Australian Government

Department of Infrastructure, Regional Development and Cities

Submission to the National Transport Commission on its Discussion Paper

Regulating government access to Cooperative Intelligent Transport Systems (C-ITS) and automated vehicle data

January 2019

Regulating government access to Cooperative Intelligent Transport Systems (C-ITS) and automated vehicle data

Submission to National Transport Commission on its Discussion Paper

Executive Summary

The Department of Infrastructure, Regional Development and Cities (the Department) welcomes the National Transport Commission's discussion paper on regulating government access to C-ITS and automated vehicle data.

The Department has prepared its submission with input from a range of other Australian Government entities including the Attorney General's Department and the Department of Home Affairs.

Connected and automated vehicle technologies have the potential to transform the transport sector and deliver a step change in the wellbeing of Australians through improved road safety, more efficient transport networks, more liveable cities, and better access to transport services. Public acceptance and trust of these technologies, particularly with regard to safety, security and privacy, is key to the uptake of these technologies in Australia.

The Department agrees with the Discussion Paper's proposition that some of the information generated by C-ITS and automated vehicles will be personal and sensitive. That said, the Department's view is that the types of information generated by these technologies will not be new in nature. Existing technologies such as mobile phones, stand-alone and vehicle-installed GPS devices, local government and road-agency video surveillance, dash-cams, smart watches, and other personal electronic devices such as fitness trackers already generate this type of information. And while people are rightly concerned about protecting this information, surveys indicate the community is more concerned about safety, cyber security and liability issues.

This submission identifies purposes for which the Australian Government may collect personal information from C-ITS and automated vehicles, such as vehicle safety regulation. It also provides information on the existing information access framework, particularly the Australian Government's privacy regime on collecting, handling and disclosing personal information.

Of the options canvassed by the discussion paper, the Department supports Option 1, to rely on the existing information access framework. Our reasons reflect the Department's view that the types of information generated by these technologies will not be new.

Our reasons also go to the strengths of the existing information access framework: the good processes that underpin the making and updating of these laws; the current arrangements that strike a reasonable balance between protecting privacy and enabling access to personal information to ensure other outcomes, such as vehicle and road safety; the technologically neutral design that allows it to grow as technology evolves.

A priority for all Australian governments will be to monitor C-ITS and automated vehicle technology as it evolves and is applied to ensure the existing information access framework is fit for purpose.

1 Nature of information from C-ITS and automated vehicle technologies

1.1 Personal information will be generated

The Department agrees with the Discussion Paper's proposition that some of the information generated by C-ITS and automated vehicles will be personal and sensitive.

1.2 Nature of community privacy concerns

The Discussion Paper argues that community concern about privacy issues will inhibit the uptake of the technologies.

Early surveys in relation to automated vehicles, both in Australia and overseas, have identified privacy as being one of a number of community concerns with these emerging technologies. For example, a late 2016 Australian Driverless Vehicle Initiative survey indicated that 72 per cent of respondents were concerned or very concerned about data privacy in relation to automated vehicles[1].

Surveys suggest other issues such as safety, cyber security and liability issues are of more concern to the community. For example, the 2018 Royal Automobile Association of South Australia Member Panel survey found that privacy was listed as the sixth highest concern about automated vehicle technology, with three of the five concerns above it relating to safety issues, one relating to cyber security and one to legal liability[2]. In fact, as shown in Table 1, of the 11 concerns identified, five of the 11 concerns were entirely about safety or had a safety aspect.

[1] See https://s3-ap-southeast-2.amazonaws.com/cdn-advi/wp-content/uploads/2017/07/ADVI-Public-Opinion-Survey-7June2016.pdf

[2] See https://www.raa.com.au/documents/member-panel-autonomous-vehicles-2018

Table 1: Community concerns about Cooperative Intelligent Transport Systems

	Concerns identified	Nature of concern	% of people concerned
1	Not being able to manually override the vehicle and take control if the system fails	Safety	87
2	Who will be responsible in the case of a crash	Liability	82
3	How driverless vehicles will interact with pedestrians and cyclists	Safety	81
4	Cyber security and threats to the system / your vehicle being hacked and overridden remotely	Cyber security	81
5	Giving up control and entrusting a machine with your safety and the safety of your family	Safety	78
6	Data privacy - who owns the information driverless vehicles may collect about the trips users are making	Privacy	68
7	Not being able to drive yourself anymore	Choice	66
8	Cost of purchasing and/or fixing a driverless vehicle	Cost	65
9	Driverless vehicles replacing people's jobs (i.e. bus drivers, taxi drivers etc.)	Employment	65
10	Driverless vehicles not driving as well as humans	Safety	54
11	Learning how to use a driverless vehicle	Training and Safety	26

