National Transport Commission

Cooperative Intelligent Transport Systems Policy Paper

Report prepared by: National Transport Commission

ISBN: 978-1-921604-47-8
Report outline

Title: Cooperative Intelligent Transport Systems: final policy paper

Type of report: Final policy paper

Purpose: For information

Abstract: This paper follows the Cooperative Intelligent Transport Systems Regulatory Policy Issues Paper published in November 2012 and comments from the submissions subsequently received. This paper proposes final positions in key policy issues and identifies other issues which need to be further addressed.

Key milestones: Approved by the Standing Council on Transport and Infrastructure – November 2013.

Key words: Cooperative Intelligent Transport Systems; privacy; liability; driver distraction; compliance and enforcement; technology; human risk factors; road safety.

Contact: National Transport Commission
L 15/ 628 Bourke Street
Melbourne VIC 3000
Ph: (03) 9236 5000
Email: enquiries@ntc.gov.au
www.ntc.gov.au
Foreword

Road trauma in Australia accounts for almost 1,300 deaths each year¹ and costs the nation an estimated $27 billion per annum.² Congestion on our roads has a major impact on productivity, air quality and carbon emissions and these impacts are likely to increase in future as the freight task rises. The introduction of Cooperative Intelligent Transport Systems (C-ITS) has the potential to improve outcomes in all of these areas.

C-ITS refer to the use of wireless communication technologies to enable different parts of the transport network to share information to improve decision making and optimise transport outcomes. C-ITS represent an opportunity to advance Australia’s road safety, through vehicles and infrastructure sharing vital information which could help avoid collisions. The technology will also offer productivity and environmental advancements through improved traffic management and decision-making by drivers. Once established as a platform, this technology can potentially be used across modes and for a variety of purposes.

While we are excited about the new opportunities offered by C-ITS, we also realise the implementation of technology with potentially broad uses needs to be carried out carefully and needs to be consistent with approaches to existing technologies. The National Transport Commission (NTC) published a Discussion Paper in November 2012 on the key regulatory policy issues, in particular the impacts on liability, privacy, compliance and enforcement and driver distraction. The Discussion Paper generated submissions from a wide range of stakeholders. The final policy paper is the culmination of this work.

This policy paper analyses the risks, barriers and potential regulatory reforms required to ensure a national, harmonised platform for C-ITS technologies, that ensures the best safety outcomes and respects the privacy of individuals. A number of these issues will need further examination as transport technologies continue to evolve.

I would like to thank all those individuals and organisations involved in the consultation to date and especially those who have made written submissions. I would also like to acknowledge the assistance of Stuart Ballingall and the Austroads C-ITS Steering Committee. Finally I would like to thank the NTC staff who developed this report, in particular Sarah Jones, Marcus Burke and James Williams.

Greg Martin PSM
Chairman

Executive summary

Introduction
The ability for vehicles and infrastructure to share information could be the next significant step forward in road safety and productivity. Cooperative Intelligent Transport Systems (C-ITS) is the term used to describe technology which allows vehicles to become connected to each other and to other parts of the transport network. In addition to what drivers can immediately see around them, and what vehicle sensors can detect, all parts of the transport system will increasingly be able to share information to improve driver decision making. This should significantly improve safety, through avoiding collisions, but also assist in ameliorating congestion and improving traffic flows. Once the basic technology is in place as a platform, an array of applications can be developed, some of which can’t be foreseen.

The National Transport Commission (NTC) has examined the potential regulatory policy issues linked to the roll out of this technology, in particular in the areas of liability, privacy, compliance and enforcement and driver distraction. The NTC published a Discussion Paper, Cooperative Intelligent Transport Systems Regulatory Policy Issues, in November 2012 for public consultation and received submissions from a wide range of organisations and individuals. The submissions provided very valuable feedback on the issues from a range of perspectives as well as raising a number of issues that hadn’t been considered in the original paper. The NTC sought to explore these policy implications in detail in order to ensure that Australia is prepared for the introduction of this technology. A failure to do so could result in either:

- the technology not being used in Australia (or not being used to its full extent), due to a lack of a policy framework to support its introduction, and hence Australia missing out on the benefits of the technology; OR

- the technology being introduced to Australia but the risks not being adequately managed due to a lack of appropriate legislative and policy frameworks.

A major concern expressed in submissions was around the potential data generated by such systems and whether this information would be able to be used to identify individuals. There are a number of ways that these concerns can be addressed, but this will depend in part on the institutional arrangements that are decided upon, along with technical implementations of the technology. The constantly developing and evolving technology creates a challenge for policy makers in setting rules.

This report makes a series of recommendations on policy and further research for consideration. Importantly, the NTC did not find any legislative roadblocks to the deployment of the technology in Australia, but a number of areas have been identified that may require further review. At the same time, the NTC agrees that there is a need for the safety benefits of the technology to be further proven before governments provide any incentives to increase uptake.

Australia will need to continue to involve itself in international standards groups to ensure that it has a voice in the standards setting process. Australian governments will also need to follow closely the results of pilots happening here and overseas to ensure that decisions are based upon the best possible data. C-ITS could be a transformative technology in the transport network, and whilst this paper aims to advance policy in this area, further work will be required.

Liability
It is expected that the introduction of C-ITS safety technology will reduce the number of crashes significantly. However crashes would still occur due to a variety reasons, including potentially failures of C-ITS systems, poor design or failures by drivers to react appropriately to warnings. As transport technology advances, the issue of who is liable in the event of a crash will potentially become more complex. The question of how liability would be resolved in the event of C-ITS system failure will be important in providing certainty to drivers, manufacturers, insurers and road managers.
The laws around liability have evolved over decades and have been adapted to a variety of situations. They have, in general, adequately been applied to new technology that has appeared, including in the transport sector. Any changes would have to be made with extreme care, in order not to disturb the appropriate allocation of risks between parties, nor adversely affect the balance between innovation and safety.

Research and stakeholder consultation indicates that liability has not been a significant hindrance to the development of new technology in the past, including in the transport sector. C-ITS technology does not appear to be sufficiently different to create a special case. As such there does not appear to be a strong case to make changes and it is recommended that no changes are made to the current approach. Further research may, however, be required on human factor issues and the implications of increasingly automated vehicles.

**Policy Finding:** No changes are recommended to current laws and approaches around liability for drivers, manufacturers and road managers in regard to the roll out of C-ITS technology.

### Privacy

Many C-ITS technologies use location as a key piece of information. The potential for this information to be linked to an individual naturally raises privacy concerns. The NTC C-ITS Discussion Paper separately examined privacy and compliance and enforcement issues; these are dealt with in the one privacy section in this paper, as both raise the key issues (amongst others) of what data is collected, who has access to it, how it can be linked to an individual and what purposes it can be used for.

Privacy issues are in part dependent upon technology and security standards still under development by international standards bodies, manufacturers and governments. Institutional arrangements for C-ITS, such as which bodies would manage key functions, are also still to be decided both in Australia and overseas. Australia must ensure that privacy considerations guide decision making in these areas.

**Policy Finding:** No changes are recommended to current privacy laws governing the private sector development of C-ITS systems and data. Companies will need to closely follow the National Privacy Principles as required, as they do for C-ITS systems that have already been developed.

**Policy Finding:** Privacy concerns represent a potential barrier to the take-up of technology that could significantly improve road safety. Australia should aim for the highest level of privacy protection in the standards set for C-ITS safety systems. This is in keeping with emerging international standards.

**Recommendation 1:** That Austroads adopt privacy by design principles, including the undertaking of a privacy impact assessment, in the development of the C-ITS operational framework.

**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.

**Recommendation 3:** That Australian Ministers explicitly consider privacy impacts on drivers in any decision relating to institutional arrangements for C-ITS. In particular, any entity that manages and stores unique identifiers is separate from agencies which hold licensing and registration information.

**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.
Driver Distraction

Driver distraction has become an increasing concern for road safety experts, with the increasing range of technologies within vehicles creating the potential for drivers to have their attention diverted from the driving task. C-ITS technology has the potential to create further distractions if not implemented correctly. The NTC Discussion paper also examined whether there are barriers within existing legislation to limits on the use of C-ITS devices by drivers.

However, C-ITS applications are one part of a wide range of technologies that are present in today’s vehicles. Driver distraction is an issue that is broader than C-ITS and must be addressed in a holistic way. C-ITS applications do, however, add weight to the need for governments to look more closely at distraction issues. Recent changes recommended to the Australian Road Rules go some way to ensuring that the approach in Australia is technology neutral.

**Policy Finding:** That current rules around distraction should not present a barrier to the deployment of C-ITS technology. Distraction issues raised by this technology should be considered as part of any broader review of driver distraction rather than in isolation.

**Recommendation 5:** That the NTC should ensure that the Australian Road Rules Maintenance Group considers C-ITS in any future revisions of the Australian Roads Rules, in order to accommodate the emerging role of C-ITS applications and other Advanced Driver Assistance Systems (ADAS) and to take into account emerging international standards relating to technology and distraction.

Incentives

Feedback on the Discussion Paper clearly indicated that further evidence of the safety and productivity benefits of C-ITS technology was required before incentives are considered. The NTC agrees that whilst much of the technology has been functionally demonstrated, there is a need for the productivity and safety benefits of C-ITS to be further proven before governments provide any new incentives for its roll out.

**Policy Finding:** There is a need for the safety benefits of C-ITS technology to be proven more fully before governments provide any new incentives towards its implementation.

Other issues

The submissions received and further analysis of the key policy areas raised a number of issues that may require further research and analysis. In particular they raised the need for further consideration of:

- Human factor issues in relation to C-ITS technology
- The impact of increasingly automated vehicle systems

The NTC recommends further research in these areas, which will be key to attaining the potential safety benefits of this technology.

**Recommendation 6:** That research, based on identified gaps in international research that are relevant to Australia, is conducted to measure the human factor impacts of C-ITS applications; and to determine whether any mitigating policy measures are required in order to obtain the safety benefits without creating additional risks.

**Recommendation 7:** That research, based on identified gaps in international research that are relevant to Australia, examine the impact of more automated vehicles from a policy and legislative perspective, including the impact on the role of the driver.
In addition, a number of stakeholders raised concerns about the effect of C-ITS technology on vulnerable road users, such as motorcyclists, cyclists and pedestrians. If these road users are not adequately considered at the planning stage, there is a risk that the roads could be made safer for some road users, but more dangerous for others.

**Recommendation 8:** That in the development of the C-ITS operational framework, Austroads explicitly takes into consideration the differential impact of C-ITS on vulnerable road users, including pedestrians, motorcyclists and cyclists.
# Table of contents

## Report outline
- Foreword...iii
- Executive summary...v
- 1. Introduction...1
  - 1.1 Australian road safety and cooperative intelligent transport systems...1
  - 1.2 Purpose...2
  - 1.3 Background and methodology...3
  - 1.4 Scope of issues...3
  - 1.5 What are cooperative intelligent transport systems?...3
  - 1.6 Establishing a C-ITS framework for Australia...5
  - 1.7 What is Dedicated Short Range Communication?...5
  - 1.8 C-ITS is multi-media...6
  - 1.9 Data messages broadcasted by C-ITS...7
  - 1.10 Summary and Conclusions...8
- 2. Liability...9
  - 2.1 Introduction to the issue...9
  - 2.2 Stakeholder feedback...10
  - 2.3 Policy Position...11
- 3. Privacy...13
  - 3.1 Privacy and the private sector...13
    - 3.1.1 Introduction to the issues...13
    - 3.1.2 Unique identifiers...14
    - 3.1.3 How surveillance laws relate to the privacy principles...15
    - 3.1.4 Surveillance device laws...15
    - 3.1.5 National Privacy Principles...16
    - 3.1.6 Stakeholder feedback...17
    - 3.1.7 Policy position...19
  - 3.2 Privacy and governments...20
    - 3.2.1 Introduction to the issues...20
    - 3.2.2 Stakeholder feedback...24
    - 3.2.3 Policy position...25
- 4. Driver Distraction...27
  - 4.1 Introduction to the issue...27
    - 4.1.1 Australian Road Rules...27
  - 4.2 Stakeholder feedback...27
  - 4.3 Policy Position...30
- 5. Incentives...31
  - 5.1 Introduction to the issue...31
  - 5.2 Stakeholder feedback...31
  - 5.3 Policy Position...32
- 6. Other issues...33
  - 6.1 Human Factors...33
  - 6.2 Automated systems...34
  - 6.3 International Standards...36
  - 6.4 Vulnerable road users...36
  - 6.5 Other Stakeholder feedback...37
List of tables

Table 1. Type of communications modes in connected vehicles: 6
Table 2. Submissions received from the discussion paper 43

List of figures

Figure 1. Total road fatalities and fatality rate 2
Figure 2. Serious injuries due to road accidents 2
Figure 3. C-ITS collision avoidance example 4
Figure 4. Vehicles broadcasting C-ITS information 8
Figure 3: Spectrum of advanced driver assistance systems 36
1. Introduction

1.1 Australian road safety and cooperative intelligent transport systems

‘Cars talking to each other is the future of motor safety’
US Transportation Secretary Ray LaHood

The number of road deaths in Australia, whilst falling, remains at almost 1,300 per year, with the annual economic cost of road crashes estimated at $27 billion per annum. Cooperative Intelligent Transport System (C-ITS) applications represent an opportunity to significantly reduce these figures and the incalculable trauma that goes along with them. C-ITS applications are part of an emerging trend of technology seeking to move from helping people to survive crashes to avoiding crashes altogether.

Australia’s National Road Safety Strategy sets the vision that “no person should be killed or seriously injured on Australia’s roads.” Australia has adopted a Safe Systems approach as part of its strategy. The Safe Systems approach includes the guiding principles that:

1. People make mistakes.
2. Humans are physically frail.
3. The road transport system should be ‘forgiving.’

The approach has four ‘cornerstone’ safe systems:

- Safe roads
- Safe speeds
- Safe vehicles
- Safe people

C-ITS are a key technology to support safer vehicles. Indeed the Strategy describes safe vehicles as:

Vehicles which not only lessen the likelihood of a crash and protect occupants, but also simplify the driving task and protect vulnerable users. *Increasingly this will involve vehicles that communicate with roads and other vehicles*, while automating protective systems when crash risk is elevated. [emphasis added]

However C-ITS can also support other areas, such as encouraging safer speeds by providing information on local speed zones. This may include vehicles sharing information with other vehicles, with roadside devices or with other parts of the network. Significant potential benefits have been estimated for C-ITS safety applications. Research in the United States suggested that C-ITS safety systems have the potential to affect 80 per cent of road collisions involving unimpaired drivers. An Austroads and Monash University Accident Research Centre (MUARC) study in Australia concluded that C-ITS applications could provide a 25-35 per cent reduction in serious casualties from road collisions. However, these are currently estimates and will need to be further quantified through various trials taking place around the world.

