30 June 2020

Luis Gutierrez
Project Manager
National Transport Commission
Government access to vehicle-generated data
Level 3/600 Bourke Street
MELBOURNE VIC 3000
lgutierrez@ntc.gov.au

Dear Mr Gutierrez

Government access to vehicle-generated data

Thank you for the opportunity to respond to the *Government access to vehicle-generated data* discussion paper (the Discussion Paper). RAC is pleased to provide this response on behalf of its 1.1 million Western Australian members.

We are a leading advocate on the mobility issues and challenges facing our State and work collaboratively with all levels of government to ensure Western Australians can move around using safe, sustainable and connected mobility options. Since 2015, RAC has been working to test and evaluate a fully driverless, electric shuttle bus (the Nayva Arma) and so we have experienced first-hand the rapid advancement of vehicle technology and considerations influencing community acceptance and willingness to embrace it.

Although most vehicle-generated data is not yet collected, and vehicles with connective capabilities make up a very small percentage of the current Australian fleet, RAC agrees there is potential for the data to inform transport policy and planning, and most importantly, to help reduce the number of people killed and injured on Australian roads. However, in considering government access to vehicle-generated information given the potential costs involved (including for manufacturers (OEMs) to collect, store and share data and the potential risks for customers where personal data is not managed appropriately), the community should be provided with greater clarity and transparency around the specific use cases, their value, and an appropriate legislative framework for all and any data that may be considered personal[1].

[1] *The Privacy Act 1988* (Cwlth) section 6 defines 'personal information' as: personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.

The National Transport Commission's (NTC) Discussion Paper identifies several data types, unique to vehicles, that may be useful to improve Australia's transportation systems including, but not limited to:

- vehicle actions and events (rapid incident responses, safety data for road users);
- driver behaviour (safe system strategic compliance activities, risk-based insurance for government price setting);
- vehicle crash analysis (crash reconstruction for enforcement, liability purposes, safety planning);
- vehicle crash response (rapid incident response, road safety evaluation);
- Cooperative Intelligent Transport Systems (C-ITS) (real-time network operations, incident detection, traffic signal prioritisation);
- asset sensing (processed events from traffic sign recognition systems, line marking quality issues, tyre pressure/suspension, vibration, machine vision analytics (e.g. pothole detection); and
- vehicle movement (location data (GNSS+UTC)).

Some of these data types will be more unique and valuable than others (for example, to improve road safety, data collected and transmitted in real time enabling a faster post-crash response (e.g. Automatic Crash Notification (ACN) systems)), and the community is likely to have varying levels of comfort for different types and use cases[2].

Regardless of the chosen policy option and nature of data (i.e. personal or not), RAC believes both clarity and transparency is necessary to strengthen digital trust[3] amongst not only the community but industry; as the Discussion Paper identifies, the vehicle industry itself has raised concerns over the breadth of uses government could use the data for given the potential for erosion of user privacy and profit for OEMs. More generally, as technology innovations and increasing digitisation raise ethical questions by giving organisations more power, it is critical they work towards higher levels of credibility and trust. As we will outline below, identity fraud and the unauthorised use of personal and sensitive information is a clear concern for many Western Australians, as is not knowing what data is being collected, stored, shared and used.

The Discussion Paper is framed around one key opportunity to facilitate government access to vehicle-generated data to reduce the number of people killed and injured on our roads, and gain insights into a framework or forum for such an exchange. The NTC identifies three main problems or barriers to realising the opportunity:

- Problem One: Vehicle-generated data is currently not provided to transport agencies.
- Problem Two: There is a lack of a data access framework to provide the necessary trust, data exchange systems, data standards/definitions, understanding of data needs and governance to establish data access and use.
- Problem Three: The level of uptake and penetration of connectivity across the Australian vehicle fleet may delay the benefits of vehicle-generated data, particularly related to safety-critical events.

[2] A recent survey of RAC members showed varying levels of support for government having access to different types of de-identified vehicle-generated data.
[3] For the purposes of this submission, digital trust refers to the confidence placed in an organization to collect, store, and use the digital information of others in a manner that benefits and protects those to whom the information pertains.

Our submission highlights areas of concern for our members and key issues we feel need to be addressed to alleviate these, as well as considerations relating to the options put forward in the Discussion Paper to enable Australia to gain the benefits of vehicle-generated data.

