



Australian Government

COMPANION GUIDE

Australian Privacy Principles

June 2010

Cabinet Secretary, Senator the Hon Joe Ludwig



MESSAGE FROM THE CABINET SECRETARY

The individual's right to privacy is a fundamental human right that must be protected. The Australian Government believes that it is the responsibility of government to provide a strong regulatory framework to protect people's right to privacy to ensure the security of their personal information. To that end, it was a Labor Government who introduced Australia's first Privacy Act in 1988.

Now, the Australian Government has begun the process of re-writing the *Privacy Act 1988* (the Privacy Act) to modernise and strengthen Australia's privacy protection.

When coming to office in 2007, we had a policy of restoring trust and integrity in government. One aspect of this policy was our commitment to considering the Australian Law Reform Commission's (ALRC) recommendations on privacy reform as a matter of priority.

In mid-2008, the ALRC delivered its report *For Your Information: Australian Privacy Law and Practice* (the report). After two years of extensive consultation and review of the effectiveness of the Privacy Act, the ALRC made 295 recommendations for reform.

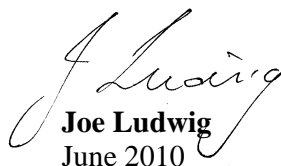
Given the large number of recommendations, the Government is responding to the report in two stages. On 14 October 2009, I publicly released the Government's first stage response, outlining the Government's position on 197 of the ALRC's recommendations. These include:

- developing a single set of Privacy Principles;
- introducing comprehensive credit reporting and enhanced protections for credit reporting information;
- enhancing and clarifying the protections around the sharing of health information and the ability to use personal information to facilitate research in the public interest; and
- strengthening and clarifying the Privacy Commissioner's powers and functions.

I am pleased to release an exposure draft of the first, and most fundamental, part of the re-written Privacy Act: the new Australian Privacy Principles.

Consistent with this Government's belief that policy can only be improved by community engagement and participation, the draft has been referred to a parliamentary committee for consultation. This is the first of a number of components that will also be released for public comment, and then be consolidated to comprise a new Privacy Act.

Australians deserve a modern privacy law, which provides robust protections about the collection and use of our personal information. The Australian Labor Government welcomes feedback from the public to ensure our privacy law has the protections they need to look after their rights well into the 21st century.


Joe Ludwig
June 2010

PART 1 - OVERVIEW

As part of its 2007 election policies, the Rudd Government announced that it would consider the ALRC's recommendations on privacy reform as a matter of priority.

REFORM IMPLEMENTATION

The release of this draft of the new Australian Privacy Principles is the first step in the Australian Government's implementation of the announced reforms to the Privacy Act.

This is the most significant reform to Australia's privacy laws since the inception of the *Privacy Act 1988* (Cth), revitalising the law for the 21st century. The reforms will respond to calls from a range of sectors on the need for reform, and particularly to calls that the law should be more consistent and less complex.

The goals of the reforms are to:

- replace the two existing sets of principles with a streamlined and harmonised set of obligations that draw on the existing principles;
- represent a proportionate set of standards to address the risk of harm from inappropriate sharing and handling of an individual's personal information;
- ensure that the standards also take into account an individual's reasonable expectations around the handling of their information; and
- ensure that regulation strikes a balance between the public's and the individual's interest in efficient, and effective service delivery and public safety.

THE PRIVACY ACT 1988

The *Privacy Act 1988* is concerned with protecting personal information (data) of individuals from unauthorised collection,

use and disclosure by Commonwealth Government agencies and certain private sector organisations (and not individuals acting in a personal capacity).

Individuals may complain to the Privacy Commissioner about acts or practices that the individual considers are interferences with the privacy of the individual.

WHAT IS INCLUDED IN THIS PART OF THE EXPOSURE DRAFT?

This part of the exposure draft contains the new Australian Privacy Principles, which will form part of a new Privacy Act.

The Australian Privacy Principles, as the cornerstone of the privacy protection framework, will appear as one of the first parts in the new Act. For further details about how this part of the reforms interacts with other parts, please see Part 5 of this companion guide.

The Australian Privacy Principles replace the Information Privacy Principles (which apply to Commonwealth agencies) and the National Privacy Principles (which apply to certain private sector organisations).

There are many concepts that exist in the existing Privacy Act that will be replicated in the new Privacy Act. Some definitions have been included in Part B of the draft, after the Australian Privacy Principles. Part 5 of this guide explains some of the concepts that are necessary for understanding the Australian Privacy Principles.

WHAT WILL HAPPEN NEXT?

Each subsequent part will be referred to a Senate Committee for consideration as the drafting of it is completed. It is anticipated that there will be a maximum of four parts (including this one) referred to the Committee.

The other parts that will be released for public consideration are:

- a part about the introduction of comprehensive credit reporting and enhanced protections for credit reporting information; and
- a part about specific privacy protections for information relating to health; and
- a part about the functions and powers of the Australian Information Commissioner (see below for an explanation of why this part does not refer to the Privacy Commissioner).

