Regulating government access to C-ITS and automated vehicle data

RAC's response to the National Transport Commission's Discussion Paper

November 2018

For the better


Imagine the possibilities
RAC Intellibus
Member of Australian Driverless Vehicle Initiative
100% driverless electric
RAC

RAC's response to the National Transport Commission's Discussion Paper: Regulating government access to C-ITS and automated vehicle data

Automated vehicle (AV) technology is rapidly advancing and is potentially the biggest disruption to the mobility sector since the invention of motor cars. Many vehicles now have built in AV or driver-assist technologies and are rapidly becoming increasingly automated, that is, requiring less driver intervention.

The National Transport Commission's (NTC) *Regulating government access to C-ITS and automated vehicle data* (Discussion Paper) is part of a national program to provide a regulatory framework for AV technology and contains four options for regulating government access to AV data and three options for C-ITS data.

Options for data generated by automated vehicle technology:

- **Option One:** rely on the existing information access framework to address the new privacy challenges of AV technology (no change).
- **Option Two:** agree broad principles on limiting government collection, use and disclosure of AV information.
- **Option Three:** limit government collection, use and disclosure of AV information from in-cabin cameras and biometric, biological or health sensors to specific purposes.
- **Option Four:** limit government collection, use and disclosure of all AV information to specific parties and purposes.

Options for data generated by C-ITS technology:

- **Option One:** rely on the existing information access framework to address the new privacy challenges of C-ITS technology (no change).
- **Option Two:** agree broad principles on limiting government collection, use and disclosure of C-ITS information.
- **Option Three:** limit government collection, use and disclosure of all C-ITS information to specific parties and purposes.

Representing over one million Western Australian members, RAC is a leading advocate on the mobility issues and challenges facing our State and we work collaboratively with all levels of government to ensure Western Australians can move around using safe, easy, and sustainable mobility options.

Since 2015, RAC has been working to test and evaluate a fully driverless, electric shuttle bus (the Navya Arma) and on the 31st of August 2016, RAC, with support from the State Government and City of South Perth, launched Australia's first automated vehicle trial on public roads. In one of the first public trials globally, the RAC Intellibus consistently operates five days per week, taking passengers along a 3.5 kilometre route in South Perth. At the time of this submission on 20 November 2018, more than 16,300 people had registered to take part in the Trial, and nearly 10,629 people had experienced the Intellibus, which had travelled over 16,300 kilometres in autonomous mode. In this purposeful trial, RAC is seeking to understand how AVs operate and consider their likely opportunities for, and impacts on Australia.

The Trial's three aims are to:

1. Increase the understanding about the potential impacts of and opportunities arising from the advent of AV technology;
2. Give Australians the chance to see, use and experience AV technology; and
3. Further help Australia prepare a roadmap for the changes needed to support and safely transition to AV technology.

In November 2017, it was announced that, along with just two other cities globally, RAC, in partnership with the State Government and Navya will be testing several driverless passenger 'AUTONOM' vehicles in Perth, which have been designed as an on-demand shared mobility service (the RAC Intellicar Trial). A prototype vehicle which arrived in September 2018, has now been commissioned and is undergoing testing on a private track. The RAC Intellicar Trial will build on the existing Intellibus Trial and will provide Western Australians with the opportunity to become acquainted with the concept of shared 'mobility as a service'.

The collection of data by vehicles is not new and has been progressing alongside technology for some time. Since the 1990s for example, cars have carried an event data recorder (EDR)[1], which collects and records information about the operation of a vehicle in the seconds immediately before and after a crash, including vehicle speed, braking and even whether a seatbelt is being used. Today, AVs collect information using sophisticated sensors such as LiDAR, GPS, and cameras. On-board, powerful computers store, use and in some cases, delete enormous amounts of this information. As identified in the Discussion Paper, both personal[2] and sensitive[3] information

[1]Bellion, P. (2002). Event Data Recorders: What Do They Tell Us? in Operations, Transport and Safety: Outside the Square: Institute of Transportation Engineers International Conference, 2002, Melbourne, Victoria, Australia.
[2]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.
[3]The Privacy Act 1988 (Cwlth) section 6 defines 'sensitive information' as: sensitive information means: (a) information about an individual's: (i) race or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) sexual orientation or practices; or (viii) criminal record; that is also personal information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates.

may be collected and stored for a limited period by AV internal and external cameras. The footage recorded through these cameras may be used by AV manufacturers (automated driving system entities (ADSEs)) when there is a need to diagnose and resolve technical issues to ensure safe operation. Further some mobile phone applications are being developed by ADSEs to enable the on-demand capabilities of AVs, which could also collect 'personal' information relating to individuals booking the vehicle (such as pick up and drop off locations and trip history), much the same as existing mobile applications for taxi and ride-sharing services.

