officer of the Assembly other than an act done, or a practice engaged in, by the officer in relation to a matter of an administrative nature;

(e) for an FOI exempt agency—an act done, or a practice engaged in, by the agency in relation to a document in relation to which the agency is exempt from the operation of the FOI Act;

(f) for an agency prescribed by regulation—an act done, or a practice engaged in, by the agency in relation to a matter prescribed by regulation.

These exemptions are in place so that the functions of specific bodies of the judiciary and the executive are kept independent from the mechanisms of government in order that those bodies can effectively perform the functions given to them by the Australian Constitution or other Commonwealth and Territory laws. This clause means that while the Act will generally apply to all public sector agencies that fall within the definition of public sector agency in section 9, some aspects of the operations or functions of specific public sector agencies will not be subject to the Act.

The Act provides sufficient flexibility to add to the exemptions expressly provided for in the Act, by enabling regulations to prescribe other exemptions.

Part 5 Information privacy commissioner

Clause 26 Appointment of information privacy commissioner

This clause states that the Executive may appoint a person as Information Privacy Commissioner under the Act.

Clause 27 Terms and conditions of appointment

This clause specifies that if an Information Privacy Commissioner is appointed that appointment must not be for more than 7 years. Similar time limits apply to appointment of

the Ombudsman under s 23 of the *Ombudsman Act 1989.* The Legislation Act provides that a person is able to be reappointed under an Act if the person remains eligible.

This clause also provides that if an ACT Information Privacy Commissioner is appointed by the Executive it will be on the terms and conditions agreed between the Executive and Commissioner subject to any determination by the Remuneration Tribunal under the *Remuneration Tribunal Act 1995.*

Section 10(1)(b) of the Remuneration Tribunal Act provides that the Remuneration Tribunal must inquire into, and determine, the remuneration, allowances and other entitlements of the holders of any position or appointment notified in writing by the Chief Minister.

Clause 28 Arrangements for privacy commissioner of another jurisdiction to exercise functions

This clause provides that if the Executive does not appoint a person as Information Privacy Commissioner under section 26, the Government may enter into arrangement with another Commonwealth, state or territory information or privacy commissioner (however described) to exercise one or more of the functions of the Information Privacy Commissioner in the ACT.

This clause allows the ACT to arrange with another jurisdiction to exercise one or more of the commissioner functions, such as privacy complaints resolution, privacy investigation and breach monitoring and auditing services.. Such arrangements must be adopted until such time as the Executive appoints a person as the Information Privacy Commissioner.

Clause 29 Information privacy commissioner's functions

This clause sets out the functions of the Information Privacy Commissioner under the Act.

The functions of the Information Privacy Commissioner are to -

(a) promote an understanding of the TPPs and the objects of the TPPs; and

(b) provide information and educational programs to promote the protection of the privacy of individuals; and

(c) help public sector agencies to comply with the TPPs and TPP codes; and

(d) investigate privacy complaints made under this Act; and

(e) exercise any other functions given to the commissioner under this Act or another territory law.

Clause 30 Disclosure of interests

This clause provides that a person appointed to be Information Privacy Commissioner must give written notice to the Executive of all financial and other interests the Commissioner has that conflict or could conflict with the proper exercise of the Commissioner's functions.

Clause 31 Delegation of information privacy commissioner's functions

This clause provides that a person appointed to be Information Privacy Commissioner may delegate the functions of the Commissioner under the Act or any other Territory law to a person.

General rules for the making and exercise of functions are found in the part 19.4 of the Legislation Act.

Clause 32 Ending of information privacy commissioner's appointment

This clause sets out the circumstances in which the information privacy commissioner's appointment may be ended. This clause is consistent with other Territory legislation establishing statutory offices.

The Executive may end the appointment -

a) if the information privacy commissioner contravenes a territory law or law of another jurisdiction; or

b) for misbehaviour; or

c) if the commissioner becomes bankrupt or personally insolvent; or

d) if the commissioner is absent, other than on approved leave, for 14 consecutive days or for 28 days in any 12-month period.

The Executive must end the Commissioner's appointment –

a) for physical or mental incapacity if the incapacity substantially affects the exercise of the commissioner's functions;

b) If the commissioner fails to comply, without reasonable excuse with the requirements of section 30 to disclose conflicts of interest.

Part 6 Privacy complaints

Division 6.1 Important concepts

Clause 33 What is a *privacy complaint* etc?

This clause defines terms used in this part of the Act. A privacy complaint is a complaint about an act or practice of a public sector agency or contracted service provider that may be an interference with an individual's privacy.

For this part of the Act, the complainant is the person making the complaint and the respondent is the agency or public sector contractor who is alleged to have interfered with the individual's privacy.

Division 6.2 Making privacy complaints

Clause 34 Who may make a privacy complaint?

This clause provides that an individual may make a privacy complaint to the Information Privacy Commissioner. If there is a claim of an interference with the privacy of two or more individuals, any of those individual may make a complaint on behalf of all the individuals. The Information Privacy Commissioner must give help to the individual to make the privacy complaint as appropriate. This help may include advising the individual about the complaints process under the Act, or helping the individual to put the complaint in writing.

Clause 35 How may a privacy complaint be made?

This clause provides that a privacy complaint must be in writing, and include the complainant's name, address and telephone number. The complaint must also identify the entity complained about and include details about the act or practice that is the subject of the complaint.

A privacy complaint may be made orally if the Information Privacy Commissioner is reasonably satisfied that exceptional circumstances justify this. An example of an exceptional circumstance may be made if the person is unable to write in English, or has other communication difficulties.