Once the Senate Committee has reported on all of the parts, the Bill will be consolidated and introduced into Parliament, along with any other legislation that is necessary to enact consequential or transitional provisions.

HOW DOES THIS FIT TOGETHER WITH THE FREEDOM OF INFORMATION REFORMS?

The *Freedom of Information (Reform) Act 2010* and the *Australian Information Commissioner Act 2010* were passed by Parliament on 13 May 2010 and received Royal Assent on 31 May 2010. These Acts will mainly commence on 1 November 2010, with some provisions commencing 6 months later on 1 May 2011.

These reforms:

- establish the Office of the Australian Information Commissioner comprising the Australian Information Commissioner as head of the Office, supported by the Privacy

Commissioner and an FOI Commissioner;

- ensure that the right of access to documents under the *Freedom of Information Act 1982* is as comprehensive as it can be, limited only where a stronger public interest lies in withholding access to documents; and
- ensure that greater weight is given to the role that the *Freedom of Information Act 1982* serves in the pro-active publication of government information (including through the establishment of a new Information Publication Scheme).

The new Office of the Australian Information Commissioner will have functions relating to the independent oversight of privacy and FOI and a function of advising Government on broader government information management.

The existing Office of the Privacy Commissioner will become part of the new Office. The Australian Information Commissioner will be vested with all of the existing functions and powers of the Privacy Commissioner.

LIST OF ABBREVIATIONS AND TERMS USED IN THIS GUIDE

Expression Meaning

ALRC Australian Law Reform Commission

existing Privacy Act *Privacy Act 1988*

IPP Information Privacy Principle set out in section 14 of the existing Privacy Act

NPP National Privacy Principle set out in Schedule 3 to the existing Privacy Act

PART 2 - GENERAL MATTERS

COVERAGE OF THE ACT

Inclusion in records

The Act is designed to protect personal information (see the definition discussed in Part 6 of this guide). However, it is not just any personal information that is protected. The Australian Privacy Principles regulate collection, holding, use and disclosure of personal information that is included in records or generally available publications (again, see the definitions of these concepts discussed in Part 6).

So, while the definition of **record** is very broad, the Act does not cover the record itself. The Act will only regulate dealings with personal information that is *contained in the record*.

Exemptions from the Act for agencies

The policy expressed in section 7 of the existing Privacy Act will not change in the new Act. Section 7 will be redrafted and re-enacted. This means that if an act or practice of a Commonwealth government agency is currently exempt from the operation of the existing Privacy Act, this exemption will continue.

Exemption from the Act for individuals acting in personal capacity

The policy expressed in section 16E of the existing Privacy Act will not change in the new Act. Section 16E will also be redrafted and re-enacted. This means that the new Privacy Act will not apply to any dealings with personal information by an individual if the dealing is only for the purposes of, or in connection with, his or her personal, family or household affairs.

Treatment of acts of certain agencies as acts of organisations

The policy expressed in section 7A of the existing Privacy Act will also not change in the new Act. This concept is particularly important in relation to the Australian Privacy Principles that only apply to organisations, such as Australian Privacy Principle 7 about direct marketing and Australian Privacy Principle 9 about adoption, use or disclosure of government related identifiers.

The small business exemption

At this stage, the exemption for small businesses will remain. However, the Government has committed to considering whether the exemption should be retained as part of the second stage response to the ALRC. Retention of the exemption means that sections 6D to 6EA of the existing Privacy Act would be re-enacted in the new Privacy Act.

Provisions about emergencies and disasters

Part VIA of the existing Privacy Act relates to information exchange between certain entities in emergency and disaster situations. The Part establishes a clear and certain legal basis for the management of the collection, use and disclosure of personal information about deceased, injured and missing individuals involved in these situations, regardless of whether it occurs in Australia or overseas.

This Part of the existing Privacy Act, will be replicated in the new Privacy Act, however its location is yet to be determined.

Extra-territorial operation

The extra-territorial operation of the existing Privacy Act is set out in section 5B of the existing Act. The existing Privacy Act extends to acts done or

practices engaged in outside Australia (which will include the External Territories) by an organisation if the act or practice relates to personal information about Australian citizens or permanent residents.

This will change in two ways in the new Privacy Act. The Act will be extended to operate in relation to acts done, or practices engaged in, outside Australia by agencies as well as organisations.

In addition, the protection of the Act will extend to every person, not just Australian citizens or permanent residents, so long as the entity that is dealing with their personal information is an agency or an organisation with an Australian link (see the definition discussed in Part 6 of this guide).

The Australian Information Commissioner will be empowered to investigate acts or practices that occur outside Australia by agencies or organisations with Australian links.

Acts or practices required by foreign law

The policy achieved by subsection 6A(4) and section 13D of the existing Privacy Act will be replicated in the new Privacy Act.

These provisions ensure that an act or practice that is done or engaged in outside Australia is not an interference with privacy if the act or practice is required by an applicable law of a foreign country.

