14 November 2018

QUEENSLAND DEPARTMENT OF TRANSPORT AND MAIN ROADS

RESPONSE TO THE NATIONAL TRANSPORT COMMISSION DISCUSSION PAPER ON REGULATING GOVERNMENT ACCESS TO C-ITS AND AUTOMATED VEHICLE DATA

Executive summary

Connected and Automated Vehicle (CAV) technologies are in their early development stages and the way in which information and data will need to be exchanged to ensure safe operations is yet to be fully established. However, the public benefits from these technologies are potentially enormous with even conservative estimates for savings in congestion ($20 billion per annum) and road trauma ($27 billion per annum) significant.

Road safety performance lags behind the safety performance of all other modes of transport (rail, air and maritime) by two to three orders of magnitude. Whilst the National Transport Commission's (NTC) discussion paper examining the regulation of government access to C-ITS and automated vehicle data acknowledges there are potential benefits from CAV technologies and associated data, it does not explore this in sufficient detail. In this sense the paper does not provide strategic advice to governments on the importance of data sharing in a CAV ecosystem. Many experts are now of the view that full automated driving is unlikely without connectivity and for connectivity there will necessarily be a requirement to share data. This sharing will need to occur in a trusted and secure manner which is a critical element of the European data security architecture. To realise the benefits of CAV data, the European Commission has acknowledged that many of the Connected Intelligent Transport Systems (C-ITS) use cases will need to be exempt from the recently adopted European General Data Protection Regulation.

The discussion paper, and associated NTC project, focuses narrowly on establishing if CAV data constitutes personal information. It does this based on a range of assumptions around how the technology will work and what access governments will have to such data. As this submission identifies, many of these assumptions are inconsistent with existing frameworks or require further testing. For example, caution should be taken in any departure from the current European Standards for C-ITS technologies (which Australian governments and industry have agreed to align with) and industry arrangements.

In addition, the discussion paper does not adequately acknowledge existing mechanisms employed by Australian Governments to regulate, manage and protect private data and information. A range of governance measures are in place to ensure appropriate consideration is given to privacy issues and personal information is treated sensitively by government agencies. This includes, parliamentary legislative processes (requiring community consultation and parliamentary review and debate) that enact specific authorising law in relation to collection, used and disclosure of personal information; adherence to privacy legislation and principles by government agencies; data handling standards and techniques; access controls, restrictions and security protections; and disciplinary measures for unauthorised access and use.

Based on the information provided, the Queensland Department of Transport and Main Roads (DTMR) is unable to indicate a preference for any of the options developed by the NTC. The existing privacy framework (option 1) may not be appropriate for CAV technologies as it is as yet unclear if it will provide for adequate access to CAV data that governments will need to perform essential services, such as law enforcement, as well as maximise public benefits. While broad principles (option 2) may assist in the consideration of future privacy reforms for CAVs, it is critical that these principles do not unnecessarily impede the development of CAV technologies. In their current form, the principles proposed by the NTC are not supported by DTMR. Finally, there are too many assumptions which have yet to be validated to consider more specific reform options (such as options 3 or 4) which will limit access to CAV data without a thorough understanding of use cases and benefits.

It is recommended that the NTC consider a broader scope to conduct a more holistic review of privacy issues associated with CAV data. As identified below, a broader mandate may be required to complete this that looks beyond traditional transport boundaries. DTMR, on behalf of the Queensland Government, looks forward to a continued and productive partnership with the NTC and other Australian governments to work through the privacy issues associated with CAV data and deliver outcomes that ensure the protection of personal information and that maximise public value and safety.

Introduction

Appropriate access to, and protection of, CAV data is critical to the technologies' deployment and for maximising the associated benefits. The regulation of CAV data must ensure that all entities act in a responsible manner and in a way that protects the individuals to whom the information relates. Similarly, legitimate use cases for CAV data must be identified and enabled to ensure that the societal benefits of these transformative technologies are realised.

State and territory governments will ultimately have to progress reforms to facilitate the introduction of CAV technologies, in the context of the reform agenda being led by the NTC. In order to be successful in achieving the desired harmonised national approach, these reforms should reflect an agreed approach across all jurisdictions. This requires policy issues to be well-considered, addressing all relevant factors and aspects.