Clause 36 Privacy complaint may be referred to commissioner

This clause permits a privacy complaint to be referred to the Information Privacy Commissioner by the Ombudsman, the Human Rights Commission, or any entity equivalent to the Information Privacy Commissioner regulating privacy in another Australian jurisdiction. Additional entities that may refer a privacy complaint can be prescribed by regulation. A privacy complaint referred to the Information Privacy Commissioner must be accompanied by all relevant information in relation to the complaint.

Clause 37 Commissioner must tell respondent about complaint

This clause provides that the Information Privacy Commissioner must give a copy of a privacy complaint to the entity complained about as soon as possible after the Commissioner receives the complaint. This requirement ensures that the agency is given appropriate notice before the Commissioner deals with a complaint. It will give the agency notice to begin gathering necessary information about the subject of the complaint and provide an early opportunity to co-operate with the Commissioner.

Division 6.3 Dealing with privacy complaints

Clause 38 Commissioner may make preliminary inquiries

This clause sets out that the Commissioner has the power to make inquiries of the public sector agency that is the subject of the complaint, as well as any other person. It is intended that the Commissioner will only make inquiries of third parties when satisfied that this approach will result in more timely and efficient complaint resolution.

Clause 39 Commissioner may decide not to deal with privacy complaint

This clause provides that the Information Privacy Commissioner may decide not to deal with a complaint if reasonably satisfied that:

a) the act or practice complained about is not an interference with an individual's privacy;

b) the complaint was made more than 12 months after the complainant became aware of the act or practice;

c) the complaint is frivolous, vexatious, misconceived, lacking in substance or not made in good faith;

d) the act or practice is the subject of an application under another Australian law, and the substance of the complaint has been, or is being, dealt with adequately under that law;

e) the complaint would be better dealt with under another Australian law;

f) dealing, or further dealing, with the act or practice is not warranted having regard to all the circumstances;

g) the complainant has complained to the respondent about the act or practice and –

   i. the respondent has dealt, or is dealing, adequately with the complaint, or

   ii. the respondent has not yet had an adequate opportunity to deal with the complaint.

This clause gives the Information Privacy Commissioner the flexibility to efficiently manage privacy complaints.

Clause 40 Dealing with privacy complaints

This clause provides that the Information Privacy Commissioner may make inquiries and investigations in relation to a complaint, as appropriate, if the Commissioner decides to deal with a complaint.

This clause also provides that the Information Privacy Commissioner may decide not to continue dealing with a complaint, or part of a complaint in the following circumstances:

a) the complainant does not comply with a reasonable request made by the Commissioner in dealing with the complaint, or part of the complaint; or

b) the Commissioner is reasonably satisfied that the complainant, without reasonable excuse, has not co-operated in the Commissioner's dealing with the complaint, or part of the complaint; or

c) the Commissioner has not been able to contact the complainant for a reasonable period of time using the contact details in the privacy complaint.

Clause 41 Commissioner must tell parties about decision to not deal with privacy complaint

This clause provides that the Information Privacy Commissioner must tell a complainant and the respondent if the Commissioner decides not to deal with a privacy complaint, or stops dealing with a privacy complaint. The Commissioner must also give the reasons for the decision.

Clause 42 Commissioner may refer privacy complaint to other entity

This clause provides that the Information Privacy Commissioner can refer a privacy complaint to another investigative entity with power to investigate the complaint, if reasonably satisfied that the complaint would be better dealt with by that entity. This clause names the Ombudsman, the Human Rights Commission, and any equivalent body regulating privacy in other Australian jurisdictions as entities to which the Information Privacy Commissioner can refer a complaint. Other entities could be prescribed by regulation as appropriate. If the Information Privacy Commissioner refers a complaint to another entity, the Commissioner must provide that entity with all relevant information about the complaint and tell both the complainant and the respondent about the referral.

Clause 43 Commissioner may report serious or repeated interferences to Minister

This clause provides the Information Privacy Commissioner with a discretion to give a report to the Attorney General in situations where the Commissioner is reasonably satisfied that a public sector agency, or contracted service provider, has done an act or engaged in a practice which is a serious interference with the privacy of an individual, or where the agency has repeatedly done an act, or engaged in a practice that is an interference with the privacy of one or more individuals.

The Minister must then table the report in the Legislative Assembly within 6 sitting days.

This clause is designed to provide accountability and scrutiny of acts or practices of an agency or government contractor where the Information Privacy Commissioner is reasonably satisfied that there has been a serious or repeated interference with the privacy of one or more individuals.

The Act does not define what constitutes a 'serious' or 'repeated' interference with the privacy of an individual. The ordinary meaning of these words would apply.

Clause 44 Commissioner may obtain information

This clause provides that the Information Privacy Commissioner may also ask anyone to give the Commissioner information so that the Commissioner may deal with a privacy complaint.

A public sector agency or public official for the agency must comply with a request for information by the Commissioner.

The term *public official* is defined for the purpose of this section.

Division 6.4 Application to court

Clause 45 Commissioner must tell parties application may be made to court

This clause provides that where the Information Privacy Commissioner is reasonably satisfied after dealing with a privacy complaint that there has been an interference with the complainant's privacy, the Commissioner must give written notice to the complainant and respondent telling them this. The Commissioner must also tell the complainant that they may apply to a court for an order.

Clause 46 Complainant may apply for court order

This clause provides that, within six months of a notification by the Commissioner, a complainant may apply to a court to make an application for one or more of the orders listed in clause 47.

Clause 47 What orders may a court make?