Australia has made significant progress in reducing both the number and rate of road fatalities, however serious injuries have in fact risen (see Figure 1 and Figure 2 below). C-ITS safety

---

[6] Ibid.
applications form part of a new wave of vehicles technologies which are moving from helping
drivers and passengers simply to survive crashes towards helping to avoid crashes altogether.

Figure 1. Total road fatalities and fatality rate

![Graph showing total road fatalities and fatality rate](image)


In addition, C-ITS applications can assist in improving productivity and environmental outcomes,
through improving the flows of traffic around the network.

1.2 Purpose

C-ITS technology is currently being extensively tested and developed in different parts of the world
and new vehicles rolling off the production line are becoming more and more connected. The ability
for cars, heavy vehicles, trains, trams, buses, cyclists, motorcycles and parts of the infrastructure to
share information has significant possibilities for improving safety, productivity and environmental
outcomes. However, this technology also raises potential policy implications. The National
Transport Commission (NTC) has sought to explore these policy implications in detail in order to
ensure that Australia is prepared for the introduction of this technology. A failure to do so could result in either:

- the technology not being used in Australia (or not being used to its full extent), due to a lack of a policy framework to support its introduction, and hence Australia missing out on the benefits of the technology; OR

- the technology being introduced to Australia but the risks not being adequately managed due to a lack of appropriate legislative and policy frameworks.

1.3 Background and methodology

The NTC published *Cooperative ITS Regulatory Policy Issues* in November 2012.\(^{10}\) It was based on significant desktop research, along with discussions with key industry and government stakeholders.

The Discussion Paper received 24 submissions from a wide range of stakeholders, including individuals, government, transport associations and manufacturers. The submissions received are listed in Appendix 1 and are available for download from the NTC website.\(^ {11}\) Both the Discussion Paper itself and the submission covered a wide range of topics.

1.4 Scope of issues

In its Discussion Paper, the NTC considered the impact of C-ITS applications in four major areas of regulatory policy:

1. **Privacy** – C-ITS applications generate significant volumes of data. This raises questions around whether such data could be linked to individuals and how C-ITS applications fit within current privacy regimes in Australia dealing with the collection, use and disposal of personal information.

2. **Liability** – as transport technology advances, the issue of who is liable in the event of a crash will likely become more complex. The question of how liability would be resolved in the event of C-ITS system failure will be important in providing certainty to drivers, manufacturers and road managers.

3. **Driver distraction** – existing rules govern the use of technology designed to prevent the driver from being distracted from the driving task. An assessment is required of how C-ITS applications fit within these existing rules and whether they raise additional risks.

4. **Compliance and enforcement** – the role of C-ITS applications within existing road compliance and enforcement activities, in particular in relation to the purposes for which C-ITS information can be used, will be critical for providing certainty to drivers on how they will be treated.

Note that in this final paper, privacy and compliance and enforcement issues are considered together; both issues turn on the questions of how C-ITS data is managed. This expanded privacy section is instead divided into government and private sector considerations.

Once vehicles are able to share information at close range, there will be a large (indeed unknown) number of applications that may run on that platform. This represents a significant challenge given the unknown extent of C-ITS applications. This report examines the policy implications of the platform and the potential range of applications that may run on it. It will avoid discussion of individual applications, except where this is required for purposes of illustration.

1.5 What are cooperative intelligent transport systems?

‘Intelligent Transport Systems’ (ITS) is an umbrella term describing the use of information and communication technology in the transport network to improve transport outcomes. The term ‘Cooperative Intelligent Transport Systems’ refers to a particular subset of ITS in which the different elements of the transport network – vehicles, roads, infrastructure – *share* information with each other to improve these outcomes. In C-ITS applications, these components of the transport network...


effectively ‘talk’ to each other, providing valuable information, including facts on conditions, incidents and traffic, enabling the coordination of movements and the avoidance of collisions.

In Europe, C-ITS have been described as:

*ITS systems based on vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I, I2V) and infrastructure-to-infrastructure (I2I) communications for the exchange of information ... Co-operative ITS is a subset of the overall ITS that communicates and shares information between ITS stations to give advice or facilitate actions with the objective of improving safety, sustainability, efficiency and comfort beyond the scope of stand-alone systems.*

The concept is most easily understood with an example. One potential C-ITS application, illustrated at Figure 1, involves vehicles broadcasting a signal as they approach an intersection, giving their location, speed and direction. Other vehicles approaching the same intersection could receive these signals and hence be aware of the first vehicle’s approach, even if the driver’s view was obstructed. An in-vehicle warning could be provided to both drivers if their trajectories indicated an imminent collision.

**Figure 3. C-ITS collision avoidance example**

Image courtesy of Cohda Wireless

A further collision avoidance example involves rail crossings. A trial by La Trobe University and Public Transport Victoria demonstrated the potential for this technology to provide warnings to car drivers of approaching trains at level crossings; this is particularly vital at crossings in rural areas that do not have boom gates and bells. This second example illustrates another important feature of C-ITS – the fact that it can be multi-modal. C-ITS could potentially assist in avoiding collisions between cars and trams; allow bicycles to indicate their location to nearby cars; or improve the movement of heavy vehicles and trains at ports. The potential applications are extensive and will continue to expand.

This technology is developing rapidly around the world. In the United States, a major pilot involving 2,800 vehicles and running for 12 months around Ann Arbor Michigan was due to report its findings at the time of writing. This will provide much more detailed information on the potential benefits and will be a key input into a decision on whether to mandate the technology. Whilst mandation is not currently being considered in Australia, decisions in the United States will have a worldwide impact on the uptake of the technology.

There is also significant work occurring at the international standards level to establish common standards, including for interoperability, security and privacy. Australia has been very involved in a number of key ISO committees and it will be important for Australia to align technical approaches with emerging standards.

In Australia, the Commonwealth and New South Wales governments have announced funding for the Cooperative Intelligent Transport System Initiative (CITI) Project, which is seeking to develop a

---

12 European Committee for Standardisation and ETSI, ‘Joint CEN and ETSI Response to Mandate M/453’ p. 3.
Cooperative ITS platform from the Hume Highway to Port Kembla, in order to test C-ITS applications in relation to heavy vehicles. This trial will focus on improving traffic flow in and out of the port precinct, as well as providing information on traffic conditions. Once set up it could become a test bed that could be used to trial other applications.

C-ITS applications will involve and impact on the full range of parties involved in the transport network today, including:

- vehicle manufacturers
- technology providers of in-vehicle systems, network technologies and roadside devices
- after-market device manufacturers
- road managers, both public and private
- C-ITS system managers
- information service providers
- drivers with C-ITS
- drivers without C-ITS
- private, public and freight transport operators.

It is assumed at this point that C-ITS safety applications would be taken up on a voluntary basis, although, as noted above, other jurisdictions are considering mandating the technology.

1.6 Establishing a C-ITS framework for Australia

There are a range of further critical issues that need to be considered as part of introducing C-ITS in Australia that are outside the scope of this report. Many of these issues are being examined by Austroads as part of their C-ITS work program. These include:

- allocation and management of the 5.9 GHz band for ITS
- establishing a licensing regime for C-ITS communications devices
- determining technical requirements and certification processes
- establishing a nationally consistent platform for C-ITS operations
- governance and institutional arrangements.

Policy and operational developments will need to be carefully coordinated and the NTC will continue to work with Austroads on these issues. In particular there will be a close link between privacy policy and institutional structures.

All of this sits under the Policy Framework for Intelligent Transport Systems in Australia which sets out the policy context for ITS in Australia (and hence for C-ITS) and includes a series of principles for ITS.

1.7 What is Dedicated Short Range Communication?

The examples in section 1.5 use ‘Dedicated Short Range Communication’ (DSRC). Although the term Cooperative ITS covers a range of systems and a range of media which allow vehicles, individuals and infrastructure to communicate, the primary focus of this report will be on DSRC given how new and different it is to existing media (such as the mobile data network) and how fundamental it is to future C-ITS applications. DSRC will allow vehicles to communicate directly with each other (rather than, for example, having to go via a central service). This raises the possibility of new applications, such as collision avoidance, which would not currently be feasible otherwise. DSRC also creates new ways for vehicles and infrastructure to share information, although it should be noted that there are similar existing examples of this, in particular electronic tolling.

---


15 Austroads Project No: NT1632 is coordinating a number of streams of work in relation to C-ITS and is considering spectrum licensing and mapping requirements. Austroads Research Report AP-R413-12 Cooperative ITS Strategic Plan, 2012.

DSRC is anticipated to use the 5.9 GHz bandwidth in order to provide direct, reliable, low latency communication at short range. These qualities allow it to be used for applications which are highly time sensitive, in particular collision avoidance.\(^\text{17}\)

Due to its properties and availability, most major jurisdictions overseas plan to use the 5.9 GHz band for C-ITS applications or neighbouring bands.\(^\text{18}\) In Australia, use of the 5.9 GHz band is currently embargoed and the Australian Communications and Media Authority (ACMA) has recognised its future potential use for C-ITS.\(^\text{19}\) Austroads is currently preparing a submission to the ACMA on the allocation and management of this band for C-ITS.

1.8 C-ITS is multi-media

DSRC will be one of a number of communications media that a modern connected vehicle will use (and sometimes seamlessly switch between). Vehicles already connect electronically in a number of ways with navigation systems, freight management systems and diagnostics applications, among others. Where possible policy approaches need to be consistent to ensure that there are not different rules for different modes of communication that achieve essentially the same ends. A number of stakeholders raised the issue of how C-ITS is defined and noted that DSRC is just one example of C-ITS (or more specifically one medium used for C-ITS). Whilst the NTC agrees with this point, the project is nonetheless primarily focussed on DSRC, due to:

- the reliance of many key applications on this platform and
- the different character of this medium compared to others that have been used previously.

The table below provides some examples of different communications media used by “connected vehicles” (broadly speaking). Sample uses are included to provide an illustration of each of these, but these are not exhaustive lists. The technology and the applications continue to change and evolve.

Table 1. Type of communications modes in connected vehicles:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Features</th>
<th>Sample uses (existing and proposed)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSRC 5.9GHz</td>
<td>Short to medium range, low latency. Data to and from vehicle, to enable vehicles to exchange data directly with each other and with infrastructure (rather than going via a central service). Generally small data messages.</td>
<td>Collision avoidance. Traffic data gathering and traffic management. Safety warnings Traveller information services</td>
</tr>
<tr>
<td>Cellular network</td>
<td>Wide-area network; long range, however does not provide coverage of whole rural road network. Varying latency (dependent in part on congestion), but latency decreasing with newer generations (4G/LTE). General purpose and can enable large data messages.</td>
<td>Phone calls. Traffic and navigation information. Infotainment. Emergency calls (e-call). Fleet management information.* Regulatory information.** Vehicle diagnostics. Internet browsing and internet applications.</td>
</tr>
</tbody>
</table>

\(^\text{17}\) In this context ‘low latency’ refers to the short delay (or alternatively the rapid response time) of signals transmitted, processed and output using this bandwidth. This feature is critical for road safety applications.

\(^\text{18}\) Except in Japan, which is utilising 5.8GHz band for C-ITS. A decision has already been made in the USA to use the 5.9GHz band for C-ITS.

\(^\text{19}\) See for example ACMA, *Five-year spectrum outlook 2011–2015: The ACMA’s spectrum demand analysis and indicative work programs for the next five years*, March 2011 at p. 113: ‘The 5850–5925 MHz band is intended to support Intelligent Transport Systems.’
| Radio (digital and analogue) | Long range  
Some coverage (e.g. DAB+ digital radio) limited to metropolitan areas.  
One way communication (car is receiver not broadcaster) | Infotainment.  
Traffic information. |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Wifi/ WLAN</td>
<td>Short range; use most commonly for internet based technologies, with devices connecting a central point (which can then connect to the internet).</td>
<td>Internet applications.</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>Very short range, used for exchanging information between devices.</td>
<td>Generally used to connect devices at short range (e.g. mobile hands-free sets). The signals generated have also been used to collect traffic information.</td>
</tr>
</tbody>
</table>
| 5.8GHz Toll Tags            | Passive system (activated by signal from roadside gantry).  
Short range | Payment systems. |
| Global Navigation Satellite System (GNSS) | Long range; one way communication (vehicle/device is receiver). | Positioning information.  
Timing information. |
| Satellite communications    | Long range, two way communication. | Phone calls and emergency communication. |

* Such as for freight vehicles, taxis, buses.  
** In particular for heavy vehicles, through such schemes as the Intelligent Access Program and Electronic Work Diaries.

There may of course also be other communication devices for parts of the vehicle fleet (e.g. 2-way radios) and in some vehicles there may be multiple devices using the one communication medium (for example, passengers with mobile phones) and individual devices that move between different media. The list also indicates that connection will be through a range of devices which may be part of the original equipment in the vehicle, be tethered to the vehicle or have no connection to the vehicle at all. Finally, the different communications media will have very different commercial models and conditions of use. This presents a challenge in creating consistent rules, particularly in the area of privacy.

Different media or communications will also have different unique identifiers with different levels of connection to an individual. This has important implications for privacy in particular.

It is also envisaged that many applications will be able to roam between communications media, using protocols established by international standards, in the same way a smart phone can move between using the mobile data network and using a local Wifi network to access the internet, without intervention from the user.

### 1.9 Data messages broadcasted by C-ITS

Many C-ITS applications are premised on vehicles sending out a ‘heartbeat’ or data message broadcast around the vehicle using DSRC. This is currently planned as a signal broadcast up to ten times per second and around 300m around,\(^\text{20}\) to inform other vehicles of its basic information, such as where it is, where it is heading and how fast it is going. Standards are under development internationally, but the information broadcast by a C-ITS enabled vehicle will likely include:

- a unique identification number for the station or device  
- position – latitude, longitude, altitude and a measure of the accuracy of the information  
- motion – speed, direction, steering angle and acceleration

\(^\text{20}\) Estimates vary in regard to this maximum range with some sources stating up to one kilometre [http://www.standards.its.dot.gov/Documents/advisories/dsrc_advisory.htm](http://www.standards.its.dot.gov/Documents/advisories/dsrc_advisory.htm) (viewed on 18/10/2012) whilst others estimate 300-500 metres. The exact distance will also be dependent on topography and obstacles such as buildings, as well as the power of the devices used, which may vary between devices in vehicles and those in road-side infrastructure.
controls – such as brake status

vehicle information – such as vehicle size and model.21

Figure 4. Vehicles broadcasting C-ITS information

This signal, visualised in Figure 2, would primarily be used by other vehicles to avoid collisions. Infrastructure could similarly broadcast information to nearby vehicles, including incident information or route guidance and receive signals from vehicles in order to monitor and manage traffic flows. Note that GNSS (which includes the US Global Positioning System, GPS, commonly used in Australia) is critical in providing the position information for these messages.