In this respect, data management and information privacy is a complex issue that needs thorough and considered policy development. To facilitate the introduction of CAV technologies a holistic approach to privacy issues is required that:

- validates all assumptions;
- considers a broad scope, including both government and non-government entities that will be responsible to collecting and managing CAV data;
- is based on a thorough understanding of use cases and their benefits;
- ensures appropriate mechanisms exist to facilitate lawful access to data;
- ensures appropriate mechanisms exist to facilitate technical assurance of CAV systems;
- provides appropriate protections for personal information; and
- aligns with international best practice, as far as is reasonably possible.

These issues are addressed below in more detail.

Validate assumptions

A number of underlying assumptions are made throughout the discussion paper that have not necessarily been tested and are inconsistent with the current C-ITS European standards for connected vehicles and current practice for vehicle based data collection. While it is acknowledged that some assumptions are listed in section 1.10 and the subject of consultation question 1, other assumptions are made without further assessment.

There is an underlying assumption that government access to CAV data will be a barrier to consumer adoption of the technologies. It is not clear if this assumption has been validated with consumers and appears inconsistent with experiences in other technology adoption. Privacy will likely be one of many factors that influence consumers' decisions to adopt CAV technologies. In addition, there may be general support for legitimate access to data that achieves a societal benefit or common good, in particular improved road network safety and law enforcement purposes. Ultimately, there is a need for transparent and comprehensive community engagement that addresses all aspects of data use and privacy.

There also seems to be an assumption made that governments will have direct access to and collection powers for a large amount of CAV data. The future technological landscape is unclear as to what data governments will directly collect. There may be a risk to the security and safety of CAV technologies if governments do not have access to some CAV data to provide appropriate oversight of technical platforms. In addition, it is very likely that the most sensitive personal information will be collected directly by industry. Analysis is required to ensure this will be treated appropriately.

There is a further assumption that that this new source of data is inadequately dealt with under information privacy laws and broader legislative frameworks. DTMR acknowledges that the purpose of this consultation is in some respects aimed at testing this assumption. As such, DTMR seeks to address this in its response to the consultation questions and options presented in this paper.

Scope of information privacy assessment

DTMR is of the view that there is a need for a future work package that comprehensively reviews the privacy issues associated with all CAV data use cases, extending to consideration of the collection, storage, use and disclosure of this data. This should include both government and non-government entities. Given the scale and depth of information collected and need to protect consumer rights, a holistic review of privacy protections is required to ensure that all entities act appropriately and responsibly. It is acknowledged that, in some cases, there are other projects underway that explore these issues. It is DTMR's preference that this work be brought together so a more comprehensive approach can be taken. This will enable jurisdictions to ultimately present a complete package of reforms to their respective governments.

Future work would also benefit from a wider consideration of what data will be held by industry that governments may need access to so as to ensure a connected and automated ecosystem operates safely and delivers on public expectations and benefits.

Policy informed by use cases

The discussion paper is based on the view that that legislative amendments are required to impose greater restrictions on government collection and use of CAV data. However, it is not possible to make this assessment at this time without knowing what powers are or should be available to support the access and use of data and then examining whether existing protections are sufficient.

While some uses for CAV data are provided in the discussion paper and listed at Appendix C, a comprehensive review of use cases is required to understand the scale and scope of legitimate uses. This should include consumers, industry and government and be the starting point for understanding what access provisions and privacy protections are required. Without a comprehensive understanding of what data will be collected and how it will be used, it is premature to consider what protections need to be put in place.

This review must look beyond the current state and plan for use cases that may be of significant advantage to the community in terms of public safety, congestion management and expenditure management. It is recommended that CAV use cases under development and described in northern hemisphere government and industry roadmaps be considered in more detail. The data generated by CAV technologies has the potential to deliver significant commercial and public value and both industry and government have legitimate interests in using this information. For instance, CAV related data has the potential to inform government investment into road infrastructure at an unprecedented granular level. While some use cases are acknowledged in the discussion paper, further work is required to understand future use cases, what authorising legal environment is required and what, if, any additional privacy protections need to be put in place. To this end, there is also a need to make a distinction between personal information and other information derived from CAV sources, and the fact that many use cases will not trigger privacy issues if data is collected and aggregated in an appropriate way or secured in a manner that makes identification of individuals improbable.