Is vehicle-generated data likely to be personal?

Vehicle-generated data may not be considered personal where the OEM, or government in the case of roadside infrastructure, is able to collect de-identified data directly from the vehicle. If, however, the vehicle identification number (VIN) or other identifying information is also collected, it could enable identification of individuals and so be considered personal. Data collected from police vehicle Automatic Number Plate Recognition cameras for example, which transfer information over WiFi to the station, could be considered personal where it could be paired with other data to identify an individual.

The Privacy Act 1988 (Cth) (the Act), requires that 'Entities' (such as OEMs) must notify the consumer where they are collecting personal information (which is reasonably necessary to perform its functions). We may assume then that, where OEMs are collecting personal data, the consumer will be made aware of this in the first instance and may have the opportunity to opt-out (assuming of course they know they can do so and noting this may result in significant limitations and/or consequences for the consumer's access to the product or service). We also acknowledge that some OEMs, to ensure they are compliant with stronger European privacy laws, have indicated they are designing connected vehicle services for Australia on an opt-in or opt-out basis. The Act also requires that consent be received in order to use personal data for secondary reasons (such as road safety). However, as Western Australia remains[4] the only Australian jurisdiction without privacy and/or data sharing legislation, there is currently no legislative requirement for State government agencies to notify road users should they be collecting their data, personal or otherwise. As a consequence of this, the WA State Government recognises[5], "the absence of comprehensive privacy and information sharing frameworks has resulted in:

- fragmented and unclear protections for those whose information is held by the WA public sector, with no specific avenue by which privacy complaints can be resolved;
- reduced public trust and confidence in how data is stored, used and shared;
- an inconsistent and generally risk adverse approach to information sharing between agencies; and
- reduced collaboration and evidence-based decision making".

It is unclear to what extent vehicle-generated data would be considered under the Act and other relevant legislation to be personal; and clarity for potential users of connected vehicles may be critical to motivate uptake and move Australia towards realisation of the benefits expected to be delivered through increased connectivity. If the data has been effectively de-identified[6], there appears to be no legal obligation on OEMs nor government to advise their consumers/the community that they are using data collected from their vehicles for a secondary purpose. Under the Act, whether information is about a 'reasonably' identifiable individual requires a contextual consideration of the particular

[4] The WA Government is proposing to introduce a whole-of-government framework to govern the way the public sector manages the information it holds to create uniform rules across the WA Public Sector that will require agencies to consider your privacy whenever they collect, use or share your information.
[5]The Government of Western Australia. (2019). *Privacy and responsible information sharing: Discussion Paper*. Available at: https://www.wa.gov.au/sites/default/files/2019-08/Discussion%20paper_Privacy%20and%20Responsible%20Information%20Sharing_1.pdf
[6] As per the Act. De-identification involves two steps. The first is the removal of direct identifiers. The second is taking one or both of the following additional steps: the removal or alteration of other information that could potentially be used to re-identify an individual, and/or the use of controls and safeguards in the data access environment to prevent re-identification.

circumstances including: "the other information that is available to the person or people who will have access to the information, and the practicability of using that information to identify an individual"[7]. Access by government to vehicle-generated information, even that which has been de-identified by the OEM may need to be carefully considered given the extent of 'other' information available to governments. For example, the proposed privacy legislation for WA would enable broad sharing of personal information across the public sector, which could include information (e.g. vehicle registration data) which, once paired with other data, could reasonably re-identify an individual. Given it may be difficult for OEMs to identify what data may be 'reasonably' identifiable in the broader context of data sharing within government, it is recommended that both industry and government seek consent regardless (noting some OEMs have already expressed the intention to do this).

Social licence and principles for personal data

According to a recent survey of more than 580 RAC members[8] in June 2020, there is a relatively high level of comfort with government having access to and using de-identified and aggregated vehicle-generated data in order to improve road safety, reduce travel times and inform the future planning of our cities, communities and transport networks. In fact, 39 per cent feel very or extremely comfortable with this and 33 per cent feel moderately comfortable[9]. Encouragingly, the majority (65 per cent) of members agree vehicle generated data will help improve safety on our roads[10].

Government access to the following types of de-identified and aggregated vehicle-generated data received the most[11] support:

- road condition information (77 per cent);
- information about the vehicle operation recorded just before and after a crash (71 per cent);
- vehicle emissions (64 per cent);
- information shared between the vehicle and the surrounding infrastructure (60 per cent); and
- locations and details of where vehicle safety technologies were engaged (59 per cent).