The Royal Automobile Club of Western Australia has also undertaken significant public opinion surveying over several years as part of its Intellibus trial program with similar results to the South Australian work. Of the 13 community concerns it identified in its 2018 Community Perceptions Monitor[3], data privacy came eighth in the list by level of concern, with safety, cyber security and liability issues dominating the concerns above it.

1.3 Types of information generated

The Discussion Paper suggests the driving need for further regulation of privacy settings is that the new technologies will generate novel types of personal information or information that is unprecedented in volume compared with existing technologies. While this may be true when considered only in terms of some road vehicles, the information generated is not novel when considered more broadly.

[3] https://www-cdn.rac.com.au/-/media/files/rac-website/about-rac/media/2018/automated-vehicles----community-perceptions-monitor.pdf?la=en&modified=20181029092909&hash=B6C17B5A578976B7BD2323FEB1E36FCB62CC688C

For example, the Discussion Paper identifies privacy risks that may be associated with enabling access to a range of data types. All of this data and any associated privacy challenges (including challenges associated with information volume) are already generated by other current technologies carried on individuals or used in the road environment. These technologies include mobile phones, stand-alone and vehicle-installed GPS devices, local government and road-agency video surveillance, dash-cams, smart watches, and other personal electronic devices such as fitness trackers.

2 Potential uses of C-ITS and automated vehicle information by the Australian Government

There are a broad range of potential Australian Government activities that may draw on information from C-ITS and automated vehicles, including to improve the operational efficiency of transport networks, and enhance decision-making around planning, investment and regulation.

Many of these uses, such as improving network operational efficiency and infrastructure investment decisions, will not require use of personal information - aggregated, de-identified information will be sufficient. These types of uses would likely create much lower concerns and lower risk to individual privacy. Other uses, such as regulatory processes to manage safety issues, are likely to require use of personal information.

The following sets out some of the potential Australian Government uses of C-ITS and automated vehicle data.

2.1 Using C-ITS and automated vehicle technology to support network operational efficiency and improve infrastructure planning and investment decisions

National Freight and Supply Chain Strategy

Australian governments are developing a National Freight and Supply Chain Strategy (the Strategy). It will be considered by the Transport and Infrastructure Council in mid-2019.

A clear focus to emerge from industry consultation on the development of the Strategy is the need for more data on the performance of Australia's supply chain networks. Information generated by C-ITS and automated vehicles may provide new data sources to assist in the performance measurement of the road component of Australia's freight network, and to inform the need for capital expenditure, maintenance and regulatory and governance reform. Most of the data uses being considered, such as network planning, will not require the use of personal information. Others, such as supply chain visibility to consumers, may involve personal information being shared among government and non-government users.

Heavy Vehicle Road Reform

The Department is working with state, territory and local governments, as well as industry and others in the community, to progress Heavy Vehicle Road Reform.

The ultimate goal of Heavy Vehicle Road Reform is to turn the provision of heavy vehicle road infrastructure into an economic service where feasible. This would see a market established that links heavy vehicle user needs with the level of service they receive, the charges they pay and the investment of those charges back into heavy vehicle road services.

Commonwealth, State and Territory Government trials are utilising data from existing in-vehicle telematics systems. Privacy protections, which are based on current frameworks, are an integral part of the trials.

Other Departmental activities, including strategic planning, investment decisions and research

In section 5.2.3, the National Transport Commission touches on the potential role of C-ITS and automated vehicle data in strategic planning. The Department places a high value on the vehicle movement data potentially available from C-ITS and automated vehicles. In addition to network planning decisions, this type of data allows for better understanding of the current state of transport-dependent industries such as freight and logistics. It also enables the Department to identify congestion points on the road network, allowing government to target road investments to areas that can most improve freight industry productivity.