Lawful access to data

Although it is noted in several sections of the discussion paper that privacy principles, as found in state, territory and commonwealth information privacy legislation, do not expressly provide access to data, the policy analysis and option development seem to be based on a contrary view. DTMR reiterates previous comments that the Information Privacy Principles contained in the Queensland *Information Privacy Act 2009* regulate the collection and management of personal information. However, they do not authorise or permit the collection or disclosure of personal information. In order for government to collect, use and disclose personal information appropriate and specific lawful mechanisms must exist. It is also worth noting that the specific legislative mechanisms can override the obligations regarding collection and management of personal information in the general privacy legislation. For clarity, it is not possible to consider if the existing privacy framework is appropriate to manage CAV data in the future, because the future regulatory landscape will need to prescribe how CAV data is to be managed. When access provisions are drafted, policy makers will need to consider and create privacy protections at the same time.

While the discussion paper alludes to a number of requirements for additional authorisations to ensure government can collect and use data for legitimate purposes, there is insufficient detail provided to understand how these will differ from current authorisations.

Although it is useful to start thinking about privacy issues associated with CAV technologies, DTMR recommends further assessment and decisions relating to privacy issues be delayed until a clearer view of the future regulatory and technological environment develops. In particular, there appears to be a need to have a greater understanding of the requirements to support the proposed safety assurance system and associated compliance and enforcement mechanisms.

Appropriate privacy protections

Appropriate privacy protections are critical to ensuring personal information is handled responsibly and in line with public expectations. Queensland and Australia have mature information privacy frameworks that already manage significant amounts of personal information and it is prudent to understand why the existing frameworks are not sufficient before considering wholesale changes. There needs to be a clear case that CAV data is different and not already appropriately addressed under legislation, or if not, whether existing policy settings for the use of personal information can be extrapolated.

It is important to recognise that transport authorities have the largest repositories of personal information relating to Australian citizens compared with any other government agency. This is due to our licensing and vehicle registration functions. This is a role that transport agencies take seriously, and have well advanced policies, systems and processes for managing individual privacy. The NTC should be looking to learn from, and build upon, this knowledge and experience.

Alignment with international best practice

Europe is leading the way in the development of C-ITS data information security standards that strike a balance between public use for societal benefit and personal privacy requirements. The Article 29 Data Protection Working Party released an opinion paper which was adopted in October 2017 that provided background information on the processing of personal data in the context of C-ITS and sought guidance on the level of data protection that will apply.

Australian governments, the Federal Chamber of Automotive Industries and other ITS industries have agreed to implement the European technical design, where possible. The easiest way for C-ITS to be available in Australia would be if Australia can harmonise with European requirements. The consideration of privacy policy principles in Australia needs to take into account the likely European approach to managing C-ITS data, including that the technical solution will put in place substantial controls to ensure information security and privacy. If Australia's data protection requirements differed from Europe, European OEMs may be unlikely to bring their technologies to our market. This is seen as a far greater barrier to consumer adoption than individual privacy concerns.

Europe is still working through security and privacy designs based on the current standards, policies, procedures and regulation. DTMR is of the view that we should not at this early stage depart from the decision to harmonise with the European approach and we should wait to see how their design balances privacy with the public good, and genuinely assess if that approach is suitable for Australia. We need to carefully consider the cost of changing any of the European implementation. Changes may impact the flow of technology and applications into Australia.

DTMR's Connected and Autonomous Vehicle Initiative (CAVI), which is the largest government run CAV trial in Australia has been designed based on the EU implementation, as far as possible.

NTC's mandate

Based on the information presented in the discussion paper and advice from the NTC at consultation sessions, DTMR is of the view that the NTC may need to seek a broader mandate to conduct a holistic review of CAV data privacy issues as detailed above. DTMR has concerns that a siloed approach to policy development will hamper the ability for jurisdictions to address all of the issues that ultimately need to be reviewed. That is, a future review should not be bound by traditional 'transport' boundaries. In addition, a future mandate should permit the review of both government and non-government access and use of CAV data.