This broadcasting of vehicle information is one of the key differences in DSRC (as compared to say communication via the cellular network). It has important implications around privacy, as policy makers need to consider who could record this information, what purposes they could use it for and whether the signals could be linked back to individuals.

1.10 Summary and Conclusions

This report makes a series of recommendations on policy and further research for consideration. Importantly, the NTC did not find any legislative roadblocks to the deployment of the technology in Australia.

At the same time, the NTC agrees with views expressed by stakeholders that there is a need for the safety benefits of the technology to be further proven before governments provide incentives towards its roll out. However the NTC has found a number of areas requiring further review. In particular there was significant concern around the uses of data generated by such systems. There are a number of ways that these concerns can be addressed, but this will depend in part on the institutional arrangements that are decided upon, along with technical implementation of the technology.

---

2. Liability

2.1 Introduction to the issue

As transport technology advances, the issue of who is liable in the event of a crash will potentially become more complex. The question of how liability would be resolved in the event of C-ITS system failure will be important in providing certainty to drivers, manufacturers, insurers and road managers. It is expected that the number of crashes would be reduced significantly in a fully C-ITS equipped environment, however crashes would still occur, with some specific C-ITS related reasons such as:

- Data communication failure or interference
- Conflicting or erroneous warnings being provided to drivers
- A driver failing to respond to a warning received
- Driver over-reliance on the technology

A number of other scenarios could also be imagined, involving either the failure of the technology, limitations of the technology in different conditions or problems in the interaction between the driver and the technology. C-ITS applications draw together the whole range of parties typically involved in the transport network, including road agencies, drivers, operators and manufacturers.

The liability regime in Australia is primarily based on common law approaches but supplemented by explicit legislation in certain areas, including no fault legislation covering personal injuries. A number of states have compulsory third party personal injury schemes, funded through registration payments. They provide compensation for personal injuries sustained in crashes on public roads. Some of these schemes are run on a no-fault basis, others are fault-based. There is a direct economic benefit to these schemes if the road toll is reduced and the schemes typically play a role in improving road safety. Product liability laws can also apply. In Australia Trade Practices Act (Cwlth) 1972 is the key piece of legislation, supplemented by a variety of state consumer protection laws. Contract law could also play a role through insurance contracts.

It should be noted that the Australian legal system allows for concepts of joint, several and contributory liability where a manufacturer or service provider could contribute in part to a collision (and be held liable for this contribution) even if they are not wholly responsible.

All of these areas of law (liability, contract, consumer protection) along with the various personal injury schemes, have evolved over decades and in some cases centuries. As such, any potential changes should proceed with extreme care.

Failure by a C-ITS application to provide appropriate warnings could result from a range of sources, including software problems (including those introduced as part of upgrades), limitations on sensors, signal interference, lack of accuracy in mapping or positioning information or other sources. The exact causes will depend on the specific applications and whether they are merely advisory or more interventionist systems. Liability concerns have been raised as a potential disincentive for manufacturers to develop C-ITS applications and other safety systems: ‘these technologies pose challenges for manufacturers and may increase their liability risk in ways that discourage the efficient introduction of these technologies.’

The introduction of airbags by the US National Highway Traffic Safety Administration (NHTSA) is a cautionary example, where even safety technology with significant benefits can have unintended consequences:

In 1977, NHTSA estimated that air bags would save in the order of 9,000 lives per year and based its regulations on these expectations. Today, by contrast, NHTSA calculates that air bags saved 8,369 lives in the 14 years between 1987 and 2001. Simultaneously, however, it

---


has become evident that air bags pose a risk to many passengers, particularly smaller passengers, such as women of small stature, the elderly, and children. NHTSA determined that 291 deaths were caused by air bags between 1990 and July 2008, primarily due to the extreme force that is necessary to meet the performance standard of protecting the unbelted adult male passenger. Houston and Richardson describe the strong reaction to these losses and a backlash against air bags, despite their benefits.\(^{24}\)

Similarly, C-ITS applications could potentially save many lives, but cause the loss of a small number of others; a net gain for society but an extremely difficult problem from a liability (and ethical) perspective. Liability risks could prevent the roll-out of C-ITS applications or severely reduce their scope of operations, as manufacturers could become excessively cautious. At the same time the threat of future litigation also acts as a safeguard, ensuring rigorous testing and research before any public release.

Key findings of the Discussion Paper included:

- Manufacturers and services providers of C-ITS technology will need to carefully consider the safety risks of their systems and the development and testing processes that they implement, along with consumer marketing and communications.
- Liability concerns may mean C-ITS applications need to log actions in significant detail in order to trace causation.
- Taking human factors into consideration will be critical to the success of C-ITS, but these factors may require further testing in order to better understand and address them.
- Information provided to drivers on system limitations and system status will be critical.
- Road managers will need to assess the risk implications of providing infrastructure-based C-ITS solutions.
- Expectations of system performance and liability implications are likely to change as C-ITS applications move from being advisory to actually overriding driver actions.

A key finding from the research and submissions was the increase in liability risks as C-ITS safety technology moves from being advisory to interventionary, and ultimately automating vehicle controls (discussed at section 6.2).

2.2 Stakeholder feedback

The majority of submissions accepted that the risk of liability needs to be managed, but there was a clear preference for liability to be dealt with under current legal principles and a view that C-ITS is not sufficiently exceptional to warrant a separate administrative or legislative regime at this time. For example, available Advanced Driver Assistance System (ADAS) technologies such as lane departure, crash avoidance and speed advisory systems have been introduced within pre-existing frameworks and without increased litigation for vehicle manufacturers. Tort law, contract law and product liability, including consumer protection laws, are seen together as providing the required level of certainty for manufacturers, road agencies, service providers and consumers that responsibility for wrongdoing can be appropriately assigned.

The Australian Logistics Council (ALC) noted that user behaviour may develop in a way not anticipated by legislation. Furthermore, the current approach carefully balances liability and innovation and it is important that C-ITS legislation to “fix” liability doesn’t then diminish innovation.

This position was advocated in a number of submissions in the context of C-ITS applications that continue to rely on driver judgement and driver control of the vehicle. It was acknowledged that if C-ITS applications move further along the spectrum towards interventionist applications and autonomous vehicles, this approach may require re-assessment. ITS Australia, for example, emphasised the potential complexity of future C-ITS applications that could use road-side devices to direct automated responses from vehicles. TCA wrote: “as C-ITS evolves or to encourage its evolution to more complex and active applications capable of overriding driver action, there may be a need to consider legislation which spreads risk and liability appropriately.”\(^{25}\) In this scenario,


\(^{25}\) Transport Certification Australia, ‘Cooperative ITS Regulatory Issues,’ *TCA Submission to the NTC Cooperative*
various approaches were discussed in the feedback, including a liability fund to process claims for loss or damage to persons caused by the operation, a no-fault compensation scheme and government accreditation of C-ITS systems.

The Truck Industry Council, which represents truck manufacturers, chose not to comment on whether current liability laws were sufficient for C-ITS applications, but agreed with the comments in the Discussion Paper relating to technology advancing faster than laws.

Bosch, a developer of in-vehicle ITS applications, focused on the rigorous product development standards already in place. For example, ISO 26262 “Road vehicles - Functional safety” addresses possible hazards caused by malfunctioning behaviour of electronic safety-related and interactive systems, which forms a core element of the design and application of vehicle safety systems. This perspective was reiterated by others: the then Commonwealth Department of Infrastructure and Transport referred to Australia’s commitment to safe system principles, established in the National Road Safety Strategy, which emphasises the responsibility of system designers (including technology providers, road agencies and regulators) to ensure the safety of road users.

The feedback strongly endorsed governments having a role educating both industry and road agencies on their responsibilities and how best to manage the risks. Practical guidance was seen as being more important than introducing more laws that may in fact further complicate the regulatory environment. The Truck Industry Council (TIC) suggested that:

Industry needs to have very clear guidelines on liability before technology suppliers will accept the risk of providing systems that may increase their liability. In fact, without further guidance on product liability specific to the use of in vehicle C-ITS technology, the development and rollout of these C-ITS technologies (that can potentially save many lives) may be hindered.26

Drivers also have a responsibility to understand the technology, and Bosch proposed that vehicle technology training form part of the 120 hours of learner experience, including some related questions on the written test. Public education similar to the Transport Accident Commission (TAC) advertising strategy for Electronic Stability Control (ESC) should be considered.27 However, information and education campaigns were not considered a sufficient response to ensure certainty of liability in the submissions. The preferred view was that public campaigns can increase general awareness of C-ITS functionality and have the potential to improve road safety, but that they should complement, not replace, pre-existing legal principles of liability and legislative frameworks. The ATA suggested that the benefits and limitations of C-ITS could be publicised, but “it is a manufacturer’s responsibility to sell C-ITS systems to users and make sure that limitations are clear. The Government should not bankroll private enterprise marketing.”28

2.3 Policy Position

The laws around liability have evolved over decades and have been adapted to a variety of situations. They have, in general, adequately been applied to new technology that has appeared, including in the transport sector. Any changes would have to be made with extreme care, in order not to disturb the appropriate allocation of risks between parties, nor adversely affect the balance between innovation and safety.

Research and stakeholder consultation indicates that liability has not been a significant hindrance to the development of new transport technologies in the past. C-ITS technology does not appear to
be sufficiently different to warrant a special case. As such there does not appear to be a strong case to make changes and it is recommended that no changes are made to the current approach.

A number of stakeholders also emphasised the fact that these systems will be secondary safety systems, providing added advice and information to the driver to improve their current driving, rather than being primary safety systems. Theoretically, this should make the failure of such a system less likely to end in a crash; however the importance of these systems will increase over time.

Various parties will need to carefully manage their risks, but feedback has indicated that in general these parties are already very conscious of safety (and hence liability) risks as part of their current systems development. Manufacturers will continue to need to ensure they conduct comprehensive testing on new systems in order to set best practice. Liability law currently acts as a strong incentive to ensure that product testing is rigorous. Road agencies will need to take an appropriate risk-based approach to the development of their roadside systems.

Stakeholder feedback does, however, indicate a concern for human factor issues, such as driver over-reliance on technology. These areas may require further research; this is discussed further in section 6.1.

The issue of increasingly automated vehicles, and how they should be managed from a liability perspective, as well as a compliance perspective, was also raised and may likewise be an area that requires further research; this is discussed further in section 6.2.

Finally, a number of stakeholders expressed concern at the potential impact of these systems on vulnerable road users. This issue is discussed further below in section 6.4.

**Policy Finding:** No changes are recommended to current laws and approaches around liability for drivers, manufacturers and road managers in regard to the roll out of C-ITS technology.
3. Privacy

The privacy chapter is in two parts. Section 3.1 considers privacy issues in relation to the collection, use and disclosure of personal information by private sector organisations. It also includes a discussion on the implications of surveillance device laws. Section 3.2 considers privacy issues in relation to the collection, use and disclosure of personal information by government agencies, including the access to C-ITS data for enforcement purposes.

3.1 Privacy and the private sector

3.1.1 Introduction to the issues

The private sector is already harnessing personal information for commercial ITS purposes. For example, navigational systems are available on the market that provide consumers with live traffic updates based on the consolidation of the location and speed of other users of the commercial application. In these situations, consumers voluntarily opt-in to a commercial application and thereby agree to share their personal information for these purposes, and providers must handle their personal information in compliance with the Commonwealth’s Privacy Act. C-ITS applications based on DSRC technology are likely to operate within the same privacy framework.

The Privacy Act regulates the collection, use, disclosure, security and access of personal information. A private sector organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way. The Privacy Act defines personal information as:

Information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

The definition of personal information is sufficiently broad to include location information if that information is about an individual whose identity is apparent or can be reasonably ascertained from that information. The Privacy Act will not apply, however, if the information does not identify an individual.

The Privacy Amendment (Enhancing Privacy Protection) Bill 2012 was passed in November 2012. The Bill amends the Privacy Act to create the Australian Privacy Principles (APPs), a single set of 13 privacy principles applying to both private sector organisations and Commonwealth agencies that will replace the National Privacy Principles (NPPs) and Commonwealth Information Privacy Principles (IPPs) from March 2014. Largely replicating the pre-existing privacy principles, the amendments will, among other things:

- require that the individual must be ‘reasonably identifiable’ – whether an individual is reasonably identifiable from certain information requires a consideration of the cost, difficulty, practicality and likelihood that the information will be linked in such a way as to identify him or her;
- relax cross-border disclosure of personal information – there will be no general prohibition on cross-border transmission of personal information, although the entity must take such steps as are reasonable in the circumstances to ensure the overseas recipient does not breach the APPs;
- make it mandatory for relevant entities to have a privacy policy.

The key privacy question is the extent to which C-ITS information will make individuals (such as drivers or registered owners) reasonably identifiable. Resolving this issue will not only determine whether the privacy principles will apply, but whether additional privacy protections (such as a privacy code or legislation) are necessary or advisable. Because C-ITS is an emerging technology

29 Privacy Act 1988 (C’wealth).
30 Privacy Act 1988 (C’wealth), section 6.
31 Privacy Amendment (Enhancing Privacy Protection) Bill 2012, Explanatory Memorandum, p. 61.
32 Privacy Amendment (Enhancing Privacy Protection) Bill 2012, Explanatory Memorandum, p. 83.
and the operational framework is still under development, it is unclear at this stage whether C-ITS users will be ‘reasonably identifiable’ based on the Australian Privacy Principles test.

3.1.2 Unique identifiers

International standards for C-ITS are in development.33 A focus of these standards is that intelligent transport systems will be developed with a privacy by design objective. There may, however, be limitations on whether true anonymity can be achieved. For security purposes, vehicles are likely to be required to have a form of security certificate (similar to those for secure websites) for their DSRC signals, in order to ensure that signals are legitimate and to prevent false signals being recognised. While standards and processes for security certificates are still under development, it is expected that these will need to be managed by a certificate authority to ensure that secure communications occur between trusted devices.

At issue is how easily, if at all, a C-ITS vehicle signal can be linked to an individual. For example, if a service provider collects a vehicle’s unique number but has no method to match that number to a vehicle registration or individual, then it is unlikely that the data would meet the ‘reasonably identifiable’ test and it would not be personal information.

On the one hand, based on the NTC’s current understanding of the development of DSRC technology, there will be a unique identifier within the data message broadcast by the DSRC, but it is unlikely that it will be readily linked to an individual. Unique identifiers are also likely to rotate regularly (perhaps weekly) so as to prevent ongoing tracking. On the other hand, there is less certainty of anonymity in relation to the use of technologies such as bluetooth and Wifi that utilise unique MAC and IP addresses.

