Austroads

Corporate Report
AP-C100-17

Privacy Impact Assessment (PIA) for Cooperative Intelligent Transport System (C-ITS) data messages

Privacy Impact Assessment (PIA) for Cooperative Intelligent Transport System (C-ITS) data messages

Prepared by

Peter van Dijk, Galexia

Project Manager

Stuart Ballingal

Publisher

Austroads Ltd.
Level 9, 287 Elizabeth Street
Sydney NSW 2000 Australia
Phone: +61 2 8265 3300
austroads@austroads.com.au
www.austroads.com.au

Abstract

This document provides a high level Privacy Impact Assessment for the Cooperative Intelligent Transport System (C-ITS) data messaging system.

Keywords

Cooperative Intelligent Transport System, C-ITS, privacy, personal information, cooperative awareness message, decentralised event notification message, legislation

Austroads Project No. NT1785

Austroads Publication No. AP-C100-17

Publication date March 2017 (Prepared August 2016)

Pages 46

About Austroads

Austroads is the peak organisation of Australasian road transport and traffic agencies.

Austroads' purpose is to support our member organisations to deliver an improved Australasian road transport network. To succeed in this task, we undertake leading-edge road and transport research which underpins our input to policy development and published guidance on the design, construction and management of the road network and its associated infrastructure.

Austroads provides a collective approach that delivers value for money, encourages shared knowledge and drives consistency for road users.

Austroads is governed by a Board consisting of senior executive representatives from each of its eleven member organisations:

- Roads and Maritime Services New South Wales
- Roads Corporation Victoria
- Queensland Department of Transport and Main Roads
- Main Roads Western Australia
- Department of Planning, Transport and Infrastructure South Australia
- Department of State Growth Tasmania
- Department of Infrastructure, Planning and Logistics Northern Territory
- Transport Canberra and City Services Directorate, Australian Capital Territory
- Australian Government Department of Infrastructure and Regional Development
- Australian Local Government Association
- New Zealand Transport Agency.

Contents

1. Executive Summary

Galexia conducted a high-level Privacy Impact Assessment (PIA) for Austroads on data messages that will be wirelessly broadcast and received by vehicles and roadside units in a Cooperative Intelligent Transport Systems (C-ITS) deployment.

This review is current as at July 2016.

Broad Purpose

This Privacy Impact Assessment (PIA) considers the privacy issues raised by the standard data messages that will be wirelessly broadcast and received by vehicles and roadside units in a Cooperative Intelligent Transport Systems (C-ITS) deployment.

The deployment of C-ITS in Australia is subject to the requirements of the *Privacy Act 1988,* including the Australian Privacy Principles (APPs) which came into force in March 2014. Parts of the deployment may be subject to additional State and Territory privacy legislation and relevant transport legislation.

The broad purpose of this privacy review is to:

- Determine whether the data messages should be considered personal information;
- Identify any immediate privacy compliance issues;
- Identify any potential future issues; and
- Assist Austroads develop a work plan and priorities for the ongoing governance of privacy issues in the development and implementation of C-ITS.

Information considered

Information contained in this privacy review is based on:

- Meetings and teleconferences with Austroads;
- Limited engagement with key stakeholders (notably the Office of the Australian Information Commissioner and Transport Certification Australia);
- Review of relevant Austroads reports;
- General research and literature review on intelligent transport systems and relevant privacy issues; and
- Review of relevant privacy legislation and guidelines.

Findings and Recommendations

This Privacy Impact Assessment has identified a number of privacy issues that may require further consideration by Austroads.

Most of the recommendations in the review are suggested enhancements to current policies and procedures, or suggested paths of action related to the implementation of C-ITS.

The key findings and recommendations are set out in the following table:

Privacy compliance issue	Finding	Notes	Recommendation
Is the data 'personal information'? Refer to section 4 at page 14.	Data that is collected, used and disclosed in the standard messages in C-ITS is personal information.	A unique identifier is broadcast by a vehicle's C-ITS equipment. However, in the day-to-day operation of C-ITS, the unique identifier is 'masked' by the use of rotating pseudonyms. In certain circumstances these identifiers can be unmasked (for example, on request by a law enforcement agency). The PIA concludes that individuals can be reasonably identified from a series of potential links from the C-ITS identifier, to a vehicle identifier and eventually to the vehicle owner and likely driver. This finding is consistent with developments in the consideration of C-ITS data messages in Europe.	Data that is collected, used and disclosed in the standard messages in C-ITS should be treated as personal information for the purposes of complying with privacy legislation.
APP 1 – Openness and Transparency Refer to section 5 at page 17.	Participants in C-ITS (including any centralised function or central hub that may be established) are required to develop specific C-ITS privacy policies to comply with the openness and transparency principles in APP1.	This principle presents some challenges for C-ITS, as the peer-to-peer structure of the C-ITS framework may not include a central organisation, hub or contact point. Participants will have to comply by adopting C-ITS specific privacy policies and making these available to the public. There may be some benefit in providing an information service to consumers that provides links to these policies. There may also be some benefit in providing central guidance (or even a template) for the principles that need to be contained in C-ITS privacy policies. Options that could be considered at this early stage of deployment include the development of an industry code of practice (for vehicle manufacturers) and / or the development of a national guide (e.g. an Austroads Guide) for road infrastructure owners and operators.	Once the structure of the C-ITS framework is established it will be easier to determine how APP 1 can be addressed. If the structure remains open in nature, without a central hub, then some further work will be required to ensure that C-ITS participant privacy policies are provided in a consistent way.

Privacy compliance issue	Finding	Notes	Recommendation
APP 2 – Anonymity and Pseudonymity Refer to section 6 at page 20.	The C-ITS framework already incorporates pseudonymity and is in compliance with this APP.	At this early stage of development the C-ITS proposal includes the use of rotating pseudonyms to limit the identification of individual vehicles across the network. The system will not result in complete de-identification, but this is permitted by privacy legislation.	No further work is required at this stage.
APP 3 – Collection of solicited personal information Refer to section 7 at page 22.	Collection of solicited personal information is likely to be in accordance with APP3, although some aspects of collection are still to be determined. No sensitive data is collected.	Most collection will be for the purpose of safety critical functions, and will therefore easily comply with APP 3. However, some additional applications may be developed. A process may need to be implemented to check that participating organisations only use the data for an approved purpose.	Some further checks will need to be made as the C-ITS system develops, to ensure compliance with APP 3. The establishment of an approval process for applications may need to be considered.
APP 4 – Dealing with unsolicited personal information Refer to section 8 at page 22.	The C-ITS messaging system is unlikely to receive unanticipated or unsolicited personal information in its day-to-day activities.	This APP is not relevant to the deployment of C-ITS.	No further action is required.
APP 5 – Notification Refer to section 9 at page 26.	The C-ITS framework (here and abroad) does not yet include a standard approach regarding the provision of notice to drivers. Compliance with APP 5 presents a significant challenge for C-ITS.	The 'notice' requirements in privacy legislation represent one of the greatest challenges for the C-ITS messaging system – mainly because the lack of structure in the C-ITS environment means that there may not be clear opportunities to give all drivers 'notice' of the use of their information. The ability of the C-ITS transponder to communicate with the driver will depend on other technology within the vehicle. A brief notice may be displayed (and possibly acknowledged) if the vehicle has the capacity to display a message to the driver on first use. Other opportunities for providing notice to the driver are limited	Further work will be required in order to: 1. Identify in-vehicle mechanisms that enable a short notice to be provided to the driver (and acknowledged); and 2. Identify alternative processes for providing notice to drivers; and 3. Providing guidance or standardisation for the content of C-ITS privacy notices.

Privacy compliance issue	Finding	Notes	Recommendation
APP 6 – Use or Disclosure Refer to section 10 at page 29.	Compliance with APP 6 requires significant further technical and policy development, in order to provide a system of 'consent markers' that works in practice.	Europe is considering an approach which concentrates on obtaining the driver's consent for disclosures, and allowing the driver to opt out by switching off the broadcast of all or part of the C-ITS messages.[1] There could be some substantial practical and technical issues with implementing this approach – can the broadcast be 'limited' to safety critical features? Can a system be developed that recognises 'consent markers' that have been added to data messages? There will also be considerable governance issues – who 'approves' the categorisation of features as 'safety critical'? Does this require specific legislative backing?	Further work is required to establish a consent based system for C-ITS messages. Tasks include: 1. Developing a policy and structure for determining whether data and messages are 'safety critical'; 2. Implementing a system of 'consent markers'; and 3. Developing an approval structure for secondary use of data.
APP 7 – Direct Marketing Refer to section 11 at page 32.	It is not expected that direct marketing will be a relevant issue in the implementation of C-ITS.	This APP is not relevant to the deployment of C-ITS.	No further action is required.
APP 8 – Cross Border Disclosure Refer to section 12 at page 33.	Some C-ITS participants, particularly vehicle manufacturers, are likely to transfer personal data outside Australia.	Most vehicles will be manufactured overseas, and service centres and even the vehicles themselves may communicate with information hubs in the country of manufacture. The relevance of these communications to C-ITS is unknown at this early stage. Also, the transponder is likely to be fitted overseas, and the station ID of the transponder may need to be communicated across borders.	Each participating organisation will need to ensure compliance with APP 8.
APP 9 – Government Related Identifiers Refer to section 13 at page 34.	There are no identifiers in the C-ITS system that are based on existing government issued identifiers.	This APP is not relevant to the deployment of C-ITS.	No further action is required.

