Information Privacy Bill 2012: Explanatory Material

Contents

Introduction

An exposure draft of the Information Privacy Bill 2012 has been prepared to facilitate discussion about the form and content of legislation regulating the handling of personal information by public sector agencies in the Territory.

The following material is designed to act as a guide to understanding the operation of the Bill as drafted. A number of questions have been included to encourage submissions to consider the draft provisions in detail. A number of assumptions have also been spelled out to explain why certain provisions have been drafted in a particular way.

Background

ACT privacy legislation

The Commonwealth *Privacy Act 1988* (the Privacy Act) applies to the ACT and is administered by the Privacy Commissioner on behalf of the ACT Government.

The Privacy Act applies 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 applies 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 number of privacy and access rights to personal health information, whether it is held within or outside of the ACT, and 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.

ASSUMPTION 1: The exposure draft Bill is designed to regulate the handling of personal information by public sector agencies in the Territory. It is not designed to regulate the private sector in the ACT, as the Commonwealth *Privacy Act 1988* already does this.

The Bill specifically excludes personal health information from the definition of 'personal information' on the basis that the *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.

The *Workplace Privacy Act 2011* will also continue to regulate when an employer may conduct surveillance on an employee.

Commonwealth privacy review

Privacy laws are under review in most Australian jurisdictions and in a number of legal systems around the world. The most significant review currently underway is the review of the Commonwealth's *Privacy Act 1988*.

In early 2006, the Australian Law Reform Commission (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 (the Privacy Amendment Bill) 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.

The explanatory statement states that the Privacy Amendment Bill amends the Commonwealth Privacy Act to:

- create the Australian Privacy Principles (APPs), a single set of privacy principles applying to both Commonwealth agencies and private sector organisations, which replace the Information Privacy Principles (public sector) and the National Privacy Principles (private sector);

- introduce more comprehensive credit reporting with improved privacy protections, at the same time rewriting the credit reporting provisions to achieve greater logical consistency, simplicity and clarity and updating the provisions to more effectively address the significant developments in the operation of the credit reporting system;

- introduce new provisions on privacy codes and the credit reporting code including powers for the Commissioner to develop and register codes in the public interest that are binding on specified agencies and organisations; and

- clarify the functions and powers of the Commissioner and improve the Commissioner's ability to resolve complaints, recognise and encourage the use of external dispute resolution services, conduct investigations and promote compliance with privacy obligations.

The Privacy Amendment Bill has been referred to the Senate Legal and Constitutional Affairs Legislation Committee with the report due on 14 August 2012.

ASSUMPTION 2: The exposure draft Bill is designed to be as consistent with the Commonwealth *Privacy Act 1988* as is relevant and appropriate to the ACT. It also incorporates the amendments to the Commonwealth *Privacy Act 1988* which are proposed in the Privacy Amendment (Enhancing Privacy Protection) Bill 2012, as introduced into the House of Representatives on 23 May 2012.

These amendments have been incorporated to elicit specific ACT views on the appropriateness of their application in the Territory. The ACT would need to consider the report of the Senate Legal and Constitutional Affairs Legislation Committee, and monitor the progress of the Bill through the Commonwealth Parliament.

ACT exposure draft bill

In acknowledging the responsibilities of ACT self-governance, and in light of reforms occurring in most Australian jurisdictions, it is timely for the ACT to consider developing its own Privacy Act applying only 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.

In recognition of the ACT as a truly self-governing Territory, it is clear that there is justification for the ACT to develop its own privacy legislation governing the public sector. This is evidenced from debates about Territories' rights to legislate associated with voluntary euthanasia and same sex relationships and the experience of the ACT in repatriating evidence law.

The real question to be determined is what form the Privacy Act should take. Similar to the recent exercise undertaken in repatriating the ACT's evidence law, it would be prudent for the ACT to repatriate privacy law for the regulation of the public sector in the Territory by adopting the Commonwealth Act, as it applies to public sector agencies, as amended by the recent Commonwealth reforms.

ASSUMPTION 3: The exposure draft Bill is designed to be as consistent with the Commonwealth *Privacy Act 1988* as is relevant and appropriate to the ACT. Any departures that have been made are considered necessary in adopting the regime in the Territory considering our size and the application of the Act to the public sector only. Departures may have also been necessary to acknowledge different drafting styles.

Submissions on the exposure draft should not be limited to commenting on the appropriateness of the provisions included in the Bill. Submissions are also encouraged on other provisions which are considered appropriate to adopt in the ACT but have not been included in the draft.