Because the new Australian Privacy Principle 8 (cross-border disclosure of personal information) will be extended to apply to agencies, these provisions will be extended to cover agencies.

STRUCTURE

The order in which the Australian Privacy Principles appear is intended to reflect the

cycle that occurs as entities collect, hold, use and disclose personal information.

This broadly consists of the following stages:

- considering whether information may or should be collected;
- collecting information;
- providing notification of collection to the individual concerned;
- using or disclosing the information for the purpose for which it was collected or for an allowable secondary purpose;
- maintaining the integrity of personal information by securely storing it and ensuring its quality; and
- when the information is no longer necessary for the functions or activities of the entity, destroying it or ensuring that it is no longer personal information.

To this end, the Australian Privacy Principles have been set out in Divisions for the purposes of this part of the exposure draft.

Division 1 sets out guide material to assist readers to navigate through the Australian Privacy Principles.

Division 2 is about the consideration of personal information privacy. This encompasses an entity's obligations in relation to maintaining privacy policies and demonstrating their compliance with the Australian Privacy Principles.

Division 3 is about the collection of personal information, including the obligation to take reasonable steps to notify the individual concerned when collection takes place. Personal information is afforded the same privacy protections regardless of whether it is solicited or unsolicited.

Division 4 is about dealings with personal information. This encompasses use, disclosure, direct marketing, cross-border disclosure and special provisions for the protection of government related identifiers.

Division 5 is about maintaining the integrity of personal information.

Division 6 is about giving individuals access to their own personal information, so that an individual can correct their own personal information.

Depending on the structure of the new Privacy Act, the Divisions may later appear at a different unit level (for example, as Subdivisions) however, the structure will continue to follow the information cycle. This will be an issue considered when other drafting decisions about the appearance of the new Act are made.

How to refer to the Australian Privacy Principles

The Australian Privacy Principles are set out in sections, however, a provision (section 18) has been included to ensure that the Principles can be referred to as Principles in the new Act.

TECHNOLOGICAL NEUTRALITY

The existing Privacy Act is intended to be technologically neutral so that it is as flexible and as relevant as possible in the presence of developing technologies.

The ALRC considered many technologies that have developed since the inception of the Privacy Act and the impact that these have on protecting personal information.

The ALRC found that maintaining a technologically neutral privacy regulatory regime is the best way to protect individual personal information.

The Government agreed with this, and accepted a number of recommendations made by the ALRC to encourage the Australian Information Commissioner to provide guidelines and education about new technologies.

PART 3 – ABOUT THE PRINCIPLES

The Australian Privacy Principles are not like other types of legislation. The Australian Privacy Principles are principles-based law. The best regulatory model for information privacy protection in Australia is this type of law.

By continuing to use high-level principles, the Privacy Act regulates agencies and organisations in a flexible way. They can tailor personal information handling practices to their diverse needs and business models, and to the equally diverse needs of their clients.

The Privacy Act combines principles-based law with more prescriptive rules where appropriate. This regulation is complemented by guidance and oversight by the regulatory body, the Office of the Australian Information Commissioner.

This is comparable to international regulatory models in Canada, New Zealand and the United Kingdom.

The Australian Privacy Principles refer to *entities* to capture both agencies and organisations. Some of the Australian Privacy Principles (or some parts of some principles), however, refer specifically to agencies or organisations where there are different provisions applying to agencies or organisations.

Australian Privacy Principle 1 – open and transparent management of personal information

The requirement for open and transparent management is the first of the Australian Privacy Principles because it will emphasise that entities should first plan **how** they will handle personal information before they collect and process it.

The principle is also intended to outline that part of complying with the Australian Privacy Principles is making sure that entities consider their privacy obligations when planning new systems.

This is part of international moves towards a “privacy by design” approach, that is, ensuring that privacy and data protection compliance is included in the design of information systems from their inception.

Australian Privacy Principle 2 – anonymity and pseudonymity

This principle ensures that individuals are permitted to interact with entities while not identifying themselves, or by using a pseudonym.

This principle emphasises the importance of first considering whether it is necessary to collect personal information at all. This offers better privacy protection to individuals because it prevents an entity collecting personal information if the entity does not need to.

In some circumstances, particularly on the internet, it is not necessary for a person to identify him or herself. The entity with which the individual is dealing is not necessarily interested in the identity of the individual, but rather that the credentials of the individual have been sufficiently established for the purposes of the transaction.

Entities are only obliged to comply with this principle where it is lawful and practicable to do so. This means that if a law requires the individual to identify him or herself to the entity, then it is not lawful and practicable for them to interact anonymously or pseudonymously.

The Australian Information Commissioner will be encouraged to provide guidance on the principle, including on the types of circumstances in which it will not be

lawful or practicable to provide this option.

Australian Privacy Principle 3 – collection of solicited personal information

Generally, personal information should only be collected where it is necessary. This is reflected in the opening statement of the principle that entities must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities (the ***functions test***).