[1] The Platform for the Deployment of Cooperative Intelligent Transport Systems in the European Union (C-ITS Platform), Final report, January 2016 <http://ec.europa.eu/transport/themes/its/doc/c-its-platform-final-report-january-2016.pdf>

Privacy compliance issue	Finding	Notes	Recommendation
APP 10 – Quality of Personal Information Refer to section 14 at page 35.	Data quality issues have not been considered at this early stage of C-ITS development.	This is a high level Privacy Impact Assessment (PIA), being conducted prior to the actual deployment or implementation of C-ITS. At this early stage, it is not possible to determine whether there are any data quality issues in the system. No major compliance issues with APP 10 are anticipated, although some further checks should be conducted following implementation.	No further action is required at this stage.
APP 11 – Security Refer to section 15 at page 36.	Privacy legislation requires some specific security compliance steps (to the extent that these are not already being undertaken): 1. Risk assessment – the OAIC Guidelines require organisations to conduct a risk and vulnerability assessment; 2. Data destruction – there is a specific requirement in APP 11 to develop a detailed data destruction plan; and 3. Broadcast data – the security review should include a discussion on the potential impact of 'eavesdropping'.	Austroads is currently reviewing potential requirements for a localised C-ITS Security Credential Management System. This PIA does not duplicate that work, but it does consider some specific security compliance issues raised by privacy legislation.	This is a high level Privacy Impact Assessment (PIA), being conducted prior to the actual deployment or implementation of C ITS. Many of the security issues in C-ITS are only at a very early stage of discussion. Privacy legislation requires organisations to undertake a risk and vulnerability assessment, and to develop a data destruction plan. These two items should be added to the work plan for the deployment of C-ITS in Australia.
APP 12 – Access Refer to section 16 at page 39.	Access requests in the C-ITS framework will be complex, and may only provide limited data to individual consumers. The system might benefit from some work on ensuring consistent access across the network.	The C-ITS framework presents some challenges in terms of access. It is a complex peer to peer network, and no single entity may have a view of all the data collected about a single individual. Most data will be pseudonymised and difficult to extract for a single C-ITS participant. Also, some work may be required to educate consumers about the limitations of the data that is likely to be available.	In order to manage consumer expectations and to drive consistency across the C-ITS network, some additional work may need to be undertaken on developing an appropriate C-ITS access policy. These tasks could include: 1. Developing a standard access request policy across the whole network; 2. Seeking agreement from all C-ITS participants to meet the higher standards in APP 12 (e.g. providing access within 30 days at no cost, even though there are exceptions to these requirements available to some organisations); and 3. Explore solutions to 'keep it simple' for the consumer, such as a single access request form.

Privacy compliance issue	Finding	Notes	Recommendation
APP 13 – Correction Refer to section 17 at page 41.	Issues related to correction have not been considered at this early stage of C-ITS development.	This is a high level Privacy Impact Assessment (PIA), being conducted prior to the actual deployment or implementation of C-ITS. At this early stage, it is not possible to determine whether there any issues related to correction in the system. No major compliance issues with APP 13 are anticipated, although some further checks should be conducted following implementation.	No further action is required at this stage.
Data breach notification Refer to section 18 at page 43.	At this stage, relevant C-ITS organisations should adopt data breach response plans that comply with the OAIC Guidelines. This approach will need to be updated if mandatory data breach notification legislation is implemented.	It is now best practice for organisations to develop a data breach response plan. In the C-ITS framework this may need to be developed as a central function or process, or by each C-ITS participant.	C-ITS participants should adopt data breach response plans that comply with the OAIC Data Breach Notification Guidelines (2014).
Future developments and governance Refer to section 19 at page 45.	It may be necessary to enhance privacy protection through the development of an industry code of practice for vehicle manufacturers and / or the development of an Austroads Guide for other C-ITS participants.	It will be difficult to implement C-ITS in Australia relying only on general compliance with existing privacy legislation. The complex peer to peer network at the heart of C-ITS does not include an entity or a structure that can maintain a level of oversight or governance for data protection.	C-ITS participants should explore options for the development of an industry code of practice for vehicle manufacturers and / or the development of an Austroads Guide for other C-ITS participants.

2. Scope and Methodology

Galexia conducted a high-level Privacy Impact Assessment (PIA) for Austroads on data messages that will be wirelessly broadcast and received by vehicles and roadside units in a Cooperative Intelligent Transport Systems (C-ITS) deployment.

The focus of this PIA is on two specific types of messages:

— **Cooperative Awareness Message (CAM)**
The CAM is continuously broadcast by a C-ITS device, at up to 10 times per second. For vehicles, the CAM contains data attributes such as the vehicle location, speed, heading, timestamp, brake status, etc.

— **Decentralised Event Notification Message (DENM)**
The DENM is generated when an event occurs, and contains information about the event. This could include traffic conditions, road hazards, road works, or a traffic signal violation warning.

2.1. Scope

The scope of this privacy review is limited to the following items:

In Scope	Out of Scope
• High level identification of potential compliance issues in the context of the Australian / New Zealand privacy legal framework,	• Compliance with specific sectoral / State or Territory legislation
• Review of *key* documents related to the C-ITS data message system	• Review of the entire suite of Austroads ITS documentation
• Limited stakeholder consultation (2-3 internal staff members and regulator officials by email and phone)	• Extensive stakeholder consultation, or assessment of public attitudes etc.
• Review of existing security assessment	• Full security audit
• High level identification and review of legal documentation	• Detailed legal advice

2.2. Privacy legislation

The deployment of C-ITS in Australia is subject to the requirements of the *Privacy Act 1988,* including the Australian Privacy Principles (APPs) which came into force in March 2014. The Act sets out the Australian Privacy Principles (APPs), which regulate the collection, use and disclosure of personal information by Commonwealth Agencies and private sector organisations. The Act also includes a complaints, audit and enforcement regime.

Parts of the deployment may be subject to additional State and Territory privacy legislation and relevant transport legislation. Austroads members include the State and Territory road authorities, the New Zealand Transport Agency, and the Australian Local Government Association.

3. C-ITS Overview

Cooperative ITS (C-ITS) is a vital part of the infrastructure being developed under the broader banner of Intelligent Transport Systems.

Austroads has defined Cooperative ITS (C-ITS) as:

> The use of wireless communications and real-time information sharing between vehicles, and with roadside infrastructure, back-end centres and personal devices, which will enable vehicle and transport applications to cooperatively work together to deliver safety, mobility and environmental outcomes beyond what standalone applications can deliver. [Austroads Project Brief, 2016]

C-ITS safety-critical applications will use Dedicated Short Range Communications (DSRC) in the 5.9 GHz band, and Austroads is working with the Australian Communication and Media Authority (ACMA) to have this band authorised and reserved for this purpose.

Potential communications scenarios include: vehicle-to-vehicle (V2V); vehicle-to-infrastructure (V2I, and also I2V); and communications with other devices (V2X), such as personal devices.

There is a range of C-ITS data messages that are planned to be broadcast and received. The two main data messages that will be included in initial deployments are:

- **Cooperative Awareness Message (CAM)**
  The CAM is continuously broadcast by a C-ITS device, at up to 10 times per second. All C-ITS devices that are within range, which could potentially be up to 1,000 metres, can receive a CAM. For vehicles, the CAM contains data attributes such as the vehicle location, speed, heading, timestamp, brake status, etc. (ETSI standard EN 302 637-2).
- **Decentralised Event Notification Message (DENM)**
  The DENM is generated when an event occurs, and contains information about the event. This could include traffic conditions, road hazards, road works, or a traffic signal violation warning. (ETSI standard EN 302 637-3).

The CAM and DENM will enable a range of potential in-vehicle safety and mobility applications. These could include (but are not limited to):

- Vehicle collision warning;
- Road hazard warning;
- Emergency braking warning;
- Traffic light violation warning;
- Traffic jam ahead warning.
- Slow or stationary vehicle(s) & Traffic ahead warning
- Road works warning
- Weather conditions
- Emergency brake light
- Emergency vehicle approaching
- Other hazardous notifications
- In-vehicle signage
- In-vehicle speed limits

Data messages broadcast by vehicles may also be received by roadside equipment and used by road operators for traffic management and congestion analysis.