Content of Information Privacy Bill 2012

Part 1: Preliminary

This part contains a number of machinery provisions which are standard in most Territory law.

Part 2: Objects and important concepts

Objects of Act

The objects clause is designed to clearly outline the underlying purpose of the Act and provide 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;
4. provide a way for individuals to complain about an alleged interference with their privacy.

These objects have been adopted from the proposed new objects clause to be inserted into the Commonwealth *Privacy Act 1988* by the Commonwealth Privacy Amendment (Enhancing Privacy Protection) Bill 2012. Only those objects relevant to the ACT have been adopted.

Question 1: Is it necessary to specify the objects of the Information Privacy Act in the Act itself? Are the four objects included in the exposure draft appropriate for the ACT? Are there are any other objects which should be adopted?

Meaning of *personal information*

A definition of ***personal information*** has been included to define the scope of information that is to be regulated by the Act.

Personal information is defined to mean information or an opinion about an identified individual, or an individual who is reasonably identifiable:

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

The definition has been adopted from Commonwealth *Privacy Act 1988* incorporating proposed 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 the 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 has been brought into line with international standards and precedents.

The definition of ***personal information*** in the ACT Act specifically excludes personal health information. This is because 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.

Question 2: Is the definition of ***personal information*** included in the exposure draft appropriate for the ACT?

Meaning of *public sector agency*

A definition of ***public sector agency*** has been included to define the scope of entities that will be regulated by the 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 2001* 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 2011 (No 3) NI2011-712[1]. 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 2001* 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 2001* 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 2001* 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 2001* to mean a Territory owned corporation under the *Territory-owned Corporations Act 1990*. An example is ACTTAB Limited;

- an ACT court – ACT court is defined in the dictionary to mean the Supreme Court, Magistrates Court, Coroner's Court or a tribunal (which includes the ACT Civil and Administrative Tribunal). The term also includes 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.

[1] This instrument can be located on the ACT Legislation Register at http://www.legislation.act.gov.au/ni/2011-712/default.asp.

In addition to the categories above, the Act would include a power to prescribe an entity by regulation.

Question 3: Are the entities specifically included in the definition of ***public sector agency*** in the exposure draft appropriate for the ACT and the intended scope of the Act? Are there any other entities which should be specifically included or excluded?

Meaning of *interference* with individual's privacy

A definition of ***interference*** has been included to outline 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 an approved 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 would be an interference with an individual's privacy if done or engaged in by the government party to the contract.

Question 4: Is the definition of ***interference*** included in the exposure draft appropriate for the ACT?

Meaning of *breach* a TPP etc

A definition of ***breach*** has been included to outline the circumstances that will result in a breach of the Territory privacy principles, or an approved 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.

Question 5: Is the definition of ***breach*** included in the exposure draft appropriate for the ACT?

Part 3: Territory privacy principles

The part starts by establishing the Territory privacy principles as the principles that are set out in schedule 1 of the Act (see below for an explanation of the principles).

The part then 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.

Meaning of *permitted general situation*

There are a number of exceptions in the Territory privacy principles 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.

Prevention of serious threat to life, health or safety

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. 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. Whether the individual has, or could be expected to have, capacity to give consent would also be a factor in determining whether it was 'reasonable' to seek consent.

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.

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.

Question 6: Is the adoption of exceptions to the Territory privacy principles appropriate for the ACT?

Compliance

A public sector agency must not do any act, or engage in a practice, that breaches a Territory privacy principle.

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

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

The Act also imposes a civil penalty where a public sector agency, or contracted service provider, does an act or engages in a practice which is a serious interference with the privacy of an individual, or where the agency repeatedly does an act, or engages in a practice that is an 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.

Question 7: Are the compliance procedures provided for in the exposure draft appropriate for the ACT? Is the extension of the Territory privacy principles to contracted service providers appropriate for the ACT? Is the maximum civil penalty provided in the exposure draft for serious and repeated interferences with privacy appropriate?

Other

The Act will provide that a public sector agency will be taken to have breached the Territory privacy principles:

- if the agency discloses personal information about an individual to an overseas recipient;
- TPP 8.1 applies to that disclosure;
- 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
- 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 recipient will protect the information consistent with the Territory privacy principles prior to any cross-border transfer occurring.

The Act also provides that the proposed Commonwealth APPs will apply to the acts and practices of certain public sector agencies as if the agency were a private sector entity, in relation to the agency's commercial activities.

Question 8: Are the provisions included in the exposure draft in relation to providing information to overseas recipients appropriate for the ACT?

Part 4: Exemptions from application of Act

The application of the Act will be limited by a number of exemptions which are set out in this part.