Collection of sensitive information is also dealt with in this principle. Generally, sensitive information should only be collected where the collection meets the functions test and the individual has consented.

However, there are a number of specific circumstances in which the public interest outweighs individual privacy and these are reflected in a number of exceptions, which allow collection of sensitive information without consent.

Generally, these are based on the existing provisions of NPP 10.1, however some new provisions have been included, mostly to deal with specific issues that arise by the application of this principle to both agencies and organisations. The new exceptions include provisions about:

- assisting in the location of missing persons (see the discussion about this in Part 4 of this guide); and
- allowing collection for diplomatic or consular processes; and
- allowing collection for war or warlike operations, peacekeeping or peace enforcement, civil aid, humanitarian assistance, medical or civil emergency or disaster relief by the Defence Force outside Australia.

The first two of these have also been included in the principle about use and disclosure. This is because it is likely that the entity that the use or disclosure for this purpose will be a secondary disclosure.

In contrast, the provision allowing collection of sensitive information by the Defence Force does not have a complementary provision in the use and disclosure provision. If the Defence Force collects sensitive information in reliance on that exemption, then it will be permissible to use or disclose the sensitive information for that primary purpose. For other personal information collected for another purpose, the Defence Force will need to rely on another allowable exemption to support later use or disclosure.

Australian Privacy Principle 4 – receiving unsolicited personal information

This principle ensures that personal information that is received by an entity is still afforded privacy protections, even where the entity has done nothing to solicit the information.

The entity must decide whether the entity could have collected the information in accordance with Australian Privacy Principle 3, had the entity solicited it.

If the entity could have, then the other Australian Privacy Principles apply to that personal information in the same way as if it had been solicited.

If the entity would not have been permitted to collect the personal information under Australian Privacy Principle 3, the entity 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).

Australian Privacy Principle 5 – notification of the collection of personal information

The purpose of this Australian Privacy Principle is to set out the obligation on entities to ensure that an individual is aware of certain matters at the time of collection of the personal information of the individual.

The notification principle requires that the individual will be made aware of how and why personal information is, or will be, collected and how the collecting entity will deal with the personal information.

Australian Privacy Principle 6 – use or disclosure of personal information

This principle sets out the circumstances in which entities may use or disclose personal information that has been collected or received.

It is implicit from the principle that entities may use or disclose personal information for the primary purpose for which the information was collected.

Generally, personal information should only be used or disclosed for purposes other than the primary purpose, that is, for a secondary purpose, if the relevant individual has consented.

However, as in collection, there are a number of specific circumstances in which the public interest outweighs individual privacy and these are reflected in the exceptions set out in the principle, which allow use or disclosure of sensitive information without consent.

These are based on the exceptions set out in existing NPP 2.1, however, some new exceptions have been included to deal with specific issues that arise by the application of this principle to both agencies and organisations.

In addition, separate principles set out special rules that apply when personal information will be used or disclosed for direct marketing (see Australian Privacy Principle 7) or when the personal information in question is a government related identifier (see Australian Privacy Principle 9).

Australian Privacy Principle 7 – direct marketing

This principle is designed to place extra limitations on organisations that use or disclose personal information to promote or sell goods or services directly to individuals.

There is significant community concern about use and disclosure of personal information for this purpose, so it is important that this type of dealing is specifically regulated to respond to this concern.

The approach taken to the drafting of this principle differs to that outlined in the Government response to the ALRC report. The language used in the Government response focussed on persons who are “existing customers” in comparison to those who are not.

The language used in the principle is different, but achieves the same policy. The policy that applies to “existing customers” is applied to individuals who have provided personal information to the entity who is undertaking the direct marketing. The policy that applies to “non-existing customers” is applied to those who have not provided personal information to the entity who is undertaking the direct marketing.

Australian Privacy Principle 8 – cross-border disclosure of personal information

General

This principle ensures that the obligations to protect personal information set out in the Australian Privacy Principles cannot be avoided by disclosing personal information to a recipient outside Australia.

Disclosure vs Transfer

This principle refers to disclosure rather than transfer. A cross-border disclosure remains a kind of disclosure and using the term ‘transfer’, which is currently contained in NPP 9, complicates the understanding of the information flow.

The ordinary meaning of disclose is to allow information to be seen or to make it known. A transfer implies that there is a cross-border movement of personal information. However, a cross-border disclosure will occur when information is accessed by an overseas recipient, whether or not the personal information that is accessed is stored in Australia or elsewhere.

Conversely, it is not intended that a disclosure will occur when personal information is routed through servers that may happen to be outside Australia.

Coverage

Unlike NPP 9, Australian Privacy Principle 8 applies to agencies as well as organisations.

When read in conjunction with the provision setting out the extra-territorial operation of the new Privacy Act, the effect is to remove citizenship requirements and extend protection to any personal information disclosed outside Australia by an entity with Australian links.

The basic rule

Unlike NPP 9, this principle does not prohibit cross-border disclosures of personal information. The basic rule is that entities will remain accountable for any disclosure of personal information outside Australia, unless one of a number of exceptions applies.