The data type that received the least[12] support was the location and time of vehicle journeys summarised at a postcode area level (43 per cent); and one in two (47 per cent) are very or extremely concerned[13] about their journeys and location being monitored.

When it comes to personal or sensitive information, 68 per cent of our members are very or extremely concerned about transport-related data[14] being used by government for reasons they have not consented to and about data breaches leading to identity fraud. Other key concerns highlighted

[7] Office of the Information Commissioner. What is personal information? Accessed 20 June 2020 at: https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/

[8] 449 respondents were from the Perth and Peel region and 136 from regional WA. Age, gender and location sampling quotas were applied, and data has been post-weighted to be representative of RAC's membership (which is broadly consistent with the WA population profile) – the margin of error at total sample level is +/- 4.1% at the 95% confidence level. Results included within this submission are as at 26 June, 2020.

[9] Respondents were asked to indicate the degree to which they were extremely, very, moderately, slightly or not at all comfortable with government having access to vehicle generated data.

[10] Respondents were asked to indicate the degree to which they strongly agreed, agreed, were neutral, disagreed or strongly disagreed with each option in a prompted list. Results and ranking are based on respondents who said they agreed or strongly agreed with each option.

[11] Respondents were asked to indicate the degree to which they Strongly supported, supported, were neutral, opposed or strongly opposed each option in a prompted list. Results and ranking are based on respondents who said they supported or strongly supported each option.

[12] Ibid.

[13] Respondents were asked to indicate the degree to which they extremely, very, moderately, slightly, or not at all, concerned with each option in a prompted list.

[14] For the purpose of the survey, transport-related data refers to data relating to the use of the transport system more broadly (e.g. vehicle-generated data, CCTV, smartphone data, sensors in the road network, SmartRider journey data etc.). Respondents were asked to indicate the degree to which they extremely, very, moderately, slightly, or not at all, concerned with each option in a prompted list.

include government using the information to identify and track people, and the inability of government to effectively manage (de-identify and protect) their personal data. Furthermore, seven in 10 are very or extremely concerned[15] with not knowing what data is being collected, stored, shared and used, and almost nine in 10 think it is very or extremely important[16] that government consults with industry and the community about this.

Action must be taken by both industry and government to create an environment where citizens and consumers have a strong level of comfort and trust that both can manage their data, including but not limited to: ongoing communication and provision of sufficient information to enable informed consent; respect for data preferences; strong and active privacy policies and cyber-security systems; and proof of meaningful benefits in exchange for data. This will of course support a future where connected vehicles (including automated vehicles) are accepted.

The NTC has proposed that for the exchange of vehicle-generated data that is considered personal, the principles resulting from its policy paper '*Regulating government access to C-ITS and automated vehicle data*' should be adopted. Following the consultation period, it was pleasing to see these principles, which are intended to guide laws and align standards for C-ITS and automated vehicles, had been redrafted to include data security and recognition of the importance of notifying users in plain English about government collection, use, disclosure and storage of C-ITS and automated vehicle data. However, to re-iterate one of our previous comments[17], balancing the benefits of government access to C-ITS and automated vehicle data with additional privacy protections to appropriately limit the collection, use and disclosure of data, is too broad for personal and sensitive information, and RAC recommends principle 6[18] (to specify data type, purpose for use and who it may be shared with) must include the process and reasons for secondary use, and associated informed consent.

The options and recommended approach

The Discussion Paper proposes three options to address Problems One and Two:

- Option One: No change to existing framework and legislation
- Option Two: Government and industry data exchange partnership
- Option Three: Legislative reform

The NTC finds that Option One will likely result in fragmented and inconsistent use cases and data standards across the States and Territories (as we have seen without a privacy framework in WA), and misses an opportunity to build trust between government and industry on a broader scale. While we agree this option may result in such inconsistencies, standardisation may still occur through developments in international standards. The NTC considers under this option that government may not fully come to understand the benefits and costs of vehicle-generated data. In this vein, Option Two may enable better coordination and provide some impetus to achieving this understanding however this could still occur otherwise through private (commercial) provision and given there