In many cases the Department will need to rely on C-ITS and automated vehicle data collected from the states and territories because it does not have a direct role in road management. Given the value of this information to the Department's activities, the Department is keen to ensure processes to manage data supports these needs.

2.2 Potential use of C-ITS and automated vehicle information to support new regulation

The Department is working with the states and territories, the National Transport Commission and Austroads on projects to provide a policy and regulatory framework to manage the challenges generated by C-ITS and higher-level automated vehicle developments. This work is managed by the Council of Australian Governments' Transport and Infrastructure Council.

Projects include early work on a safety assurance system, motor vehicle insurance and changes to driving laws for automated vehicles, and projects to implement a nationally consistent structure for the deployment of C-ITS in Australia.

The deployment of automated vehicles and related technologies will have implications for regulators who manage the safety of Australia's vehicle fleet. For example, in the future, consideration of whether an automated vehicle is safe to deploy and use on public roads may be informed by the ability of automated vehicle systems to carry out over-the-air updates. Some of these updates may be in the nature of security patches to prevent a cyber-attack. These sorts of updates are common in other types of connected devices such as mobile phones.

Other types of updates may have a major impact on an automated vehicle's operation compared to when the vehicle was first deployed. For example, the update may increase the range of environments where the vehicle is able to operate in an automated mode. In

such circumstances, the community may well expect that regulatory oversight will occur to ensure the security patch is installed or that the new operating mode is safe.

Whether these new functions come to the Australian Government or the states and territories, the balance of privacy and other regulatory pressures will require careful consideration.

3 Current arrangements for protecting sensitive information

3.1 The Privacy Act and Australian Privacy Principles

The *Privacy Act 1988* (Privacy Act) generally applies to Australian Government agencies, private sector organisations with an annual turnover of $3 million or more, and some smaller private sector organisations. The 13 Australian Privacy Principles contained in the Privacy Act regulate how those subject to the Privacy Act must handle personal information in cases where no stricter requirements apply in other legislation. This includes regulating when these entities can disclose personal information to Commonwealth, state or territory government agencies.

For example, the Privacy Act allows these disclosures to occur where they are required or authorised by a Commonwealth, state or territory law, in accordance with a court order, or where the entity believes the disclosure is reasonably necessary for particular kinds of law enforcement activities.

A copy of the Australian Privacy Principles is at **Attachment A**.

A key objective of the Privacy Act is to balance the protection of privacy with the interests of entities in carrying out their lawful and legitimate functions, including functions related to law enforcement and community safety.

The balance struck in the Privacy Act is the result of an extensive consultation and policy development process. The Australian Privacy Principles commenced in March 2014 as a modernised set of privacy obligations. They were based on the 2008 Australian Law Reform Commission review of Australian privacy legislation, *For Your Information: Australian Privacy Law and Practice*, and substantial further consultation.

3.2 Specific laws that enable access to information

C-ITS and automated vehicle data present a range of cyber security and national security challenges. Given the significant impact that malicious cyber activity could have on connected and automated vehicles, it is particularly critical that the integrity and availability of C-ITS and automated vehicle data is maintained. In order to maintain the security of these systems, it is essential that the Australian Government, working within the framework provided by the Privacy Act, has the ability to access automated vehicle and C-ITS data in order to identify, defend and respond to malicious cyber activity on Australian networks.

The Discussion Paper highlights two Australian Government laws as providing access to telecommunications content and telecommunications data, also referred to as non-content data: the *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004*, that work to meet these challenges.

Interception and access to stored communications and telecommunications data

The Telecommunications (Interception and Access) Act provides the framework under which law enforcement and national security agencies can lawfully intercept communications, access stored communications, and access telecommunications data. Each of the three types of access provides for a specific prohibition on interception or access unless that action is subject to a warrant or authorisation.

These access protocols only apply to certain law enforcement and national security agencies, with appropriate warrants or authorisations granted only where certain thresholds, usually regarding the minimum penalty, have been met.