There are specific exemptions from the operation of the Act for particular public sector agencies whose functions are of an investigative nature. The Act will also not apply to the acts and practices of:

- a Minister to the extent that they do not relate to the public sector agency for which they are responsible;
- ACT courts and tribunals to the extent that they are not of an administrative nature;

- The Office of the Legislative Assembly to the extent that they do not relate to a proceeding of the Legislative Assembly;
- public sector agencies to the extent that they relate to a document in relation to which the agency is exempt under freedom of information legislation.

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

Question 9: Are the specific exemptions to the Act generally included in the exposure draft appropriate? Are there any other exemptions which need to be specified in the Act?

Part 5: Information Privacy Commissioner

Currently, under a memorandum of understanding between the ACT and the Commonwealth, the ACT receives its privacy services from the Commonwealth Office of the Australian Information Commissioner.

The core service provided by the Information Commissioner is to receive and handle complaints about ACT public sector agencies concerning alleged breaches of privacy obligations. Other responsibilities include the provision of training of public sector agencies, policy advice and the provision of a 'privacy hotline' for complaints.

As a small jurisdiction, the ACT must tailor its privacy regime according to the capacity to manage it. In developing its own legislation, which remains similar to the Commonwealth Act, it is open for the ACT to continue to purchase services from the Commonwealth Commissioner.

The ACT Government receives valuable services under the MOU with the Commonwealth Commissioner, and it is not apparent that these services could be replicated with equivalent funds in an ACT Privacy Commission.

At this point in time, it is not feasible for the ACT to establish its own Privacy Commission, and therefore, it is anticipated that the practice of procuring the services of the Commonwealth Commissioner would continue despite the repatriation of privacy law in the

Territory. It is not anticipated that the work of the Commonwealth Commissioner would increase.

ASSUMPTION 4: Part 5 contains provisions for the establishment of the office of the Information Privacy Commissioner in the ACT. The part contains the provisions which would be necessary if the ACT were to no longer procure its privacy services from the Commonwealth.

Appointment provisions

The Act would provide that the Executive must appoint a person as Information Privacy Commissioner for the Territory. The person appointed could not be appointed for more than seven years. The conditions of appointment would be those that are agreed between the Executive and the Commissioner, subject to any determination under the ACT's *Remuneration Tribunal Act 1995*.

Section 10(1)(b) of the *Remuneration Tribunal Act 1995* 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.

If the ACT were to no longer procure its privacy services from the Commonwealth, it is anticipated that the Remuneration Tribunal would be requested to inquire into and determine the remuneration, allowances and other entitlements of the Information Privacy Commissioner appointed for the Territory.

The Act provides that a number of grounds on which the Executive may end the appointment of the Information Privacy Commissioner. Because the Commissioner is an independent statutory office, the incumbent may only be dismissed by showing cause.

The Executive has discretion to end the appointment if there is a contravention of a Territory law or a law of another jurisdiction, for misbehaviour, if the Commissioner becomes bankrupt or personally insolvent, or if the Commissioner is absent on unapproved leave for a specified length of time.

The Executive must end the appointment for mental or physical incapacity (where the incapacity affects the exercise of functions), and for failing to comply, without reasonable excuse, with provisions that require the Commissioner to disclose conflicting interests under section 30.

Question 10: Are the appointment provisions included in the exposure draft appropriate for the office of Information Privacy Commissioner? Are there any other grounds that need to be included in the Act for ending the appointment of the Commissioner? Should consideration be given to changing the discretionary or mandatory nature of the grounds included in the exposure draft?

Functions

The Information Privacy Commissioner has the following functions:

- promote an understanding of the Territory privacy principles and the objects of the principles;
- provide information and educational programs to promote the protection of the privacy of individuals;
- help public sector agencies to comply with the Territory privacy principles and approved Territory privacy principles codes;
- investigate privacy complaints made under the Act;
- exercise other functions given to the Commissioner under the Act, or another Territory law.

These functions may be delegated to a person.

Question 11: Are the functions set out for the office of the Information Privacy Commissioner appropriate in the ACT? Are there any other functions of the Commissioner that should be included in the Act?

Disclosure of interests

This provision obliges the Information Privacy Commissioner to give written notice to the Executive of any direct or indirect financial, and other, interests he or she might have or

acquire that conflict or could conflict with the proper exercise of the Commissioner's functions.

Question 12: Is the inclusion of a requirement for the Information Privacy Commissioner to disclose conflicting interests appropriate for the ACT? Should timeframes be included in the Act for when disclosures are required to be made? For example, the time of appointment, annually, and as soon as there is a change in an interest.