[15] Supra note 13.
[16] Respondents were asked to indicate the degree to which they thought it was extremely, very, moderately, slightly or not at all important that government consults with industry and the community about how they intent to collect, use and share transport related data.
[17] RAC. (2018). *RAC's response to the National Transport Commission's Discussion Paper: Regulating government access to C-ITS and automated vehicle data*. Available at: https://www-cdn.rac.com.au/-/media/files/rac-website/about-rac/public-policy/16793---public-policy_cits-automated-vehicle-data_8pp_ebook.pdf?la=en&modified=20190613020359&hash=A7EBEFFEB2FAABD329D91175C8A3F6370C93A513&hash=A7EBEFFEB2FAABD329D91175C8A3F6370C93A513&_ga=2.193056494.2145006800.1592796037-950717362.1572919333.
[18] Principle 6: "To specify the C-ITS and automated vehicle data covered, the purposes for which the data can be used and the parties to whom the purpose limitations apply while not impeding access to data with a warrant or court order authorising a different use".

appears to be slow-growing demand for this data, the case for government intervention is limited. In addition, the Discussion Paper identifies that many transport agencies are not ready to make the most from this data. At the point at which they are, we may expect demand to significantly increase, likely leading to supply (for example governments are already purchasing telematics data).

Through the development of a data exchange framework under Option Two, we may have the opportunity to capitalise on the greater breadth and depth of data available. Additionally, we agree that the framework would provide an opportunity to standardise data within the industry, however this would be limited without significant participation. Further, it is not clear how the framework would operate in practice, and while it would seek to build data trust between government and industry, it could be quite transactional in nature with little consideration of community/consumer concerns and/or preferences. We believe the community/consumers should be adequately considered and reflected in any potential exchange framework which includes education about what (and why) data is being collected and used, and how it is being de-identified. As the Discussion Paper has highlighted, whether people opt-in or out of connected technologies will be impacted in part by whether they see direct value from the use of their data.

It is also unclear, whether incentives for participation beyond the exchange of information would be enough for OEMs to overcome potential risks including: data that highlights product deficiencies; any liability associated with the de-identification and sharing of data (linked to a desire to protect their customers' privacy); competitive disadvantages (e.g. competitor access to data); and opportunity costs of not commercialising the data they exchange. As there may be some reluctance from OEMs to participate in an exchange (particularly if the data is personal), we need to consider how effective data partnerships are operating around the world. Perhaps the closest comparison outlined within the Discussion Paper is the European Union's (EU) Data Taskforce and Data for Road Safety Proof of Concept (PoC), which has demonstrated there is a willingness for industry to exchange data with transport industries and in January it was announced that five new public and private members were joining the PoC. However, the 12-month PoC (which concluded in June 2020), highlighted that participants entered the agreement with a degree of uncertainty. The uncertainties to be resolved include clarification of the commercial use of data and information acquired and created; a scalable approach to manage non-commercial use; and measures to avoid 'free-riders' through reciprocity. RAC recommends Option Two only be implemented once more is known about the outcomes of the EU PoC.

As highlighted in the Discussion Paper, a telematics exchange platform (developed by Transport Certification Australia (TCA)) is already being used by heavy vehicle and transport agencies. Where industry may be apprehensive about the liability associated with collecting, de-identifying and aggregating data, we agree a national broker such as TCA may be beneficial. An intermediary which provides a nationally consistent open market, with services covering multiple vehicle types and digital infrastructure, may help develop the necessary trust between industry and government in the short term.

There are of course, some data exchange partnerships between industry and government that have been successfully operating for some time, particularly in the healthcare sector. Looking to examples from healthcare, where medical records contain personal and sensitive information, may also help address user privacy issues in sharing vehicle-generated data. Noting the obvious difference in scale

and data types, eHealth Exchange (see case study below) may provide some insight, particularly with regard to governance and exchange obligations, proof of value, and data governance.

Case study: eHealth Exchange

eHealth Exchange (the Exchange) in the United States (U.S.) "is a group of federal agencies and non-federal organizations that came together under a common mission and purpose to improve patient care, streamline disability benefit claims, and improve public health reporting through a secure, trusted, and interoperable health information exchange (HIE)."[19] The network spans 50 states, four federal agencies, 65 percent of U.S. hospitals, 50,000 medical groups, supporting more than 100 million patients, and is the largest health data sharing network in the U.S[20].