Certain other requirements relevant to C-ITS and automated vehicle data would need to be met before these interception or access powers could be used for the purposes addressed in the National Transport Commission Discussion Paper. These include whether:

- the C-ITS or automated vehicle technology would utilise the Australian telecommunications network as the backbone of any communications network associated with that technology, and
- C-ITS and automated car technology providers would be considered 'carriage service providers' for the purposes of the *Telecommunications Act 1997*.

The selection of communications technology may affect the application of the Telecommunications (Interception and Access) Act. For example, one of the options for C-ITS systems involves radiocommunications. Radiocommunications are specifically excluded from the statutory definitions of telecommunications network and telecommunications service under the Telecommunications (Interception and Access) Act.

Australian Government surveillance device laws

The Surveillance Devices Act regulates the use of surveillance devices by Australian Government law enforcement and national security agencies. It allows certain surveillance activities to be conducted under a judicial warrant, under an emergency authorisation, or without a warrant in limited circumstances. The Surveillance Devices Act also includes a number of reporting and record-keeping obligations, as well as restrictions on the use, disclosure, communication and publication of protected information.

The Surveillance Devices Act intentionally does not cover the field in relation to the use of surveillance devices because each state and territory has enacted its own legislation to regulate the authorised use of listening devices, optical surveillance devices, tracking devices and data surveillance devices.

It is uncertain whether C-ITS and automated vehicle technologies will fit within the Australian Government Surveillance Devices Act; for example, 'computers' as defined by section 6 may apply to some automated driving systems. If this is the case, those systems could be considered data surveillance devices for the purposes of the Surveillance Devices Act.

Balancing privacy and law enforcement activities in the Telecommunications (Interception and Access) Act and Surveillance Devices Act

The existing framework governing lawful access to communications under the Telecommunications (Interception and Access) Act and the use of surveillance and tracking devices under the Surveillance Devices Act recognises that investigatory methods can be covert and intrusive by nature. To balance privacy and the interests of law enforcement and security agencies, each regime relies on warrant and authorisation frameworks, explicit restrictions on the use and disclosure of personal or sensitive information, and robust oversight.

These frameworks have been subject to considerable debate and parliamentary scrutiny since the inception of the Telecommunications (Interception and Access) Act and the Surveillance Devices Act, including around how information can be used and disclosed for related purposes (including prosecutions).

One example of how the Telecommunications (Interception and Access) Act balances privacy with access is with regard to those who can authorise warrants (an eligible judge or an Administrative Appeal Tribunal member) or authorisations (senior law enforcement officers in most cases). These decision-makers are required to have regard to various criteria when deciding whether the access to data is reasonable, proportionate and necessary.

3.3 Other Australian Government regulatory powers that may apply to C-ITS and automated vehicle information

There are a range of Australian Government laws with broad information gathering powers, including policing, customs, competition, consumer and tax laws. Some of these laws may be applicable to information generated by C-ITS and automated vehicle systems.

4 Consideration of Discussion Paper options

The Discussion Paper outlines four options for government to consider. Option 1 is to rely on the existing information access framework at this time for both C-ITS and automated vehicles. Option 2 is to agree broad principles for limiting government collection, use and disclosure of information from these technologies. Options 3 and 4 for automated vehicles and option 3 for C-ITS technology propose immediate changes to privacy settings and potentially limit beneficial future uses of automated vehicle information.

The Department supports Option 1 for automated vehicles and C-ITS.

The Department recognises that there may be a need to consider the privacy principle model of Option 2 in the future. The principles outlined in the Discussion Paper will need to be carefully analysed, particularly noting the extensive consultation undertaken in developing the existing Australian Privacy Principles.

Our reasons for supporting Option 1 reflect the Department's view that the types of information generated by these technologies will not be new in nature. And that while people are rightly concerned about protecting this information, surveys indicate the community is more concerned about safety, cyber security and liability issues.

They also go to the strengths of the existing information access framework, particularly the Privacy Act and specific laws that enable access to personal information, such as the Telecommunications (Interception and Access) Act and the Surveillance Devices Act, namely:

- The good processes that underpin the making of these laws. They are the result of extensive consultation and deliberation.
- The current arrangements strike a reasonable balance between protecting privacy and enabling access to personal information to ensure other social outcomes, such as vehicle and road safety; and law enforcement.
- The existing framework is designed to be technologically neutral so as to provide flexibility and to preserve the Act's relevance as new technologies emerge, including C-ITS and automated vehicle technology.