It is recommended that the NTC seek this broader mandate from the Transport and Infrastructure Council at the next available opportunity.

DTMR Response to consultation questions

1. Are the assumptions the NTC has identified for this discussion paper reasonable?

As noted above, there are a number of assumptions made throughout the discussion paper that don't appear to have been tested.

- The assumption that government access to CAV data will be a barrier to technology adoption needs to be validated. Premature adoption of principles may be a bigger barrier to realising public benefits than the assumed privacy concerns by the public. Whilst privacy is one of the relevant factors, there will be a number of other relevant considerations. Many legitimate use cases such as law enforcement are already widely accepted across vehicle and other technologies and do not present barriers to consumer adoption. It is perhaps more likely that the wide scale use of personal information by private sector parties will present as a barrier to technology if not appropriately limited by law and relevant sanctions. It would be helpful to develop a range of use cases to test these issues with the community.
- The assumption that governments will have automatic and unfettered access to CAV data is a distortion. Although there are a number of unknowns about the future technology, it is far more probable that the Automated Driving System Entity and the vehicle owner will have primary control of AV data. That is, governments will need overt powers to access this data in specific use cases. Whilst data from C-ITS systems may be different, existing privacy parameters arguably exist that could be applied to this new data source. The assumption that these new data sources are inadequately dealt with under existing laws would ordinarily be tested at the time of mobilising the deployment of C-ITS use cases.
- The assumption that all CAV data is personal information and cannot be de-identified is unhelpful in ensuring that the associated benefits of this data can be maximised. There are many legitimate uses that could use aggregated data and it is preferable to consider data in this form as not personal information. For example, many road infrastructure planning, management and safety projects rely on a thorough understanding of how roads are used and the richness provided by CAV data would significantly improve these practices. In addition C-ITS architecture places security protections over data collected, making the identification of an individual very difficult/almost impossible, an overview of C-ITS technology

as it relates to government collection of data is provided with this submission **(see Attachment)**.

- The assumption that because international approaches are inconsistent, Australia should not align with international experience is flawed. Departures from international approaches will act as a barrier to the adoption of CAV technologies in Australia. Australia is a small player in the global automotive industry and should seek to align requirements with international experience wherever possible. While this is most true of technical specifications, which vehicles will be manufactured to, it is also important to ensure alignment of policy principles relating to data protections as far as possible.
- The separation of projects that consider appropriate mechanisms for collection and use of data and this project examining privacy protections is likely hamper the ability of governments to form policy positions. While it is assumed that the safety assurance system will include data recording and sharing criteria and that the NTC will propose specific legislative access powers, without a clear understanding of what this will look like and how it will operate, it is challenging for government authorities to make an informed assessment of the adequacy of existing privacy arrangements or the need for additional protections.
- The assumption that there needs to be restrictions and increased privacy protections on law enforcement use of CAV data is not supported. This implies that because of the volume of data that will be collected, there will be widespread use and direct access to the data by law enforcement agencies for proactive policing. However, law enforcement agencies are already well versed in managing data privacy issues associated with new technologies. For example, law enforcement access to and use of data generated by smart phones, automated number plate recognition cameras, CCTV cameras and facial and biometric technologies has been managed within the existing privacy frameworks or with the creation of specific authorising law, subject to the scrutiny of parliament. In addition:
  - Law enforcement agencies access and use personal information in accordance with strict legislative parameters. These powers are taken seriously, the requirements are well documented in supporting internal policies and any misuse of information is identified and addressed within existing disciplinary processes.
  - The availability of CAV data is another source of information that should be accessible for legitimate law enforcement purposes. For example, the investigation of serious and violent crimes. The risk of placing increased protections on CAV data is that it will not be accessible for these legitimate law enforcement purposes.
  - Community perceptions associated with legitimate law enforcement use of CAV data should be tested and not assumed. Most members of the community may be comfortable with necessary and appropriate law enforcement access to their information, providing appropriate restrictions are put in place. This is based on the wide scale adoption of other technologies that do not specifically preclude law enforcement access to the data generated.
- While not identified as an assumption, as indicated previously DTMR does not agree with the de-scoping of industry access and use of data from this discussion paper. A holistic review of privacy protections relevant to all involved entities is required once CAV data outputs are known and use cases are well understood.