Steps required before disclosure

Before an entity can disclose personal information outside Australia the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to the personal information.

This means that, before any actual cross-border disclosure of personal information occurs, an entity must have put into place appropriate arrangements in relation to the information.

It is expected that entities will ordinarily have a contractual relationship with overseas recipients, and that contract would set out the obligations of the overseas recipient.

This requirement is not described in the Government response to the ALRC report, however, it has been included to ensure that entities have obligations to ensure that personal information will be provided with adequate protection before the entity allows it to leave Australia.

Exceptions

The principle sets out a number of exceptions under which an entity will not be accountable for the cross-border disclosure of personal information to an overseas recipient.

Where an overseas recipient is subject to a law or binding scheme in their own jurisdiction, it must protect the personal

information in a way that is at least substantially similar to the Australian Privacy Principles. This means that the level of protection must be substantially similar, or provide a higher level of protection, when considered against the overall level of protection offered by the Australian Privacy Principles. It is not intended that each Australian Privacy Principle should be replicated.

In addition, this exception only operates where an individual has access to mechanisms that enforce the protections of the substantially similar law or binding scheme. For these purposes ‘binding scheme’ is intended to have the same meaning as in NPP 9, and include self-regulatory or other international arrangements that provide the necessary level of protection.

In extending this principle to agencies, it has been necessary to insert specific exceptions to ensure that current information sharing activities of agencies are still permitted. This includes:

- where information sharing occurs pursuant to international agreements;
- disclosures made for diplomatic or consular purposes; and
- allowing use or disclosure for war or warlike operations, peacekeeping or peace enforcement, civil aid, humanitarian assistance, medical or civil emergency or disaster relief by the Defence Force outside Australia.

The remaining exceptions are based on those that apply to Australian Privacy Principle 6.

Accountability

The entity is made accountable for the overseas recipient’s acts and practices by section 20.

The specific word “accountability” (as mentioned in the Government’s response to the ALRC report) is not used. However, section 20 clearly sets out the policy intention described by the Government response, namely that if a breach of the Australian Privacy Principles occurs:

- the overseas recipient’s act or practice will be taken to be that of the entity who disclosed the information to the overseas recipient; and
- the act or practice will be taken to be an interference with privacy for the purposes of the Privacy Act.

This means that if the overseas recipient does an act or practice that would be a breach, then the entity will be liable. The entity may, in turn, be able to pursue the overseas recipient depending on the terms of their relationship with the overseas recipient.

If one of the exceptions applies to the entity, section 20 will not apply to the entity.

Australian Privacy Principle 9 – adoption, use or disclosure of government related identifiers

This principle is aimed at ensuring that organisations (not agencies) do not refer to individuals within their own systems according to identifiers (for example, Medicare numbers) issued by government agencies. Further, it prevents the facilitation of unlawful data-matching by organisations through use and disclosure of such identifiers.

The key goal of this principle is to restrict general use of identifiers issued by government agencies and prevent such identifiers from becoming de facto national identity numbers.

This principle is similar to existing NPP 7, but Australian Privacy Principle 9 goes

beyond the scope of NPP 7 to regulate identifiers issued by State and Territory government agencies (for example, drivers' licence numbers).

It is not intended to restrict the capacity of organisations to use or disclose a government-issued identifier for the sole purpose of verifying an individual's identity.

For example, the principle is not intended to prevent a courier service from checking a person's driver's licence to ensure that a parcel is being delivered to the correct recipient. It is, however, intended to prevent the courier service from then adopting the person's driver's licence number as their customer number within that organisation.

Australian Privacy Principle 10 – quality of personal information

This principle protects the quality of personal information collected, used or disclosed by entities. Having this principle reassures the public that the use of their personal information by entities is not based on misleading or erroneous personal information. It also promotes improved consistency of personal information handling practices by various entities.

Australian Privacy Principle 11 – security of personal information

This principle imposes specific obligations about protecting personal information. It is in line with international best practice regarding privacy protection.

Additionally, keeping personal information for only as long as is reasonably necessary is an effective way of reducing the risk that it may be mishandled.

Australian Privacy Principle 12 – access to personal information

This principle, together with Australian Privacy Principle 13, replaces existing IPPs 6 and 7 (for agencies) and NPP 6 (for organisations).

The Government response to the ALRC report stated that there would be one principle dealing with access and correction. For readability, this matter has been dealt with in two separate principles.

Its purpose is to ensure that individuals have access to personal information that entities hold about them and can correct the information where it is inaccurate, irrelevant, out-of-date or incomplete.

There are a limited number of circumstances in which an entity may refuse to give individuals access to their own personal information.

In such circumstances, entities have an obligation to provide as much access as is possible in the circumstances to meet the needs of the individual and the entity.

For further information about the way these principles interact with Part V of the *Freedom of Information Act 1982*, see Part 5 of this guide.