It is important to note that as a vehicle is driven, information (including potential personal information) is disclosed or broadcast or displayed in a number of ways. C-ITS is only a small part of this information exchange. The following is a non-exhaustive list of potential data exchanges for vehicles:

— **Vehicle registration number**
The vehicle registration (number plate) is visible to witnesses and cameras, including automatic plate number recognition systems, law enforcement cameras and safety cameras. For each vehicle registration the potential owner or driver is relatively easy to identify.

— **Vehicle attributes**
The make, model and colour of the vehicle is visible to witnesses and cameras, and for some rare vehicles there will only be a limited pool of potential owners and drivers.

— **Vehicle manufacturer information systems**
Information systems built into the car by manufacturers may broadcast or disclose vehicle information, including a unique identifier. Principally this data will be exchanged with service centres or a central information system established by the manufacturer. The scope and type of data varies considerably.

— **Accident information retrieval systems**
Many modern vehicles include a 'black box' capability, that records critical information relevant to an accident. The data is typically deleted on a regular basis, but is retained if an accident occurs. The scope and type of data varies considerably, but it will usually include a unique vehicle identifier.

— **Navigation and driver assistance devices**
Navigation devices, either fitted to or added to a vehicle, retain detailed information on vehicle location and movements. Most systems do not communicate this data, and they cannot be remotely queried. However, the data is available to anyone in possession of the device.

— **Bluetooth devices**
A broad range of connected devices may be operating in a vehicle, potentially displaying their presence and / or other data. The presence of Bluetooth connected devices is commonly monitored by remote sensors in congestion management and traffic analysis systems.

— **Cellular devices**
The location and movement of smart phones can also be monitored remotely. The scope and type of data varies considerably – in some smart phone applications the exact location and movements of the phone's owner will be tracked remotely as part of a navigation service.

— **Electronic tags (toll roads)**
Many vehicles carry electronic tags that can be read by road infrastructure (usually for toll road services). The tag number is often linked to a unique identifier for a vehicle and the payment arrangements may require a direct link to an individual.

— **Electronic tags (employers, rental cars etc.)**
Many vehicles carry electronic tags that can be read remotely, or queried when the vehicle is returned. This is common in employment situations where a driver is using a company vehicle (couriers, public transport, taxis) or where the vehicle is rented. Some of these system allow remote monitoring of the vehicle, and even some control over the vehicle. These systems are also fitted to some private vehicles as anti-theft devices.

— **Vehicle / driver log-books**
Many drivers and / or vehicles are subject to log-books (both manual and electronic) that record the location and movement of the driver / vehicle. This is common in heavily regulated industries (heavy goods vehicles, chauffer services etc.).

The overall amount of information disclosed when a vehicle is being driven is therefore complex and highly dependent on the individual circumstances of the vehicle, the driver and the various devices in the car. The C-ITS component is just a small part of this broader information exchange regarding vehicles.

4. Is the data 'personal information'?

4.1. The Law

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable.

The Office of the Australian Information Commissioner has provided some further guidance on whether an individual is 'reasonably identifiable':

> Whether an individual is 'reasonably identifiable' from particular information will depend on considerations that include:
>
> 1. The nature and amount of information
> 2. The circumstances of its receipt
> 3. Who will have access to the information
> 4. Other information either held by or available to the APP entity that holds the information
> 5. Whether it is possible for the individual or entity that holds the information to identify the individual, using available resources (including other information available to that individual or entity). Where it may be possible to identify an individual using available resources, the practicability, including the time and cost involved, will be relevant to deciding whether an individual is 'reasonably identifiable'
> 6. If the information is publically released, whether a reasonable member of the public who accesses that information would be able to identify the individual.

The guidelines are available at:
https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#personal-information

These guidelines also include a specific example / illustration related to driving:

> Most entities and individuals would encounter difficulty in using a licence plate number to identify the registrant of a car, as they would not have access to the car registration database. By contrast, an agency or individual with access to that database may be able to identify the registrant. Accordingly, the licence plate number may be 'personal information' held by that agency or individual, but may not be personal information if held by another entity.

However, these guidelines are not binding, and the definition of personal information is the subject of ongoing debate. The definition is currently the subject of an Appeal[2] by the Privacy Commissioner from a decision by the Administrative Appeals Tribunal (AAT), so some binding guidance on the definition may become available later in 2016. The AAT decision concentrates on whether or not information is 'about an individual', and broadly concludes that even though data might identify someone, it is not 'personal data' if it wasn't about the individual (e.g. where the individual's identity is revealed by accident). That approach, if upheld on appeal, may be relevant in the C-ITS environment.

The Guidelines conclude with the following warning:

> Where it is unclear whether an individual is 'reasonably identifiable', an organisation should err on the side of caution and treat the information as personal information.

[2] The Commissioner is appealing the decision in Telstra Corporation Limited and Privacy Commissioner [2015] AATA 991 which overturned a previous determination by the Privacy Commissioner in Ben Grubb and Telstra Corporation Limited [2015] AICmr 35.

4.2. C-ITS – Overview

With regards to identification in C-ITS, the international model that is emerging involves each CAM and DENM being signed using Public Key Infrastructure (PKI) to verify its authenticity. However, rather than maintaining a single identifier to sign each message, the messages are signed using a pseudonym. Each vehicle maintains a list of pseudonyms that are rotated periodically to mitigate the possibility of the vehicle being tracked across a road network.

A person who received a single signed message would therefore be unable to identify an individual vehicle (or driver) without access to further information. Similarly, a person receiving multiple signed messages over a period of time would not be able to identify a pattern concerning a single vehicle (with any degree of certainty).

However, the use of pseudonyms does not mean that a vehicle cannot be identified full stop. An organisation with access to other information, or vast amounts of data messages, or direct access to the original registration of the certificate and its associated pseudonyms, could potentially identify a vehicle from some of its messages. The process would be complex and resource intensive, but not impossible – especially for the agency or organisation with overall responsibility for managing the authenticity of certificates.

Once the identity of a vehicle is identified, it is likely that the identity of the driver and / or owner can be 'reasonably identified', because many of the participants in C-ITS also have access (either direct access or 'on request' access) to other information related to the vehicle, such as registration records.[3]

There are a number of scenarios where the unmasking of the vehicle identity may be required:

- A C-ITS participant (or a central C-ITS authority if one is established) may wish to investigate the authenticity of a message. Authenticity is a vital part of the safety critical applications of C-ITS and such an investigation would justify attempts to unmask the identity of a vehicle broadcasting specific messages.
- A law enforcement agency may have the legal authority to request information (and cooperation) from a C-ITS participant regarding messages. This may include requests to unmask identity. Such requests would not necessarily need to be authorised by a specific law related to C-ITS – they could be based on broader law enforcement powers.
- Other individuals and organisations may have the ability to request access to information subject to legal authority (e.g. a court subpoena). These cases will be rare and there may be greater scope for resisting the requests.
- Individual drivers and owners will have the right to access their own personal information, subject to some restrictions set out in privacy legislation. This scenario is discussed in more detail below in the section on Access requests.

[3] The NTC (2013) policy paper suggested that C ITS participants could be separated from the driver registration records, and therefore break the ability to link vehicle identifiers with owners / drivers. This appears to be unrealistic considering the close working relationships of the various stakeholders, and the ability for a very wide range of organisations to get access to registration records on request (court orders, law enforcement etc.). See: National Transport Commission (NTC), Cooperative Intelligent Transport Systems, *Final policy paper*, December 2013 <http://www.ntc.gov.au/Media/Reports/(55AFE902-73F4-073B-E6ED-AE684E3BE595).pdf>

Australia is not the only jurisdiction that has been considering this issue. C-ITS is being developed in Australia on the understanding that the system will need to be interoperable with global standards. European authorities have been considering data protection issues in C-ITS in some detail, and Working Group 4 from the European C-ITS Platform reached the following conclusion on whether or not the data was 'personal data':

> After various consultations, in particular with the European Data Protection Supervisor (EDPS) and privacy experts, the C-ITS platform considers these messages as 'personal data' because of their potential of indirect identification of users. Therefore the EU legislation (Directive 95/46/EC) on data privacy and data protection applies. [4]

4.3. 'Personal information' finding

The Privacy Commissioner warns that

> where it is unclear whether an individual is 'reasonably identifiable', an organisation should err on the side of caution and treat the information as personal information

This advice is relevant to C-ITS.

Although the message system is designed to mask the identity of vehicles in everyday use (through the imposition of rotating pseudonyms), the system is not completely anonymous. The identity of a vehicle can be unmasked in a number of scenarios.

Once a vehicle has been identified, the driver and owner of a vehicle can be readily identified, usually by the addition of just one other source of data. Most participants in C-ITS (vehicle manufacturers, road authorities, toll-road operators etc.) are used to linking vehicles and their owners /drivers.

In these circumstances, the data messages that are broadcast by vehicles in C-ITS should be treated as personal information for the purpose of Australian privacy legislation.