Part 6: Privacy complaints

Making privacy complaints

The Act 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.

The Act 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.

Question 13: Are there any other requirements that should be mandated in the Act for how a privacy complaint is made?

The Act permits a privacy complaint to be referred to the Information Privacy Commissioner by other investigative entities and specifically refers to the Ombudsman, the Human Rights Commission, and any equivalent body regulating privacy in another Australian jurisdiction. Other entities could be prescribed by regulation.

Question 14: Is the provision about the referral of privacy complaints to the Information Privacy Commissioner appropriate for the ACT?

The Act 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 an early opportunity to co-operate with the Commissioner.

Question 15: Is the provision about telling relevant public sector agencies about privacy complaints made against them appropriate for the ACT?

Dealing with privacy complaints

The Act provides that the Information Privacy Commissioner may make preliminary inquiries for the purpose of deciding whether to deal with a complaint, or whether the Commissioner has the power to investigate the complaint. To do this, the Commissioner has the power to make inquiries of the public sector agency, the subject of the complaint, as well as any other person. It is intended that the Commissioner will only use this power when satisfied that making inquiries of third parties will result in more timely and efficient complaint resolution.

The Act provides a list of circumstances where the Information Privacy Commissioner may decide not to deal with a complaint. The list includes the following:

- the act or practice complained about is not an interference with an individual's privacy;
- the complaint was made more than 12 months after the complainant became aware of the act or practice;
- the complaint is frivolous, vexatious, misconceived, lacking in substance or not made in good faith;
- 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;

- the complaint would be better dealt with under another Australian law;
- dealing, or further dealing, with the act or practice is not warranted having regard to all the circumstances;
- the complainant has complained to the respondent about the act or practice and the respondent has dealt, or is dealing, adequately with the complaint, or the respondent has not yet had an adequate opportunity to deal with the complaint.

Question 16: Are the circumstances where the Information Privacy Commissioner may decide not to deal with a complaint appropriate for the ACT? Are there any other circumstances that should be included in the Act?

The Act 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.

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

- the complainant does not comply with a reasonable request made by the Commissioner in dealing with the complaint, or part of the complaint;
- 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;
- the Commissioner has not been able to contact the complainant for a reasonable period of time using the contact details in the privacy complaint.

Question 17: Are the circumstances where the Information Privacy Commissioner may decide not to continue to deal with a complaint, or part of a complaint, appropriate for the ACT? Are there any other circumstances that should be included in the Act?

The Act provides for the Information Privacy Commissioner to tell a complainant and the public sector agency that is the subject of the complaint 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.

Question 18: Should the Commissioner's decision not to deal with a privacy complaint, or to stop dealing with a privacy complaint, be reviewable by the ACT Civil and Administrative Tribunal?

The Act 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. The Act specifically refers to the Ombudsman, the Human Rights Commission, and any equivalent body regulating privacy in other Australian jurisdictions. Other entities could be prescribed by regulation as appropriate.

Application to court

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, and telling the complainant that they may apply to a court (including a tribunal) for an order.

The complainant then has six months after the day they have been notified to apply to court (including a tribunal) for one or more of the following orders:

- an order that the complaint, or part of the complaint, has been substantiated, together with, if appropriate, one or more of the following orders:
    - 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;
    - that the respondent must engage in a stated reasonable act or practice to compensate for loss or damage suffered by the complainant;
    - that the respondent must make a stated amendment of a record it holds;

- 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;

- 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;

- 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;

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

Question 19: Is the provision about complainants applying to a court (including a tribunal) in relation to acts or practices that the Commissioner is reasonably satisfied are an interference with privacy appropriate for the ACT? Should the Commissioner's decision that they are reasonably satisfied that an act or practice is an interference with privacy be reviewable by the ACT Civil and Administrative Tribunal? Is the time period of six months for a complainant to apply to a court (including a tribunal) for an order appropriate? Are the orders listed in the Act appropriate for the ACT? Are there any other orders that should be included in the Act?

Part 7: TPP codes

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

The provisions have been developed based on the new codes of practices (APP codes) to be established under the Commonwealth *Privacy Act 1988* by the Privacy Amendment (Enhancing Privacy Protection) Bill 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.

What is a TPP code?