This clause specifies the types of orders that the court may make to resolve a privacy complaint which has been determined to involve an interference with an individual's privacy. The court may make:

a) an order that the complaint, or part of the complaint, has been substantiated, together with, if appropriate, one or more of the following orders:

   i. that an act or practice of the respondent is an interference with the privacy of the complainant and that the respondent must not repeat or continue the act or practice;

   ii. that the respondent must engage in a stated reasonable act or practice to compensate for loss or damage suffered by the complainant;

   iii. that the respondent must make a stated amendment of a record it holds;

   iv. that the complainant is entitled to a stated amount, of not more than $100 000, to compensate the complainant for economic loss or damage suffered by the complainant because of the act or practice complained of;

b) an order that the complaint, or part of the complaint, has been substantiated together with an order that no further action is required to be taken;

c) an order that the complaint, or part of the complaint, has not been substantiated, together with an order that the complaint or part is dismissed;

d) an order than the complainant be reimbursed for expenses reasonably incurred in relation to making the complaint.

Division 6.5 Contracted service providers

Clause 48 Private sector agency must be kept informed about privacy complaint involving contracted service provider

This clause provides that if a privacy complaint relates to an act or practice of a contracted service provider under a government contract and the Commissioner is required by the Act to tell or give a thing to the respondent, the Information Privacy Commissioner must also tell or give the same information to the agency who has contracted with the service provider.

Part 7 TPP Codes

This part provides for the development of codes of practice about information privacy.

The provisions have been developed based on the new codes of practices (APP codes) that were established under the Commonwealth *Privacy Act 1988* by the *Privacy Amendment*

(Enhancing Privacy Protection) Act 2012. In the Commonwealth, the new APP codes will apply to the public sector and the private sector. The provisions have been adapted as appropriate to the small scale of the Territory, given that the TPP codes will only apply to public sector agencies and contracted government service providers.

Clause 49 Meaning of TPP code

This clause defines what a TPP code is and what form it must take. For the purposes of the Act a TPP code is a code of practice about information privacy.

The clause states the matters that a TPP code must deal with. These are the minimum requirements of every TPP code. The first requirement is that a TPP code must set out how one or more of the TPPs are to be applied or complied with. This requirement addresses the fundamental purpose of TPP codes, which is to provide detailed information on the application of, or compliance with, at least one TPP.

Depending on the circumstances, this may include setting out procedures that will be followed or undertakings to comply with additional obligations that go beyond the requirements of a TPP but which the agencies subscribing to the TPP code are willing to accept. This may be because, for example, the obligations represent a best practice commitment, or the obligations more accurately deal with particular circumstances in the industry, or the obligations address customer expectations in that industry.

The Act states the matters that a TPP code may deal with. The purpose is to provide an indicative list of matters that may be included in a code, but a code is not required to include any of these matters. The TPP codes do not replace the Territory privacy principles, but operate in addition to the requirements of the principles. Accordingly, there cannot be a provision in a code that replaces a TPP. A TPP code may impose additional requirements to those imposed by one or more of the TPPs. Agencies bound by a code must always comply with the TPPs as well as the obligations imposed by the code by which they are bound.

A TPP code may also deal with the internal handling of privacy complaints and reporting of complaints to the Information Privacy Commissioner. Agencies may wish to specify particular procedures or other matters that agencies bound by the code will implement to ensure a consistent approach to the internal handling of complaints by all code subscribers. A TPP code does not affect an individual's right to complain to the Commissioner or the process set out in the Act or used by the Commissioner to deal with complaints.

A TPP code may also deal with any other relevant matters. The list of matters specified does not limit the privacy issues that can be set out in a TPP code. However, these other matters must be relevant to privacy in general and the TPPs in particular.

A TPP code must also specify the TPP agencies to be bound by the code, or a way of identifying the agencies bound by the code. Because a TPP code is binding on subscribers to

the code it is essential that the code itself identifies those bound by it. However, there may be situations in which it is more effective for a code to describe a way in which agencies that are bound by the code can be identified.

Finally, a TPP code must set out the period during which the code is in force. Clearly identifying the period during which the code is in force is essential. It is not necessary for a code to commence operation on notification. For example, a public sector agency may wish to specify a commencement date for the code, or a specific time for commencement after notification of the code, to provide time for training of agencies bound by the code. A code may be expressed to operate until a specific date or for a specific period, but it is expected that agencies will choose to state that the code continues in force until a specified event, such as the amendment of the code.

Clause 50 Development of TPP codes and proposed amendment of TPP codes

TPP codes may be developed by a public sector agency, in consultation with any other entity the agency considers appropriate. Agencies can also develop an amendment to an existing approved code.

The public sector agency must publish the draft TPP code, or draft amendment on the agency's website or in a daily newspaper and invite submissions within a stated period of at least 28 days. The agency must consider any submissions made within this period.

This process recognises that effective consultation with stakeholders is an important element in developing an effective code. Consultation will provide an opportunity to identify all relevant issues, options to address the issues, and likely effects on agencies that are bound by the code and others, such as members of the community, who deal with these agencies. The 28-day consultation period is the minimum period that must be offered, but the agency may consider a longer period, depending, for example, on the expected level of interest in the draft code, the number of expected stakeholders, or the complexity of the code.

Under this clause a TPP code which is to be adopted by the public sector agency after consultation is a notifiable instrument. By requiring the agency to table the code as a notifiable instrument there is opportunity for public scrutiny and oversight of the proposed code.

Clause 51 Public sector agencies must comply with TPP codes

This clause provides that a public sector agency bound by a notified TPP code must not do an act, or engage in a practice, that breaches that code.

A breach of a TPP code which has been notified will be an interference with privacy by the public sector agency under section 11 of the Act and may be subject to investigation by the Information Privacy Commissioner under part 6 of the Act.

Part 8 Miscellaneous

Clause 52 Protection of officials from liability

This clause is a standard provision included in many Territory laws to provide protection for individual public sector officials from personal liability. This clause means that under the Act the Information Privacy Commissioner or a person authorised to exercise functions under the Act cannot be sued.