Where we stand

As outlined in the Discussion Paper, AVs and Cooperative Intelligent Transport Systems (C-ITS)[4] will generate an even greater breadth and depth, as well as more widespread and new data than our current vehicles and infrastructure. While on the one hand this data will be invaluable to support evidence-based policy, strategic planning, and investment decision-making to ensure the safety and efficiency of transport systems, it presents privacy challenges regarding the collection, storage and use of both personal and sensitive information. The NTC identifies the primary problem associated with these new data challenges to be the possibility that community trust in and uptake of the technology could be impeded by concerns over access to personal and sensitive information. Delayed uptake would therefore prolong the realisation of the anticipated positive outcomes of AVs for the community, most importantly the potential to significantly reduce crashes and save lives. RAC believes the problem is broader than the risk of delayed take-up and benefits realisation and should also focus on the role of government to protect privacy, irrespective of C-ITS/AV saturation. The Discussion Paper does not go far enough in this respect, placing greater emphasis on the potential for uptake without sufficiently addressing privacy protections.

Understanding and appropriately managing community expectations regarding AVs operating on our roads is acknowledged as being essential in helping to prepare for and shape the driverless future. This is a key component of our trials and we are gaining invaluable insights through pre and post-ride surveys of participants that have experienced the Intellibus. We have also commissioned independent research exploring Western Australians' perceptions relating to AVs and to date, three survey waves have been undertaken tracking changes in sentiment over time. When it comes to their concerns, 63 per cent of Western Australians do have some level of concern about data privacy (specifically, who owns the information AVs may collect about the trips users are making), however this is ranked eighth out of 13 prompted concerns[5].

A deeper analysis considering the relationship between attitudes towards AVs and these concerns has also revealed that data privacy has a weaker influence on negative feelings towards AVs than other concerns (ranking 11th out of the 13 prompted concerns)[6]. While it is still a crucial consideration which does need to be carefully regulated and managed by government, this suggests data privacy may not currently be a main driver impacting take-up by Western Australians (giving up control / entrusting a machine, AVs not driving as well as humans and interacting with AVs whilst driving a vehicle have the strongest influence on negative feelings towards AVs).

Personal autonomy is concerned with individual control and self-determination and is the ability of people to make independent choices about themselves and "the desire to avoid being manipulated or dominated wholly by others"[7]. Autonomy privacy regards the right to make choices free from observation. AVs/C-ITS present new challenges arising from the ability of technology to more readily identify, track, and profile individuals (with significant room for error). Lack of control by individuals over their personal and sensitive information is a key issue to be addressed by the Information Access Framework (IAF) in relation to AVs. In a report by the Australian Productivity Commission in 2016, Productivity Commission Chair, Peter Harris, noted most consumers would be surprised that, as individuals, they currently have no rights to own the data that is collected about them.

Development and implementation of an IAF for AVs and C-ITS which upholds the protection of personal autonomy is an important step to encourage confidence and trust in the technology. The Discussion Paper outlines four options to address the new privacy challenges relating to AVs, and three in relation to C-ITS, and identifies option two as the preferred option for each. In both cases, option two establishes broad principles for limiting government collection, use and disclosure of AV/C-ITS information. Overall, it is agreed and supported that the principles provide flexibility to reflect the fact that these are emerging technologies, however it is considered that they may be insufficient to achieve the desired goal of securing trust and encouraging take up if the reasons for government access to the personal and/or sensitive information collected by AVs and C-ITS are not made explicitly clear. Regardless of the extent to which data privacy concerns may impact AV uptake, in the shorter term the proposed principles may not provide suitable privacy protection given they will have no legislative basis and only require government organisations to "consider" notification and consent (principles six and seven, page five). Furthermore, the principles do not cover secondary uses nor specific reasons for use, and consent has been limited to data collection by C-ITS, however should also apply to AVs.

The remainder of our submission outlines a few key considerations associated with AV and C-ITS data privacy and concludes with eight broad recommendations.

[4]C-ITS is a technology platform that enables wireless communication and real-time information sharing between vehicles, roads, roadside infrastructure and other infrastructure. In the context of Vehicle-to-Everything (V2X) communications, this could also include other road users such as pedestrians and cyclists.
[5]RAC (2018). Automated vehicles: Community perceptions monitor.
[6]Note the survey did not evaluate the extent to which the community understands what data could be collected and how it might be used.
[7]Westin, A. (1967). Privacy and freedom (1st ed.] ed.). New York: Atheneum.p.7.

Informed consent

Informed consent is a central tenet to data privacy concerns associated with AVs and C-ITS. One of the main purposes of Australia's IAF and the *Privacy Act 1988* (Cth), is to provide individuals greater control over the way their personal information is handled by government and industry[8]. When people provide consent, they must often surrender nearly all control over their information[9].