Australian Privacy Principle 13 – correction of personal information

This principle imposes obligations on entities to correct personal information if it is inaccurate, out-of-date, incomplete or irrelevant.

It is becoming increasingly common for organisations operating in the online environment to allow individuals access to their own personal information by providing access to a personal profile on a website.

This principle is not intended to discourage this practice. In fact, this approach is encouraged as good privacy practice, as it ensures individuals have control of their personal information.

PART 4 – SPECIFIC MATTERS

THE ‘REASONABLY NECESSARY’ TEST

A number of the Australian Privacy Principles allow for collection, use or disclosure where the entity believes that the collection, use or disclosure is “reasonably necessary” for a particular purpose. It is intended that this be interpreted objectively and in a practical sense.

In relation to the requirement that an entity must not collect personal information unless it is reasonably necessary for their functions or activities, this is intended to reflect two things. The first is that from the perspective of a reasonable person the function or activity is legitimate for that type of entity. The second is that the information collected is genuinely necessary to pursue that function or activity.

If an agency or organisation cannot, in practice, effectively pursue a function or activity without collecting personal information, then that personal information would be regarded as reasonably necessary for that function or activity.

An agency or organisation 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 REQUIREMENT TO TAKE REASONABLE STEPS

A number of the Australian Privacy Principles require an entity to take “reasonable steps”. In some cases the words “(if any)” are used to ensure that, in that particular case, if there are no steps that an entity needs to take to fulfil its obligations, it need not take any steps.

MISSING PERSONS

A new provision is being included to permit collection, use or disclosure of personal information where it would assist to locate a person who has been reported missing.

This will assist agencies and organisations who undertake activities in locating such persons, particularly where there has been an emergency or disaster, to let their loved ones know that they are alive and well.

However, in some circumstances, individuals choose to discontinue contact with their friends and relatives and it is important that the permission to collect, use or disclose personal information strikes the right balance, ensuring that persons who have intentionally chosen to discontinue contact remain undisturbed.

To this end, this permission will only be able to be relied on where the collection, use or disclosure is done in accordance with Australian Privacy Rules issued by the Australian Information Commissioner.

CONSENT

Consent is a defined concept within the existing Privacy Act, and the new Privacy Act will contain a definition on the same terms.

Consent is defined to mean “express consent or implied consent”.

Express consent exists where a person makes an informed decision to give their voluntary agreement to collection, use or disclosure taking place.

Whether consent can be said to be implied depends entirely on the circumstances. Consent may be implied when, in the circumstances, the individual and the relevant entity have each engaged in conduct that means that it can be inferred

the individual has consented, even though the individual may not have specifically stated that he or she gives consent.

Consent, in many circumstances, can be withdrawn at any time. In such circumstances, the consent no longer exists, and an entity would no longer be able to rely on consent having been given when dealing with the individual's personal information.

However, it is important to note that in many circumstances it will not be possible for an individual to withdraw his or her consent. Such a circumstance might arise where an agency seeks and obtains consent to collect personal information. Once the agency has collected the personal information, another law may oblige the agency to undertake particular dealings with the personal information (for example, the *Archives Act 1983*). In such a circumstance, the capacity for the individual to withdraw consent is overtaken by the course of events.

REFERENCES TO THE COMMISSIONER

At the moment, the provisions in this part of the exposure draft confer functions and powers on the "Commissioner". Under the current Privacy Act, these references would be to the Privacy Commissioner because of the definition of *Commissioner* in section 6 of the existing Privacy Act.

However, with the enactment of the *Freedom of Information (Reform) Act 2010*, this definition will be changed to refer to the Australian Information Commissioner.

The new Privacy Act will confer powers and functions on the Australian Information Commissioner, so references in this part of the exposure draft should be read as if they were references to the Australian Information Commissioner. This is because it is likely that the

legislation containing the Australian Privacy Principles will commence after the Office of the Australian Information Commissioner commences operations on 1 November 2010.

This companion guide discusses the conferral of functions and powers on the Australian Information Commissioner, as this is the office on which functions and powers will be principally conferred once the *Freedom of Information (Reform) Act 2010* is fully implemented.

In practice, the Privacy Commissioner will be mainly performing the privacy functions, both leading up to, and after, the *Freedom of Information (Reform) Act 2010* and this new Privacy Act have been implemented.

REMOVAL OF REQUIREMENT ON AGENCIES TO PREPARE PERSONAL INFORMATION DIGESTS

Agencies will be required, as organisations are under the existing Privacy Act, to maintain privacy policies.

This will replace the existing requirement on agencies to maintain and publish annual Personal Information Digests (currently required by IPP 6.3 and paragraph 27(1)(g) of the existing Privacy Act).

Agencies' compliance with Australian Privacy Principle 1 (open and transparent management of personal information) will provide appropriate transparency as to how agencies deal with personal information. Agencies will meet their obligations by publishing up-to-date privacy policies electronically.