The Australian Government would have concerns about specific regulations governing the ability of law enforcement and national security agencies to undertake data and computer-based surveillance on new technologies (including on non-traditional devices). For example, increased prohibitions on access to automated vehicle and C-ITS data may negatively impact agencies' ability to investigate and prosecute serious crimes. Like the Privacy Act, these laws were designed to be technologically neutral, where possible.

Efforts to directly regulate access to automated vehicle data outside existing data access frameworks may risk introducing inconsistencies with existing access mechanisms. Further, direct regulation may inadvertently create a legislative regime that, given the fast evolution of technology, may be outpaced quickly and will not provide an effective legislative mechanism to facilitate law enforcement and national security agency access to data.

A priority for all Australian governments will be to monitor C-ITS and automated vehicle technology as it evolves and is applied, to ensure the existing privacy provisions and information access framework are fit for purpose.

If changes are required, it is important that there is good opportunity for public consultation and deliberation. Any sector or industry specific principles or laws must be critically assessed to ensure they do not undermine or are not at odds with current broad-based arrangements.

Privacy fact sheet 17

Australian Privacy Principles

January 2014

From 12 March 2014, the Australian Privacy Principles (APPs) will replace the National Privacy Principles and Information Privacy Principles and will apply to organisations, and Australian Government (and Norfolk Island Government) agencies.

This privacy fact sheet provides the text of the 13 APPs from Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012,* which amends the *Privacy Act 1988*. For the latest versions of these Acts visit the ComLaw website: www.comlaw.gov.au.

Part 1—Consideration of personal information privacy

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

1.1 The object of this principle is to ensure that APP entities manage personal information in an open and transparent way.

Compliance with the Australian Privacy Principles etc.

1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

(a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and

(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.

APP Privacy policy

1.3 An APP entity must have a clearly expressed and up to date policy (the *APP privacy policy*) about the management of personal information by the entity.

1.4 Without limiting subclause 1.3, the APP privacy policy of the APP entity must contain the following information:

(a) the kinds of personal information that the entity collects and holds;

(b) how the entity collects and holds personal information;

(c) the purposes for which the entity collects, holds, uses and discloses personal information;

(d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;

(e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(f) whether the entity is likely to disclose personal information to overseas recipients;

(g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

Availability of APP privacy policy etc.

1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:

(a) free of charge; and

(b) in such form as is appropriate.

Note: An APP entity will usually make its APP privacy policy available on the entity's website.

1.6 If a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

Australian Privacy Principle 2—anonymity and pseudonymity

2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

2.2 Subclause 2.1 does not apply if, in relation to that matter:

(a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or

(b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

Part 2—Collection of personal information

Australian Privacy Principle 3—collection of solicited personal information

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity 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.

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:

(i) if the entity is an agency—the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(ii) if the entity is an organisation—the information is reasonably necessary for one or more of the entity's functions or activities; or

(b) subclause 3.4 applies in relation to the information.

3.4 This subclause applies in relation to sensitive information about an individual if:

(a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(b) a permitted general situation exists in relation to the collection of the information by the APP entity; or

(c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or

(d) the APP entity is an enforcement body and the entity reasonably believes that:

(i) if the entity is the Immigration Department—the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or

(ii) otherwise—the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(e) the APP entity is a non-profit organisation and both of the following apply:

(i) the information relates to the activities of the organisation;

(ii) the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Note: For *permitted general situation*, see section 16A. For *permitted health situation*, see section 16B.

Means of collection

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency:

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Solicited personal information

3.7 This principle applies to the collection of personal information that is solicited by an APP entity.

Australian Privacy Principle 4—dealing with unsolicited personal information

4.1 If:

(a) an APP entity receives personal information; and

(b) the entity did not solicit the information;

the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.

4.2 The APP entity may use or disclose the personal information for the purposes of making the determination under subclause 4.1.

4.3 If:

(a) the APP entity determines that the entity could not have collected the personal information; and

(b) the information is not contained in a Commonwealth record;

the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

4.4 If subclause 4.3 does not apply in relation to the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had collected the information under Australian Privacy Principle 3.

