Submission by the

Office of the Information Commissioner

National Transport Commission

SAFETY ASSURANCE FOR AUTOMATED DRIVING SYSTEMS CONSULTATION REGULATION IMPACT STATEMENT – MAY 2018

July 2018

The Queensland Office of the Information Commissioner (Queensland OIC) is an independent statutory authority. This submission does not represent the views or opinions of the Queensland Government. The statutory functions of the Queensland Information Commissioner under the Information Privacy Act 2009 (Qld) include commenting on issues relating to the administration of privacy in the Queensland public sector environment. Queensland OIC is available to provide further information or assistance to the Commission as required.

Thank you for the invitation to comment on the National Transport Commission's (NTC) Safety Assurance for Automated Driving Systems Consultation Regulation Impact Statement (Consultation RIS). The OIC welcomes the opportunity to provide a short statement on privacy considerations involved with automated driving systems (ADSs) and the responsibilities of automated driving system entities (ADSEs).

The OIC is also aware of the NTC's concurrent examination of Australia's information privacy framework in the context of regulating government access to cooperative intelligent transport systems and automated vehicle data. We look forward to participating in that stakeholder consultation process later this year.

The OIC notes the potential of ADSs to improve personal and public safety, flexibility of travel, and enhancement of individuals' mobility, and acknowledges NTC's thorough assessment of the three potential problems with deployment of ADSs outlined in the Consultation RIS (safety risks, consumer confidence and regulatory uncertainty).

OIC sees merit in the NTC's preferred option of a legislative safety assurance system with a primary safety duty, which also requires ADSEs to address principles-based safety criteria in a Statement of Compliance.

However, the OC would like to draw NTC's attention to some concerns about privacy, data recording and sharing, and cybersecurity.

Privacy concerns

The OIC is concerned to ensure that privacy risks are appropriately considered through the principles-based safety criteria. Regrettably, the importance attributed to these risks seems to have diminished as the NTC has progressed from its previous papers in 2016 and 2017[1], to the Consultation RIS of May 2018.

It is noted that the removal of privacy from the safety criteria mirrors a change in US policy, from the *Federal Automated Vehicles Policy 2016* to the most recent Voluntary Guidance for the US market *Automated Driving Systems 2.0*. However, in reflecting on international developments, consideration should also be given to recent policy dynamics in Europe. The General Data Protection Regulation, which came into effect on 25 May 2018, applies to data generated by ADSs and it grants individuals explicit privacy rights and imposes on entities explicit privacy responsibilities. Given the capability of ADSs to generate, store and transmit an extensive range of users' personal data (from location and behaviour patterns to music and restaurant preferences), European policy makers are aware of the significance of privacy considerations in ensuring acceptance by end-users[2]. Advisors to vehicle manufacturers in the European Union are encouraging them to 'rethink their fundamental approach to privacy and establish it as a core tenet of their business'.[3]

In discussing the removal of privacy from the safety criteria, the Consultation RIS asserts that privacy is 'not specifically a safety issue, and private sector access to and use of data is a significant societal issue that is much broader than automated vehicle policy and regulation'[4]. It is arguable that this view underestimates the risks germane to ADS-generated data that can be mitigated by privacy protections, for example, the genuine physical safety risks associated with real time location data and behaviour pattern data for victims of domestic and family violence. In the context of ADSs, some argue that location data is 'deserving of special protection due to safety/security concerns', should only be collected with free and informed consent of the individual to whom it pertains, and only used for the specific purpose for which that consent was given. [5]

[1] *Regulatory options for automated vehicles,* Discussion Paper, May 2016 – public perceptions about automated vehicles will be impacted by how consumers' personal information is handled and whether there are clearly defined privacy protections (page 12); *Regulatory options to assure automated vehicle safety in Australia*, Discussion Paper, June 2017 – the design of the safety assurance system should not preclude valid policy objectives being realised through the safety process (page 41); and A*ssuring the safety of automated vehicles*, Policy paper, November 2017 – improvements based on stakeholder feedback included the inclusion of privacy as a safety criterion and consumer confidence as a policy objective (page 18).

[2] European Parliamentary Research Service, *EU strategy on cooperative intelligent transport systems*, September 2017, page 4, accessed at http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608664/EPRS_BRI(2017)608664_EN.pdf

[3] Bearing Point Institute, *Connected cars and privacy: shifting gear for GDPR?* accessed on 22 June 2018 at https://www.bearingpoint.com/en/our-success/thought-leadership/connected-cars-and-privacy-shifting-gear-for-gdpr/

[4] NTC, *Safety Assurance for Automated Driving Systems Consultation Regulation Impact Statement*, May 2018, page 90.

[5] Warren, David et al, *All roads lead to the internet: privacy in the age of autonomous vehicles*, May 2018, accessed at http://www.corrs.com.au/thinking/insights/all-roads-lead-to-the-internet-privacy-in-the-age-of-autonomous-vehicles/

As the scope and volume of personal data generated and collected grows, so too does the frequency, scale and impact of privacy breaches. In this climate, privacy considerations warrant greater scrutiny, not less.

RECOMMENDATION – An ADSE's ability to demonstrate compliance with the *Privacy Act 1988 (Cth)* and the Australian Privacy Principles is vital, and OIC recommends that privacy be reinstated as a criteria to be addressed in a Statement of Compliance.

Data recording and sharing

The consultation RIS appropriately recognises that the *Privacy Act 1988 (Cth)* requires compliance with the Australian Privacy Principles that cover, among other things, the collection, use and disclosure of personal information. While these obligations are likely to apply to ADSEs by virtue of the $3 million turnover catchment of the Act, it may be appropriate for the NTC to make this explicit in the criterion relating to Data Recording and Sharing. While OIC understands that the intent of this criterion is to ensure the recording and sharing of crash and near-miss data, the use of the phrase 'without limiting the data to be recorded and shared' may create (avoidable) confusion.

Further, as can be seen across many commercial sectors, personal data is being used extensively for analytics and marketing. The secondary uses of ADS-generated data warrant scrutiny and would be an appropriate inclusion in the reporting requirements for ADSEs.

RECOMMENDATION – NTC may wish to consider removing or clarifying the phrase 'without limiting the data to be recorded and shared' in the Data Recording and Sharing criterion, and requiring ADSEs to report on secondary uses of personal data.

Cybersecurity

OIC notes the relatively narrow interpretation of cybersecurity in the Consultation RIS' description of the criterion. It is arguable that the focus on the risk of 'cyber intrusion' in the proposed criteria neglects data security vulnerabilities associated with non-cyber-intrusive threats, such as physical, human, governance and information-misuse risks, all of which may impact the safety of an ADS.

RECOMMENDATION – NTC may wish to clearly articulate the range of risk factors relating to cybersecurity to avoid potential for a narrow, cyber-intrusion based assessment of cybersecurity.