The provisions make clear that a TPP code must be in writing and must be about information privacy. It is not intended that a TPP code would deal with matters unrelated to information

privacy. However, it is also intended that the information privacy matters dealt with in the TPP code are directly related to the TPPs set out in the Act. To the extent that a TPP code includes matters that are not about information privacy, these matters would not form part of the TPP code and would not be considered by the Information Privacy Commissioner. If a public sector agency wished to include other matters in a TPP code it would be preferable to clearly identify the other matters and deal with them in a document separate to the TPP code. That document would not form part of the TPP code submitted to the Commissioner for approval, nor would it form part of any approved TPP code. Those matters would not be binding under the Act on agencies bound by the TPP code.

The Act 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 even 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. A TPP code is not required to deal with all the TPPs, although it may do so, but it must deal with at least one TPP.

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. It will be a matter for the Commissioner to determine, when considering approval of the code, whether a way used to determine agencies bound by the code is sufficiently clear and specific.

Finally, a TPP code must set out the period during which the code is in force. Clearly identifying the period 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 specific commencement date for the code, or a specific time for commencement

after registration 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 repeal of the code.

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. A TPP code must set out how one or more of the principles are to be applied or complied with. 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.

Question 20: Are the provisions included in the exposure draft about TPP codes appropriate for the ACT?

Development and approval

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, or propose the repeal of, an existing approved code.

Public sector agencies must consult the Information Privacy Commissioner about a draft TPP code, or draft amendment, before the agency publishes it. The agency must also consult with the Commissioner about a proposed repeal before publishing a notice about it.

The public sector agency must publish the draft TPP code, draft amendment or repeal notice 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. The agency will need to be able to demonstrate compliance with these obligations when lodging an application for approval with the Commissioner.

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.

Following publication and consideration of submissions, the public sector agency may give a TPP code or amendment of an approved TPP code to the Commissioner for approval. The agency may also recommend that the Commissioner repeal an approved TPP code.

The Commissioner may approve the TPP code or amendment, or repeal the approved TPP code. In deciding whether to approve the TPP code or amendment, or repeal the approved TPP code, the Commissioner may consult anyone the Commissioner considers appropriate. The Commissioner must consider any relevant guidelines that have been made.

Question 21: Are the provisions included in the exposure draft about the development, approval and notification of TPP codes appropriate for the ACT?

Compliance

A public sector agency that is bound by an approved TPP code must not do an act, or engage in a practice, that breaches the approved code.

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

Question 22: Are the provisions included in the exposure draft about compliance with TPP codes appropriate for the ACT?

Part 8: Miscellaneous

Protection of officials from liability

This is a standard provision included in Territory law that provides protection for individuals from personal liability. In the Act the individual protected is an official, meaning the Information Privacy Commissioner or a person authorised to exercise functions under the Act.

Protection is afforded to the official for things done (including omissions) in the exercise of a function under the Act provided that they act honestly and not recklessly. It 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.

Offences – use or divulge protected information

This is a standard provision included in Territory law that protects information provided to the Information Privacy Commissioner, or any other person, because of the exercise of a function under the Act.

Offences are created in certain circumstances where information holders make or divulge protected information about someone else. The following exceptions apply to these offences:

- the protected information is used or divulged under the Act, or another Territory law;
- the protected information is used or divulged in the exercise of a function under the Act, or another Territory law;
- the protected information is used or divulged in a court proceeding.
- the protected information is used or divulged with the consent of the person the information is about.

The provision is consistent with other ACT legislation.

Report by Information Privacy Commissioner

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

- the total number of privacy complaints made or referred to the Commissioner; and
- the total number of privacy complaints dealt with by the Commissioner;
- the total number of privacy complaints that the Commissioner has determined that they were reasonably satisfied that involved an interference with the complainant's privacy.

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

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

Guidelines

The Information Privacy Commissioner may issue 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 an approved TPP code, and matters in relation to TPP 6.3(d).

Question 23: Are the provisions included in the exposure draft about guidelines appropriate for the ACT?

Instruments made by the Information Privacy Commissioner

This provision will permit the Information Privacy Commissioner to 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.

Other

Two standard provisions have been included to facilitate the effective operation of the Act:

- A power for the Executive to make regulations under the Act. Regulations made under the Act must be notified on the Legislation Register (http://www.legislation.act.gov.au), and presented to the Legislative Assembly.

- A power for the Information Privacy Commissioner 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 must be notified on the Legislative Register (http://www.legislation.act.gov.au).

Question 24: Are the provisions included in part 8 of the exposure draft appropriate for the ACT? Is there anything else that needs to be included in part 8 of the Act?

Schedule 1: Territory privacy principles

Schedule 1 sets out the Territory privacy principles (TPPs).