Wherever possible, informed consent for AVs should be affirmative (not implied) and looked on as a process rather than a signature on a form at a single point in time.

Informed consent must be preceded by disclosure of sufficient, easy-to-understand information. Individuals must have enough information to weigh up the risks of consenting to the collection, use and storage of both their personal and sensitive information. Both government and industry will need to consider how to convey complex information about AV/C-ITS data privacy to the public. Other complex sectors (such as health) may offer some guidance.

In line with human rights frameworks such as the *International Covenant on Civil and Political Rights*, individuals should be able to choose whether to provide consent; they should also be able to withdraw it; and have a right to be forgotten. Earlier in 2018, the European Union made changes to its *General Data Protection Regulation* to strengthen privacy protection for consumers across multiple industries. Specifically, the amendments include, but are not limited to: clearer language, affirmative consent, greater transparency for the use and transfer of data; stronger rights to be informed and control personal data (including access, modification, and the right to be forgotten); and stronger enforcement. RAC recommends a stronger approach to the protection of autonomy privacy, similar to the GDPR, should be considered in the context of the Discussion Paper for personal and sensitive information.

Government access, use and storage of personal and sensitive information

The Discussion Paper identifies that: "while privacy principles do not authorise the collection of personal information, they do not restrict (because they allow/permit) direct collection of personal information by government organisations if the information is necessary for one or more of its functions or activities".

RAC recognises that C-ITS and AVs present significant potential to capture information which will be invaluable for the optimisation of the existing transport system, including in real-time, and to enable evidence-based policy, strategic planning and investment decision-making in catering for future demands.

Specifically, the Discussion Paper identifies the potential of this data for enhanced decision-making for law enforcement, traffic management and road safety, infrastructure and network planning. Whilst the use of de-identified data is critical in delivering value to the public, the use of private and sensitive information by the public sector in performing its broader functions (particularly for secondary uses) may be inappropriate.

The Discussion Paper has focussed on roads and the opportunities for road agencies as the responsible authorities, however the reality is these technologies should be applied to deliver benefits for all modes of transport, all users of our transport systems, and across all tiers of government. For example, while Main Roads WA has responsibility for building (including planning and designing), maintaining and operating (including optimising) the state road network to ensure safety and efficiency, local roads are under the control of local governments and the national network, the Federal Government. Within the State Government, transport responsibilities are also shared by the Public Transport Authority (PTA) and the Department of Transport (DoT). The PTA has

[8]Office of the Australian Information Commissioner website: https://www.oaic.gov.au/privacy-law/rights-and-responsibilities.
[9]Solove, D. (2001). Privacy and power: Computer databases and metaphors for information privacy. Stanford Law Review,53(6), 1393-1462.

a responsibility for planning and delivering passenger transit infrastructure and services, including on-road public transport which could be significantly enhanced through C-ITS, as well as AVs, not least by facilitating increased levels of priority at intersections, and turn-up-and-go and on-demand services. The DoT has the strategic planning and policy function for the transport system as a whole.

Given the distinct but interconnected responsibilities for transport, some C-ITS and AV enabled data collected by Main Roads through government-owned infrastructure and roadside units used for Vehicle-to-Infrastructure (V2I) or Vehicle-to-Everything (V2X) communication, will be important to the roles and functions of other areas of government. This should be acknowledged and considered in determining the permitted data collection purposes and intended uses, as well as the respective government organisations that are permitted access for specific reasons. It is important that these uses/processes be made clear to transport system users. Further through V2X, data may be collected and utilised on multiple road or transport system user groups, including pedestrians and cyclists for instance. The IAF for AVs and C-ITS should be developed cognisant of existing public transport systems which already track the trip information of individual users, such as the Transperth SmartRider ticketing system.

The potential for secondary use by government is significant and may be a particularly important consideration in the Western Australian context given there is no privacy law specifically regulating state government access as there is in other parts of the country. Under the existing IAF, secondary uses could be far removed from the original collection purpose and be justified by government due to the data's contribution towards fulfilment of one or more of its functions. Government should consider whether there is potential for personal and sensitive information to be provided to broader government organisations, even beyond the transport, road safety and law enforcement portfolios, to support policy-making and service planning and provision. Even if the data is de-identified, should it be permissible in such circumstances? The principles propose a regulatory framework that balances individual privacy with the need to deliver value to the public. This is too broad for personal and sensitive information, and RAC recommends principle five should be amended to include the process and reasons for secondary use, and the associated informed consent.

More broadly, government should consider a variety of scenarios in assessing the effect government access could have on autonomy privacy. For example, would it ever be appropriate for law enforcement purposes be extended to broad monitoring of individual travel routines or proactive investigations where there is reasonable suspicion of wrong-doing? Should law abiding AV users have to worry about government scrutiny of their actions? Should they have to be concerned about ending up on a suspicious-persons list because they have some unusual habits that are entirely legal?