The Exchange is overseen by the Coordinating Committee (with both federal and non-federal representatives), who provide governance, oversight, management, and support the Exchange participants. All participants within the Exchange agree to a legal, multi-party trust agreement called the Data Use and Reciprocal Support Agreement (the DURSA)[21]. The DURSA is founded on the legal requirements applicable to the privacy and security of health information, and describes the mutual responsibilities, obligations and expectations of all participants (including Intellectual Property rights). These clearly defined set of standards and expectations form the foundation of a secure, trusted, and interoperable network for the standardised flow of information[22]. The DURSA further reflects consensus among the state-level, federal and private entities on a number of issues including permitted purposes, participant eligibility, and allocation of liability and risk. In recognition of ongoing changes in the legal, policy, technical and business environment, the DURSA remains a living document and its multi-purpose interoperability platform has the ability to grow and integrate new use cases[23].

The Exchange has a federated structure, meaning the network does not have a central hub through which all data passes. Instead, participants can securely connect and share data using a standardised process over the Internet[24]. As participants must agree to the common set of standards and legal/governance agreements under the DURSA, data can be shared without needing to develop one-off contracts (reducing associated legal fees). Participants within the Exchange make a commitment to a minimum level of data sharing so that all other participants are aware of, and can rely on, each participant's commitment[25]. When signing the DURSA, participants within the Exchange agree to not redisclose to any person or entity, nor use for its own benefit, any confidential participant information[26] obtained (unless required by law, whereby the Discloser must be notified). The DURSA also contains a clear dispute resolution process to resolve issues that arise between the participants.

[19] eHealth Exchange™. (2019). *What we do.* Available at: https://ehealthexchange.org/what-we-do/
[20] eHealth Exchange™. (2019). *Testimonials.* Available at: https://ehealthexchange.org/participants/testimonials/
[21] eHealth Exchange™. (2019). *Data Use and Reciprocal Support Agreement.* Available at: https://ehealthexchange.org/onboarding/dursa/
[22] The Sequoia Project. (2018). *eHealth Exchange.* Available at: https://s3.amazonaws.com/seqprojectehex/wp-content/uploads/2018/09/12051759/eHealth-Exchange-Overview-2-20-18.pdf
[23] Supra note 22.
[24] The Sequoia Project, (Accessed on 26 June 2020). *What's the Difference Between eHealth Exchange, Carequality, and The Sequoia Project?* Available at: https://sequoiaproject.org/about-us/whats-difference-ehealth-exchange-carequality-sequoia-project/.
[25] Supra note 21.
[26] eHealth Exchange™. (2019). *Data Use and Reciprocal Support Agreement.* Available at: https://ehealthexchange.org/onboarding/dursa/. The DURSA provides reasonable clarity regarding what is meant by confidential participant information.

To become a participant and share information through the Exchange parties must undergo the eHealth Exchange Participant Testing Program to certify compliance against relevant standards and network requirements. Participant fees apply for the testing program and ongoing services and maintenance of the Exchange.

RAC broadly agrees that a data sharing partnership could be beneficial in establishing trust and minimum expectations between industry and government, noting our previous comments about consumers seemingly being an afterthought. However, given the nascence of sharing vehicle-generated data and the rapid technological advancements in this area, we submit the initial framework should act as a PoC to determine whether it could work at this point in time, and inform the way forward for other transport-related uses of data as the penetration of connectivity in our fleet grows. Given data sharing is not so new in some industries and in some countries, it may be prudent to conduct further research and/or interviews with participants of such exchanges.

Option Three proposes to introduce nationally consistent legislation that would require industry to capture, store and process vehicle-generated data, which would then be provided to road agencies. The Discussion Paper contains limited detail in articulating a rationale for this option. We agree there appears to be no clear market failure, nor significant demand for this type of data given, as identified, penetration of vehicles with connectivity is currently low, and many transport agencies do not have specific use cases in mind and/or do not have the capability currently to ingest and use it. Once use cases are better understood and greater demand for such data is created, we may see issues with supply arise which may justify the need for legislative reform, but we agree this is not an option to pursue at the current time. The framework and lessons from the establishment of a data sharing partnership PoC would be expected to help inform the necessary changes. In addition, as Australia is a technology taker, we must be cognisant of introducing obligations for OEMs which would drive up the current costs of doing business and, if we are to consider road safety-related vehicle-generated data as a pure public good (as the EU has done), the rationale for this must be made clear. Potentially, by the time we are able to benefit more broadly from vehicle data that is generated within Australia, OEMs will have the necessary systems already in place from their experiences in other jurisdictions where vehicle connectivity technologies have been more rapidly embraced and will have found cost-effective ways to manage data provision.