PART 5 – INTERACTIONS WITH OTHER PROVISIONS

INTERACTION WITH OTHER PARTS THAT WILL BE RELEASED FOR PUBLIC CONSULTATION

As has already been mentioned, this part of the exposure draft is just the first step in the Australian Government's implementation of the announced reforms to the Privacy Act.

The other parts will be released for public consultation as they are ready. It is likely that some consequential changes will need to be made to the Australian Privacy Principles and the other provisions in this draft in order to make it clear how each part interacts.

A part about the introduction of comprehensive credit reporting and enhanced protections for credit reporting information will be provided for public consultation. This will replace Part IIIA of the existing Privacy Act.

A part about specific privacy protections for information relating to health will also be provided for public consultation. Currently, many provisions providing for specific regulation of dealings with health information are contained in the IPPs and the NPPs. These provisions do not currently appear in the Australian Privacy Principles, as a decision has not yet been taken as to the best location for them in the new Act.

Finally, a part about the functions and powers of the Australian Information Commissioner will be released for public consultation.

The aim of reforming the functions and powers of the Australian Information Commissioner is to:

- provide for more efficient and effective enforcement of the legislation;
- deliver effective complaint resolution services;
- assist the Australian Information Commissioner to be proactive in commencing compliance action;
- enhance the role of the Australian Information Commissioner in encouraging compliance beyond his or her capacity to investigate complaints; and
- ensure that the Australian Information Commissioner has the power to provide guidance to individuals about their rights under the Act and to entities to assist them to fulfil their obligations.

The reform of the functions and powers of the Australian Information Commissioner is far-reaching, and it is likely that some changes are needed to the Australian Privacy Principles when this part of the legislation is prepared.

INTERACTION WITH PART V OF THE *FREEDOM OF INFORMATION ACT 1982*

Access to and correction of own personal information is currently dealt with (in most circumstances) under the *Freedom of Information Act 1982*.

On 24 March 2009, the Government announced (as part of its reforms to that Act) a proposal to amend the Privacy Act to enact an enforceable right of access to, and correction of, an individual's own personal information, rather than maintain the existing regime.

This means that where an individual requests access to, or correction of, their own personal information, there will be

mechanisms in the Privacy Act for merits review of a decision by an agency to refuse to comply with such a request.

This does not appear on the face of Australian Privacy Principles 12 and 13 (which concern access and correction). This is because there are a large number of technical issues in relation to the way that the Privacy Act and the *Freedom of Information Act 1982* will interact that have not yet been fully resolved.

Australian Privacy Principles 12 and 13 do, however, set up some of the technical infrastructure that will link into other provisions of the Act and provide the means for this merits review. This can be seen in the way in which the principles deal separately with agencies and organisations in imposing timeframes within which decisions must be made. There is also provision for additional notice requirements to be prescribed by the regulations.

This ensures that there is basic content for notification of decisions contained in the legislation, but with capacity to prescribe additional requirements so that the provisions of the Privacy Act are consistent with those in the *Freedom of Information Act 1982*.

INTERACTION WITH STATE AND TERRITORY LAWS

Section 3 of the existing Privacy Act preserves the effect of any State or Territory law that makes provision about interferences with privacy, if it is capable of operating concurrently with the existing Privacy Act.

The Government does not intend to change its policy in this regard, so an equivalent provision to this effect will be included in the new Privacy Act.

INTERACTION WITH OTHER INSTRUMENTS

The new Privacy Act will be the premier source of regulation for the protection of personal information privacy, however the Act will be bolstered by other instruments, the making of which will be provided for by the Act. These are:

- regulations made by the Governor-General about matters for which the Act provides;
- the Australian Privacy Rules: binding rules made by the Australian Information Commissioner;
- Guidelines made by the Australian Information Commissioner: material in which the Australian Information Commissioner offers explanation and guidance to users of the legislation, but which are not binding; and
- privacy codes: written codes by which an organisation is bound and that regulate acts and practices of the organisation that affect privacy.

The provisions providing for the making of the Australian Privacy Rules and the regulations are included in this draft (see sections 21 and 22). The final location of these provisions in the new Act has not yet been determined. It is also important to note that matters about which rules and regulations may be made may be added to these provisions as drafting progresses.

PART 6 - DEFINITIONS

The Australian Privacy Principles are intended to be a stand-alone regulatory regime, however, there are some concepts that are necessary for their interpretation, which will not appear in the principles themselves. Some of these definitions appear at the end of the draft. Some have not yet been drafted, but will be along the

same lines as the concepts that appear in the existing Privacy Act.

The following table sets out the definitions that appear in the draft and notes specific information that may assist in using the definitions for the purposes of interpreting the principles.

It is important to note that this is not an exhaustive list of definitions that will appear in the new Privacy Act.