Protection is afforded to the official for things done (including omissions) in the exercise of a function under the Act provided that the official has acted honestly and without recklessness. This clause also provides that any civil liability that would have attached to an official attaches to the Territory instead. The provision is consistent with other ACT legislation.

Clause 53 Offence – use or divulge protected information

This clause protects information which has been obtained through the exercise of functions under this Act from being abused or recklessly misused.

A person can be convicted under this provision if:

- the person uses or divulges information and that information is protected information about someone else; and
- the person is reckless about whether the information is protected information about someone else.

The maximum penalty for these offences is 50 penalty units, imprisonment for 6 months or both. These offences are in line with the principles set out in the JACS Guide to Framing Offences and are aimed at ensuring that the personal information which can come into the possession of individual public sector officers by virtue of their position in a public sector agency is not misused. Creating offences to discourage the abuse of personal information is necessary to ensure trust in the ability of the Commissioner and other officials to responsibly manage information obtained or compelled from ACT residents by the operation of the Information Privacy Act.

The following defences apply to a charge of these offences:

a) the protected information is used or divulged under the Act, or another Territory law;

b) the protected information is used or divulged in the exercise of a function under the Act, or another Territory law;

c) the protected information is used or divulged in a court proceeding;

d) the protected information is used or divulged with the consent of the person the information is about.

In this clause protected information means any personal information which is obtained because of the exercise of a function under the Act.

The provision is consistent with other ACT legislation. It is a standard protection for information provided to the Information Privacy Commissioner, or any other person, because of the exercise of a function under the Act.

Clause 54 Report by information privacy commissioner

This clause provides that, each financial year, the Information Privacy Commissioner must give a report to the Minister about:

a) the total number of privacy complaints made or referred to the Commissioner; and

b) the total number of privacy complaints dealt with by the Commissioner;

c) the total number of privacy complaints that the Commissioner is reasonably satisfied involved an interference with the complainant's privacy.

d) anything else prescribed by regulation.

The Act provides flexibility to add to the items expressly provided for in the Act that the Commissioner must include in the report, by allowing regulations to prescribe other items.

A report produced under this clause must identify the respondent in relation to each privacy complaint reported on but must not include the complainant's personal information.

The Minister must present the report to the Legislative Assembly within 15 sitting days after the day the report is given to the Minister.

Clause 55 Information privacy commissioner may make guidelines

This clause provides that the Information Privacy Commissioner may make guidelines to provide assistance in the development of, and compliance with, TPP codes. The Commissioner may also make guidelines about matters the Commissioner may consider in deciding whether to approve or vary a TPP code, or repeal a TPP code, and matters in relation to TPP 6.3(d). Guidelines are notifiable instruments.

Clause 56 Instruments made under this Act

This clause provides that the Information Privacy Commissioner may apply, adopt or incorporate another instrument in making an instrument under the Act. This is designed to allow material prepared by equivalent offices in other jurisdictions, in particular the Commonwealth, to be used in the Territory where appropriate.

Clause 57 Approved forms

This clause provides the Information Privacy Commissioner with the power to approve forms for the Act. If a form has been approved by the Commissioner for a particular purpose, the approved form must be used for that purpose. An approved form is a notifiable instrument.

Clause 58 Regulation-making power

This clause provides the Executive with the power to make regulations for this Act. Regulations made under the Act must be notified and presented to the Legislative Assembly.

Schedule 1 Territory privacy principles

Schedule 1 sets out the TPPs. The TPPs have been drafted to mirror and align with the Australian privacy principles in the Commonwealth APPs. Some of the APPs are not relevant to the regulation of information privacy by ACT public sector agencies and have been omitted. This has resulted in slight inconsistencies in the numbering of the TPPs. Where an APP has not been adopted as a TPP it is noted below and in the Act.

Part 1.1 sets out principles that require public sector agencies to consider the privacy of personal information, including ensuring that public sector agencies manage personal information in an open and transparent way.
TPP 1 – open and transparent management of personal information
TPP 2 – anonymity and pseudonymity

Part 1.2 sets out principles that deal with the collection of personal information including unsolicited personal information.
TPP 3 – collection of solicited personal information
TPP 4 – dealing with unsolicited personal information
TPP 5 – notification of the collection of personal information

Part 1.3 sets out principles about how public sector agencies deal with personal information. This part includes principles about the use and disclosure of personal information.
TPP 6 – use or disclosure of personal information
TPP 8 – cross-border disclosure of personal information

TPPs 7 & 9 are not substantive TPPs but refer to Commonwealth APPs which are not relevant to the handling of information by public sector agencies. APP 7 prohibits direct marketing and APP 9 regulates the adoption, use or disclosure of government-related identifiers (for example, Medicare numbers and driver's licence numbers).

Part 1.4 sets out principles about the integrity of personal information. The part includes principles about the quality and security of personal information.
TPP 10 – quality of personal information
TPP 11 – security of personal information

Part 1.5 sets out principles that deal with requests for access to, and the correction of, personal information.
TPP 12 – access to personal information
TPP 13 – correction of personal information

Explanation of each TPP

1 TPP 1-open and transparent management of personal information

TPP 1 requires public sector agencies to manage personal information in an open and transparent way. The principle is designed to ensure that privacy and data protection compliance is included in the design of information systems from their inception.

TPP 1 requires a public sector agency to consider how it will handle personal information in compliance with the TPPs or a TPP code.

Under TPP 1.2 a public sector agency must take steps that are reasonable in the circumstances to implement practices, procedures and systems relating to the agency's functions and activities that will ensure compliance with the TPPs or a TPP code that binds the agency. These practices, procedures and systems must also enable the agency to deal with inquiries or complaints from individuals.