2. **Have we accurately captured current vehicle technology and anticipated C-ITS and automated vehicle technology (and the information produced by it)? Please provide reasons for your view, including whether there are any other devices that are likely to collect information internal and external to the vehicle.**

The discussion paper takes a very narrow assessment of CAV technologies and appears to be limited to initial uses. The discussion paper does not appear to have considered the connected vehicle concept of which C-ITS is an important component or how it is intended to evolve from awareness information to connected (cooperative) automated driving in the future. C-ITS vehicle applications will, for the most part, use the same sensor data as an automated vehicle applications. So whilst C-ITS data may ultimately have different technical standards which are designed to protect personal privacy, this information is likely to interact with AV data in such a way that necessitates the application of consistent privacy policy settings.

Given the rapidly changing technological environment, it is impossible to accurately capture all technologies that will collect CAV data. As such, considerations regarding privacy issues should be principle-based, informed by use cases and be technology agnostic.

3. Have we accurately captured the new privacy challenges arising from information generated by C-ITS and automated vehicle technology relevant to government collection and use?

DTMR acknowledges that there are privacy issues that need to be fully considered in relation to CAV data. However, as previously stated, a holistic approach to privacy needs to be undertaken that considers challenges associated with all entities that will be responsible for collection, use and disclosure of CAV data.

In the case of AV data, most, if not all, data will be collected by industry and not by government. Appropriate provisions must exist to ensure this data is treated in a responsible and lawful manner by such parties. Furthermore, powers will need to be put in place to allow for government access and use of such data in specific circumstances. Appropriate privacy protections must be designed in this context.

Despite the analysis in the discussion paper, it is still not clear what new privacy challenges are created by CAV technologies in relation to government collection and use. Queensland and Australia have mature information privacy frameworks that operate under the general principle that government must have lawful access to data to be able to collect, use and disclose it. Road transport and enforcement agencies currently manage and use personal information about a large majority of citizens in a responsible way as authorised by law. Although CAV technologies will certainly generate more and richer data, DTMR is not convinced that this in itself presents challenges that have not already been dealt with in comparable contexts.

4. Based on your assessment, what information generated by C-ITS and automated vehicle technology is ‘personal information’ and/or ‘sensitive information’ under current law?

Until we understand what data is produced by CAV technologies and how it will be collected, it is not possible to provide definitive advice regarding what is and is not personal information. This determination will depend on how the information is collected and in what context. It is not possible to make a wholesale determination that all CAV data is personal information. It may be possible to collect some information in an aggregated manner ensuring it is not personal information and therefore allowing it to be used for a wide variety of legitimate use cases. In addition, security protocols may effectively anonymise some information.

If implemented with appropriate technical security standards, as is being proposed in Europe, the identification of individuals using C-ITS data collected by government infrastructure would be improbable. For C-ITS data to constitute personal information there needs to be an extensive collection system. Collection stations need to be closely placed and cover large areas to enable linking of anonymised vehicles by position and repetitive behaviour. In Queensland, it is unlikely a single government agency would have such an extensive network nor the ability to capture and retain data at this scale. Additionally, even were the vehicle to be identified, the link between vehicle and driver is only held by a limited number of entities and is protected and not available to the general public. Even then, those entities have no way of positively identifying the actual driver of a vehicle or passengers within, just the registered operator.

As noted in the attached overview of C-ITS data collection, C-ITS system design and security specifications may be sufficient to minimise the likelihood that the positioning data can be linked in such a way to threaten individual privacy.

Direct access to data stored in the vehicle poses the biggest privacy threat as the process ties the information to an identifiable vehicle whereas wireless access can anonymise the vehicle. However, even in the case where an AV manufacturer is (through AV in-car sensors) able to identify the biometric characteristics of the driver, they still need the identity of the driver. The collection of this link should be explored with regard to privacy.

5. Have we broadly identified the key reasons why governments may collect information generated by vehicle technology? Please outline any additional reasons governments may collect this information.