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

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

(a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of any such matters.

5.2 The matters for the purposes of subclause 5.1 are as follows:

(a) the identity and contact details of the APP entity;

(b) if:

(i) the APP entity collects the personal information from someone other than the individual; or

(ii) the individual may not be aware that the APP entity has collected the personal information;

the fact that the entity so collects, or has collected, the information and the circumstances of that collection;

(c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order—the fact that the collection is so required

or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);

(d) the purposes for which the APP entity collects the personal information;

(e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;

(f) any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;

(g) that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;

(h) that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(i) whether the APP entity is likely to disclose the personal information to overseas recipients;

(j) if the APP entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Part 3—Dealing with personal information

Australian Privacy Principle 6—use or disclosure of personal information

Use or disclosure

6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:

(a) the individual has consented to the use or disclosure of the information; or

(b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.

6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:

(a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:

(i) if the information is sensitive information—directly related to the primary purpose; or

(ii) if the information is not sensitive information—related to the primary purpose; or

(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or

(d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or

(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Note: For *permitted general situation*, see section 16A. For *permitted health situation*, see section 16B.

6.3 This subclause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if:

(a) the agency is not an enforcement body; and

(b) the information is biometric information or biometric templates; and

(c) the recipient of the information is an enforcement body; and

(d) the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.

6.4 If:

(a) the APP entity is an organisation; and

(b) subsection 16B(2) applied in relation to the collection of the personal information by the entity;

the entity must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the entity discloses it in accordance with subclause 6.1 or 6.2.

Written note of use or disclosure

6.5 If an APP entity uses or discloses personal information in accordance with paragraph 6.2(e), the entity must make a written note of the use or disclosure.

Related bodies corporate

6.6 If:

(a) an APP entity is a body corporate; and

(b) the entity collects personal information from a related body corporate;

this principle applies as if the entity's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Exceptions

6.7 This principle does not apply to the use or disclosure by an organisation of:

(a) personal information for the purpose of direct marketing; or

(b) government related identifiers.

Australian Privacy Principle 7—direct marketing

Direct marketing

7.1 If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Exceptions—personal information other than sensitive information

7.2 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from the individual; and

(b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) the individual has not made such a request to the organisation.

7.3 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from:

(i) the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or

(ii) someone other than the individual; and

(b) either:

(i) the individual has consented to the use or disclosure of the information for that purpose; or

(ii) it is impracticable to obtain that consent; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) in each direct marketing communication with the individual:

(i) the organisation includes a prominent statement that the individual may make such a request; or

(ii) the organisation otherwise draws the individual's attention to the fact that the individual may make such a request; and

(e) the individual has not made such a request to the organisation.

Exception—sensitive information

7.4 Despite subclause 7.1, an organisation may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

Exception—contracted service providers

7.5 Despite subclause 7.1, an organisation may use or disclose personal information for the purpose of direct marketing if:

(a) the organisation is a contracted service provider for a Commonwealth contract; and

(b) the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and

(c) the use or disclosure is necessary to meet (directly or indirectly) such an obligation.

Individual may request not to receive direct marketing communications etc.

7.6 If an organisation (the first organisation) uses or discloses personal information about an individual:

(a) for the purpose of direct marketing by the first organisation; or

(b) for the purpose of facilitating direct marketing by other organisations;

the individual may:

(c) if paragraph (a) applies—request not to receive direct marketing communications from the first organisation; and

(d) if paragraph (b) applies—request the organisation not to use or disclose the information for the purpose referred to in that paragraph; and

(e) request the first organisation to provide its source of the information.

7.7 If an individual makes a request under subclause 7.6, the first organisation must not charge the individual for the making of, or to give effect to, the request and:

(a) if the request is of a kind referred to in paragraph 7.6(c) or (d)—the first organisation must give effect to the request within a reasonable period after the request is made; and

(b) if the request is of a kind referred to in paragraph 7.6(e)—the organisation must, within a reasonable period after the request is made, notify the individual of its source unless it is impracticable or unreasonable to do so.

Interaction with other legislation

7.8 This principle does not apply to the extent that any of the following apply:

(a) the *Do Not Call Register Act 2006*;

(b) the *Spam Act 2003*;

(c) any other Act of the Commonwealth, or a Norfolk Island enactment, prescribed by the regulations.