Reasonable steps could include:

- training staff and communicating to staff information about the agency's policies and practices;
- establishing procedures to receive and respond to complaints and inquiries;
- developing information to explain the agency's policies and procedures; and
- establishing procedures to identify and manage privacy risks and compliance issues, including in designing and implementing systems or infrastructure for the collection and handling of personal information by the agency.

TPP 1.3 requires public sector agencies to have a clearly expressed and up-to-date privacy policy about the management of personal information by the agency. An 'up-to-date' privacy policy should be a privacy policy that is a 'living document' and is reviewed regularly.

TPP 1.4 sets out the information that must be included in a public sector agency's privacy policy, including the kinds of personal information collected and held; how such information is collected and held; the purposes for which the agency collects, holds, uses and discloses personal information; access and correction procedures; complaint-handling procedures; and information about any cross-border disclosure of personal information that might occur.

Where agencies have particularly significant information handling practices, these should be included in their privacy policies by clearly setting out how they collect, hold, use and disclose personal information. For example, where agencies have specific information retention or destruction obligations under specific pieces of legislation, these additional rules should be described as a necessary part of how they handle personal information.

Under TPP 1.5, a public sector agency must take all steps that are reasonable in the circumstances to make their privacy policies available to the public free of charge, and in an appropriate form. An example of how an agency may achieve is by placing the privacy policy prominently on the home page of the agency's website.

Under TPP 1.6, if a person (including a body) requests a copy of the TPP privacy policy of a public sector agency in a particular form, the agency must take steps that are reasonable to give the person a copy in that form. Person is defined in the *Legislation Act 2001* to include a reference to a corporation. This clarifies that entities other than individuals (for example, media organisations) are able to request a copy of the policy.

2 TPP 2- anonymity and pseudonymity

TPP 2 provides that individuals must have the option of dealing with an agency anonymously or through use of a pseudonym in relation to a particular matter. The privacy of individuals will be enhanced if their personal information is not collected unnecessarily.

A public sector agency will not be required to comply with TPP 2 where that agency is required or authorised by or under an Australian law, or a court or tribunal order, to deal with individuals who have identified themselves. For example, if individuals are required under an Australian law to identify themselves to a public sector agency, then it will not be lawful or practical for the agency to deal with them anonymously or pseudonymously.

A public sector agency will also not be required to comply with TPP 2 where it is impracticable for the agency to deal with individuals who have not identified themselves. For example, where a law enforcement agency is investigating a criminal offence and needs to know a person's identity to assist in that investigation.

3 TPP 3- collection of solicited personal information

TPP 3 outlines the rules applying to the collection of personal information and sensitive information.

Under TPP 3.1, a public sector agency must not collect personal information unless the information is reasonably necessary for, or directly related to, one or more of the agency's functions or activities. This requirement is intended to operate objectively and practically in the following manner.

Whether the collection is reasonably necessary is to be assessed from the perspective of a reasonable person (not merely from the perspective of the collecting agency). An agency's

functions or activities are only those functions or activities that are legitimate for that type of agency.

If a public sector agency cannot, in practice, effectively pursue a legitimate function or activity without collecting personal information, then the collection of that personal information would be regarded as necessary for that legitimate function or activity. Where a reasonable person would not regard the function or activity in question as legitimate for that type of agency, the collection of personal information will not be 'reasonably necessary' even if the agency cannot effectively pursue that function or activity without collecting the personal information. An agency should not collect personal information on the off-chance that it may become necessary for one of its functions or activities in the future, or that it may be merely helpful.

The 'directly related to' test ensures that there must be a clear connection between the collection of personal information and the public sector agency's functions or activities. The 'directly related to' test is designed for agencies that need to collect solicited personal information in order to carry out legitimate and defined functions or activities, but may not be able to meet the 'reasonably necessary' test. While the 'directly related to' test may, depending on the circumstances, be a slightly lower threshold, agencies are subject to a wider range of accountability mechanisms (for example, through the Ombudsman, Ministers and the Legislative Assembly) in relation to information that they handle.

In the Commonwealth *Privacy Act 1988*, APP 3 includes an extra sub-principle (TPP 3.2) which has not been reproduced in the ACT because it applies to certain private sector entities. APP 3.2 provides that a private sector organisation must not collect personal information unless the information is reasonably necessary for one or more of the organisation's functions or activities.

TPP 3.3 provides for the collection of 'sensitive information', which is a subset of personal information. The definition of sensitive information is in section 14 of the Bill. Sensitive information must not be collected by agencies unless the collection meets the criteria outlined in TPP 3.1 and the individual has consented to the collection.

TPP 3.4 provides for exceptions to this general rule. These have been included to allow the collection of sensitive information without consent where it is in the public interest to do so when balanced with the interest in protecting an individual's privacy. These exceptions are outlined in detail below:

(a) Where required or authorised by or under Australian law or a court or tribunal order

This exception is intended to allow a public sector agency to collect sensitive information without consent where it is required or authorised by or under Australian law or a court or tribunal order.

(b) Permitted general situations

The meaning of a permitted general situation in relation to the collection of personal information is set out in part 3 of the Bill, section 19.

The Commonwealth APP 3.4 provides for a permitted health situation exception which has not been reproduced in the ACT because it applies to certain private sector entities rather than public sector agencies.

(d) Enforcement bodies

This exception is intended to allow an enforcement body to collect sensitive information without consent where it reasonably believes that the collection is reasonably necessary for, or directly related to, one or more of the body's functions or activities. The definition of 'enforcement body' is in the dictionary of the Bill.