At minimum, there will need to be clear legislated collection mechanisms for governments and other third parties who have responsibilities for roadside enforcement and insurance investigations. Efficient data collection mechanisms will need to be created, in both legislation and systems, to enable the identification of liability for traffic offences and crashes, quickly and without timely and costly court processes. This needs to be considered as part of future projects examining the requirements of Automated System Driving Entities under a future Safety Assurance System.

The discussion paper has not explored the full scope of the use of C-ITS data and has limited itself to some initial applications only. Future applications by government and industry are not explored.

Processing of C-ITS information is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

There are hundreds of connected vehicle use-cases across multiple modes with a variety of societal benefits including safety, mobility, emissions and comfort. These are available from Day 1. A list is available at https://local.iteris.com/arc-it/html/servicepackages/servicepackages-areaspsort.html

A few examples of vehicle-to-infrastructure (and visa versa) use cases involving government include:

- A vehicle generates a Decentralised Environmental Notification Message (DENM) that they are a hazard (crashed or broken down). The vehicle shares their DENM with oncoming traffic and roadside stations. Government relays the roadside station data to traffic services, who then distribute more widely for traffic routing services. This data is generally stored by government for optimising infrastructure works – such as safety related projects.
- A vehicle approaches a traffic signal and shares its Continuous Awareness Message (CAM) or Signal Request Message (SRM) with the roadside stations. The roadside station provides the information to the signal controller to provide an earlier green (to reduce the vehicle's delay) or hold a green light (to reduce the likelihood the vehicle will run a red light). This data is generally stored by government for optimising signal timing parameters to reduce delays and improve safety.
- A number of vehicles approach a road segment nearing capacity, and share their CAM with the roadside station. Government relays the roadside station data to a central system to determine the interventions – specifically speeds – that could be used to delay the flow breakdown. This data is generally stored by government for optimising infrastructure works – such as capacity projects.

Several business cases have been prepared based on initial connected vehicle applications showing a high benefit:cost ratio (above 3). The Queensland CAVI business case estimated a reduction in crashes of around 20%. Limiting connected data sharing means that these large savings in lives and long term reduction in injuries cannot be realised.

There is also an emerging consensus that a fully automated vehicle is not possible unless it is connected with other users and infrastructure. Limits imposed on connected data sharing may result in a fully automated vehicle being unlikely to be realised beyond some limited use cases or applications.

The paper has not adequately explored the law enforcement use of CAV technology and makes the assumption that there needs to be increased privacy protection placed on law enforcement agencies. As mentioned earlier in this submission, the powers of law enforcement agencies are already clearly legislated and subject to strong governance. Constraints around law enforcement uses of CAV data should be carefully considered. Significant public value is delivered by ensuring law enforcement agencies have efficient access to data to perform timely investigations. While a number of other law enforcement actives are listed this should not be considered an exhaustive list.

It is unlikely that governments will act as the collection agencies for all data to enable these use cases. As noted before, it is likely that in many cases, CAV data will be collected by industry and not governments. Ensuring appropriate mechanisms exist to access that information is critical and should be part of this conversation. It is these mechanisms that will establish the lawful parameters for access, use, disclosure and management. DTMR reiterates the point that privacy principles do not provide authorisations to access information and also that information privacy laws are not reflective of the broader legislative mechanisms used to manage personal information and privacy.

6. Is the current information access framework for government collection sufficient to cover privacy challenges arising from C-ITS and automated vehicle technology? Please provide reasons for your view, including what parties may be affected if there is no change.

The most significant issue with the current information access framework for government collection is that it does not authorise the collection, use and disclosure of CAV data for legitimate government use cases. Before an assessment of privacy protections can be completed, it is first important to understand the authorising environment. It is noted that the discussion paper acknowledges that these authorising provisions will be the subject of future projects. More information is required about how this will be captured in the future work program to ensure a holistic approach is taken. Addressing data collection, use and protections in a piecemeal approach has the potential to result in gaps, deficiencies and unintended consequence, including inadequate consideration of all the privacy issues.

DTMR is of the view that the discussion paper has taken a narrow view of current information privacy frameworks that govern potential vehicular data. In addition to the *Information Privacy Act 2009*, access to and use of personal information generated by vehicles or transport products is dealt with under many other pieces of specific legislation. A non-exhaustive list is provided below.