RAC believes the collection and use of identifiable information should be limited and must be supported by robust due process which upholds an individual's right to privacy to the extent possible, not practicable. This should include a clear process for appeal by individuals.

Private sector access, use and storage of personal and sensitive information

The Discussion Paper finds private sector access to data is a significant societal issue that is much broader than AV policy and regulation and claims the existing IAF is sufficient for regulation of the private sector in relation to new AV and C-ITS challenges. Whilst RAC agrees private sector access to and use of private and sensitive information is broader than AVs and C-ITS, lack of attention to the new data privacy challenges as they relate to the private sector may still adversely impact community trust of these technologies (particularly so for those not aware of existing protections). The *Australian Privacy Principles* (Schedule One of the *Privacy Act 1988* (Cth)) provide a number of protections including but not limited to: the right to know why your personal information is being collected, how it will be used and who it will be disclosed to; options to not identify yourself, or use a pseudonym (in limited circumstances); access to your information and the right to correct it.

Consistent with government's role to protect and regulate, a more complete consideration of the AV/C-ITS data challenges is necessary. ADSEs will have access to and hold all the data collected by AVs. Given the potential for this information to be both personal and sensitive, strict controls must be in place restricting the ADSEs ability to use, share and store it. For example, the NTC identifies the potential for (and current practice of) third parties to give government access to personal information without being legally obliged to. Striking the right balance between maximising the benefits of data collection and managing privacy risks is critical. In addition to regulation, government and industry should also consider ways to motivate ADSEs to improve their privacy policies, cybersecurity systems, and also their communication with consumers and service users. The Office of the Australian Information Commissioner should continue to play an important role in this.

Safety and security

It is government's role as 'protector' to ensure a suitable framework is in place for the safety, security and privacy of AV users (this should also apply to C-ITS). In 2015, Chrysler announced a recall for 1.4 million vehicles after hackers demonstrated they could remotely hijack a Jeep's digital systems over the internet. Further in 2016, researchers in China demonstrated they could affect in-vehicle functions of a Tesla including the brakes, from as far as 12 miles away.

Data privacy is closely related to cyber security, and whilst it is acknowledged the latter to be out of scope, RAC believes the Safety Assurance System (SAS) may not provide a suitable level of assurance to users. As previously outlined, the most recent wave of RAC's AV community perceptions surveys demonstrated data protection is of concern and three in four Western Australians are also concerned about issues around cyber security (this actually ranked second out of the prompted list of concerns, preceded only by fears about not being able to manually override the vehicle and take back control if the system fails).

The SAS will require ADSEs to demonstrate how cybersecurity risks will be both controlled and managed, however will not require a consistent approach to be taken by the industry. To provide greater clarity and comfort to users, government may need to consider a standard process for all ADSEs to manage cyber security threats and intrusions to uphold data privacy and personal autonomy.

A summary of RAC's recommendations:

1. The proposed principles to address the data privacy challenges in relation to C-ITS and AVs should be strengthened to ensure greater protection for individuals whilst maximising the benefits of this emerging technology for government decision-making and delivering value for transport system users. Specifically:
   a. The wording of the principles should be strengthened, e.g. "must" notify and not only "consider".
   b. The secondary uses and specific reasons for using personal and sensitive information should be clarified. Principle five should be amended to include the process and reasons for secondary use, and the associated informed consent.
   c. The principles should cover access by specified government organisations, considering all tiers of government and the applications of these technologies.
   d. Informed consent should not be limited to C-ITS and should be extended to AVs.
   e. The principles should have legislative weight.
2. Development of a framework around permitted usage of C-ITS and AV data should be informed by state and local government, industry and community consultation and communicated effectively from an early stage to build community trust in the technology.
3. Informed consent must be followed by sufficient, easy to understand information, and should be affirmative, not implied.
4. Where possible, personal and/or sensitive information should be encrypted and de-identified.
5. Government should reconsider whether the SAS will deliver a high level of cyber security, which is critical to the protection of both personal and sensitive information. A standard process for managing intrusions and threats should be considered.
6. The access, use and storage of personal and sensitive information by private industry should not be overlooked because it reflects a broader societal issue. Strong restrictions should be placed on ADSEs regarding use, storage, and sharing of personal and private information. In addition, government and industry should also consider ways to motivate ADSEs to improve their privacy policies, cybersecurity systems, and also their communication with consumers and service users.
7. There should be clear processes for individuals to make appeals, withdraw consent and 'be forgotten'. This will provide some level of ownership for individuals over their personal and sensitive information.
8. Government should consider a broad range of scenarios to gain a thorough understanding of the impact each option could have on the autonomy privacy of individuals.

RR6793

For further information please
contact advocacy@rac.com.au

RAC
For the better