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. The part includes principles about the use and disclosure of personal information. [2]

TPP 6 – use or disclosure of personal information

[2] Part 1.3 is equivalent to part 3 of the Commonwealth Australian Privacy Principles (APPs). Part 3 of the Commonwealth APPs includes two extra principles which have not been reproduced in the ACT because they apply to certain private 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).

TPP 8 – cross-border disclosure of personal information

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

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 an approved TPP code.

Under TPP 1.2 a public sector agency must take all 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 an approved TPP code that binds the agency. These practices, procedures and systems must also enable the agency to deal with inquiries or complaints from individuals.

Policies and practices under TPP 1.2 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.

Under TPP 1.4, these policies must contain certain information relating to 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, these 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 this is included in the principle – on 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 all steps that are reasonable in the circumstances 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.

<u>TPP 2 – anonymity and pseudonymity</u>

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 principle emphasises that it is often not necessary for an agency to identify the individuals with whom they are

dealing. 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.

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.

First, the information collected is reasonably necessary to pursue that function or activity. 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. [3]

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 ACT Bill. The general rule is that sensitive information can only be collected by agencies where the collection meets the criteria outlined in TPP 3.1 and where the individual has consented to the collection.

However, TPP 3.4 will provide for exceptions to this general rule. These have been included to enable 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.

TPP 3.4(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.

TPP 3.4(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. [4]

[3] TPP 3 is equivalent to the Commonwealth Australian Privacy Principle (APP) 3. APP 3 includes an extra sub-principle 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.

[4] TPP 3.4 is equivalent to the Commonwealth APP 3.4. APP 3.4 includes an extra exception which has not been reproduced in the ACT because it applies to certain private sector entities. APP 3.4(c) provides for a permitted health situation.

APP 3.4(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 ACT Bill.

The exception is necessary to enable public sector agencies with law enforcement functions and activities to be able to collect sensitive information without consent to perform their lawful and legitimate functions and activities. There is a strong public interest in enabling law enforcement agencies to enforce the criminal law. A major part of this important function is the ability to collect information about individuals. An additional safeguard is that these agencies are also subject to significant accountability and oversight arrangements over their activities. [5]

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 general 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.

[5] TPP 3.4(d) is equivalent to the Commonwealth Australian Privacy Principle (APP) 3.4(d). APP 3.4(d) includes a provision which has not been reproduced in the ACT because it applies to the Commonwealth Immigration Department. APP 3.4(e) has also not been reproduced in the ACT because it applies to non-profit organisations.

TPP 3.7 provides that TPP 3 applies to the collection of personal information that is solicited by a public sector agency. The concept of 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 a solicited collection covered by 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.

TPP 4 – dealing with unsolicited personal information

TPP 4 will ensure 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 to determine whether it could have collected the information, TPP 4.2 allows that agency to use or disclose the personal information for that limited purpose.

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.

It is not the intention of TPP 4 to prevent the practice of public sector agencies forwarding incorrectly addressed correspondence. The receipt of correspondence by Ministers, Members of the Legislative Assembly, and government directorate and agencies would, in normal circumstances, be unsolicited. Under APP 4, these entities must, within a reasonable period after receiving the information, determine whether the unsolicited personal information could have been collected under TPP 3 if the entity had solicited the information. It is clear that, in some circumstances, where considering and responding to concerns of members of the public, and referring them to appropriate recipients, are legitimate functions of the entity, the unsolicited information could have been collected under TPP 3. Once an entity has determined that the personal information could have been collected under TPP 3, it would be possible for the agency to use or disclose the information under TPP 6.

Under TPP 6, disclosure to another Minister or government directorate would be permitted where the individual has consented to the use and disclosure. Consent may be implied if it may reasonably be inferred in the circumstances from the conduct of the individual. Disclosure would also be permitted under TPP 6 where the disclosure is related to the primary purpose of collection (or directly related, if the information is sensitive information), and the disclosure is within the individual's reasonable expectations. As the individual has written with queries, views or representations on particular issues, it is within their reasonable expectation that their correspondence will be referred to the appropriate entity within the Legislative Assembly or government.

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, the 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 creates the general requirement for a public sector agency to provide notification. That must occur at or before the time or, if that is not practicable, as soon as practicable after the agency collects personal information about an individual. At that time, the agency must take all steps that are reasonable in the circumstances to notify the individual of such matters referred to in TPP 5.2 that are reasonable in the circumstances or otherwise ensure that the individual is aware of any such matters.

The phrase 'reasonable in the circumstances' is an objective test that ensures that the specific circumstances of each case have to be considered when determining the reasonableness of the steps in question. 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 in the circumstances 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, it would not be reasonable in the circumstances for a law enforcement agency to notify an individual, who is under investigation for a criminal offence, particularly where that agency is undertaking covert surveillance, that information is being collected about them.