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

8.1 Before an APP entity discloses personal information about an individual to a person (the overseas recipient):

(a) who is not in Australia or an external Territory; and

(b) who is not the entity or the individual;

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 (other than Australian Privacy Principle 1) in relation to the information.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

8.2 Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

(a) the entity reasonably believes that:

(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;

(ii) after being so informed, the individual consents to the disclosure; or

(c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or

(e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or

(f) the entity is an agency and both of the following apply:

(i) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;

(ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

Note: For *permitted general situation*, see section 16A.

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

Adoption of government related identifiers

9.1 An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless:

(a) the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(b) subclause 9.3 applies in relation to the adoption.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Use or disclosure of government related identifiers

9.2 An organisation must not use or disclose a government related identifier of an individual unless:

(a) the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions; or

(b) the use or disclosure of the identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

(c) the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier; or

(e) the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(f) subclause 9.3 applies in relation to the use or disclosure.

Note 1: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Note 2: For *permitted general situation*, see section 16A.

Regulations about adoption, use or disclosure

9.3 This subclause applies in relation to the adoption, use or disclosure by an organisation of a government related identifier of an individual if:

(a) the identifier is prescribed by the regulations; and

(b) the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and

(c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

Note: There are prerequisites that must be satisfied before the matters mentioned in this subclause are prescribed, see subsections 100(2) and (3).

Part 4—Integrity of personal information

Australian Privacy Principle 10—quality of personal information

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up to date and complete.

10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

Australian Privacy Principle 11—security of personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

11.2 If:

(a) an APP entity holds personal information about an individual; and

(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and

(c) the information is not contained in a Commonwealth record; and

(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

Part 5—Access to, and correction of, personal information

Australian Privacy Principle 12—access to personal information

Access

12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Exception to access—agency

12.2 If:

(a) the APP entity is an agency; and

(b) the entity is required or authorised to refuse to give the individual access to the personal information by or under:

(i) the Freedom of Information Act; or

(ii) any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;

then, despite subclause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access.

Exception to access—organisation

12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:

(a) the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

(b) giving access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or

(e) giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) giving access would be unlawful; or

(g) denying access is required or authorised by or under an Australian law or a court/tribunal order; or

(h) both of the following apply:

(i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;

(ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

Dealing with requests for access

12.4 The APP entity must:

(a) respond to the request for access to the personal information:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Other means of access

12.5 If the APP entity refuses:

(a) to give access to the personal information because of subclause 12.2 or 12.3; or

(b) to give access in the manner requested by the individual;

the entity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual.

12.6 Without limiting subclause 12.5, access may be given through the use of a mutually agreed intermediary.

Access charges

12.7 If the APP entity is an agency, the entity must not charge the individual for the making of the request or for giving access to the personal information.

12.8 If:

(a) the APP entity is an organisation; and

(b) the entity charges the individual for giving access to the personal information;

the charge must not be excessive and must not apply to the making of the request.

Refusal to give access

12.9 If the APP entity refuses to give access to the personal information because of subclause 12.2 or 12.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

12.10 If the APP entity refuses to give access to the personal information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.

Australian Privacy Principle 13—correction of personal information

Correction

13.1 If:

(a) an APP entity holds personal information about an individual; and

(b) either:

(i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or

(ii) the individual requests the entity to correct the information;

the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

Notification of correction to third parties

13.2 If:

(a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and

(b) the individual requests the entity to notify the other APP entity of the correction;

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

Refusal to correct information

13.3 If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

Request to associate a statement

13.4 If:

(a) the APP entity refuses to correct the personal information as requested by the individual; and

(b) the individual requests the entity to associate with the information a statement that the information is inaccurate, out of date, incomplete, irrelevant or misleading;

the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

Dealing with requests

13.5 If a request is made under subclause 13.1 or 13.4, the APP entity:

(a) must respond to the request:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).

The information provided in this fact sheet is of a general nature. It is not a substitute for legal advice.

For further information

telephone: 1300 363 992
email: enquiries@oaic.gov.au
write: GPO Box 5218, Sydney NSW 2001
or visit our website at **www.oaic.gov.au**