The exception will allow public sector agencies with law enforcement functions and activities to be able to lawfully collect sensitive information without consent. There is a strong public interest in enabling law enforcement agencies to enforce the criminal law. These agencies are subject to significant legislative constraints with accountability and oversight arrangements over their activities which act as a safeguard against inappropriate collection and use of information. For example section 60A of the *Australian Federal Police Act 1979* creates an offence of unlawfully recording, using or divulging information that would be personal information under the Commonwealth *Privacy Act 1988.*

In the Commonwealth Privacy Act, APP 3.4 includes additional provisions APP 3.4(d)(i) and 3.4(e) which apply to the Commonwealth immigration department and non-profit organisations. These provisions are not relevant to this Act.

TPP 3.5 provides that a public sector agency must collect personal information only by lawful and fair means. The Commonwealth Office of the Australian Information Commission has interpreted 'fair' to mean without intimidation or deception. The concept of fair would also extend to the obligation not to use means that are unreasonably intrusive.

TPP 3.6 provides that a public sector agency must collect personal information about an individual only from the individual. However, there are two exceptions to this rule.

First, a public sector agency may collect personal information about an individual from a third party where the individual has consented to that collection; or where it is authorised or required under Australian law, or a court or tribunal order. In the context of dealings with public sector agencies, the ability for an individual to consent would minimise the need for that individual to provide the same personal information to different agencies.

Secondly, a public sector agency may collect personal information about an individual from a third party where it is unreasonable or impractical to collect that personal information directly from the individual. For example, a law enforcement agency may be investigating an individual for a criminal offence, but could prejudice that investigation by being forced to seek particular information directly from the individual.

TPP 3.7 provides that TPP 3 applies to the collection of personal information that is solicited by a public sector agency. Soliciting personal information refers to the situation where an agency requests another entity (which includes an individual) to provide the personal

information, or to provide a kind of information in which that personal information is included. If an agency has not requested the personal information, but only received it from another entity (including where, for example, a law enforcement agency has asked another agency to examine the personal information), that will not be solicited information under TPP 3. However, as noted below, where personal information is unsolicited, it will still be required to be handled in accordance with other relevant TPPs, if it is not destroyed or de-identified.

4 TPP 4-dealing with unsolicited personal information

TPP 4ensures that personal information that is received by a public sector agency is still afforded privacy protections, even where the agency has done nothing to solicit the information.

Under TPP 4.1, where unsolicited personal information is received by a public sector agency, the agency must, within a reasonable period, determine whether it could have collected the information under TPP 3 as if it had solicited the information. If it could have been collected, TPPs 5 to 13 will apply to that information as if it had been solicited.

To assist the agency, TPP 4.2 allows that agency to use or disclose the personal information for the limited purpose of determining whether it could have collected the information.

TPP 4.3 provides that, if the public sector agency could not have collected the information, and if the information is not contained in a Territory record, the agency must take steps to destroy the information or ensure that it is no longer personal information (for example, by taking steps to remove any reference to the individual to whom the information relates). Information will no longer be personal information when it does not satisfy the definition of 'personal information' in the ACT Bill. The compliance burden entailed by TPP 4 will be eased by the provision that the agency must destroy the personal information 'as soon as practicable'.

The reference in TPP 4.3 to information 'contained in a Territory record' ensures that the requirements on public sector agencies to retain such information under the Territory Records Act will override the TPP 4 destruction or de-identification requirements.

TPP 4.3 contains the important qualifier 'only if it is lawful and reasonable to do so'. An example of where this would be applicable is where a public sector agency has received unsolicited personal information from a law enforcement agency to assist that agency in its investigations. If the public sector agency decides that it could not have collected the information, it would normally have to destroy it in accordance with TPP 4.3. However, it would not be 'lawful and reasonable' to destroy such information until the assistance that the agency has given to the law enforcement agency has ended.

Under TPP 4.4, if the public sector agency cannot destroy or de-identify the information under TPP 4.3 (because the information is contained in a Territory record or because it would not be lawful and reasonable to do so), it must still handle the personal information in

accordance with TPPs 5 to 13. This will ensure that the information will be accorded the same privacy protections as any other personal information being held by the entity.

5 TPP 5-notification of the collection of personal information

TPP 5 sets out the obligation for a public sector agency to ensure that an individual is aware of certain matters when it collects that individual's personal information. Generally, an individual must be made aware of how and why personal information is, or will be, collected and how the agency will deal with that personal information.

TPP 5.1 requires a public sector agency to take necessary steps to notify individuals about matters set out in TPP 5.2. Notification must occur at or before the agency collects the personal information. If that is not practicable, the individual must be notified as soon as possible. The phrase 'reasonable steps' is an objective test that ensures that the specific circumstances of each case have to be considered when determining the reasonableness of the steps taken. This flexibility is necessary given the different types of agencies and functions or activities that are to be regulated under the TPPs. In many cases, it would be reasonable for a public sector agency to provide the information outlined in TPP 5.2.

However, for public sector agencies with particular functions and activities, this may not be the case. For example, if a person is under surveillance, it may not be reasonable for a law enforcement agency to notify that person that information is being collected about them.

TPP 5.2 states that information about which an individual must be notified includes contact details of the agency; whether information has been collected from a third party or under an Australian law or court or tribunal order (and details about that collection); the purpose of the collection; complaint-handling and access or correction information in the agency's privacy policy; disclosure information, including to overseas recipients, and the consequences of not collecting the information.

Part 1.3 Dealing with personal information

6 TPP 6- use or disclosure of personal information

TPP 6 sets out the circumstances in which public sector agencies may use or disclose personal information that has been collected or received. It is implicit from the principle that agencies may use or disclose personal information for the primary purpose for which the information was collected. This is outlined in TPP 6.1, which creates the general prohibition on secondary disclosure (that is disclosure for a purpose other than the purpose for which it was collected).

How broadly the primary purpose can be described will need to be determined on a case-by-case basis and it will depend on the circumstances.