This is similar to the conclusion reached by Working Group 4 from the European C-ITS Platform in their consideration of C-ITS and data protection.[5]

[4] The Platform for the Deployment of Cooperative Intelligent Transport Systems in the European Union (C-ITS Platform), Final report, January 2016

[5] Ibid.

5. APP 1. Open and transparent management of personal information

5.1. The Law

APP 1 requires organisations to ensure the open and transparent management of personal information. This is mainly achieved by developing and publishing a 'clearly expressed and up to date' privacy policy.

More information:
http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-1-app-1-open-and-transparent-management-of-personal-information.

5.2. C-ITS – Overview

The deployment of C-ITS is likely to take the form of a complex peer-to-peer network. These types of systems are difficult to assess from a privacy compliance perspective, as privacy legislation assumes that a single organisation will be 'collecting' personal information for a specific purpose.

This PIA provides advice for both 'participating organisations' and a 'central process or central hub'. However, this does not mean that a central process or central hub has to be developed.

A central process or central hub might take the form of a registration service, or simply a central contact and information point.

Participating organisations will include (but not be limited to) vehicle manufacturers, transport operators, road infrastructure providers and regulators.

Openness and transparency (APP 1)	Compliant	Relevant Exception	Notes
A. Does C-ITS provide a public privacy policy?	To be developed	–	**Central hub / process** A central hub could provide a single overarching privacy policy and / or links to the privacy policies of relevant participating organisations. **Participating organisations** Each participating organisation could provide its own privacy policy or adopt the central privacy policy. Options that could be considered at this early stage of deployment include the development of an industry code of practice (for vehicle manufacturers) and / or the development of a national guide (e.g. an Austroads Guide) for road infrastructure owners and operators. Austroads Guides are adopted by the relevant road operators in each jurisdiction. They also cover private sector providers of road infrastructure (e.g. toll-road operators). Examples of Austroads Guides are available at: http://www.austroads.com.au/about-austroads/austroads-guides

Openness and transparency (APP 1)	Compliant	Relevant Exception	Notes
B. Does the Policy include the kinds of personal information that the entity collects and holds;	To be developed	–	**Central hub / process** A central privacy policy could provide a broad overview of the collection of information across the network. **Participating organisations** Specific privacy policies could describe the information collected by participating organisations (e.g. car manufacturers).
C. Does the Policy include how the entity collects and holds personal information;	To be developed	–	**Central hub / process** Required. **Participating organisations** Required.
D. Does the Policy include the purposes for which the entity collects, holds, uses and discloses personal information;	To be developed	–	**Central hub / process** Required. **Participating organisations** Required.
E. Does the Policy include how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;	To be developed	–	**Central hub / process** The central hub (if one is created) may not have direct access to data. It may be necessary to refer individuals to the relevant participating organisation/s. The amount of data available may be very limited – this is discussed in further detail in the section on Access below. **Participating organisations** This may potentially be addressed through reference to a single contact point if the central hub takes on that role. Otherwise each entity must take on this role.
F. Does the Policy include how an individual may complain about a breach of the APPs / registered code, and how the entity will deal with such a complaint;	To be developed	–	**Central hub / process** Required. **Participating organisations** Required.
G. Does the Policy include whether the entity is likely to disclose personal information to overseas recipients;	To be developed	–	**Central hub / process** Required. **Participating organisations** It is likely that some of the participating organisations may in fact be foreign entities or affiliates.
H. Does the Policy include 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.	To be developed	–	**Central hub / process** Required. **Participating organisations** Required.

5.3. APP 1. Finding

The deployment of C-ITS may take the form of a peer-to-peer network. Each part of the network will be broadcasting and receiving messages from other parts of the network – there may not be a central message hub. CAM and DENM messages are designed to be broadcast and the standards focus on the ability to broadcast and read the messages – records of messages may not exist in many circumstances (or records may be deleted very quickly).

The future structure of the overall C-ITS deployment is not clear at this stage. However, at least one central body is likely to be established in order to administer the systems for managing security certificates.

The absence of a central authority may make compliance with privacy legislation difficult. One option for addressing this issue may be establishing a consumer information portal, with explanations of how C-ITS works, and links to further information and contacts for the C-ITS deployment.

The establishment of a single privacy policy covering all C-ITS messages appears unlikely, but there may be room for the development of a template privacy policy that sets out key principles to be followed by all C-ITS participants.

Options that could be considered at this early stage of deployment include the development of an industry code of practice (for vehicle manufacturers) and / or the development of a national guide (e.g. an Austroads Guide) for road infrastructure owners and operators.

Austroads Guides are adopted by the relevant road operators in each jurisdiction. They also cover private sector providers of road infrastructure (e.g. toll-road operators). Examples of Austroads Guides are available at: <http://www.austroads.com.au/about-austroads/austroads-guides>

6. APP 2. Anonymity and Pseudonymity

6.1. The Law

APP 2 provides individuals with the option of anonymity and pseudonymity where this is lawful and practicable.

More information:
http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-2-app-2-anonymity-and-pseudonymity.

6.2. C-ITS – Overview

The development of C-ITS in both Australia and overseas has included an emphasis on the use of pseudonyms to mask the identity of vehicles in every-day use.

Indeed, the National Transport Commission 2013 policy paper on Co-operative Intelligent Transport Systems stated:

> Recommendation 2: That in the development and implementation of a C-ITS operational framework, in particular regarding standards for data messages broadcast by C-ITS stations, Australian governments seek the highest possible level of anonymity for drivers and that this be a key focus for Austroads in developing the framework.[6]

The current C-ITS messaging system is based on the use of rotating pseudonyms. This helps to ensure that messages are authentic, without revealing the identity of an individual vehicle in regular day-to-day use. However, the vehicle identity can be unmasked in certain scenarios.

The Austroads concept of operations for core C–ITS functions states:

> Security certificates are used in the public key infrastructure by C-ITS devices and services to sign messages so the receiver knows that the message is from a trustworthy source. Security certificates are uploaded onto C-ITS devices by a certificate authority once the device is tested for compliance with the appropriate standards and requirements and has been registered. Different applications and services may have different security certificates. Certificates are valid for a limited amount of time (e.g. 5 minutes or a day) and vehicles will have several simultaneously valid certificates, which makes it difficult to track a vehicle by following its trail of certificates.[7]

Discussions with stakeholders reveal that the exact details of this system of rotating pseudonyms are still being determined, but the objective is to mask the identity of the vehicle in general day-to-day interactions.

[6] National Transport Commission (NTC), Cooperative Intelligent Transport Systems, Final policy paper, December 2013 <http://www.ntc.gov.au/Media/Reports/(55AFE902-73F4-073B-E6ED-AE684E3BE595).pdf>

[7] Austroads, Concept of Operations for C-ITS Core Functions, 2015 <https://www.onlinepublications.austroads.com.au/items/AP-R479-15>

Anonymity and Pseudonymity (APP 2)	Compliant	Relevant Exception	Notes
A. Where lawful and practicable, are individuals given the option of: not identifying themselves OR identifying themselves with a pseudonym?	Yes	–	At this early stage of development the C-ITS proposal includes the use of rotating pseudonyms to limit the identification of individual vehicles across the network. The system will not result in complete de-identification, but this result is anticipated (and permitted) in privacy legislation.

6.3. APP 2. Finding

The C-ITS deployment will easily comply with APP 2, as the use of pseudonyms is an integral part of the messaging system.

However, the use of pseudonyms may raise other issues for vehicle manufacturers and road operators, including the issue of public perception. Will consumers understand that the vehicles identity is masked, and can be unmasked in certain circumstances? Pseudonyms are a difficult technical concept to explain to consumers.

7. APP 3. Collection of solicited personal information

7.1. The Law

APP 3 concerns the collection of solicited personal information. For personal information other than sensitive information the collection must be reasonably necessary or directly related to core C-ITS functions or activities.

For sensitive information there is an additional requirement that the individual must consent to the collection.

APP 3 also requires organisations to collect personal information only by lawful and fair means, and the collection must be from the individual in most circumstances.

More information:
http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-3-app-3-collection-of-solicited-personal-information.

7.2. C-ITS – Overview

Collection of solicited information (APP 3)	Compliant	Relevant Exception	Notes
Central hub / process **A.** Is collected information reasonably necessary for, or directly related to, one or more of the entity's functions or activities?	Yes	–	The broadcast of data messages and its use (especially by road infrastructure and other vehicles) is necessary for safety critical functions. Other information collection is directly related to these functions. The purpose of collection may, in time, be further limited by legislation (see discussion below).
Participating Organisations **B.** Is collected information reasonably necessary for one or more of the entity's functions or activities?	Yes	–	This will need to be determined on a case-by-case basis. An entity (potentially the central hub or a regulator) may need to implement a process for checking that participating organisations only use the data for an approved purpose. Alternatively, C-ITS participants could be bound by either an industry code of practice (for vehicle manufacturers) or a national guide (e.g. an Austroads Guide) for road infrastructure owners and operators. The purpose of collection may, in time, be further limited by legislation.
C. Is NO sensitive information about an individual collected (unless a relevant exception applies)?	Yes	–	No sensitive data (using the definition in the Act) has been included in any of the potential C-ITS scenarios considered to date.
D. Is personal information collected only by lawful and fair means?	Yes	–	**Required**
E. Is personal information about an individual collected only from the individual (unless a relevant exception applies)?	Yes	–	**Required**

†

One important issue that has arisen in discussions with stakeholders is whether or not C-ITS should be underpinned by specific legislation that sets out the purposes and objectives of the messaging system, and restricts data collection to a series of pre-approved functions.