- *Transport Operations (Road Use Management) Act 1995*
- *Transport Operations (Passenger Transport) Act 1994*
- *Transport Planning and Coordination Act 1994*
- *Police powers and Responsibilities Act 2005*
- *Public Safety Preservation Act 1986*
- *Motor Accident Insurance Act 1994*

The Acts above, along with associated subordinate legislation make up the majority of the privacy framework that governs access to and use of information generated by the transport system. In each case, specific provisions relating to information collection, use and disclosure override the more general provisions within the *Information Privacy Act 2009*. As identified above, this current framework does not provide an appropriate authorising environment to enable legitimate uses of CAV data.

7. **Is the current information access framework for government use, disclosure and destruction/de-identification sufficient to cover privacy challenges arising from C-ITS and automated vehicle technology? Please provide reasons for your view, including what parties may be affected if there is no change.**

   DTMR considers that at this stage insufficient analysis of the issues has occurred to determine whether the existing privacy framework in Queensland is sufficient to cover the protection of personal information generated by CAV technology and collected by government. We also note that an assessment of non-government use of this data has not been conducted and so we cannot comment in relation to the appropriateness of existing frameworks in this case.

   However, DTMR is of the view that existing privacy policies could be applied in-principle to this new data source. The nature of CAV data is unlikely to be something that hasn't been considered elsewhere in existing legislative and policy frameworks. Government already collects and uses significant amount of legitimate personal and sensitive information, and these policy and legislative settings are likely to be applicable. The premise that the current privacy framework in Australia is inadequate for CAV data has not been substantiated.

   For example, the discussion paper assumes that personal information collected by road agencies is provided by default to law enforcement agencies. This is not correct. In Queensland, specific authorising law is required to share personal information between road agencies and law enforcement agencies. These specific provisions stipulate the amount of personal information that can be shared and for what purpose, as well as what destruction requirements apply.

   The discussion paper also infers that Bluetooth collected data and C-ITS data are ostensibly different in nature due to likely density of deployed infrastructure and that the Bluetooth data is ammonised and C-ITS data is not when in fact these two technologies are likely to operate in very similar fashions for the foreseeable future.

8. **Are separate options for addressing the privacy challenges of C-ITS technology and of automated vehicle technology reasonable for achieving any future reform? Please provide reasons for your view.**

   As identified in the discussion paper, the most significant difference between C-ITS and AV data is likely to be the level of direct government collection of the information. However, despite this, it is unclear why there are different privacy challenges associated with collection, use and disclosure of C-ITS data compared to AV data. DTMR believes it is unnecessary and difficult to separate the data generated by these technologies from a regulatory perspective.

   From a policy perspective, DTMR is of the view that once information is classified as personal or sensitive information, the protections that must be afforded to that information are not unique depending on how that information was collected or by what technology. Furthermore, existing policy settings for protecting the privacy of personal information are likely to be a basis on which any specific controls for C-ITS data can be developed. As previously noted, the information privacy framework that regulates access to and protection of CAV data should be technology agnostic.

   The policy principles for protecting personal and sensitive information are unlikely to be different for C-ITS and AV data. In the same way that the existing policy principles, as imbedded in current privacy frameworks, are likely appropriate for the protection of both sources of data.

A thorough review of privacy frameworks is needed, including specific legislation that overrides general privacy legislation, to understand the authorising environment for the collection, use and disclosure of CAV data. This will provide a more informed view of new privacy challenges, if any, in order to understand what options are required.

9. Are the criteria for assessing the automated vehicle reform options comprehensive and reasonable?

As noted above, a more holistic approach to addressing this issue is required before reform options can be considered. However, if and when reform options are considered, the identified criteria are appropriate considerations to make. It will be essential to ensure information privacy frameworks maximise societal benefits and provide flexibility for future AV reforms, while ensuring that appropriate privacy protections are in place that align with consumer expectations. In addition, it is suggested that a fourth criteria be included to ensure that it is possible to implement possible reform options within the broader information privacy landscape in Australia.

10. Is there is a need for reform to address the identified problem and the privacy challenges of automated vehicle technology (that is, option 1 is not viable)? At this stage of automated vehicle development, which option best addresses these privacy challenges while recognising the need for appropriate information sharing and why?