Generally, personal information must only be used or disclosed for a secondary purpose, if the relevant individual has consented, or exceptions in TPP 6.2 and 6.3 apply. These

exceptions list a number of specific circumstances in which allowing secondary disclosure is in the public interest when balanced with the interest in protecting an individual's privacy.

The exceptions apply to sensitive information as well as to other personal information. In the particular case where the individual would reasonably expect the public sector agency to use or disclose the information for the secondary purpose:

- for *sensitive information*, the use or disclosure must be directly related to the primary purpose;
- for personal information which is not sensitive information, the secondary purpose must be related to the primary purpose.

As with TPP 3, there are a number of exceptions allowing the use or disclosure of personal and sensitive information where required or authorised by or under Australian law or a court or tribunal order; in permitted general situations (see section 19); and where a public sector agency reasonably believes that the use of disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body. The final exception is aimed at allowing a public sector agency to co-operate with an enforcement body where it may have personal information relevant to an enforcement related activity of that enforcement body.

TPP 6.3 provides that an agency will be allowed to disclose biometric information or templates if the recipient is an enforcement body and the disclosure is conducted in accordance with the guidelines made by the Information Privacy Commissioner. This approach recognises that non-law enforcement agencies have current, and will have future, legitimate reasons to disclose biometric information and templates to enforcement bodies.

TPP 6 is equivalent to the Commonwealth APP 6. APP 6 includes a sub-principle (APP 6.4) which has not been reproduced in the ACT because it applies to health information.

TPP 6.5 provides that if a public sector agency uses or discloses personal information because it is reasonably necessary for an enforcement related activity, the agency must make a written note of the use or disclosure. The requirement ensures accountability for such disclosures, but is extended to other exceptions to the rule against use or disclosure for a secondary purpose because of the compliance burden it would impose on agencies.

TPP 6.6 provides that if a public sector agency is a corporation which collects personal information from a related body corporate, the related body corporate will be taken to have collected the personal information for the same primary purpose as the first corporation. This ensures that, unless one of the exceptions listed in APP 6 applies, the related corporation has to obtain the individual's consent before using or disclosing his or her personal information for a secondary purpose.

APP 6 includes a sub-principle which has not been reproduced in the ACT because it applies to certain private sector entities. APP 6.7 provides that APP 6 will not apply to the use or disclosure of personal information for the purposes of direct marketing or to government related identifiers because these matters are dealt with elsewhere in the APPs.

APP 7 has not been adopted into this Act as it applies to direct marketing by private sector organisations.

However, this APP will apply to a public sector agency if the agency engages in commercial activities (see section 23).

8 TPP 8-cross-border disclosure of personal information

TPP 8 requires a public sector agency that chooses to disclose personal information to overseas recipients to take all steps that are reasonable in the circumstances to ensure that the overseas recipient does not breach the TPPs.

The purpose of this principle is to permit cross-border disclosure of personal information and ensure that any personal information disclosed is still treated in accordance with the Act.

Although TPP 8 explicitly adopts the term 'disclosure' rather than 'transfer', TPP 8 (and related provisions) would not apply to the overseas movement of personal information if that movement is an internal use by the public sector agency, rather than a disclosure. TPP 8 will apply where an organisation sends personal information to a 'related body corporate' located outside Australia.

It is not intended to apply where personal information is routed through servers that may be outside Australia. However, public sector agencies will need to take a risk management approach to ensure that personal information routed overseas is not accessed by third parties. If the information is accessed by third parties, this will be a disclosure subject to TPP 8 (among other principles).

In terms of the reach of TPP 8, the chain of accountability for public sector agencies would not be broken simply because the overseas entity engaged a subcontractor. For example, the requirements of TPP 8 will still apply where an agency contracts a function to an overseas entity (thereby making a cross border disclosure), and that overseas entity then engages a subcontractor.

In practice, the concept of taking reasonable steps' will normally require a public sector agency to enter into a contractual relationship with the overseas recipient.

The general requirement to take reasonable steps to ensure compliance is qualified by a number of exceptions:

a) When the public sector agency reasonably believes that the overseas recipient is subject to legal or binding obligations to protect information in at least a substantially similar way to the protection provided by the TPPs, the requirement will not apply. For this exception to apply, there must be accessible mechanisms which allow the individual to enforce those protection obligations.

   The 'reasonable belief' test allows public sector agencies to make decisions based on the information available to them and the context of a particular disclosure. The term 'substantially similar' (TPP 8.2(a(i)) is not defined, and provides flexibility in

considering the regulatory elements of the overseas jurisdiction. The term 'at least' will be used to ensure that stricter obligations than the TPPs will still be compliant.

b) The requirement will not apply when an individual consents to the cross-border disclosure, after the public sector agency informs the individual that TPP 8.1 will not apply if consent is given.

   To reduce the compliance burden, this exception should not mean that consent is required before every proposed cross-border disclosure. Rather, it will apply where an individual has the explicit option of not consenting to certain disclosures which may include cross-border disclosures. In addition, a public sector agency is required to give individuals notification about other entities to which the agency usually discloses personal information of the kind collected by the agency (TPP 5.2(f)), and whether the agency is likely to disclose the personal information to overseas recipients (TPP 5.2(i)).

c) When the disclosure is required or authorised by or under and Australian law or a court or tribunal order the requirement will not apply.

d) When some (but not all) permitted general situations exist (see section 19), the requirement will not apply.

e) When the disclosure is required or authorised by or under an international agreement relating to information sharing, the requirement will not apply if Australia or the Territory is a party to the agreement.

f) The requirement will not apply if the public sector agency reasonably believes that the disclosure is reasonably necessary for enforcement related activities by, or on behalf of, an enforcement body and the overseas recipient's functions or powers are similar to those of an enforcement body. The purpose of this amendment is to allow an enforcement body to co-operate with international counterparts for enforcement related activities.