In 2011, the Information and Privacy Commissioner of Ontario published a paper that considered the privacy implications of Wifi and MAC addresses.34 The Discussion Paper discusses the privacy challenges associated with MAC addresses and makes the following suggestions:

- privacy is predicated on providing individual mobile device users with personal control, alongside openness and transparency on the part of the provider
- in no case should the MAC address of an individual’s mobile device be collected or recorded without the individual’s consent
- privacy by design is now the international standard for privacy and should be used by engineers to ensure privacy is embedded in the systems architecture; the potential for possible unintended uses should form part of the privacy risk analysis
- Wifi protocols should seek to randomise MAC addresses or ensure privacy through a proxy-like method of assigning addresses; innovative solutions will be required to change the existing model of using persistent MAC addresses that remain uniquely bound to a mobile device.35

Industry does not necessarily agree that an IP or MAC address will always constitute personal information,36 and it has been observed that:

A MAC address or an IP address information is rarely going to be in and of itself information about an identifiable individual in the sense of having a precise connection and being directly related to an identifiable individual. It is the context of how the MAC address or IP address is combined with other information (or could be reasonably be combined with other information) that has privacy advocates concerned.37

---

37 Ibid.
Further work therefore needs to be done to establish whether communications media such as Wifi or bluetooth can provide C-ITS functionality without it being possible for an entity to link the unique address to the identity of the owner.

In the event that the individual ‘owner’ of a C-ITS signal can be reasonably identifiable, both State and Territory surveillance device laws and privacy principles will apply.

3.1.3 How surveillance laws relate to the privacy principles

The applicability and inter-relationships between the various privacy regimes and the surveillance laws that have been introduced across jurisdictions can be complex and require further explanation. Put simply, the Commonwealth and State privacy laws do not set limits on, or define, what can be collected. Under the privacy laws the collection must simply be “not unlawful,” or “not unfair” or “not unreasonable” or required to undertake the legal task. While the phrasing changes in each jurisdiction, it is clear that Australia’s privacy laws are concerned with what happens to the personal information once it is collected – for example, how it is used and secured, who it is disclosed to and how it is discarded. The surveillance laws, on the other hand, are not focused on what is done with the personal information once it is collected, but on the legality of the collection itself. The surveillance laws therefore serve as a gateway to ensure that a device is not used for covert surveillance purposes. In this sense, the privacy and surveillance regimes are complementary.

Further to this, surveillance laws can be separated into two distinct groups: the Surveillance Devices Act 2004 (Cth) which sets out conditions for federal law enforcement agencies to use surveillance devices to track locations and to listen to conversations (which is discussed in the next section on “Privacy and governments”) and State and Territory-based surveillance laws which are much broader and prohibit covert surveillance of any person and by any public or private entity. The extent to which State and Territory surveillance laws impact on private entities accessing C-ITS personal information is discussed below.

3.1.4 Surveillance device laws

The definition of a surveillance tracking device is largely consistent across jurisdictions. For example, in New South Wales a tracking device means “any electronic device capable of being used to determine or monitor the geographical location of a person or an object.” This is sufficiently broad to capture vehicle movements identified within a C-ITS system.

The surveillance laws will not apply if the subject of the tracking device, or the person controlling the object being tracked, provides his or her consent. For example, in Western Australia, the Surveillance Devices Act legislates that:

\[\ldots\] a person shall not attach, install, use, or maintain, or cause to be attached, installed, used, or maintained, a tracking device to determine the geographical location of a person or object without the express or implied consent of that person or, in the case of a device used or intended to be used to determine the location of an object, without the express or implied consent of the person in possession or having control of that object.\]

The variations between the jurisdictions are small but notable. For example, in New South Wales the prohibition on the installation, use and maintenance of a tracking device does not apply when the tracking device is for a lawful purpose; while a surveillance Bill currently before the Parliament of South Australia states that a person must not knowingly install, use or maintain a tracking device to determine the geographical location of a person or a vehicle or thing without the express or implied consent of the owner, or a person in lawful possession or control, of that vehicle or thing. C-ITS systems would not require consent of individuals in Queensland, which does not have equivalent surveillance legislation in place.

The extent to which C-ITS communications generate unique identifiers that can be matched to the owner of the device or vehicle is a technical question. If it is possible, however unlikely, then State and Territory surveillance laws will apply and consent, whether express or implied, must be

---

40 Surveillance Devices Act 2007 (NSW), subsection 9(2).
41 Surveillance Devices Bill 2012 (SA), section 6.
obtained to use that information for C-ITS purposes. As discussed earlier, C-ITS will utilise a number of different communications media to connect vehicles and other elements of the transport network.

If a privacy by design approach that anonymises C-ITS signals is not feasible, alternative means to establish implied or express consent should be investigated. In circumstances where identification data and location data can be matched without the consent of the owner, it is clear that this information could be used to track the location of individuals and would be in direct contravention of surveillance laws. It is argued that community acceptance of C-ITS will be significantly reduced if the surveillance laws are amended to exempt C-ITS in such a way that undermines the spirit and intent of those laws.

Consent to use pre-existing technologies (such as an IP or MAC address) will be particularly challenging given that the owner of a C-ITS device could be any person in the vehicle – not necessarily the driver – and the IP or MAC address could be accessed without an application to enable C-ITS functionality (which could have provided an interface to secure consent from consumers).

3.1.5 National Privacy Principles

The NPPs set out how private sector organisations should manage personal information. They cover the collection, use, disclosure and secure management of personal information. They also allow individuals to access that information and have it corrected if it is wrong.

An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities. The privacy principles do not prescribe under what conditions or circumstances the collection of personal information is necessary. Therefore, what can be collected, as opposed to how the information is collected or used, is very broad in scope given that private sector organisations self-assess what personal information is required in order to undertake any of their functions or activities.

The NPPs do not require individual consent to collect personal information for a primary purpose, however at, or before, personal information is collected, the organisation must take reasonable steps to ensure that the individual is made aware of:

- the identity of the organisation and how to contact it
- the fact that he or she is able to gain access to the information
- the purposes for which the information is collected
- the organisations (or the types of organisations) to which the organisation usually discloses information of that kind
- any law that requires the particular information to be collected
- the main consequences (if any) for the individual if all or part of the information is not provided.

The contractual point of purchase of a C-ITS enabled vehicle or smartphone application (e.g. a privacy policy included as part of the terms and conditions) may be an appropriate stage to do this, however there remains an issue of how this could be managed for fleets and used cars.

In circumstances where a private sector organisation is obtaining personal information on behalf of a public sector entity (e.g. a public-private partnership toll road), that organisation will be bound by the relevant IPPs.

The Privacy Act also exempts a number of entities and activities from the NPPs, including small businesses with an annual turnover of $3,000,000 or less (unless the small business collects or discloses personal information for a benefit, service or advantage), political activities, employee records or any part of the NPPs exempted under a privacy code. Most of these exemptions will not have a significant impact on C-ITS, except perhaps the small business exemption, although the threshold is relatively low for the profile of companies that are potential C-ITS service providers.

---

42 Privacy Act 1988 (C’wealth), Schedule 3
43 NPP 1.1.
44 NPP 1.3.
Event data recorders (EDRs, or black boxes as they are sometimes colloquially known) provide a point of comparison. These devices collect key data for vehicles, generally for diagnostic purposes, but also for investigation in the event of a crash and can be used as evidence in court. The data captured is limited in important ways – key pieces of data are only retained in the event of a major incident and only for a certain period in the lead up to the incident. This has largely evolved through original equipment manufacturer (OEM) practices, rather than through legislation (although it should be noted there is legislation in other jurisdictions which has influenced the market). Location is typically not collected, which is an important privacy protection. Drivers are generally notified of the collection of information via the vehicle’s manual. The data from these devices has been successfully used as evidence in court in regard to crashes.

3.1.6 Stakeholder feedback

In the event that C-ITS data is reasonably identifiable and genuine anonymity is not attainable, consideration should be given as to how privacy can be protected. The Discussion Paper raised five options for discussion:

- rely on existing privacy principles to protect personal information
- register a C-ITS privacy code with the Australian Information Commissioner that binds governments, employers and small businesses
- publish privacy best practice guidance material to assist C-ITS parties to meet their obligations under the law
- legislate C-ITS governance arrangements and use of information
- legislate technical standards to protect privacy

There was general consensus amongst submissions that privacy protections are of vital importance to C-ITS given that the technology utilises precise vehicle location and has the potential to track the movement of vehicles and hence individuals. Privacy is considered by many as a fundamental human right and intimately related to security and trust. Understanding the trade-off people are willing to make between privacy and improved driving safety and efficiency is an important area of investigation.

However, there were divergent views on how personal information should be protected and the submissions referred to a wide breadth of solutions: privacy by design, privacy impact assessments, legislative protections, the development of a privacy code and published guidelines.

There has been no suggestion that the Privacy Act 1988 solves the C-ITS privacy issues on its own, although some reflected that C-ITS privacy protections should be framed by the existing privacy regimes. Mr Williams suggested that C-ITS personal information should be covered by the same regulations as any other personal information captured in a database, and that C-ITS “should not make itself a special case for more onerous treatment.” Queensland Transport and Main Roads (TMR) echoed these views. The ALC commented that, in addition to the privacy principles, commercial contracts may provide the required legal compliance and any other special provisions.

An alternative view was held by Bosch, which argued that current arrangements do not appear to be appropriate measures for protecting privacy, largely due to the fast and dynamic nature of technology development.

Privacy by design Privacy by design is a ‘whole-of-business’ life-cycle approach to privacy that embeds privacy protections in the design of new business systems, operations and technologies, rather than implementing mitigations after the implementation of a system. Under a privacy by design approach the collection of personal information is restricted to what is necessary to carry out intended functions, and thereby limits information flows to only those entities required to carry out those functions. Submissions referred to a range of design features that are relevant to C-ITS.

including such elements as the use of international standards for data messages, security and the use of pseudonyms, rolling security certificates and nightly cleansing of personal information.

The WA Government, NICTA, Bosch, Victorian Privacy Commissioner, Victorian Motorcycle Council (VMC), ITS Australia and TMR supported the incorporation of privacy protections into the design of C-ITS systems, for example by ensuring anonymity, or pseudo-anonymity, of C-ITS signals where possible. The Victorian Privacy Commissioner recommended that personal information should not be indefinitely retained if it is not necessary to achieve the system’s stated purposes and that time limits be placed on the retention of personal information.

The WA Government, Victorian Privacy Commissioner and ATA supported physically separating data collection and storage responsibilities from the organisation that collects and holds the personal information (such as the vehicle registration details) as an important privacy by design measure. The WA Government wrote:

\[
\text{Ensuring privacy protection is paramount to gaining C-ITS acceptance. If personal anonymity is not able to be guaranteed, then a robust approach may be to separate the collection and storage of vehicle data from the holder of data linking the unique C-ITS identifier to a vehicle registration owner. It is considered that implementing C-ITS governance arrangements around the use of the data is the most effective way to maintain control over the separation of data types.}^{46}
\]

This approach is consistent with the preferred model in the United States, whereby the Certificate Authority will not hold personal driver and licensing information.

**Privacy Impact Assessment** A Privacy Impact Assessment (PIA) is a tool to help manage privacy impacts and can assist organisations to develop a privacy by design approach. While not required under the Privacy Act 1988, a PIA enables organisations to understand the flow of personal or sensitive information and the extent to which a proposed scheme is compliant with the privacy principles. Where there are potential privacy impacts, a PIA can recommend potential solutions.

The Victorian Privacy Commissioner and the SA Privacy Committee recommended that PIAs are undertaken, not only by the organisation responsible for the C-ITS system but other organisations intending to participate in C-ITS, such as infrastructure providers.

**Legislative protections** For technology-based schemes that collect the geographical location of a large number of vehicles in real time, such as Citylink and the Intelligent Access Program (IAP) for heavy vehicles, privacy protections in enabling legislation have provided consumers with a high level of certainty as to the purpose of collection and a high level of confidence that their personal information will not be misused. The Victorian Privacy Commissioner, ATA, WA Government and Bosch each supported the introduction of C-ITS legislation to address governance, permitted storage and use of data and technical standards.

Whilst legislative protections offer a high level of certainty for consumers, this option did not receive universal support, notably from state road agencies. Some stakeholders considered it to be the most inflexible, interventionist and regulatory-intensive approach that is least suited to meeting changing requirements and evolving technology. The FCAI explicitly argued against the adoption of legislative protections.

**Privacy Code** An industry code is a form of self-regulation that allows entities operating in a specific market to adopt agreed standards and practices. Codes are voluntary and generally maintained by peak industry bodies or associations. A privacy code works in a similar way, but deals specifically with how parties to the code will protect personal information. The benefit of a privacy code is that it is agreed to, and logged with, the relevant privacy or information commissioner, thereby enabling a privacy code to exempt parties from a particular element of the Privacy Principles.

A C-ITS privacy code could provide a framework to enable industry to agree to common protections and processes and could ensure that parties otherwise exempt from the NPPs, namely employers, small businesses and state agencies, could voluntarily agree to a common approach,

---

thereby providing consumers with additional certainty that their personal information will be appropriately collected, handled and disclosed.

ITS Australia supported the introduction of a C-ITS privacy code; the Victorian Privacy Commissioner also supported a code in the event that legislative protections were not available. In contrast, a privacy code was not the preferred approach of other submissions. Bosch, for example, did not think that privacy codes were sufficiently flexible. The ATA wrote:

> Implementing privacy codes for specific industries creates a manner of complex privacy 'laws', that grant exceptions but do not enshrine that exception in privacy law. States are also not obliged to comply with the privacy codes and this limits the usefulness of such a scheme. 47

**Guidelines** C-ITS guidance material developed for governments and industry, including manufacturers, service providers, enforcement agencies and record keepers, was welcomed in a number of submissions as a flexible, practical and effective framework by which the privacy principles can be reflected in the C-ITS system and operational environment.

The Livestock and Rural Transport Association of WA (LRTA WA), TIC, Bosch, ITS Australia, Mr Williams and Mr Glenn supported the use of guidelines to make it easier for entities to comply. Further to this, Bosch suggested that guidelines, or legislation, is required in relation to the storage of personal data in vehicle systems (which is also an issue for EDRs). It is also noted that the Victorian Privacy Commissioner, ATA and ITS Australia suggested that in the event that legislation is enacted, it should be supplemented by non-regulatory controls such as guidance material.

TCA suggested that the certification of service providers by an independent body, in addition to the development of common standards, policies and guidelines, would also assist in ensuring privacy protection by making privacy compliance an essential component of the approval process.

**3.1.7 Policy position**

The NTC acknowledges the importance of protecting the privacy of C-ITS users and recognises the diverse range of views expressed by stakeholders in relation to the most effective and appropriate forms privacy protection should take.