The argument in favour of this approach is that it will build user confidence in the system. As the system is likely to be opt-out, the best way of maximising participation is ensuring that the data will only be used for purposes that are accepted by the public.

One key concern is that the CAM message includes data on the speed at which a vehicle is traveling. Is the driving public prepared to accept a system that constantly broadcasts their driving speed to road infrastructure? The answer to this may depend on the potential use of that information. If, for example, drivers believe that they will face law enforcement consequences for minor speeding offences based on the CAM message, they may choose to opt-out of participation. If the use of the speeding data is restricted to more serious offences or is only used for accident investigation purposes, then the public may be more likely to participate. All of this is untested – there has been no public discussion and no market research has been conducted. Nevertheless, these scenarios have been raised by stakeholders and they have also been the subject of discussion in the National Transport Commission (NTC) review of Intelligent Transport Systems (2013) and automated vehicles (2016).

For example, the NTC 2013 Final policy paper included a discussion of concerns relating to law enforcement access (under surveillance devices legislation) to the content of the messages. The Paper also noted that many intelligence agencies are exempt from privacy legislation. The Paper included the following recommendation:

> **Recommendation 4:** In the event that individuals can be reasonably identified from the safety data message broadcast by C-ITS devices, that specific legislative protections are developed to define in what circumstances organisations that are exempt from compliance with privacy principles, including enforcement agencies, may access C-ITS personal information.[8]

The NTC also noted that 'One of the challenges for C-ITS is that, once the data exists, if it can be legally accessed by an enforcement agency it is for the courts to determine whether the data is relevant and reliable and therefore admissible. Policy-makers must therefore understand the circumstances in which governments could legally access the C-ITS data today and – in the event that it could be accessed – whether those circumstances will be a disincentive to consumers, which in turn would reduce uptake and curb the attainable safety benefits.'[9]

In the NTC 2016 Discussion paper on automated vehicles, they reached a similar conclusion:

> 'Public perceptions about automated vehicles will be impacted by how the personal information of consumers is handled and whether there are clearly defined privacy protections. To protect consumers and provide market certainty, government access to automated vehicle data may warrant additional legislative privacy protections.'[10]

[8] Refer to: National Transport Commission (NTC), Cooperative Intelligent Transport Systems, *Final policy paper*, December 2013 <http://www.ntc.gov.au/Media/Reports/(55AFE902-73F4-073B-E6ED-AE684E3BE595).pdf>

[9] ibid

[10] National Transport Commission (NTC), Regulatory options for automated vehicles, Discussion paper, May 2016 <http://www.ntc.gov.au/Media/Reports/(049B1ED1-5761-44D5-9E3C-814A9195285D).pdf>

7.3. APP 3. Finding

Data in the C-ITS messaging system is collected fairly and lawfully, and in full compliance with APP 3. The core safety critical functions do not require explicit consent, as long as other APPs (such as openness and notice) are complied with.

The system is likely to be implemented as an opt-out system, and that is entirely appropriate for an application of this type.

However, in order to build trust and confidence in the system, and to maximise participation,[11] it may be necessary to impose some additional restrictions on the purposes for which data can be used. This could include one or both of the following options:

— **Option 1:** Limiting C-ITS participant applications to 'approved' uses that are related to the broad objectives of C-ITS (e.g. road safety, traffic management, environmental benefits etc.). This would require the establishment of some infrastructure and governance, but would have significant benefits in maintaining the quality and focus of the use of C-ITS data. This option could be implemented by the development of an industry code of practice and / or an Austroads Guide.

— **Option 2:** Limiting the use of specific data by legislative means in circumstances where the use of data may have a negative impact on participation rates (the most likely scenario here is 'speed' data, but there may be others). This would require the implementation of specific legislation, and would need to be the subject of a costs benefits analysis or a regulatory impact assessment.

There is insufficient data available at this early stage to support one of these options. Further research will have to be undertaken to understand the likely consumer concerns (and level of take-up), and to explore industry attitudes to the development of potential codes or legislation.

[11] 'An overall conclusion is that a **strong uptake** is an essential prerequisite for achieving meaningful benefits.' (page 15). See: The Platform for the Deployment of Cooperative Intelligent Transport Systems in the European Union (C-ITS Platform), Final report, January 2016

8. APP 4. Dealing with unsolicited personal information

8.1. The Law

APP 4 requires organisations who receive unsolicited personal information are required to determine whether or not they could have collected the information under APP 3. If they determine that they could *not* have collected the personal information; the information must be destroyed.

More information:
http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-4-app-4-dealing-with-unsolicited-personal-information.

8.2. C-ITS – Overview

The C-ITS messaging system is unlikely to receive unanticipated or unsolicited personal information in its day to day activities.

8.3. APP 4. Finding

This APP is not relevant to the deployment of C-ITS.

9. APP 5. Notification of the collection of personal information

9.1. The Law

APP 5 requires organisations to notify individuals of key items, including:

- The identity and contact details of the collecting party;
- The purposes of collection; and
- Any other organisations (or the types of organisations) to which the organisation usually discloses personal information.

More information:
http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information.

9.2. C-ITS – Overview

The deployment of C-ITS is likely to take the form of a complex peer-to-peer network. These types of systems are difficult to assess from a privacy compliance perspective, as privacy legislation assumes that a single organisation will be providing notice to consumers regarding the collection of their personal information.

This PIA includes advice for both 'participating organisations' and a 'central hub or central process'. However, this does not mean that a central hub or central process has to be developed. A central hub might take the form of a registration service, or simply a central contact and information point. Participating organisations will include (but not be limited to) car manufacturers, transport operators, road infrastructure providers and regulators.

The 'notice' requirements in privacy legislation represent one of the greatest challenges for the C-ITS messaging system – mainly because the lack of structure in the C-ITS environment means that there may not be clear opportunities to give all drivers 'notice' that their vehicle is broadcasting information, along with information about how that data may be used.

Also, CAM and DENM are simple broadcast messages – there is no two-way communication. This means that a vehicle transponder will not be able to determine who has read or accessed the messages. Some data uses can be anticipated in advance – for example some road operators will capture and analyse probe data for congestion management. However, some data uses cannot be anticipated in advance.

Nevertheless, privacy legislation requires users to be informed about the potential use of their data. The absolute minimum requirement is that drivers must be informed that the vehicle is broadcasting data, including a quick summary of the type of data broadcast and the potential use of that data by third parties.

Notification (APP 5)	Compliant	Relevant Exception	Notes
A. Does the entity provide notice of its identity and contact details?	To be developed	–	**Central hub / process** Required. In practice, this will be very difficult to implement. The C-ITS messaging system relies on a tamper proof, passive transponder fitted to a vehicle. The ability of this transponder to communicate with the driver will depend on other technology within the vehicle. A brief notice may be displayed (and possibly acknowledged) if the vehicle has the capacity to display a message to the driver on first use. However, this PIA presumes that the vehicle can still be operated without the driver specifically receiving or acknowledging any 'notice' regarding the operation of the transponder. Other opportunities for providing notice to the driver are limited. Many vehicles will not be driven by **owners**, so notices may have to be added to commercial leases and rental agreements. The ability of a central hub to provide appropriate notice in these circumstances is very limited. **Participating organisations** Required. Participating organisations will also face difficulties in providing appropriate notice to consumers.
B. Does the entity provide notice of third party collection? (if relevant)	To be developed	–	**Central hub / process** Required. **Participating organisations** Required.
C. Does the entity provide notice of the fact that the collection is required or authorized? (if relevant)	To be developed	–	**Central hub / process** Required. **Participating organisations** Required.
D. Does the entity provide notice of the purpose of collection?	To be developed	–	**Central hub / process** Required. **Participating organisations** Required.
E. Does the entity provide notice of the main consequences (if any) for the individual if all or some of the personal information is not collected?	To be developed		**Central hub / process** Required. Very challenging requirement. **Participating organisations** Required.
F. Does the entity provide notice of 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?	To be developed	–	**Central hub / process** Required. **Participating organisations** Required.