To address Problem Three, the NTC proposes the Commonwealth considers introduction of technologies such as eCall into the Australian Design Rules. While RAC supports the adoption of in-vehicle technologies that have the ability to support faster emergency response times (our recent survey[27] found that more than 3 in 4 supported[28] the mandatory introduction of an ACN system), it is unclear the extent to which this will promote the uptake of connected vehicles and, if it does, the potential road safety benefits may be limited if this is the only type of data collected and used. Further, as our members are comfortable with the provision of some types of data for some purposes and not others, comfort and satisfaction with ACN systems may not necessarily lead to an increase in the

[27] Supra note 8.

[28] Respondents were asked to indicate the degree to which they strongly supported, supported, were neutral, opposed or strongly opposed an automatic crash notification system that sends an alert to emergency services about the location of the vehicle in the event of a serious crash being in mandatory for all new vehicles sold in Australia. Results and ranking are based on respondents who said they supported or strongly supported this initiative.

uptake of connected vehicles that collect an even greater breadth of data. In addition, to realise the full operability of eCall, government would need to commit to installing the associated enabling infrastructure. Whilst the EU estimates eCall can speed up emergency response time by 50 per cent in the countryside, WA's geographically distant, sparsely populated and lightly trafficked regional areas (currently with limited network coverage) present a considerable challenge when allocating limited resources and investment funds.

Concluding remarks and recommendations

Reducing the number of people killed and injured on our roads should be the priority for access to, and use of, vehicle-generated data. The potential benefits of government access to this data are various and include the ability to get people to medical care faster following a serious crash and enabling the creation of a road environment that is more forgiving to road user error through improvements informed by data collected on the location of potential safety risks. However, striking the *right* balance between maximising these benefits and managing privacy risks is critical. Importantly, we must ensure the community's interests are prioritised irrespective of the chosen policy option and this must be informed by an ongoing two-way dialogue with government/industry.

RAC recommends:

- To build digital trust with industry and the community, government should consider ways to improve the level of communication and information provided regarding data collection, storage, use and sharing, beyond what is required by relevant legislation. Ongoing dialogue with the community must include a component of education to ensure a level of understanding around how the data will be used to improve road safety for example, and how information generated by their vehicles will be effectively de-identified and protected.
- Government should consult on the development of a framework(s) around permitted usage of data collected by new and emerging technologies to support deployment, encourage community trust and take-up, and accelerate benefits realisation. As above, this must include sufficient information and clarity around use cases for the data and both government and industry should ensure that any framework developed recognises and appropriately responds to the preferences and concerns of the community.
- Further work should be undertaken to identify (and therefore provide greater clarity around) what vehicle-generated data could be considered personal. Our recent member survey highlights that while there is a relatively high level of comfort for government access to, and use of vehicle-generated data that is de-identified to improve road safety, reduce travel times and aid planning, there are still strong concerns over the management and use of personal information.
- Given it may be difficult for OEMs to identify what data may be 'reasonably' identifiable in the broader context of data sharing across government, it is recommended both industry and government seek consent to use and share data regardless.
- Option Two should be further developed (particularly with regard to use cases and governance), with the intention to initiate a PoC to assess whether industry, government and the community are ready, willing and able to effectively participate at this point in time, and also whether access to this data genuinely has potential to create public value through the improvement of road safety and transport systems more broadly. Option Two should only be implemented once more is known about the successes and/or failures of the EU PoC.

- Option Three should not be implemented unless it is clearly demonstrated and agreed that vehicle-generated information is a pure public good and that a market failure exists.
- Further work may be needed to consider options to respond to Problem Three, as introduction of an ACN system alone is unlikely to achieve the broader uptake of connected vehicles.

We trust RAC's response will be of assistance to the NTC in considering government access to vehicle-generated data.

Should you require further information, please do not hesitate to contact Sarah Macaulay, Senior Manager Public Policy on (08) 9436 4903 or at sarah.macaulay@rac.com.au.

Anne Still
GENERAL MANAGER, PUBLIC POLICY & MOBILITY
ADVOCACY AND MEMBERS