The NTC notes that current ITS applications are effectively managed within existing privacy frameworks. The NTC does not believe that C-ITS is sufficiently exceptional to warrant a comprehensive legislative privacy regime that determines the roles, responsibilities and personal information flows across private sector entities engaged in C-ITS activities.

The NTC recommends that a privacy by design approach should be adopted as international best practice in the design and development of a new scheme that handles personal information, and that this should include the undertaking of PIAs by key entities that have responsibility for personal information generated by C-ITS, including the system manager, certification authority, road agencies and service providers. This approach will seek to ensure that the collection, use and disclosure of personal information is compliant with the Privacy Act. Where appropriate, this approach should be supplemented with published guidelines to provide certainty for all C-ITS providers and consumers as to how personal information should be handled. Best efforts to develop privacy by design solutions to protect personal information, including pseudo-anonymous C-ITS signals, will also reinforce community confidence that C-ITS systems will not breach surveillance laws.

In circumstances where C-ITS relies on emerging technologies such as DSRC, commercial arrangements should seek to ensure compliance with surveillance device laws by ensuring that consumers provide their consent to use their information for C-ITS purposes (e.g. by including consent in the terms and conditions when purchasing a vehicle or smartphone application). It is imperative that consumers are informed of the implications of their consent, and it should be included as part of any education or information campaign to promote the benefits of C-ITS.

---

It is not clear if the C-ITS system and operational environment will require exemptions from any of the privacy principles or sufficiently attract businesses to sign up to the code. In 2012, the Biometrics Institute Privacy Code was revoked by the Australian Information Commissioner at the request of the Biometrics Institute, in part due to a low level subscription to the code. Nonetheless, organisations should be encouraged to set clear and comprehensive privacy policies and the NTC would encourage the creation of a privacy code by participants in order to establish common practices and to build consumer confidence in C-ITS handling of personal information.

**Policy Finding:** No changes are recommended to current privacy laws governing the private sector development of C-ITS systems and data. Companies will need to closely follow the National Privacy Principles as required, as they do for C-ITS systems that have already been developed.

### 3.2 Privacy and governments

#### 3.2.1 Introduction to the issues

Commonwealth, State and Territory IPPs regulate the collection, use, disclosure, security and access of personal information by public sector entities, including police and road agencies. While terminology and form may vary, particularly in South Australia, the general approach across jurisdictions is consistent. Namely, a public sector agency must not collect personal information unless the information is collected for a lawful purpose that is directly related to a function or activity of the agency, and the collection of the information is reasonably necessary for that purpose.

In addition to the state-based IPPs, which are general and principle-based in nature, most road agencies have also legislated controls on the use and handling of registration and licensing data. For example, in Victoria, the Road Safety Act provides that VicRoads must enter into information protection agreements with those parties that are permitted access and use registration or licensing information. To the extent that these road agencies use registration or licensing data in relation to C-ITS functions, these specific provisions will apply.

The challenge for policy makers is that not every jurisdiction has these additional privacy protections, so they cannot be uniformly relied on in a nationally consistent approach. It also remains to be determined the extent to which road agencies’ roles and responsibilities in relation to C-ITS will overlap with registration and licensing functions. It is possible that this patchwork of IPPs and road agency provisions can be relied upon to provide the required privacy framework for public sector entities — accepting that the relevant framework could vary, even within a single agency, according to whether the C-ITS functionality is in relation to registration or licensing, or whether the road agency is handling personal C-ITS information as an infrastructure provider in V2I applications. It will also be complicated by Western Australia not having IPPs and relying on the Freedom of Information Act and the Road Traffic Act to afford drivers privacy protection.

Western Australia’s Freedom of Information Act enables individuals to ensure their documented personal information is accurate, complete, up to date and not misleading. Western Australian law also imposes limitations on which entities the Director General of WA Main Roads can disclose vehicle licensing data to, and under which circumstances; again, the relevance of these provisions will be dependent on the extent to which a road agency’s C-ITS responsibilities are in relation to registration (‘vehicle licensing’) functionality.

---


49 E.g., Privacy and Personal Information Protection Act 1998 (NSW), section 8.

50 Road agencies that rely on state-based IPPs and do not have additional registration and licencing data protections are: New South Wales, Tasmania and the Northern Territory.

51 Road Safety Act 1986 (Vic). A bill is currently before the Parliament of Victoria to ensure that the Act only applies to ITS functions, these specific provisions will apply.


53 Sections 8-13 of the Road Traffic Act 1974 (WA).
Returning to IPPs, the key issue for C-ITS is that in all jurisdictions the IPPs have an exemption for law enforcement purposes. For example, in Tasmania the substance of the IPPs in Schedule 1 of the relevant Act:

> do not apply to any law enforcement information collected or held by a law enforcement agency if it considers that non-compliance is reasonably necessary –
>
> (a) for the purpose of any of its functions or activities; or
> (b) for the enforcement of laws relating to the confiscation of the proceeds of crime; or
> (c) in connection with the conduct of proceedings in any court or tribunal.\(^{54}\)

A law enforcement agency includes police in any Australian jurisdiction, the Australian Crime Commission, and a personal information custodian responsible for the protection of public revenue or any function under a law that imposes a penalty or sanction.\(^{55}\) In Tasmania, a personal information custodian can also apply to the Minister for an exemption from the Act, for example on the grounds of a public benefit involved in doing so.\(^{56}\)

This means that pre-existing privacy protections will not prevent governments from accessing C-ITS personal information for law enforcement purposes.

While road safety and productivity are the key objectives for introducing C-ITS, the Discussion Paper recognised that there may be opportunities for road agencies to shift their compliance approach from the roadside to back-office enforcement that focuses on patterns of behaviour rather than isolated breaches. However the Discussion Paper also noted concerns that C-ITS enabled vehicles may then be exposed to greater scrutiny under the law which could inhibit uptake. Above all, the Discussion Paper acknowledged concerns raised in the international literature that if C-ITS were proposed “as a surveillance tool for law enforcement purposes, concerns with regard to privacy and civil liberties would be raised by the public and its representatives and advocates, which would threaten the implementation of such a Program.”\(^{57}\)

Various scenarios can be envisaged where C-ITS data could be misused by enforcement agencies, or where the seriousness of the matter under investigation would justify a court-issued warrant to obtain the evidence. Some examples:

- data being used to show a driver has been a recklessly driving in the past
- police officer accessing location data of a suspect in a criminal investigation
- “fishing” for speed offences by matching C-ITS location information to speed limit maps.

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. The evidentiary value of the data is also to be determined.

The NTC is therefore seeking an appropriate balance: certainty for citizens in regard to the when, how and on what basis C-ITS information will be used for enforcement purposes, with restrictions where appropriate; and certainty for agencies in regard to accessing C-ITS information when it is reasonable and beneficial to the community to do so.

The appropriate response is dependent on a number of factors: one, the extent to which C-ITS signals can be anonymised. This is yet to be determined but, as discussed earlier, initial discussions with industry suggest that while complete anonymity is unlikely, governance arrangements may make it difficult for agencies to link C-ITS signals to registration numbers and

\(^{54}\) Personal Information Protection Act 2004 (No. 46 of 2004) (TAS), section 9.
\(^{55}\) Personal Information Protection Act 2004 (No. 46 of 2004) (TAS), section 3.
\(^{56}\) Personal Information Protection Act 2004 (No. 46 of 2004) (TAS), section 13.
\(^{57}\) RITA, Vehicle Infrastructure Integration: Privacy Policies Framework, quoted in the NTC Discussion Paper, p. 52. Such concerns were also raised in the recent Electronic Work Diary Operational Pilot in Australia.
therefore individuals. But an element of possibility still exists. Two, the extent to which surveillance laws restrict access for enforcement purposes. This is discussed below. And three, what the community is prepared to accept in return for increased safety and productivity (including reduced congestion). This is reflected in the stakeholder feedback in the following section.

A key question is to what extent enforcement agencies are currently restricted in their access to C-ITS information under surveillance device laws. If it can be shown that the patchwork of Commonwealth, State and Territory surveillance device laws will apply to C-ITS information, this significantly diminishes any requirement to introduce legislation to restrict government access to, and use of, C-ITS information for enforcement purposes.

**Commonwealth surveillance laws** The Surveillance Devices Act 2004 (Cth) sets out conditions for law enforcement agencies to use surveillance devices to track locations and to listen to private conversations. One of the main purposes of the Act is “to establish procedures for law enforcement officers to obtain warrants, emergency authorisations and tracking device authorisations for the installation and use of surveillance devices in relation to criminal investigations.”\(^{58}\) The Act does not affect any other Commonwealth or state laws that prohibit or regulate surveillance devices.

Generally, federal officers must obtain a warrant from an eligible judge to use a surveillance device for law enforcement purposes. In certain circumstances a surveillance device can be used without a warrant if use of the device does not involve entry onto premises, or interference with the interior of a vehicle without permission.\(^{59}\)

Relevant definitions in the Surveillance Devices Act 2004 include:

- **Surveillance device** means a data surveillance device, a listening device, an optical surveillance device or a tracking device, a device that is a combination of any two or more of these types of devices, or a device prescribed by regulations.

- **Data surveillance device** means any device or program capable of being used to record or monitor the input of information into, or the output of information from, a computer, but does not include an optical surveillance device.

- **Computer** means any electronic device for storing or processing information.

- **Tracking device** means any electronic device capable of being used to determine or monitor the location of a person or an object or the status of an object.\(^{60}\)

In circumstances where, through accessing system manager, service provider and/ or road agency records, it is possible for an enforcement agency to locate a vehicle in time and place, and thereby locate an individual by inference, then it is likely that C-ITS data could meet the definition of a surveillance device and, more specifically, a tracking device. That its use as a tracking device is contingent on the enforcement agency taking a number of steps to obtain that information should not diminish the fact that C-ITS could be any electronic device capable of being used to determine or monitor the location of a person or an object or the status of an object. This position is taken on the assumption that C-ITS signals will not be completely anonymous and that access to the relevant information is possible.

Therefore, based on these assumptions, the Surveillance Devices Act 2004 will probably apply to federal agencies seeking to use C-ITS information. To be clear, however, this does not apply to state road agencies or state police forces, which are perhaps the most likely entities to seek C-ITS information in the first instance.

The Surveillance Devices Act 2004 will not apply if enforcement agencies obtain implied or express consent from the subject of the surveillance. There is a concern that because C-ITS is a voluntary technology, in the sense that consumers would opt-in to C-ITS when they purchase a C-ITS enabled vehicle, implied consent could be established by the courts, especially if it is generally known to the public that C-ITS information is accessed for federal law enforcement purposes. Consent could also be express if it is written into a contract to purchase for a C-ITS device (or more

---

\(^{58}\) Surveillance Devices Act 2004 (Cth), section 3.

\(^{59}\) Surveillance Devices Act 2004 (Cth), section 39.

\(^{60}\) Surveillance Devices Act 2004 (Cth), section 6.
likely, the vehicle that the device sits within), that the signals it generates can be accessed for federal law enforcement purposes. However, this again raises the issue of how used cars, fleet cars and others are dealt with.

Finally, the Surveillance Devices Act 2004 was not drafted with C-ITS in mind, and therefore does not easily adapt itself to C-ITS circumstances. For example, the Surveillance Devices Act 2004 presupposes that the federal law enforcement agency is seeking authorisation “for the installation, use, maintenance or retrieval of a surveillance device.” The extent to which this includes accessing C-ITS information from a third party which has legally obtained the information is untested, particularly given that the privacy laws have a disclosure exemption for enforcement purposes. If a narrow interpretation of the Surveillance Devices Act 2004 is applied, and accessing information falls outside the Act, then federal agencies would rely on access powers attached to specific enforcement responsibilities and these access powers are unlikely to require a warrant to access the relevant information.

**State and Territory surveillance laws** The previous section (“Privacy and the private sector”) discussed State and Territory surveillance laws in relation to surveillance tracking by any persons, which includes private entity organisations. The same laws apply to government agencies in their respective jurisdictions, but a surveillance warrant can be obtained for law enforcement purposes. Section 8 of Victoria’s Surveillance Devices Act provides an example:

Subject to subsection (2), a person must not knowingly install, use or maintain a tracking device to determine the geographical location of a person or an object –

- (a) in the case of a device to determine the location of a person, without the express or implied consent of that person; or
- (b) in the case of a device to determine the location of an object, without the express or implied consent of a person in lawful possession or having lawful control of that object.

Penalty: In the case of a natural person, level 7 imprisonment (2 years maximum) or a level 7 fine (240 penalty units maximum) or both; In the case of a body corporate, 1200 penalty units. […]

(2) Subsection (1) does not apply to-

- (a) the installation, use or maintenance of a tracking device in accordance with a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation; or […]
- (b) the installation, use or maintenance of a tracking device in accordance with a law of the Commonwealth. 62

The Surveillance Devices Act 2004 sets out in what circumstances a surveillance warrant may be applied for by an enforcement agency and issued by a supreme court justice or magistrate. Legislation in all other states and territories except Queensland is largely consistent and the meaning of surveillance tracking is sufficiently broad to capture vehicle movements through C-ITS technology. This has a number of implications for C-ITS operations:

1. In circumstances where it is possible to link C-ITS information to the identity of a person, road agencies or any other public entity will be prohibited from accessing C-ITS information without the express or implied consent of the subject.

The extent to which state and territory surveillance laws apply to road agencies seeking to access the information for non-enforcement purposes (such as traffic management) is dependent on the technical feasibility of that agency linking C-ITS information to the identity of a person.

---

61 Surveillance Devices Act 2004 (Cth), section 4.
2. Surveillance device laws will not always provide certainty for consumers that C-ITS personal information will not be accessed by State or Territory enforcement agencies and potentially used as evidence against them. This is based on the following observations:

a. Express or implied consent is a relatively low threshold to meet: governments may seek to include enforcement grounds in the contractual terms and conditions for purchasing C-ITS services; or seek to establish implied consent if consumers voluntarily purchase C-ITS and it is generally known that C-ITS information is accessed for law enforcement purposes.

b. It is not envisaged that an enforcement agency would install C-ITS on a particular vehicle and then engage in tracking surveillance. It is more likely that an enforcement agency would seek location information of a particular vehicle from the C-ITS system manager or service provider. As discussed in relation to the Commonwealth’s Surveillance Devices Act 2004, the extent to which the surveillance laws apply to the access of C-ITS information from a third party (as opposed to the “installation, use and maintenance”) is untested. If the access of C-ITS information falls outside the interpretation of “use,” then agencies can rely on access powers attached to specific enforcement responsibilities and there is no certainty for consumers that C-ITS will not be used for enforcement purposes.

c. Queensland does not have a surveillance device or surveillance tracking regime. There are also some minor variations across jurisdictions, e.g. in relation to exempted activities. This makes it challenging to establish a nationally consistent approach based on current laws.