Notification (APP 5)	Compliant	Relevant Exception	Notes
G. Does the entity provide notice that the privacy policy contains information about how the individual may access their personal information and seek the correction of such information?	To be developed	–	**Central hub / process** Required. **Participating organisations** Required.
H. Does the entity provide notice that the privacy policy contains information about how the individual may complain?	To be developed	–	**Central hub / process** Required. **Participating organisations** Required.
I. Does the entity provide notice of whether the entity is likely to disclose the personal information to overseas recipients (and if so, where)?	To be developed	–	**Central hub / process** Required. **Participating organisations** Required.

9.3. APP 5. Finding

The C-ITS framework (here and abroad) does not yet include a standard approach regarding the provision of notice to drivers.

The 'notice' requirement in privacy legislation represents one of the greatest challenges for the C-ITS messaging system – mainly because the lack of structure in the C-ITS environment means that there may not be clear opportunities to give all drivers 'notice' of the use of their information.

The ability of the C-ITS transponder to communicate with the driver will depend on other technology within the vehicle. A brief notice may be displayed (and possibly acknowledged) if the vehicle has the capacity to display a message to the driver. Other opportunities for providing notice to the driver are limited.

Further work will be required in order to:

- 1. Identify in-vehicle mechanisms that enable a short notice to be provided to the driver (and acknowledged); and
- 2. Identify alternative processes for providing notice to drivers; and
- 3. Providing guidance or standardisation for the content of C-ITS privacy notices.

It is possible that these issues could be addressed as part of the development of an industry code of practice for vehicle manufacturers.

10. APP 6. Use or disclosure of personal information

10.1. The Law

APP 6 states that if an organisation holds personal information about an individual that was collected for a particular purpose (the primary purpose), they must not use or disclose the information for another purpose (the secondary purpose) unless the individual has consented.

More information:
http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-6-app-6-use-or-disclosure-of-personal-information.

10.2. C-ITS – Overview

This APP really concerns the role of consent in C-ITS. Consent plays an important role in privacy legislation, although it is not the only option for complying with APP 6.

In Europe, Working Group 4 from the European C-ITS Platform has been considering options for protecting privacy in the deployment of C-ITS. The European discussions are closely monitored in Australia.

The European Working Group has reached the following conclusion on the issue of consent:

> (a) Data provision conditions: Consent
>
> The data subject (owner of the vehicle and/or through the use of the vehicle or nomadic devices) decides if data can be provided and to whom, including the concrete purpose for the use of the data (and hence for the identified service). There is always an opt-out option for end customers and data subjects. This is without prejudice to requirements of regulatory applications.

The European Working Group provide some further guidance on how this might be implemented:

> It is recommended to implement the principle of 'informed consent' by providing the vehicles with ad-hoc technologies allowing to attach 'consent markers' to personal data.
>
> An opt-out possibility should be offered to the drivers, authorising the driver to shut down the broadcast, while fully informing him/her about possible adverse consequences.[12]

However, relying on consent is not the only option available for complying with privacy legislation, both in Australia and Europe.

The European Working Group has recognised that some safety critical features may not require explicit consent, and other options may be available:

> Other identified potential legal bases are 'vital interests of data subject' and 'public interest'… which could allow the processing of data without drivers' explicit consent. For C-ITS road safety and traffic management applications, where a 'vital or public interest' is at stake and is demonstrated, a limited number of applications could process the data without drivers' explicit consent, provided that the legal basis to process the data (according to the legal framework in place) and these applications are strictly defined and the data collected under these conditions are not further processed or re-purposed beyond these applications.[13]

[12] The Platform for the Deployment of Cooperative Intelligent Transport Systems in the European Union (C-ITS Platform), Final report, January 2016 <http://ec.europa.eu/transport/themes/its/doc/c-its-platform-final-report-january-2016.pdf>

[13] ibid.

There could be some substantial practical and technical issues with implementing this approach – can the broadcast be 'limited' to safety critical features? Can a system be developed that recognises 'consent markers' that have been added to data messages. There will also be considerable governance issues – who 'approves' the categorisation of features as 'safety critical'? Does this require specific legislative backing?

It is possible that these issues could be addressed as part of the development of an industry code of practice for vehicle manufacturers and / or the development of an Austroads Guide for other C-ITS participants.

The NTC 2016 Discussion paper on automated vehicles concluded that there were three possible options:

> **Option 1:** continue current approach – regulate privacy protection through Australian Privacy Principles and state-based Information Privacy Principles, or
>
> **Option 2:** Option 1, plus governments and industry develop best-practice guidance for automated vehicles, or
>
> **Option 3:** governments legislate access to automated vehicle data, including identifiable location information.[14]

The NTC states that it supports Option 1 'until the privacy risks of automated vehicles are established'. However, this Privacy Impact Assessment has identified several issues that will be very difficult to address without further specific governance arrangements for C-ITS participants. Relying on Option 1 is unlikely to work well in a complex peer to peer network like C-ITS.

APP 6 also manages the secondary use of data, which is likely to be a significant issue in C-ITS. The following is a non-exhaustive list of some potential secondary uses of C-ITS data:

- **Probe data**
  Some European deployments are considering a scenario where roadside infrastructure captures CAM data messages and uses them as probe data to support traffic management and long term planning activities for the road network. They may be interested in the routes that vehicles take, but are not interested in identifying specific vehicles. A number of Australian road authorities have similar programs in place using Bluetooth readers.
- **Statistical data**
  Massive data records for statistics in one spot (e.g. for traffic management, planning, 'accidentology') and massive records in different places for comparison purposes (e.g. social studies);
- **Big data analytics**
  Potential private initiatives to aggregate data and derive business opportunities (e.g. as a data broker) or for big data research (e.g. matching data with other data sets).

Any secondary use would have to be based on consent or an exception to APP6. The most relevant exceptions include where:

- The individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection;
- The secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order; or
- The organisation reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

[14] National Transport Commission (NTC), Regulatory options for automated vehicles, Discussion paper, May 2016 <http://www.ntc.gov.au/Media/Reports/(049B1ED1-5761-44D5-9E3C-814A9195285D).pdf>

The following table summarises the key compliance tasks relevant to APP 6:

Use or Disclosure (APP 6)	Compliant	Relevant Exception	Notes
A. Has the entity clearly defined the primary purpose of collection and identified any secondary purposes?	To be developed	–	**Central hub / process** Required. **Participating organisations** Required.
B. Will the entity only disclose personal information for a secondary purpose with consent (or a relevant exception)?	To be developed	–	**Central hub / process** Required. It may be necessary to establish a process for checking that consent has been obtained or 'approving' secondary uses that meet one of the exceptions in APP 6. **Participating organisations** Required.
C. Is any biometric information only disclosed in accordance with Clause 6.3 and the relevant OAIC Guidelines?	–	–	Not relevant.
D. Is a written note made of any disclosures that are made relying on the law enforcement exception?	To be developed	–	**Central hub / process** Required. This will be an important aspect of the deployment of C-ITS. The legislation permits disclosure of information to law enforcement agencies in a broad range of circumstances – it is very permissive – but it does require a written note to be made for each of these disclosures. **Participating organisations** Required.

10.3. APP 6. Finding

The Australian deployment of C-ITS is likely to align with European deployments, and thus the European Working Group proposal to include driver consent to C-ITS data messages being broadcast will need to be appropriately considered. In practice this will take several forms:

- The ability to opt-out of most messages that broadcast personal information;
- The use of 'consent markers' on some data messages; and
- The collection of consent for most secondary uses of data.

However, there are likely to be some exceptions to this approach. For example, some safety critical functions may be implemented without the use of 'consent markers'. Also, some secondary uses may occur relying on the APP 6 exceptions rather than consent – particularly in relation to law enforcement.

Further work is therefore required to establish a consent-based system for C-ITS messages. Tasks include:

- 1. Developing a policy and structure for determining whether data and messages are 'safety critical';
- 2. Implementing a system of 'consent markers'; and
- 3. Developing an approval structure for secondary use of data.

It is possible that these issues could be addressed as part of the development of an industry code of practice for vehicle manufacturers and / or the development of an Austroads Guide for other C-ITS participants.

11. APP 7. Direct marketing

11.1. The Law

APP 7 provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies.

More information:
http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-7-app-7-direct-marketing.

11.2. C-ITS – Overview

It is not expected that direct marketing will be a relevant issue in the implementation of C-ITS.

11.3. APP 7. Finding

This APP is not relevant to the deployment of C-ITS.

12. APP 8. Cross-border disclosure of personal information

12.1. The Law

APP 8 states that before an organisation discloses personal information to an overseas recipient, they must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information. The organisation that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient. Several exceptions apply.

More information:
http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information.