TPP 5.2 lists specific matters of which the individual must be notified. This, coupled with TPP 1, is intended to give the individual detailed and enhanced information about how their personal information is to be handled by a public sector agency. This information 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.

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 general in TPP 6.1, which creates the general prohibition on secondary disclosure.

The provision allows for a situation where there is a general primary purpose (for example, assessing a person's suitability to enter Australia). 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 purposes other than the primary purpose, that is, 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 will 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 use or disclosure must be related to the primary purpose.

As with TPP 3, there are a number of exceptions enabling 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 will provide 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. A practical example of the effect of this option would be to enable, consistent with the Commissioner's guidelines, the automatic provision of biometric information and templates by a non-enforcement agency into a database operated by an enforcement body. [6]

TPP 6.5 will provide 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 aims to ensure accountability for such disclosures, but will not be 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 will provide that if a public sector agency, which is a corporation, 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 will ensure that, unless one of the exceptions listed in APP 6 applies, the related corporation will have to obtain the individual's consent before using or disclosing his or her personal information for a secondary purpose. [7]

TPP 8 – cross-border disclosure of personal information

TPP 8 sets out a requirement for 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 principle will aim to permit cross-border disclosure of personal information and ensure that any personal information disclosed is still treated in accordance with the ACT Bill.

[6] 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.

[7] TPP 6 is equivalent to the Commonwealth APP 6. 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.

Although TPP 8 explicitly adopts the term 'disclosure' rather than 'transfer', the 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 'all steps that are reasonable in the circumstances' 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 will be qualified by a number of exceptions:

- When the public sector agency has a reasonable belief 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 will allow public sector agencies to make decisions based on the information available to them and the context of a particular disclosure. The term 'substantially similar' 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.

- The requirement will not apply when an individual consents to the cross-border disclosure, after the public sector agency informs the individual that the consequence of giving their consent is that the requirement in TPP 8.1 will not apply.

  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)).

- When the disclosure is required or authorised by or under law, the requirement will not apply.

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

- 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.

- 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. This is intended to allow an enforcement body to co-operate with international counterparts for enforcement related activities.

<u>TPP 10 – quality of personal information</u>

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

TPP 10 is intended to ensure that personal information is accurate, up-to-date and complete. In relation to use and disclosure, the personal information should also be 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 so much of the personal information it holds 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 all steps that are reasonable in the circumstances' will raise 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.

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 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.

TPP 12 – access 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.

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 will require the agency to take such all steps that are reasonable in the circumstances to give access in a way that meets the needs of the individual and the agency. This will ensure that agencies work with individuals to try to satisfy their request.

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.

The principle will provide 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 will also require the agency to give written reasons for the refusal. Written reasons will not be required, though, to the extent that it would be unreasonable with regard to the grounds for the refusal.

TPP 13 – correction of personal information

TPP 13 will set 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 will be 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 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. The statement should address matters relevant to the information being inaccurate, out-of-date, incomplete, irrelevant or misleading, and should not be unreasonably lengthy. The appropriate content and length of any statement will depend on the circumstances of the case.

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 2001* of terms used in the Act.

Question 25: Are there any words or expressions used in the Act which are not included in the dictionary that require defining?

Summary of Assumptions

ASSUMPTION 1: The exposure draft Bill is designed to regulate the handling of personal information by public sector agencies in the Territory. It is not designed to regulate the private sector in the ACT, as the Commonwealth *Privacy Act 1988* already does this.

The Bill specifically excludes personal health information from the definition of 'personal information' on the basis that the *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.

The *Workplace Privacy Act 2011* will also continue to regulate when an employer may conduct surveillance on an employee.

ASSUMPTION 2: The exposure draft Bill is designed to be as consistent with the Commonwealth *Privacy Act 1988* as is relevant and appropriate to the ACT. It also incorporates the amendments to the Commonwealth *Privacy Act 1988* which are proposed in the Privacy Amendment (Enhancing Privacy Protection) Bill 2012, as introduced into the House of Representatives on 23 May 2012.

These amendments have been incorporated to elicit specific ACT view on the appropriateness of their application in the Territory. The ACT would need to consider the report of the Senate Legal and Constitutional Affairs Legislation Committee, and monitor the progress of the Bill through the Commonwealth Parliament.