Definition	Comments
<i>agency</i>	This definition is substantially similar to that used in the existing Privacy Act.
<i>Australian law</i>	This definition is new and has been included to clarify the scope of provisions that allow collection, use or disclosure where it is required or authorised by or under law.
<i>Australian link</i>	This is a signpost definition. The provision that defines it is the same as that set out in subsection 5B(2) of the existing Privacy Act.
<i>Australian Privacy Principles</i>	This definition refers the reader to section 18, which is a technical provision to ensure the Australian Privacy Principles can be referred to as the Australian Privacy Principles (rather than having to refer to them as sections of an Act).
<i>Australian Privacy Rules</i>	This is a signpost definition to refer the reader to the rules made under section 21.
<i>collects</i>	This is substantially similar to the concept captured by existing subsection 16B(1) of the existing Privacy Act.
<i>Commonwealth contract</i>	This definition encompasses the same concept as that in the existing Privacy Act that is comprised by the definition of <i>Commonwealth contract</i> with the addition of the concept in subsection 6(9) of the existing Privacy Act.
<i>Commonwealth enactment</i>	This definition is substantially similar to that used in the existing Privacy Act.
<i>consent</i>	This definition is the same as that set out in the existing Privacy Act.
<i>contracted service provider</i>	This definition is the same as that set out in the existing Privacy Act, however, the language has been made easier to read.
<i>corporation</i>	This definition is the same as that set out in the existing Privacy Act.
<i>Department of the Commonwealth</i>	This is a new label, but the concept is the same as the defined term <i>Department</i> in the existing Privacy Act.
<i>enforcement body</i>	This definition is substantially similar to that used in the existing Privacy Act, however, a number of entities have been added to the definition.
<i>enforcement related activity</i>	This definition captures, in a substantially similar way, the matters that are currently set out in NPP 2.1(h). A new element has been added to ensure that the definition covers the conduct of surveillance activities, intelligence gathering activities or other monitoring activities.
<i>entity</i>	This is a new concept used to refer to both agencies and

	organisations throughout the Australian Privacy Principles. It makes the principles much easier to read.
<i>generally available publication</i>	This definition is similar to that used in the existing Privacy Act, however, it has been made explicit that a publication will be a generally available publication whether or not payment of a fee is required to access it.
<i>government related identifier</i>	This concept is used in Australian Privacy Principle 9 – adoption, use or disclosure of government related identifiers.
<i>holds</i>	This is substantially similar to the concept captured by existing subsection 16B(2) of the existing Privacy Act.
<i>identifier</i>	This concept is used in Australian Privacy Principle 9 – adoption, use or disclosure of government related identifiers.
<i>misconduct</i>	This is a new concept to assist in clarifying the scope of provisions that allow collection, use or disclosure for the purposes of taking action against persons who have engaged in serious misconduct.
<i>non-profit organisation</i>	This concept is similar to that used in existing NPP 10.5 of the existing Privacy Act.
<i>order of a court or tribunal</i>	This definition is new and has been included to clarify the scope of provisions that allow collection, use or disclosure where it is required or authorised by or under law.
<i>organisation</i>	This definition is similar to that used in the existing Privacy Act.
<i>overseas recipient</i>	This concept is used in Australian Privacy Principle 8 – cross-border disclosure of personal information.
<i>personal information</i>	<p>The proposed definition does not significantly change the scope of the existing concept in the existing Privacy Act. The key conceptual difference revolves around the concepts of ‘identity’ as used in the current definition, and ‘identification’ as referred to in the recommended definition. The ALRC considered that ‘identification’ is more consistent with international language and international jurisprudence, and that explanatory material based on the terms “identified” and “identifiable” will be more directly relevant.</p> <p>The aspect of the definition that the individual be reasonably identifiable ensures that the definition continues to be based on factors which are relevant to the context and circumstances in which the information is collected and held. Generally this would mean that the information must be able to be linked to other information that can identify the individual. The ‘reasonable’ test limits possible identification based on the context and circumstances. While it may be technically possible for an entity to identify a person by the information it holds, it may be that it is not practically possible (for example due to logistics, legislation or contractual restrictions).</p> <p>The test requires consideration of all the means that are reasonably open for an information holder to identify an individual.</p>
<i>privacy policy</i>	This is a signpost definition to refer the reader to the substantive definition in subsection 2(3).
<i>record</i>	This definition is similar to that used in the existing Privacy Act, however, it has been updated to reflect new technologies.
<i>registered political party</i>	This definition is the same as that used in the existing Privacy Act.

<i>related body corporate</i>	This will have the same meaning as this concept has in the <i>Corporations Act 2001</i> .
<i>Secretary</i>	This definition is the same as that used in the existing Privacy Act.
<i>sensitive information</i>	This definition is substantially similar to that used in the existing Privacy Act, however there are new provisions relating to biometric information.
<i>solicits</i>	This definition is the same as that used in the existing Privacy Act.
<i>State contract</i>	This definition encompasses the same concept as that in the existing Privacy Act that is comprised by the definition of <i>State contract</i> with the addition of the concept in subsection 6(9) of the existing Privacy Act.
<i>State or Territory authority</i>	This definition is substantially similar to that used in the existing Privacy Act.
<i>subcontractor</i>	This definition is substantially similar to that used in the existing Privacy Act.