It is further noted that the IAP and CityLink – two existing regimes that utilise technology-based vehicle tracking – have not relied on general surveillance laws but have legislated that enforcement agencies must obtain a warrant to access personal information they hold.

These observations suggest that current surveillance device laws do not provide the level of certainty required by community expectations. This conclusion was reinforced by the stakeholder feedback.

3.2.2 Stakeholder feedback

The four options raised in the Discussion Paper sought to address these issues and identify what level of regulation is appropriate. The four options were:

1. Do not intervene: allow jurisdictions to develop their own policies.

2. Provide specific protections for C-ITS information from use for enforcement purposes (potentially through legislation or policy).

3. Provide guidance on appropriate use of data.

4. Amend each surveillance device act to ensure that beneficial C-ITS applications (such as an evidence base for traffic management) is not excluded, provided appropriate safeguards are in place.

Many of the submissions expressed concern about personal information being accessed by governments for enforcement purposes, and that if C-ITS is used for enforcement purposes uptake will be low and safety objectives will not be met. To provide certainty for citizens, the Victorian Privacy Commissioner and TCA suggested that enforcement bodies should be required to obtain a warrant to access personal information, including location information, held by the C-ITS system manager or service providers.

The ATA stated that the level of individual identifier information built into the design of C-ITS will have implications for enforcement: “if signals cannot be made anonymous there is a genuine
concern that these vehicles will have greater enforcement focus as they are an easy target. Therefore, in ATA’s view, the focus of C-ITS should be on the safety benefits, not enforcement opportunities that could penalise early adopters. This position was reinforced by TMR which stated that the primary purpose of C-ITS should be to keep the driver safe and within the road rules rather than as an enforcement tool:

_TMR has the view that allowing the data and information to be used for the detection of offences would not be consistent with encouraging people to use the technology to improve road safety outcomes. However, if a driver was involved in an accident it would be reasonable for police to obtain data about the operation of a vehicle driven by the driver in the minutes leading up to the accident or if a person was suspected of a criminal act then C-ITS data may be used._

Therefore, while both the ATA and TMR recognised that C-ITS may have an important role in crash analysis and forensic investigation, this was differentiated from accessing C-ITS data for other compliance and enforcement purposes. The ATA suggested that, at the very least, enforcement uses of data should be explicitly legislated so that all C-ITS users understand how their data is used, who it is disclosed to, and the length of time it is kept.

In the heavy vehicle context, the ATA observed that C-ITS could provide operators with valuable data to improve compliance and driver behaviour, but cautioned against C-ITS tools completely replacing roadside enforcement, which could be less effective and have resource implications for enforcement agencies. Mr Glenn proposed that enforcement activities should be based on patterns of behaviour rather than one-off breaches, and that pattern definitions would need to be understood by the public or the notion is unlikely to be acceptable.

### 3.2.3 Policy position

C-ITS may be able to be used to identify individuals in time and place, enforcement activities are largely exempt from privacy principles and the Surveillance Devices Act 2004 is likely to have limited restrictive impact on enforcement activities. Furthermore, C-ITS uptake is expected to be low if personal information is easily and widely accessed for enforcement purposes. For these reasons, the NTC recommends that if individuals can be identified in some way via the data message broadcast by C-ITS, legislative provisions should be enacted to limit access to C-ITS information for enforcement purposes. These provisions should set out the circumstances in which police, or another enforcement agency, should seek an access warrant by court order to obtain C-ITS information, in addition to information sharing provisions. Legislation could also state in what circumstances a warrant is not required by an agency (e.g. for non-enforcement purposes, such as traffic management, provided appropriate safeguards are in place).

This approach is aligned with option 2 in the Discussion Paper – specific protection of data (through legislation). This approach should be sufficiently clear not to require published guidelines as discussed in option 3. Further, option 4 (amendment to Surveillance Device legislation) is not feasible given that Queensland does not have equivalent legislation and the apparent ease with which the surveillance device acts can be circumvented by obtaining the subject’s express or implied consent.

This recommendation seeks to determine in what circumstances C-ITS information may be accessed by public entities for enforcement purposes; such legislative provisions should not prescribe roles, responsibilities and personal information flows of a general nature between C-ITS entities. This is consistent with the recommendation made in section 3.1.3.

---

63 Australian Trucking Association, ATA Submission: NTC Cooperative ITS Regulatory Policy Issues Page, 2013, p.10  
64 Queensland Department of Transport and Main Roads, Submission to National Transport Commission: Cooperative ITS Regulatory Policy issues Discussion Paper, 2013, p.6
**Policy Finding:** Privacy concerns represent a potential barrier to the take-up of technology that could significantly improve road safety. Australia should aim for the highest level of privacy protection in the standards set for C-ITS safety systems. This is in keeping with emerging international standards.

**Recommendation 1:** That Austroads adopt privacy by design principles, including the undertaking of a privacy impact assessment, in the development of the C-ITS operational framework.

**Recommendation 2:** That in the development and implementation of a C-ITS operational framework, in particular regarding standards for the data message 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 C-ITS operational framework.

**Recommendation 3:** That Australian Ministers explicitly consider privacy impacts on drivers in any decision relating to institutional arrangements for C-ITS. In particular, any entity that manages and stores unique identifiers is separate from agencies which hold licensing and registration information.

**Recommendation 4:** In the event that individuals can be reasonably identified from the safety data messages 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.
4. Driver Distraction

4.1 Introduction to the issue

Driver distraction has become an increasing concern amongst road safety experts, with the increasing range of technologies within vehicles creating the potential for drivers to have their attention taken away from the driving task.

C-ITS has the potential to create further distractions if not implemented appropriately. The NTC Discussion Paper also examined whether existing legislation place any limits on the use of particular C-ITS devices.

C-ITS have the potential to increase safety, and collision warning systems will be designed to only notify a driver by exception – i.e. an alarm would be generated only when a crash was likely and the driver needed to take evasive action. These alarms should therefore not affect the general driving task the majority of the time. However, designers will need to be careful to ensure that collision warning alarms are sufficiently intuitive that drivers immediately know what to do; poorly designed alarms could decrease safety if they divert attention from the immediate risk or create confusion.

‘Infotainment’ applications may create more of an on-going distraction risk; this is however an existing risk with infotainment systems today. Further C-ITS channels may create new ways for this content to be shared with a vehicle but will not substantially change the risks involved.

4.1.1 Australian Road Rules

Australian Road Rule 299 prescribes the use of in-vehicle televisions or visual display units. Generally, a driver cannot drive a vehicle that has a television receiver or visual display unit that is visible to the driver or could distract other drivers, unless the unit is part of a driver’s aid and is either an integrated part of the vehicle design or is secured in a mounting affixed to the vehicle while being used. Relevant examples of driver’s aids include:

- closed-circuit television security cameras
- dispatch systems
- navigational or intelligent highway and vehicle system equipment
- rear-view screens
- vehicle monitoring devices.

Relevant terms such as ‘visual display unit’ and ‘driver’s aid’ are not specifically defined; but the nature of the examples provided, particularly reference to navigational or intelligent highway and vehicle system equipment, correspond sufficiently with C-ITS technology to suggest that it would be considered a driver’s aid for the purposes of Rule 299.

The NTC recently released the Australian Road Rules 10th Amendment Package Explanation of Amendments July 2013. Amongst the changes proposed is an amendment to Rule 299 “to create consistency by bringing rule 299 in line with rule 300 so that a visual display unit which comprises a driver’s aid includes one which is operating on a mobile phone.” This change would go some way to ensuring a “technology neutral” approach, by allowing a mobile phone to be used as a driver’s aid, which would conceivably include C-ITS applications. However there will remain a difference in treatment between the two, as a mobile phone used as a driver’s aid cannot be touched whilst driving, whilst this is not the case for other driver’s aids.

4.2 Stakeholder feedback

There was general agreement that C-ITS systems need to meet safety objectives while not causing unnecessary driver distraction. Driver distraction was considered to be a potentially significant risk by many, especially for aftermarket devices that will interact with other in-vehicle warnings and information signals. Professor Regan, for example, suggested that C-ITS and Advanced Driver

66 Ibid, p.11.
Assistance Systems (ADAS) need to be integrated from a Human-Machine Interface (HMI) perspective. Warnings need to be carefully integrated, as well as timed and prioritised.

TMR stated that OEMs are addressing HMI issues through international standards\(^{67}\) and reasoned that “an OEM integrated unit should have the best chance of minimising any negative effects,”\(^{68}\) whereas there could be some difficulties at the moment for the aftermarket devices to cooperate with the warning systems developed by auto-manufacturers. However, TMR also observed that while third party systems have a greater potential to cause unwanted distraction, they are also critical for rapid penetration of C-ITS into the vehicle fleet.

ITS Australia placed the distraction issue in a different context:

\[ C-ITS, \text{ unlike many other technologies deployed in vehicles such as ADAS or navigation aids, will for the most part be unobtrusive and hopefully rarely activated unless in the event of a potential incident, dependent on driver behaviour – unlike routine route setting in GPS units or activating Advanced Cruise Control on the daily drive.} \]

This assumes that C-ITS warnings will be infrequent, but some applications such as level crossing warnings could be routine and certainly more frequent than imminent crash warnings. But ITS Australia makes a valid observation and further research may be needed to understand what impact the frequency of warnings has on driver distraction (and driver responsiveness).

Driver distraction should be understood in the context of situational awareness and the behavioural psychology of driving. Professor Regan challenged the comparatively fixed understanding of driver distraction in the Discussion Paper. He suggested that consideration should be given to how drivers’ expectations of the road system, their own driving task and other C-ITS equipped vehicles, will change with the introduction of C-ITS. For example, “danger levels could fluctuate over time depending on the response to the warnings of other drivers with whom they interact.”\(^{70}\) It should also be recognised that driver distraction, like other areas of road safety such as fatigue, has an element of subjectivity. TMR wrote: “what is acceptable for one driver may not suit another driver.”\(^{71}\)

Various submissions proposed further research on a range of issues. For example, NICTA suggested research is needed to understand HMI risks when C-ITS is incorporated into devices such as smartphones, and research is urgently required to understand technical limitations of C-ITS that may also impact upon the driver, such as preventing false alarms when driving under elevated roadways. Professor Regan suggested that the training implications of moving from a C-ITS vehicle to a non-CITS vehicle also need to be explored. Finally the VMC raised that the distraction issues for motorbikes may be very different to those for other vehicles.

**International standards**

Ongoing international research and the development of HMI international standards may resolve many of these challenges and reduce the need for regulatory intervention by governments. Professor Regan observed that the ISO has been active in the development of standards for the integration and prioritisation of warnings from ADAS technologies, while the European Commission-funded AIDE project is also focused on HMI integration.\(^{72}\) NICTA suggested that policy regulation of driver reaction to warnings would be premature at this stage, but that policy makers should keep informed of developments in driver distraction research to facilitate timely and evidence-based policy formulation as the knowledge base evolves.

---

\(^{67}\) Developed by ISO, SAE and UNEC.


The TIC suggested that there is an opportunity for Australia, in consultation and co-development with overseas agencies, to lead the development of an international standard for in-vehicle systems and display devices that can utilise multiple applications.

Not all submissions accepted that the development of standards will ameliorate the risks. TMR proposed an approach that includes both standards and specific regulations that set a limit for visual and audible notifications.

**Amend current road rules** Many of the submissions agreed that current laws may prevent C-ITS benefits from being fully realised due to device format restrictions. TCA suggested that there is not so much a need to use regulatory tools to set uniform standards, as to bring the existing regulations up to date. The ATA, TMR and ITS Australia supported amending the Australian Road Rules to acknowledge changing uses of mobile phones as ‘visual display units.’ The ATA stated that the Australian Road Rules should enable the market to evolve, not constrain innovation, and ITS Australia echoed this view and spoke of ‘technology neutral’ rules. However, ITS Australia also suggested that, to encourage uptake, the Australian Road Rules need to have regard to third party and aftermarket technologies which are more difficult to integrate with other in-vehicle systems and may increase driver distraction.

**Create guidelines or principles for manufacturers** As discussed above, a number of submissions referred to guidelines as an important and appropriate role for government, but primarily to complement international standards. TMR, for example, suggested that a statement of principle for HMI not limited to C-ITS may be needed (in combination with certification). Transport for New South Wales (TfNSW), TCA and Mr Williams supported the introduction of good practice guidelines. The ATA suggested replicating guidelines from the U.S. and Europe, given that most trucks in Australia are of American or European design.

**Certification** The certification of C-ITS systems was raised in some submissions. The WA Government, TMR and Mr Glenn supported certification of C-ITS systems to capture the HMI issues as an alternative to regulations: “this approach would avoid the present situation where road rules are straining to keep up with the current speed of technological change.”

Mr Glenn proposed that the total functioning of a vehicle system needs to be considered by one entity, or system integrator, that can assess proposed subsystems from industry that are put forward as candidate units to fit to vehicles (either in OEM vehicles or after-market devices), then publish and maintain a list of authorised devices.

**Examine technology options as they develop** The Discussion Paper suggested that anti-distraction technologies, such as in-vehicle cameras that track drivers’ eyes, could provide market solutions with a government role overseeing appropriate and agreed standards consistent with the Australian Design Rules (ADRs). Submissions focused more on the development of an integrated vehicle platform to help offset “the trend of bringing disparate ICT into the vehicle.” C-ITS applications do not necessarily have to compete with other information-providing systems and technologies, and can be integrated and prioritised through a single Graphical User Interface (GUI), arbitrated by an in-vehicle ITS station. This approach could create a single interface that prioritises warnings and masks similar alerts originating from various systems which are warning the driver of the same issue.

Much is also being done by industry to develop in-car interface connectivity. Most prominently, in 2011 a leading group of automotive, mobile communications and consumer electronics companies formed the Car Connectivity Consortium to establish global standards for smartphone in-car connectivity. They have produced MirrorLink – a technology standard that allows consumers to access their phones using the same controls they use for accessing the car radio, climate control,

---


and navigation system.\(^75\) Bosch observed that research is also in progress to determine how the driver’s attention should be most appropriately restored from a distraction.

### 4.3 Policy Position

C-ITS applications are one part of a wide range of technologies that are present in today’s vehicles and driver distraction is an issue that is broader than C-ITS and must be addressed in a holistic way. However, C-ITS applications do add weight to the need for governments to look more closely at distraction issues. For example, while feedback from the Discussion Paper did not indicate a need for ADRs to address C-ITS specifically, ADRs should be consistent with the international development of C-ITS driver distraction guidelines and regulations as they emerge.