ASSUMPTION 3: The exposure draft Bill is designed to be as consistent with the Commonwealth *Privacy Act 1988* as is relevant and appropriate to the ACT. Any departures that have been made are considered necessary in adopting the regime in the Territory considering our size and the application of the Act to the public sector only. Departures may have also been necessary to acknowledge different drafting styles.

Submissions on the exposure draft should not be limited to commenting on the appropriateness of the provisions included in the Bill. Submissions are also encouraged on other provisions which are considered appropriate to adopt in the ACT but which have not been included in the draft.

ASSUMPTION 4: Part 5 contains provisions for the establishment of the office of the Information Privacy Commissioner in the ACT. The part contains the provisions which

would be necessary if the ACT were to no longer procure its privacy services from the Commonwealth.

Summary of Questions

Question 1: Is it necessary to specify the objects of the Information Privacy Act in the Act itself? Are the four objects included in the exposure draft appropriate for the ACT? Are there are any other objects which should be adopted?

Question 2: Is the definition of personal information included in the exposure draft appropriate for the ACT?

Question 3: Are the entities specifically included in the definition of ***public sector agency*** in the exposure draft appropriate for the ACT and the intended scope of the Act? Are there any other entities which should be specifically included or excluded?

Question 4: Is the definition of ***interference*** included in the exposure draft appropriate for the ACT?

Question 5: Is the definition of ***breach*** included in the exposure draft appropriate for the ACT?

Question 6: Is the adoption of exceptions to the Territory privacy principles appropriate for the ACT?

Question 7: Are the compliance procedures provided for in the exposure draft appropriate for the ACT? Is the extension of the Territory privacy principles to contracted service providers appropriate for the ACT? Is the maximum civil penalty provided in the exposure draft for serious and repeated interferences with privacy appropriate?

Question 8: Are the provisions included in the exposure draft in relation to providing information to overseas recipients appropriate for the ACT?

Question 9: Are the specific exemptions to the Act generally included in the exposure draft appropriate? Are there any other exemptions which need to be specified in the Act.

Question 10: Are the appointment provisions included in the exposure draft appropriate for the office of Information Privacy Commissioner? Are there any other grounds that need to be included in the Act for ending the appointment of the Commissioner? Should consideration be given to changing the discretionary or mandatory nature of the grounds included in the exposure draft?

Question 11: Are the functions set out for the office of the Information Privacy Commissioner appropriate in the ACT? Are there any other functions of the Commissioner that should be included in the Act?

Question 12: Is the inclusion of a requirement for the Information Privacy Commissioner to disclose conflicting interests appropriate for the ACT? Should timeframes be included in the Act for when disclosures are required to be made? For example, the time of appointment, annually, and as soon as there is a change in an interest.

Question 13: Are there any other requirements that should be mandated in the Act for how a privacy complaint is made?

Question 14: Is the provision about the referral of privacy complaints to the Information Privacy Commissioner appropriate for the ACT?

Question 15: Is the provision about telling relevant public sector agencies about privacy complaints made against them appropriate for the ACT?

Question 16: Are the circumstances where the Information Privacy Commissioner may decide not to deal with a complaint appropriate for the ACT? Are there any other circumstances that should be included in the Act?

Question 17: Are the circumstances where the Information Privacy Commissioner may decide not to continue to deal with a complaint, or part of a complaint, appropriate for the ACT? Are there any other circumstances that should be included in the Act?

Question 18: Should the Commissioner's decision not to deal with a privacy complaint, or to stop dealing with a privacy complaint, be reviewable by the ACT Civil and Administrative Tribunal?

Question 19: Is the provision about complainants applying to a court (including a tribunal) in relation to acts or practices that the Commissioner is reasonably satisfied are an interference with privacy appropriate for the ACT? Should the Commissioner's decision that they are reasonably satisfied that an act or practice is an interference with privacy be reviewable by the ACT Civil and Administrative Tribunal? Is the time period of six months for a complainant to apply to a court (including a tribunal) for an order appropriate? Are the orders listed in the Act appropriate for the ACT? Are there any other orders that should be included in the Act?

Question 20: Are the provisions included in the exposure draft about TPP codes appropriate for the ACT?

Question 21: Are the provisions included in the exposure draft about the development, approval and notification of TPP codes appropriate for the ACT?

Question 22: Are the provisions included in the exposure draft about compliance with TPP codes appropriate for the ACT?

Question 23: Are the provisions included in the exposure draft about guidelines appropriate for the ACT?

Question 24: Are the provisions included in part 8 of the exposure draft appropriate for the ACT? Is there anything else that needs to be included in part 8 of the Act?

Question 25: Are there any words or expressions used in the Act which are not included in the dictionary that require defining?