APP 9 has not been adopted into this Act as it applies to the adoption, use and disclosure of Commonwealth government-related identifiers used by private sector organisations.

However, this APP will apply to a public sector agency if the agency engages in commercial activities (see section 23).

Part 1.4 Integrity of personal information

10 TPP 10- quality of personal information

TPP 10 sets out the obligation for a public sector agency to take reasonable steps to ensure that the personal information it collects, uses and discloses meets certain quality requirements.

Requirements include that personal information collected, uses or discloses is accurate, up-to-date and complete. In relation to use and disclosure, the agency must take reasonable steps to ensure that the personal information is relevant and of a quality appropriate to the purposes of that use or disclosure. This will require agencies to assess the relevance of personal information against the particular reason for its use or disclosure and only share as much personal information as is relevant to that purpose. The quality assessment of personal information should occur at the time of collection, at the time of use and at the time of disclosure.

The requirements in TPP 10.1 and 10.2 to 'take reasonable steps' raises particular issues for information that might be out-of-date. For public sector agencies, out-of-date information may become relevant for future activities (for example, prosecution of an individual for a criminal offence). In these circumstances, it may not be reasonable to update information if it may, in its preserved form, continue to be relevant into the future for a legitimate function or activity of the agency.

11 TPP 11-security of personal information

TPP 11 sets out a public sector agency's obligations relating to the protection and destruction of personal information it holds.

The principle will require a public sector agency to take all steps that are reasonable in the circumstances to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. This should involve active measures by an agency to ensure the security of personal information.

The inclusion of 'interference' in TPP 11 is intended to recognise that attacks on personal information may not be limited to misuse or loss, but may include interference with the information in a way that does not amount to a modification of the content of the information (such as attacks on computer systems). This element may require additional measures to be taken to protect against computer attacks and other interferences of this nature, but the requirement is conditional on steps being 'reasonable in the circumstances'. Practical measures by agencies to protect against interference of this nature are becoming more commonplace. The use of the term 'interference', which focuses on the result of the activity rather than the means used to achieve that result, ensures that the technologically neutral approach to the TPPs is retained.

If a public sector agency no longer needs personal information for any purpose for which it may be used or disclosed under the TPPs, and if the information is not contained in a Territory record or legally required to be retained by the agency, the principle will require that the agency destroy the information or ensure that it no longer meets the definition of 'personal information'. This would require the entity to permanently remove from a record any information by which an individual may be identified, in order to prevent future re-identification from available data. Destruction should be proportional to the form of the record.

The principle will be flexible, in that the circumstances of each public sector agency will determine when any personal information it holds is no longer necessary for any permitted purpose. The principle will in effect impose an obligation on agencies to justify their retention of personal information.

Part 1.5 Access to, and correction of, personal information

12 TPP 12access to personal information

TPP 12 provides that individuals must be granted access to personal information held about them by a public sector agency on request by the individual, subject to specific exceptions where the public sector agency is required or authorised to refuse to give the individual access to the information by or under - :

a) the *Freedom of Information Act1989;* or

b) another law in force in the Territory that provides for access by people to documents.

APP 12.3 relates to certain private sector organisations and has not been adopted into the TPPs.

Under TPP 12.4, there are requirements for responding to the request within a certain timeframe and giving access to the information in the manner requested, if reasonable and practicable to do so.

If a public sector agency refuses to give an individual access to their personal information due to one of the exceptions, or in the manner requested, TPP 12.5 requires the agency to take reasonable steps to give access in a way that meets the needs of the individual and the agency. This ensures that agencies work with individuals to try to satisfy their request.

The principle provides for the possibility of alternative access through the use of a mutually agreed intermediary (TPP 12.6).

Under TPP 12.7, a public sector agency must not charge an individual for making a request or for giving access to the individual's personal information.

If public sector agency refuses access to an individual's personal information due to one of the exceptions, or in the manner requested, TPP 12.9 requires the agency to give written reasons for the refusal. Written reasons are not required, though, to the extent that it would be unreasonable with regard to the grounds for the refusal.

13 TPP 13- correction of personal information

TPP 13 sets out the obligation for public sector agency to take all steps that are reasonable in the circumstances to correct the personal information it holds about an individual if it is satisfied that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading,

with regard to the purpose for which it is held, or on request by the individual. This obligation may include making appropriate deletions or additions.

The principle is not intended to create a broad obligation on entities to maintain the correctness of personal information it holds at all times. The principle will interact with TPP 10, such that when the quality of personal information is assessed at the time of use or disclosure, a public sector agency may need to correct the information before use or disclosure if the agency is satisfied that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading.

If personal information is held for a range of purposes, and it is considered incorrect with regard to one of those purposes, the obligation to take reasonable steps to correct the information should apply.

If a public sector agency corrects the personal information of an individual, TPP 13 will require it to take all reasonable steps to notify any other agency to which it had previously disclosed the information, if that notification is requested by the individual. The compliance burden is reduced by not requiring notification if it would be impracticable or unlawful.

If a public sector agency refuses to correct personal information in response to an individual's request, the principle will provide a mechanism for individuals to request that a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading be associated with the information. The agency must take reasonable steps to associate the statement with the information so that it is apparent to users of the personal information. This will ensure that individuals retain control of how their personal information is handled.

Under TPP 13.5, there are requirements for responding to requests under TPP 13 within a time frame. A public sector agency must respond to requests within 30 days after the request is made, or must not charge the individual for the making of the request.

Dictionary

The dictionary defines various words and expressions used in the Act. It also contains references to definitions in the Legislation Act of terms used in the Act.