In the event that international standards are adopted by the market, governments may have a minimal role regulating driver distraction in addition to ADRs and Australian Road Rules, though consideration should be given to a government contribution to the development of industry guidelines or code that formalises the commitment to agreed international standards.

Certification provides additional certainty of standardisation and compliance on a case-by-case basis, but also has cost implications and could potentially impact innovation compared to rule-based self-regulatory approaches.

The recently recommended change to the Australian Road Rules will go some way to ensuring a technology neutral approach, by allowing a mobile phone to be used as a driver’s aid, which would conceivably include C-ITS applications. It may however still leave some differences in the way that a driver can interact with a mobile phone that is being used as a driver’s aid, as opposed to a stand-alone device. The Australian Road Rules may require further examination as the technology continues to evolve.

**Policy Finding:** That current rules around distraction should not present a barrier to the deployment of C-ITS technology. Distraction issues raised by this technology should be considered as part of any broader review of driver distraction rather than in isolation.

**Recommendation 5:** That the NTC should ensure that the Australian Road Rules Maintenance Group considers C-ITS in any future revisions of the Australian Roads Rules, in order to accommodate the emerging role of C-ITS applications and other Advanced Driver Assistance Systems (ADAS) and to take into account emerging international standards relating to technology and distraction.

5. Incentives

5.1 Introduction to the issue

The Discussion Paper included a section on whether benefits should be offered to drivers, manufacturers or operators to encourage the use of Cooperative ITS technology. A number of potential incentives were identified.

5.2 Stakeholder feedback

There was strong and consistent feedback that incentives to encourage C-ITS uptake should depend on clearly demonstrated safety benefits, and that “the size of these benefits would steer the type and size of the incentive.” TCA suggested that incentives should be considered where the community at large benefits rather than the investor directly. There was generally no significant support to target high-risk vehicles or specific driver populations, although Mr Williams focused on heavy vehicles given their significant impact on society.

TMR noted that C-ITS benefits will increase with a higher uptake and therefore suggested that “incentives if required should target uptake by all users rather than a select few.” The ATA also supported incentives and called for a wider discussion about how to increase voluntary uptake, “facilitated by regulatory policy that respects all stakeholder rights,” but warned against governments over-promising rewards which has been the experience in the heavy vehicle sector. TfNSW noted that some of the incentives will be market-driven and not reliant on direct government action, including safety benefits, improved traffic navigation and reduced insurance costs.

Mr Williams proposed that incentives or legislation should be based on a calculable benefit to society in the near and mid-term (based on reduction of fatalities, serious injuries and congestion delays, etc) rather than simply to accrue a high level of penetration. It is recognised that some benefits, such as infrastructure-based warnings related to roadworks, low bridges and unprotected railway crossings, will not require substantial penetration in the fleet population to be effective. Incentives for these applications could be based on per-vehicle benefits without recourse to fleet penetration levels. Nonetheless, a greater challenge exists for those C-ITS applications that require a significant vehicle penetration to have any positive effect whatsoever, such as collision avoidance and blind spot detection. Incentives may therefore be required to accelerate C-ITS uptake for these applications that arguably have the greatest safety benefits.

A number of submissions framed the discussion on incentives as a choice between mandating or incentivising C-ITS. It was suggested that the focus should be on the choice between mandating C-ITS with reflection in ADRs – or unregulated voluntary adoption based on incentives. TMR suggested that “maybe the system is mandated once projected benefits are confirmed.” It is noted that the NHTSA plans to make a decision in late 2013 on whether to mandate C-ITS for light vehicles.

Mr Glenn advocated that mandating C-ITS would reduce the need for incentives and, without it, society would not gain the optimum advantages of C-ITS. Mr Glenn commented that if mandating is not accepted the incentives need to be explicit and significant. These could include registration and insurance discounts, reduced road user charges and priority roads for C-ITS vehicles.

Bosch focused on gaining acceptance and uptake of C-ITS though education and awareness. Bosch drew parallels with Electronic Stability Control (ESC), which has been successfully introduced though informal partnerships between experts, consumer groups, road agencies and insurers, and which grew to include a public awareness campaign:

---


77 Ibid.

78 Australian Trucking Association, ATA Submission: NTC Cooperative ITS Regulatory Policy Issues Page, 2013, p.3
The media joined the call with car magazines (e.g. Wheels) allowing only ESC equipped cars to be considered for their Car of the Year award. At the same time safety rating organisations worldwide (e.g. ANCAP), made ESC mandatory for a 5 star rating. One by one state and federal governments made ESC a compulsory feature on their own fleets and soon after mandated the system through a new ADR.79

The role of education and experience to increase C-ITS uptake was echoed by TMR. Bosch further suggested that C-ITS should not be associated with premium vehicles (e.g. by including it as an optional extra with non-safety features) and noted procurement strategies of governments and industry could focus on ensuring purchasing polices consider new safety systems such as C-ITS.

Other disincentives that need to be overcome were also raised. The VMC observed that some C-ITS applications will not be compatible with powered two-wheelers (PTWs) and the development of C-ITS applications for PTWs could involve higher costs, therefore putting riders at a significant disadvantage. ITS Australia was concerned that potentially complex and proprietary servicing requirements will increase vehicle service costs. TCA made a similar comment: “there is a possibility that, once a commercial market for C-ITS applications develop, the private sector will likely find ways to create streams of revenue from the legitimate sale of services to vehicle owners.”80

5.3 Policy Position

The NTC agrees with the position of stakeholders that safety and productivity benefits of the technology need to be more clearly demonstrated before financial or other incentives are considered. Information from the American trial (which had yet to release its findings at the time of writing) will be an important input for this. Trials and tests will be needed (i) to show whether there is in practice a safety benefit to this technology and (ii) to quantify the value of this benefit in order to determine the appropriateness and level of incentives.

The NTC recommends that Ministers revisit the issue of incentives in the 2014-2015 financial year, once any benefits of the technology have been better quantified.

The NTC notes that the Australiasian New car assessment program (ANCAP) has included V2V and V2I technologies as one of its ‘Safety Assist Technologies’81 for the purposes of counting towards a vehicle’s star rating. The number of Safety Assist Technologies required in order to attain a five star rating rises each year as part of the ANCAP Rating Road Map 2011-2017. The standard used is yet to be determined however. Encouraging the use of safety technologies in a flexible manner through the ANCAP rating system may be the most appropriate form of incentive at this early stage of development.

| Policy Finding: There is a need for the safety benefits of C-ITS technology to be proven more fully before governments provide any new incentives towards its implementation. |

---

6. Other issues

6.1 Human Factors

Human factor considerations can have a significant impact on whether safety technology delivers on predicted benefits. Humans can often behave in complex and unpredictable ways, whereas technology behaves as programmed, so the interaction of the two can lead to unforeseen results. A study of recent crash avoidance technology, based on insurance claims data, concluded that:

An early crop of advanced crash avoidance technologies includes some clear success stories when it comes to preventing crashes... Forward collision avoidance systems, particularly those that can brake autonomously, along with adaptive headlights, which shift direction as the driver steers, show the biggest crash reductions. Lane departure warning appears to hurt, rather than help, though it's not clear why, and other systems, such as blind spot detection and park assist, aren't showing clear effects on crash patterns yet.\textsuperscript{82}

In assessing safety and hence liability issues, it is vital to look at the technical and human factors which may impact on safety. These factors, outlined below, range from over-reliance by drivers on the new technology to failure to use it.\textsuperscript{83}

Drivers’ over-reliance/ behavioural adaptation: with any new driving technology there is a risk of over-reliance by drivers: ‘avoiding false expectations will be important to ensure safety.’\textsuperscript{84} Drivers may adapt their behaviour based on safety systems, for example where the use of a reverse collision warning leads to drivers’ failing to look behind them when reversing. Systems always have limitations and this adaptation can lead to additional dangers, particularly in an environment where not all vehicles are connected.

Awareness of capabilities and limitations: a related issue is that if users are not aware of a system’s capabilities and limitations they can overestimate its capability.

Risk compensation: a potential issue for any new safety system is risk compensation, that is the notion that drivers may drive in a more risky fashion due to a greater feeling of safety as a result of additional safety systems.

Distraction: driver distraction is an increasing concern as in-car systems and their interfaces become more complex. Designers will need to ensure warnings are not startling and that the design of information is ergonomically appropriate. Well-designed warnings ‘should be carefully calibrated in the sense of being decipherable, comprehensive, parsimonious, obvious and executable’.\textsuperscript{85}

Risk exposure change: technology can change people’s travel patterns, with a resultant change in their exposure to risk. An example is GPS navigation systems, which may have led more drivers to complete trips in unfamiliar locations; increasing their driving and changing their risks. Changes in driving as a result of C-ITS are at this stage difficult to predict.

Skill loss: increasing driver aids may lead to a loss of driver skill, which can be critical when a driver aid fails and the driver no longer has the collision avoidance skills to deal with a critical situation. Airlines seek to avoid this with their pilots through flight simulator training. In comparing automatic cruise control and C-ITS applications, the European Commission’s Cooperative Vehicle-Infrastructure Systems project (CVIS) found that:

\textsuperscript{82} Insurance Institute for Highway Safety, Crash avoidance features reduce crashes, insurance claim study shows; autonomous braking and adaptive headlights yield biggest benefits, news release, 3 July 2012, http://www.iihs.org/news/rss/pr070312.html (viewed on 18/10/2012).

\textsuperscript{83} This section is based in large part on discussions with Professor Mike Regan and the NTC would like to acknowledge his contribution to our understanding of these issues.

\textsuperscript{84} Rand Corporation, Liability and Regulation of Autonomous Vehicle Technologies, 2009.

The overall probability of a simultaneous failure of an automated system and the driver, resulting in an accident, is the product of the probability of a system failure and the probability of a failure by the driver to respond if the system cannot. Clearly, the issue here is to ensure that the level of driver attention does not fall so low that the overall performance is worse than without the system. In fact, the result needs to be substantially better in order to justify the benefits.

Driver acceptance: drivers may not accept and use the technology. A historical example is seat belts. Regulation was required to ensure that seat belts were fitted on all vehicles to change driver and passenger habits (and there still remains a percentage of drivers and passengers who do not use them). Regulatory policy issues can also have an effect on public perception and uptake – will the public perceive these systems as a benefit to themselves and their safety? Initial studies indicate strong public interest, with a recent on-road trial in the United States finding that ‘more than 90 per cent of the participants believed a number of specific features of the connected vehicle technology would improve driving in the real world, including features alerting drivers about cars approaching an intersection, warning of possible forward collisions, and notifying drivers of cars changing lanes or moving into the driver’s blind spot.’

The study did, however, also indicate a limit on what consumers are willing to pay, with drivers indicating that such systems would not be worth purchasing if they were over US$250. Regulatory policy issues – in particular privacy, compliance and enforcement issues – may also have a significant impact on acceptance.

**Recommendation 6:** That research, based on identified gaps in international research that are relevant to Australia, is conducted to measure the human factor impacts of C-ITS applications; and to determine whether any mitigating policy measures are required in order to obtain the safety benefits without creating additional risks.

### 6.2 Automated systems

Over recent years there has been an increasing focus internationally on the potential of fully automated vehicles. Driverless trains have been in use for a number of years; mining companies in Australia and elsewhere are also beginning to use driverless trucks. These are however based in very controlled environments, quite different to the open road. However even on public roads companies in the United States are trialling autonomous vehicles and at least two US States have set up a process for the licensing of such vehicles.

Many elements of the legal system for our roads are based on the assumption that the driver is considered to be in control of the vehicle. This is derived from the Vienna Convention on Road Traffic. Although Australia is not a signatory to this convention, a similar principle is included in the Australian Road Rules: ‘a driver must not drive a vehicle unless the driver has proper control of the vehicle.’

---


90 Australian Road Rules, Regulation 297.
The NHTSA has recently released a Preliminary Statement of Policy Concerning Automated Vehicles\(^\text{91}\) which states that “America is at a historic turning point for automotive travel.” The Statement sets out a series of four levels of automation:

- Level 1 – Function-specific Automation
- Level 2 – Combined Function Automation
- Level 3 – Limited Self-Driving Automation
- Level 4 – Full Self-Driving Automation

It also lists current NHTSA research streams, which include human factors; electronic control systems safety (including reliability and cyber-security); and system performance requirements.

NHTSA Preliminary Statement of Policy Concerning Automated Vehicles

I—Recommendations for Licensing Drivers to Operate Self-Driving Vehicles for Testing

A—Ensure that the Driver Understands How to Operate a Self-Driving Vehicle Safely

II—Recommendations for State Regulations Governing Testing of Self-Driving Vehicles

A—Ensure that On-road Testing of Self-driving Vehicles Minimizes Risks to Other Road Users

B—Limit Testing Operations to Roadway, Traffic and Environmental Conditions Suitable for the Capabilities of the Tested Self-Driving Vehicles

C—Establish Reporting Requirements to Monitor the Performance of Self-Driving Technology during Testing

III—Recommended Basic Principles for Testing of Self-Driving Vehicles

NHTSA does not recommend that states attempt to establish safety standards for self-driving vehicle technologies, which are in the early stages of development.

A—Ensure that the Process for Transitioning from Self-Driving Mode to Driver Control is Safe, Simple, and Timely

B—Self-Driving Test Vehicles Should Have the Capability of Detecting, Recording, and Informing the Driver that the System of Automated Technologies has Malfunctioned

C—Ensure that Installation and Operation of any Self-Driving Vehicle Technologies Does not Disable any Federally Required Safety Features or Systems

D—Ensure that Self-Driving Test Vehicles Record Information about the Status of the Automated Control Technologies in the Event of a Crash or Loss of Vehicle Control

IV—Regulations Governing the Operation of Self-Driving Vehicles for Purposes Other than Testing

NHTSA does not recommend that states authorize the operation of self-driving vehicles for purposes other than testing at this time. We believe there are a number of technological issues as well as human performance issues that must be addressed before self-driving vehicles can be made widely available.

Stakeholders that the NTC has consulted with for this project have expressed very different views as to the likely timeframes for commercial deployment of automated vehicles; some consider that it will happen quite quickly while others believe that it is decades away.

There is undoubtedly growing research and development in this area and a variety of elements of the driving experience are becoming more supported and eventually more automated. The NTC believes that there would be benefit for Australia to examine the potential implications of more automated vehicles, moving towards full automation, on the Australian transport system.

Figure 3: **Spectrum of advanced driver assistance systems**

<table>
<thead>
<tr>
<th>Driver-warning systems (e.g., forward collision warning)</th>
<th>Short-term driving systems (e.g., ACC and lane keeping combined)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conventional vehicles</td>
<td>Partial control systems (e.g., ACC and precrash safety)</td>
</tr>
<tr>
<td></td>
<td>Autonomous vehicles with driver-in-the-loop</td>
</tr>
<tr>
<td></td>
<td>Driverless cars</td>
</tr>
</tbody>
</table>

**Recommendation 7:** That research, based on identified gaps in international research that are relevant to Australia, examine the impact of more automated vehicles from a policy and legislative perspective, including the impact on the role of the driver.