12.2. C-ITS – Overview

Cross-border Disclosure (APP 8)	Compliant	Relevant Exception	Notes
A. Has the entity identified all relevant cross border disclosure of personal information?	To be developed		**Central hub / process** Required. It is unlikely that any central organisation would need to transfer personal data across borders related to CAM or DENM messages. Some minor transfer of data may occur in relation to the management of security certificates. **Participating organisations** Some C-ITS participants, particularly vehicle manufacturers, are likely to transfer personal data outside Australia. Most vehicles will be manufactured overseas, and service centres and even the vehicles themselves may communicate with information hubs in the country of manufacture. The relevance of these communications to C-ITS is unknown at this early stage. Also, the transponder is likely to be fitted overseas, and the station ID of the transponder may need to be communicated across borders.
B. Has the entity taken such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs? (unless a relevant exception applies)	To be developed		**Central hub / process** Required. **Participating organisations** Required. Each participating organisation will need to ensure compliance with APP 8.

12.3. APP 8. Finding

It is likely that some C-ITS participants will transfer data overseas, particularly vehicle manufacturers. Each participating organisation will need to ensure compliance with APP 8.

13. APP 9. Adoption, use or disclosure of government related identifiers

13.1. The Law

APP 9 states that an organisation must not adopt a government related identifier of an individual as its *own* identifier. In addition, an organisation must not use or disclose a government related identifier of an individual unless the use or disclosure is reasonably necessary for the organisation to verify the identity of the individual. Some other exceptions apply, but these are not relevant to the deployment of C-ITS.

More information:
http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-9-app-9-adoption-use-or-disclosure-of-government-related-identifiers.

13.2. C-ITS – Overview

The C-ITS does include a unique transponder identifier that may potentially be linked to a vehicle identifier. However, it is not based on any exiting government issued identifier.

13.3. APP 9. Finding

This APP is not relevant to the implementation of C-ITS.

14. APP 10. Quality of personal information

14.1. The Law

APP 10 requires organisations to take reasonable steps to ensure that the personal information it collects and uses is accurate, up-to-date and complete.

More information:
http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-10-app-10-quality-of-personal-information.

14.2. C-ITS – Overview

Road operators capturing CAM and DENM messages using a roadside unit are not requesting any information – they are simply receiving standardised messages broadcast in a channel. If they deems that the information is trustworthy they may use the message (and in some circumstances, store it). However, they do not have the means to determine whether the data that they receives are accurate. Thus, not really sure what other steps a road operator could take to ensure accuracy.

Data Quality (APP 10)	Compliant	Relevant Exception	Notes
A. Has the entity taken such steps (if any) as are reasonable in the circumstances to ensure that the personal information **collected** is accurate, up-to-date and complete?	To be developed	–	**Central hub / process** Required. **Participating organisations** Required.
B. Has the entity taken 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?	To be developed	–	**Central hub / process** Required. **Participating organisations** Required.

14.3. APP 10. Finding

This is a high level Privacy Impact Assessment (PIA), being conducted prior to the actual deployment or implementation of C-ITS. At this early stage, it is not possible to determine whether there any data quality issues in the system.

No major compliance issues with APP 10 are anticipated, although some further checks should be conducted following implementation.

15. APP 11. Security of personal information

15.1. The Law

APP 11 requires organisations to take such steps as are reasonable in the circumstances to protect personal information from misuse, interference and loss; and from unauthorised access, modification or disclosure.

Also, if the organisation no longer needs the information for any purpose for which the information may be used or disclosed, they must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

More information:
http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-11-app-11-security-of-personal-information

APP 11 has a very wide scope for interpretation, as it includes multiple tests for what is 'reasonable in the circumstances'. Some additional guidance is available from the Office of the Australian Information Commissioner (OAIC) in the form of guidelines:

> *Guide to securing personal information*, OAIC, 2015 <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-securing-personal-information>

15.2. C-ITS Overview

With regards to security of the data messages, the international model that is emerging involves each CAM and DENM being signed using Public Key Infrastructure (PKI) to verify its authenticity.

The 2016 European Working Group report states:

> Security is paramount to the deployment of C-ITS in the EU. No security, no C-ITS.

Austroads is currently reviewing potential requirements for a localised C-ITS Security Credential Management System (SCMS). This high-level Privacy Impact Assessment is not intended to replace the requirement for a more specific security review.

However, some high-level observations regarding security issues may be useful for Austroads.

1. Risk assessment

The OAIC Guidelines mentioned above require organisations to conduct a risk and vulnerability assessment.

2. Data destruction

There is a specific requirement in APP 11 (see APP 11.2), and a clear recommendation in the OAIC Guidelines (see page 39) to develop a detailed data destruction plan.

3. Broadcast data

The 2016 European Working Group Report notes:

> CAN/DENM messages are not encrypted. Thus a 'rogue' actor could eavesdrop and illegally process the data exchanged via CAN/DENM. This issue is typical of applications using broadcast communications and not specific to C-ITS. A parallel can be drawn with Wi-Fi or mobile devices where personal information can also be collected and processed.

The ability of third parties to 'eavesdrop' on broadcast messages was also mentioned in some stakeholder discussions. A more detailed security review could consider the potential impact of eavesdropping, and consider conducting a cost-benefit analysis of steps to counter eavesdropping (such as encrypting the content of the messages). Although it is unlikely to be feasible for encryption to be used with C-ITS messaging (as it adds latency and could prevent C-ITS from achieving its safety benefits), this issue should at least be discussed as part of a risk and vulnerability assessment.

4. Certificate revocation and incident reporting

The C-ITS implementation is based on a Public Key Infrastructure. The Austroads concept of operations for core C-ITS functions paper notes the existence of some specific PKI security issues that may require further consideration.

In particular, certificate revocation lists (CRLs) may be used for misbehaviour management to expel misbehaving C-ITS devices for the secure bounded managed domain. The emerging US and EU platforms are only starting to determine how to implement misbehaviour management. It is not clear if certificate revocation lists will be sent to vehicles as a core data message. The large size of the certificate revocation lists could create communication capacity issues.

Certificate Revocation Lists are an important security measure, but they also rise privacy risks, as they can leave a record of organisations that have accessed the CRL, including the time and location of the request.

Security (APP 11)	Compliant	Relevant Exception	Notes
A. Has the entity taken such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss?	To be developed		**Central hub / process** Required. **Participating organisations** Required.
B. Has the entity taken such steps as are reasonable in the circumstances to protect the information from unauthorised access, modification or disclosure?	To be developed		**Central hub / process** Required. **Participating organisations** Required.
C. Does the level of security in the application match the potential harm caused by breaches of privacy?	To be developed		**Central hub / process** Required. **Participating organisations** Required.
D. Will detailed access trails be retained and scrutinised for security breaches?	To be developed		**Central hub / process** Required. **Participating organisations** Required.

Security (APP 11)	Compliant	Relevant Exception	Notes
E. Will a data retention policy / destruction schedule be developed which requires retention of personal information only for the period required for use?	To be developed		**Central hub / process** Required. **Participating organisations** Required.
F. Is personal information de-identified as soon as possible?	To be developed		**Central hub / process** Required. **Participating organisations** Required.

15.3. APP 11. Finding

This is a high level Privacy Impact Assessment (PIA), being conducted prior to the actual deployment or implementation of C-ITS. Many of the security issues in C-ITS are only at a very early stage of discussion.

Privacy legislation requires organisations to undertake a risk and vulnerability assessment, and to develop a data destruction plan. These two items should be added to the work plan for the deployment of C-ITS in Australia.

16. APP 12. Access to personal information

16.1. The Law

APP 12 requires organisations to provide, on request by the individual, access to any of their own personal information. A long and complex list of exemptions apply, most of which are not relevant in the day-to-day running of the C-ITS.

More information:
http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-12-app-12-access-to-personal-information.

16.2. C-ITS – Overview

Access (APP 12)	Compliant	Relevant Exception	Notes
A. Can the individual ascertain whether the entity has records that contain personal information, the nature of that information and the steps that the individual should take to access their record?	To be developed		**Central hub / process** Required. **Participating organisations** Required.
AGENCIES **B.** If an agency holds personal information about an individual, does the agency, on request by the individual, give the individual access to the information? (unless relevant exceptions apply in FOI legislation)	To be developed		
ORGANISATIONS **C.** If an organisation holds personal information about an individual, does the organisation, on request by the individual, give the individual access to the information? (unless relevant exceptions in the Privacy Act apply)	To be developed		
AGENCIES **D.** Will information be provided within 30 days?	To be developed		
ORGANISATIONS **E.** Will information be provided within a reasonable period?	To be developed		
AGENCIES **F.** Will accessing personal information be provided at no cost?	To be developed		
ORGANISATIONS **G.** Will the costs incurred in accessing personal information be reasonable?	To be developed		

16.3. APP 12. Finding

The C-ITS framework presents some challenges in terms of access. It is a complex peer to peer network, and no single entity may have a view of all the data collected about a single individual. Most data will be pseudonymised and difficult to extract for a single C-ITS participant.

In order to manage consumer expectations and to drive consistency across the C-ITS network, some additional work may need to be undertaken on developing an appropriate C-ITS access policy. These tasks could include:

- Developing a standard access request policy across the whole network;
- Seeking agreement from all C-ITS participants to meet the higher standards in APP 12 (e.g. providing access within 30 days at no cost, even though there are exceptions to these requirements available to some organisations);
- Explore solutions to ‘keep it simple’ for the consumer, such as a single access request form.