DTMR is of the view that there is insufficient information at this stage to be developing options and recommendations for reform of privacy frameworks to support the deployment of CAV technologies. However, there is a case for further work in this regard.

Existing information privacy frameworks will need to be amended to ensure that authorising laws allow for legitimate use cases of CAV data. Once this authorising environment is known, there may also be a need to new or amended privacy protections. Some high-level privacy principles and development of conceptual policy positions in response to possible use cases may assist in the development of data access provisions. This is discussed further in response to question 13 below.

11. Are the criteria for assessing the C-ITS reform options comprehensive and reasonable?

See response to question 9.

12. Is there is a need for reform to address the identified problem and the privacy challenges of C-ITS technology (that is, option 1 is not viable)? At this stage of C-ITS development, which option best addresses these privacy challenges while recognising the need for appropriate information sharing and why?

See response to question 10.

13. Would the draft principles adequately address the privacy challenges of C-ITS and automated vehicle technology?

While DTMR is of the view that it is too soon to support any of the reform options as presented, there may be some value in agreeing to some high-level privacy principles that can be used to inform future work packages that seek to develop and implement new data access provisions for government. Any additional principles should supplement the existing privacy principles found in Commonwealth, state and territory privacy Acts.

The current principles as drafted in the discussion paper are likely to limit future use cases for CAV data. Care must be taken to ensure the principles do not limit future considerations of access, use and protection of information generated by CAV technologies. DTMR does not support the proposed principles 2, 5, 6 and 7 for the following reasons.

- *Principle 2:* A pragmatic assessment of whether CAV information is considered personal information needs to be undertaken, rather than a collective view. There are likely many scenarios when this information is not personal information if it can be collected and stored in a way that does not identify an individual. More information is required about potential technologies to understand if this principle is appropriate. The attached overview of C-ITS data collection, provides some technical information to assist in the categorisation of C-ITS information as personal information, or not.
- *Principle 5:* In the creation of authorising law to enable access to CAV data it is likely that specific purpose limitations will be considered. However, these limitations should not impede general law enforcement powers that are subject to other checks and balances and are in the public interest. For example, law enforcement agencies may need access to a variety of CAV data in the investigation of serious criminal offences. In such circumstances, provided a warrant is obtained, there should be no additional impediments to access.
- *Principle 6a:* It will not always be practical to notify users of how CAV information will be collected, used, disclosed and stored. As noted above, it is possible that not all of this information will be personal information and it will be impractical to notify every single road user in all circumstances.
- *Principle 6b:* There may be a need to retain a sub-set of CAV information for legitimate purposes, including law enforcement, without destroying it.
- *Principle 7a:* It's unclear at this stage if this is possible and in addition many use cases of C-ITS information require information at an individual vehicle level. Please see the attached overview of C-ITS data collection for more information.
- *Principle 7b:* Obtaining consent from all road users is impractical. It is noted that the discussion paper suggests that Registration and Licensing (R&L) systems could be used. However, this would only capture R&L customers and not other road users (for example, pedestrians, cyclists, vehicle passengers and interstate/overseas licence holders) and would only apply when the collection agency is DTMR rather than other government agencies or industry. In addition, costly R&L system changes would be required to record consent and there would be a significant delay in obtaining consent from all R&L customers as some renewal cycles can take up to 5 years. It would also seem redundant to seek forced consent using R&L systems, when those who wish not to consent would then be subsequently prevented from accessing significant portions of the transport network. As noted throughout this paper, privacy frameworks include specific authorising law. Governments will need to authorise legitimate use cases for CAV data in law, this will negate the need to seek explicit consent from users.
- *Principle 7c:* It is impractical and potentially impossible to offer users the ability to opt out of CAV data collection when considering that the sharing of this data is critical to the operation of these vehicles on roads and the interaction with a range of infrastructure.

In addition to the principles provided, DTMR believes that two additional principles should be considered when examining information privacy issues associated with CAV data in the future. These are:

1. As much as reasonably possible, privacy protections and legislative frameworks should allow CAV data to be used in cases that deliver common good or societal benefit, by both government and industry.
2. Appropriate privacy protections must be placed on all entities that are responsible for collecting and managing information generated by CAV technologies.