### 6.3 International Standards

A number of stakeholders emphasised the importance of aligning Australia with international C-ITS standards. While there are opportunities for Australian organisations to innovate and develop new technologies and solutions, most C-ITS components will likely be imported (as most of our vehicles are) and it will be crucial that C-ITS implementation in Australia is consistent with international standards. Standards Australia is already seeking to ensure Australian practices are harmonised with international standards, while undertakings by Europe and the United States to improve harmonisation, particularly in relation to vehicle platform standards, should facilitate the development and implementation of international standards in Australia.

Australian representatives are also involved in a number of international standards-making organisations and committees, and Australia should continue to actively contribute to the development of international standards. The development of Australian applications should reference international standards wherever possible.

### 6.4 Vulnerable road users

A number of stakeholders, both in written submissions as well as in broader discussions, expressed concern over the potential impact of C-ITS technology on vulnerable road users, including motorcyclists, cyclists and pedestrians. It would make little sense from a community perspective if C-ITS applications make driving safer for motor vehicle drivers, but in fact increase risks for other road users.

At the same time, there is potential for C-ITS to also increase safety for these users. The current trial of C-ITS technology in Ann Arbor includes a small number of equipped cyclists and

---

92 Rand Report, op. cit.
motorcyclists. These road users are able to broadcast their position to surrounding traffic, potentially significantly increasing their visibility to car and heavy vehicle drivers and thus reducing the risk of collisions. However, such conclusions are still to be proven by the data.

While pedestrians are unlikely to carry devices that broadcast their position in this way, there have been suggestions that this could be done through a person’s mobile phone. Pedestrians could also be affected if drivers come to rely heavily on signals sent by other vehicles and hence pay less attention on the road; they could be affected if for example C-ITS applications lead to more dynamic traffic signalling which (from a pedestrian’s perspective) could result in less certainty of the sequencing of traffic lights.

The NTC did not focus on vulnerable road users in its Discussion Paper, however it certainly acknowledges the importance of these road users and the need for any new applications to take them into account.

**Recommendation 8:** That in the development of the C-ITS operational framework, Austroads explicitly takes into consideration the differential impact of C-ITS on vulnerable road users, including pedestrians, motorcyclists and cyclists.

### 6.5 Other Stakeholder feedback

In relation to driver training, the VMC observed in the context of PTWs that many C-ITS applications will compensate for driving errors and, when warnings are initiated, users must still know what to do with the information that C-ITS provides. C-ITS technologies will not, therefore, obviate the need to maintain and improve riding (and driving) skills; “better training could in and of itself provide substantial safety benefits particularly if conducted system wide.”93 While these comments were made in relation to PTWs, there is a clear need to ensure that technologies are not introduced at the expense of reduced driving skills more generally. Bosch suggested that technology and distraction could be designed as part of the assessment program for young drivers, similar to the German approach of driver training and licensing.

The NTC agrees that the attainable safety benefits of C-ITS will in part be reliant on driver training and driving skills adapted to the introduction of C-ITS. Research to investigate human machine interface issues specific to C-ITS, recommended in this paper, would also be expected to have regard to the issues raised here, including further understanding how drivers react to advisory warnings.

In relation to heavy vehicle applications, TCA called on governments to raise awareness of current heavy vehicle initiatives to increase acceptability of C-ITS more widely: “the regulated vehicle sector is an area where the population can quickly see the benefits both in managing the consequences of the presence of commercial vehicles, and in the reduction of the cost of administration.”94 TCA suggested three areas where C-ITS could support the heavy vehicle sector: safe and secure parking for heavy vehicles, Smart Roadside Infrastructure (that streamlines heavy vehicle enforcement checks and information sharing), and eCall. ATA and ALC both noted that the Heavy Vehicle Charging and Investment (HVCI) reform is also considering options to utilise telematics devices to measure heavy vehicle mass, distance and location for charging purposes, which may also have a role for C-ITS applications, but without delaying the charging reforms. This interest in the role of heavy vehicles was supported by TfNSW which sees C-ITS as an effective tool to support the regulation of heavy vehicles as well as to enhance safety for heavy vehicle drivers and the community. The Commonwealth Department of Infrastructure and Regional Development suggested that future strategic uses of C-ITS should also consider how the technology could facilitate new ways of regulating more generally.

---


The NTC agrees that C-ITS technology presents a unique opportunity to improve the operational, safety and compliance practices of heavy vehicle operations. While this policy paper does not consider specific applications or commercial sectors in detail, it does note that compliance and enforcement activities underpinned by C-ITS should be consistent with privacy principles and surveillance device laws. While acknowledging the compliance and enforcement potential of C-ITS, this paper suggests that community expectations – including the expectations of drivers in the heavy vehicle sector – are such that C-ITS technologies will have a low uptake unless the use of C-ITS personal information for enforcement purposes is clearly demarcated in legislation.
7. Conclusion

C-ITS have significant potential to improve outcomes in the Australian transport network. However, the implementation of this technology and the policy settings around it will need to be carefully thought through to ensure Australia gains the maximum benefits, without creating unforeseen consequences. Policy needs to ensure that beneficial technology can be used in this country while also appropriately managing the risks. Importantly, the NTC did not find any legislative roadblocks to the deployment of the technology in Australia.

It will be critical to provide individuals with assurance around privacy and how data will be used. The highest level of protections should be made available. It will also be crucial to consider the impact of C-ITS technology on vulnerable road users to ensure that risks are not reduced for some road users but increased for others.

Some of these issues will need to be revisited over time as the technology and its use evolve.

The NTC has also recommended further research in the areas of human factor issues and the role of increasingly automated systems in vehicles. Again, this research will be important in understanding and managing any additional risks.

7.1 Summary of Findings and Recommendations

**Liability**

**Policy Finding:** No changes are recommended to current laws and approaches around liability for drivers, manufacturers and road managers in regard to the roll out of C-ITS technology.

**Privacy – Private Sector**

**Policy Finding:** No changes are recommended to current privacy laws governing the private sector development of C-ITS systems and data. Companies will need to closely follow the National Privacy Principles as required, as they do for C-ITS systems that have already been developed.

**Privacy – Public Sector**

**Policy Finding:** Privacy concerns represent a potential barrier to the take-up of technology that could significantly improve road safety. Australia should aim for the highest level of privacy protection in the standards set for C-ITS safety systems. This is in keeping with emerging international standards.

**Recommendation 1:** That Austroads adopt privacy by design principles, including the undertaking of a privacy impact assessment, in the development of the C-ITS operational framework.

**Recommendation 2:** That in the development and implementation of a C-ITS operational framework, in particular regarding standards for the 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.

**Recommendation 3:** That Australian Ministers explicitly consider privacy impacts on drivers in any decision relating to institutional arrangements for C-ITS. In particular, any entity that manages and stores unique identifiers is separate from agencies which hold licensing and registration information.
**Recommendation 4:** In the event that individuals can be reasonably identified from the safety data messages 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.

**Driver Distraction**

**Policy Finding:** That current rules around distraction should not present a barrier to the deployment of C-ITS technology. Distraction issues raised by this technology should be considered as part of any broader review of driver distraction rather than in isolation.

**Recommendation 5:** That the NTC should ensure that the Australian Road Rules Maintenance Group considers C-ITS in any future revisions of the Australian Roads Rules, in order to accommodate the emerging role of C-ITS applications and other Advanced Driver Assistance Systems (ADAS) and to take into account emerging international standards relating to technology and distraction.

**Incentives**

**Policy Finding:** There is a need for the safety benefits of C-ITS technology to be proven more clearly for governments to provide any new incentives towards its implementation.

**Other Issues**

**Recommendation 6:** That research, based on identified gaps in international research that are relevant to Australia, is conducted to measure the human factor impacts of C-ITS applications; and to determine whether any mitigating policy measures are required in order to obtain the safety benefits without creating additional risks.

**Recommendation 7:** That research, based on identified gaps in international research that are relevant to Australia, examine the impact of more automated vehicles from a policy and legislative perspective, including the impact on the role of the driver.

**Recommendation 8:** That in the development of the C-ITS operational framework, Austroads explicitly takes into consideration the differential impact of C-ITS on vulnerable road users, including pedestrians, motorcyclists and cyclists.
8. Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACMA</td>
<td>Australian Communications and Media Authority</td>
<td>The Commonwealth agency responsible for planning and regulating the radiofrequency spectrum in Australia.</td>
</tr>
<tr>
<td>ADAS</td>
<td>advanced driver assistance systems</td>
<td>A broad category of vehicle technology that does not necessarily use C-ITS. ADAS includes Advanced Cruise Control.</td>
</tr>
<tr>
<td>ADR</td>
<td>Australian Design Rules</td>
<td>Performance-based national standards for vehicle safety, anti-theft and emissions.</td>
</tr>
<tr>
<td>ANPR</td>
<td>automatic number plate recognition</td>
<td>Optical character recognition software to convert images of vehicle registration numbers into data matching information used for law enforcement or other purposes, such as tollway operations.</td>
</tr>
<tr>
<td>C-ITS</td>
<td>cooperative intelligent transport systems</td>
<td>A technology platform that enables components of the transport network to share real-time information to improve safety and traffic outcomes.</td>
</tr>
<tr>
<td>CVIS</td>
<td>cooperative vehicle-infrastructure systems</td>
<td>European Commission research and development project to design, develop and test C-ITS technologies.</td>
</tr>
<tr>
<td>DSRC</td>
<td>dedicated short range communication</td>
<td>A short to medium range communication service allocated for automotive and transport use. C-ITS are based on DSRC-technology.</td>
</tr>
<tr>
<td>EDR</td>
<td>event data recorders</td>
<td>An in-vehicle device that records information relating to a vehicle crash or incident and is triggered by an engine fault or an abrupt change to speed.</td>
</tr>
<tr>
<td>GNSS</td>
<td>global navigation satellite system</td>
<td>A satellite navigation system that provides geospatial positioning with global coverage, based on longitudinal, latitudinal and altitudinal data.</td>
</tr>
<tr>
<td>IAP</td>
<td>Intelligent Access Program</td>
<td>A program that uses GNSS technology to monitor a heavy vehicle’s road use, providing an operator with flexible access to the network to suit specific business and operational needs.</td>
</tr>
<tr>
<td>IPP</td>
<td>Information Privacy Principles</td>
<td>Commonwealth and state privacy principles introduced for the public sector.</td>
</tr>
<tr>
<td>NHTSA</td>
<td>National Highway Traffic Safety Administration</td>
<td>US agency that directs motor vehicle and highway safety and consumer programs.</td>
</tr>
<tr>
<td>NPP</td>
<td>National Privacy Principles</td>
<td>Commonwealth privacy principles introduced for the private sector.</td>
</tr>
<tr>
<td>Acronym</td>
<td>Organisation</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>NTC</td>
<td>National Transport Commission</td>
<td>An independent body established to develop national regulatory and operational reforms and implementation strategies for safer, more efficient and sustainable road, rail and intermodal transport across Australia.</td>
</tr>
<tr>
<td>RiTA</td>
<td>Research and Innovation Technology Administration</td>
<td>US agency that coordinates the Department of Transportation’s research and education programs, including advanced transport technologies.</td>
</tr>
<tr>
<td>TIC</td>
<td>Truck Industry Council</td>
<td>Peak body representing heavy vehicle manufacturers and major component supplier groups in Australia.</td>
</tr>
<tr>
<td>V2I</td>
<td>vehicle-to-infrastructure</td>
<td>Cooperative ITS information exchanged between vehicles and infrastructure, such as roadways or traffic lights.</td>
</tr>
<tr>
<td>V2N</td>
<td>vehicle-to-nomadic device</td>
<td>Cooperative ITS information exchanged between a vehicle and a nomadic device, which may be located on a pedestrian, cyclist or inside another vehicle.</td>
</tr>
<tr>
<td>V2V</td>
<td>vehicle-to-vehicle</td>
<td>Cooperative ITS information exchanged between two or more vehicles.</td>
</tr>
<tr>
<td>VMC</td>
<td>Victorian Motorcycle Council</td>
<td>An organisation supporting and representing Victorian motorcyclists.</td>
</tr>
</tbody>
</table>
9. Stakeholder feedback to the discussion paper

Table 2. Submissions received from the discussion paper

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mr Bob Williams - CSI (UK) Ltd</td>
<td></td>
</tr>
<tr>
<td>Mr Ross Lang - private submission</td>
<td></td>
</tr>
<tr>
<td>Mr Ron Glenn - private submission</td>
<td></td>
</tr>
<tr>
<td>Australian Logistics Council (ALC)</td>
<td></td>
</tr>
<tr>
<td>WA Main Roads</td>
<td></td>
</tr>
<tr>
<td>Livestock and Rural Transport Association of Western Australia</td>
<td></td>
</tr>
<tr>
<td>Professor Marcus Wigan - private submission</td>
<td></td>
</tr>
<tr>
<td>NICTA</td>
<td></td>
</tr>
<tr>
<td>ITS Australia</td>
<td></td>
</tr>
<tr>
<td>Truck Industry Council</td>
<td></td>
</tr>
<tr>
<td>Bosch (Australia)</td>
<td></td>
</tr>
<tr>
<td>Captain Chris Skinner - private submission</td>
<td></td>
</tr>
<tr>
<td>Professor Mike Regan - Transport and Road Safety (TARS) Research School of Aviation University of New South Wales</td>
<td></td>
</tr>
<tr>
<td>Victorian Motorcycle Council</td>
<td></td>
</tr>
<tr>
<td>Dr Clive Boughton - private submission</td>
<td></td>
</tr>
<tr>
<td>Commonwealth Department of Infrastructure and Transport – now Infrastructure and Regional Development</td>
<td></td>
</tr>
<tr>
<td>Royal Automotive Club Queensland (RACQ)</td>
<td></td>
</tr>
<tr>
<td>Australian Trucking Association (ATA)</td>
<td></td>
</tr>
<tr>
<td>Privacy Victoria</td>
<td></td>
</tr>
<tr>
<td>Queensland Department of Transport and Main Roads (TMR)</td>
<td></td>
</tr>
<tr>
<td>SA Privacy Committee</td>
<td></td>
</tr>
<tr>
<td>Transport Certification Australia (TCA)</td>
<td></td>
</tr>
<tr>
<td>Transport for NSW (TfNSW)</td>
<td></td>
</tr>
<tr>
<td>Federal Chamber of Automotive Industries (FCAI)</td>
<td></td>
</tr>
</tbody>
</table>