Compliance with these requirements could potentially be made a condition of participation in C-ITS, although this may be challenging if there is no central hub or central regulator for C-ITS. It is possible that these issues could be addressed as part of the development of an industry code of practice for vehicle manufacturers and / or the development of an Austroads Guide for other C-ITS participants.

17. APP 13. Correction of personal information

17.1. The Law

APP 13 requires organisations to correct information if, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading. Corrections must be notified to relevant third parties. A long and complex list of exemptions apply, most of which are not relevant in the day-to-day running of the C-ITS.

More information:
http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-13-app-13-correction-of-personal-information

17.2. C-ITS – Overview

Correction (APP 13)	Compliant	Relevant Exception	Notes
UPON REQUEST **A.** Does the entity take such steps (if any) as are reasonable in the circumstances to correct that information?	To be developed		**Central hub / process** Required. **Participating organisations** Required.
UPON LEARNING OF INACCURACIES **B.** Does the entity take such steps (if any) as are reasonable in the circumstances to correct that information? (where the inaccuracy relates to a purpose for which the information is held)	To be developed		**Central hub / process** Required. **Participating organisations** Required.
UPON REQUEST ONLY **C.** Will corrections and annotations be disseminated to third parties to whom personal information has previously been disclosed?	To be developed		**Central hub / process** Required. **Participating organisations** Required.
UPON REQUEST ONLY **D.** Will the entity take such steps as are reasonable in the circumstances to associate a statement by the data subject that the accuracy of the information is challenged in such a way that will make the statement apparent to users of the information?	To be developed		**Central hub / process** Required. **Participating organisations** Required.
AGENCIES (Government) **E.** Will requests for corrections be addressed within 30 days?	To be developed		
ORGANISATIONS (Private sector) **F.** Will requests for corrections be addressed within a reasonable period?	To be developed		

17.3. APP 13. Finding

This is a high level Privacy Impact Assessment (PIA), being conducted prior to the actual deployment or implementation of C-ITS. At this early stage, it is not possible to determine whether there any issues regarding correction.

No major compliance issues with APP 13 are anticipated, although some further checks should be conducted following implementation.

18. Data Breach Notification Requirements

18.1. The Law

Australia does not impose mandatory data breach notification requirements on organisations. However, *voluntary* guidelines are in place:

> OAIC, *Data breach notification — A guide to handling personal information security breaches*, 2014, <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches>

There is no current data on the number of organisations who have adopted the voluntary guidelines, but the expectation is that larger organisations with high risk data sets should at least consider adopting the guidelines.

The OAIC guidelines are quite complex, but the best practice requirements are summarised as follows:

- Is there a data breach response plan and does it flow logically from any broader information security plan?
- Is the plan regularly tested?
- Does the plan include a strategy to assess and contain breaches?
- Does the plan clearly identify those actions that are legislative or contractual requirements?
- Are your staff educated about the plan and how to identify and respond to data breaches?
- Does the plan enable staff to identify data breaches and require that breaches be reported?
- Does the plan establish clear lines of command and indicate responsible officers?
- Does the plan outline clearly when affected individuals should be notified of breaches?
- Does the plan include a strategy to identify and address any weaknesses in data handling/data security that contributed to the breach?

It is possible that the Australian Government may pass mandatory data breach notification rules at some point in the near future. The issue is the source of ongoing debate in Canberra.

18.2. C-ITS Overview

The C-ITS framework presents some challenges in terms of data breach notification. It is a complex peer to peer network, and no single entity may have responsibility for managing data breaches across the entire system.

Also, most data will be pseudonymised and it will be difficult to know whether any specific data breach will lead to a release of personal information. There may be a risk of 'overkill' if drivers are notified about a data breach where there is very little risk that individuals can be identified from the data, without considerable access to additional data.

Nevertheless, it is now best practice for organisations to develop a data breach response plan. In the C-ITS framework this may need to be developed by the C-ITS central hub (if one exists) or by each C-ITS participant. At this stage, the relevant organisations should adopt plans that comply with the OAIC Guidelines. This approach will need to be updated if mandatory data breach notification legislation is implemented.

18.3. Data Breach Notification Requirements Finding

It is now best practice for organisations to develop a data breach response plan. In the C-ITS framework this may need to be developed by a C-ITS central function or process, or by each C-ITS participant. At this stage, the relevant organisations should adopt plans that comply with the OAIC Data Breach Notification Guidelines (2014).

19. Future Programs and Governance

19.1. C-ITS Overview

Governance will be a vital issue in the deployment of C-ITS, but there is no clear structure or framework for ensuring privacy protection in C-ITS at this early stage.

A process may need to be established in order to approve / reject applications for use of the CAM and DENM data, including any secondary use, in order to provide assurances to consumers regarding the use of their data. However, it is not clear at this stage how this process would be implemented.

The benefits of an overall privacy governance arrangement are that one organisation can conduct regular reviews and audits, and can from complaints and implement systemic improvements. It is difficult to see how this can be achieved in a complex peer to peer network.

It is possible that many of the issues raised in this privacy review could be addressed as part of the development of an industry code of practice for vehicle manufacturers and / or the development of an Austroads Guide for other C-ITS participants. However, it is important to note that in Australia a privacy code of practice can only be approved by the Office of the Australian Information Commissioner if it is equivalent to (or stronger than) the APPs.

The National Transport Commission is currently conducting a public consultation on automated vehicles. They also consider whether a code of practice could play a role:

> Guidance could take the form of a privacy code, registered by an industry group with a privacy commissioner. A privacy code can exempt parties from a particular element of the privacy principles, or ensure that parties otherwise exempt from the Australian Privacy Principles, such as small businesses and state agencies, could voluntarily agree to a common approach. A privacy code could also provide a framework to enable industry to agree to common protections and processes.[15]

However, the NTC conclude that it is 'too early' to pursue a code of practice at this time, and that more work should be done on identifying privacy risks.

19.2. Finding

It will be difficult to implement C-ITS in Australia relying only on general compliance with existing privacy legislation. The complex peer to peer network at the heart of C-ITS does not include an entity or a structure that can maintain a level of oversight or governance for data protection.

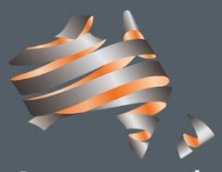
It may be necessary to enhance privacy protection through the development of an industry code of practice for vehicle manufacturers and / or the development of an Austroads Guide for other C-ITS participants.

[15] National Transport Commission (NTC), Regulatory options for automated vehicles, Discussion paper, May 2016 <http://www.ntc.gov.au/Media/Reports/(049B1ED1-5761-44D5-9E3C-814A9195285D).pdf>

20. Appendix 1 – Information Review

The following information resources were supplied to Galexia or were publicly available as at June 2016.

Doc ID	Document Citation	Status
1.	National Transport Commission (NTC), Cooperative Intelligent Transport Systems, Final policy paper, December 2013. <http://www.ntc.gov.au/Media/Reports/(55AFE902-73F4-073B-E6ED-AE684E3BE595).pdf>	Public
2.	National Transport Commission (NTC), Regulatory options for automated vehicles, Discussion paper, May 2016. <http://www.ntc.gov.au/Media/Reports/(049B1ED1-5761-44D5-9E3C-814A9195285D).pdf>	Public
3.	Standing Council on Transport and Infrastructure, Policy Framework for Intelligent Transport Systems in Australia, 2012. <http://transportinfrastructurecouncil.gov.au/publications/files/ITS_Framework.pdf>	Public
4.	Austroads, Cooperative ITS Strategic Plan, 2012. <https://www.onlinepublications.austroads.com.au/items/AP-R413-12>	Public
5.	Austroads, Concept of Operations for C-ITS Core Functions, 2015 <https://www.onlinepublications.austroads.com.au/items/AP-R479-15>	Public
6.	ETSI EN 302 637-2 (2014-11) (European Standard), Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, <www.etsi.org>	Public
7.	ETSI EN 302 637-3 (2014-11) (European Standard), Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service, <www.etsi.org>	Public
8.	The Platform for the Deployment of Cooperative Intelligent Transport Systems in the European Union (C-ITS Platform), Final report, January 2016. <http://ec.europa.eu/transport/themes/its/doc/c-its-platform-final-report-january-2016.pdf> (Working Group 4 (WG.4) considered data protection and privacy issues).	Public
9.	National Transport Commission (NTC), Regulatory options for automated vehicles, Discussion paper, May 2016 <http://www.ntc.gov.au/Media/Reports/(049B1ED1-5761-44D5-9E3C-814A9195285D).pdf>	Public



Austroads

Level 9, 287 Elizabeth Street
Sydney NSW 2000 Australia

Phone: +61 2 8265 3300

austroads@austroads.com.au
www.austroads.com.au