Office of the Information Commissioner
Queensland

Submission to the National Transport Commission

Regulating Government Access to C-ITS and Automated Vehicle Data – Discussion Paper

November 2018

The Office of the Information Commissioner (OIC) is an independent statutory authority. The statutory functions of the OIC under the *Information Privacy Act 2009* (Qld) (IP Act) include commenting on the administration of privacy in the Queensland public sector environment. This submission does not represent the views or opinions of the Queensland Government.

The OIC appreciates the NTC's consideration of this submission and is available to provide further information or assistance as required.

1. The OIC welcomes the opportunity to provide a brief submission in response to the National Transport Commission's (**NTC**) Discussion Paper – *Regulating Government Access to C-ITS and Automated Vehicle Data* (**Discussion paper**).

2. This submission highlights some of the key principles and considerations the OIC contends should be embedded in legislative, policy and operational regimes that facilitate C-ITS and Automated Vehicle (AV) technologies. It also briefly summarises OIC's views in response to the questions raised in the Discussion paper.

Balancing risks and benefits

3. The OIC notes the potential benefits of autonomous and connected vehicle technologies to improve driver safety, reduce road deaths and trauma, provide flexible travel options and enhance individuals' mobility.

4. In realising these benefits, governments must be aware of the significant implications for privacy that can flow from existing and emerging technologies. Privacy breaches can lead to devastating consequences for individuals, for example, the tracking and location of a domestic violence victim.

5. OIC recognises that the right to privacy is not absolute, and in some circumstances privacy rights must give way in light of compelling public benefits. However, initiatives requiring or authorising the collection, use or disclosure of personal information should always be reasonable, necessary, proportionate and minimise the data collected.

Transparency

6. Collection and use of data generated by C-ITS and AV technologies by government, including by law enforcement agencies, needs to be transparent and subject to rigorous oversight through a range of regulatory frameworks, including appropriate legislative constraints.

7. Personal information can also be exploited for commercial purposes with the use of personal information for data analytics and marketing expanding rapidly. Governments and the NTC need to be alert to, and prohibit, the potential exploitation of personal information in this way.

8. OIC notes that the scope of the Discussion paper is limited to examining government collection and use of information generated by C-ITS and AV technologies, and does not extend to the private sector. However, OIC considers a holistic review of collection, use and disclosure of information that includes the private sector would allow for a more meaningful analysis of whether additional privacy protections are required.

9. Further, as public-private partnerships and private sector delivery of government services increase, the distinction between private and public sector use of data can become blurred. Therefore, consistent, minimum standards for privacy and data security should apply irrespective of the type of entity collecting or using data for such purposes.

Privacy and data security for consumer confidence

10. Privacy breaches, as well as uncertainty about the collection or use of personal information, can reduce consumer confidence. Low levels of consumer confidence may detrimentally effect the take up rates of technologies that could make road travel safer and provide other public benefits as outlined in the Discussion paper.

Privacy by design

11. Privacy Impact Assessments (PIAs), which are systematic examinations of projects to assess impacts on the privacy of individuals, can identify potential impacts on privacy and recommend options for managing, minimising or eliminating negative impacts on privacy. PIAs should be conducted early in the policy process and should be revisited frequently as projects mature.

12. Bodies seeking to access C-ITS and AV data, whether private or public sector, should be required to conduct PIAs to ensure that privacy obligations are identified, understood and met. PIAs should include community and stakeholder consultation to help ensure use of data is consistent with community expectations.

'Personal information' by default

13. To enhance consistency across jurisdictions and ensure application of some minimum privacy protections, all data generated by C-ITS and AV technologies should be deemed personal information by default, consistent with Principle 2. Given the potential for data sets to be combined to identify individuals, and the difficulty in securing de-identified data against re-identification, treating all data as personal information may provide protections that would otherwise be easily circumvented.

Consent

14. Securing timely, meaningful, informed consent from all occupants of vehicles generating C-ITS and AV data is extremely difficult, if not impossible. Therefore, it is essential that legislation, policy and operational frameworks embed robust privacy protections and require that collection and use of data is authorised, necessary and transparent.

Information access laws

15. Right to Information and Freedom of Information laws also need to be considered in this context as they provide a right of access to government held information. Vast amounts of data will be generated by C-ITS and AV technologies, to which governments may be required to provide access.

In summary –

i. The OIC considers the assumptions identified by the NTC to be generally reasonable, and notes that one of these assumptions is that the NTC's safety assurance system is likely to include a data recording and sharing criterion. It is strongly recommended that this criterion establishes strict transparency and reporting requirements, especially with respect to any secondary uses of personal information. (Question 1)

ii. As new privacy challenges arise from information generated by C-ITS and automated vehicle technology, it is inevitable that new privacy challenges will emerge as technology becomes more sophisticated, its use becomes more widespread, and new uses for data and means of data re-combining are operationalised. Therefore, it is essential that broad and comprehensive privacy protections are built into legislative, policy and operational frameworks, and comprehensive PIAs are conducted and refreshed. (Question 3)

iii. The OIC contends that all C-ITS and AV data be treated as personal information by default, consistent with Principle 2. (Question 4)

iv. The types of government collection of data as broadly identified in the Discussion Paper appear to appropriately reflect the nature of government collection. However, currently unanticipated uses are likely to emerge and frameworks need to be sufficiently robust and transparent to accommodate future uses. (Question 5)

v. Current privacy frameworks for government collection and use of data, especially given inconsistencies across jurisdictions, are unlikely to comprehensively address all privacy challenges arising from new technologies. Legislative reform could enable consistent privacy standards and protections to data collection and use across jurisdictions, and across the public and private sectors. Privacy Impact Assessments should be mandated for all data collection and use, and be revisited as projects and technologies mature. (Questions 6 and 7)

vi. OIC considers separate options for addressing the privacy challenges of C-ITS and AV technology are warranted. This is due to the ability of C-ITS and AV technologies to operate independently of each other, the nature of data collected through C-ITS and AV technologies, and the different risks associated with these different types of data. (Question 8)

vii. The assessment criteria proposed by the NTC for both C-ITS and AV data appear reasonable. (Questions 9 and 11)

viii. OIC considers Option 2 the most credible option for both C-ITS and AV technology. This option recognises that legislative reform to govern collection, use and disclosure is required, while acknowledging that more detail is necessary before committing to a specific legislative framework. (Questions 10 and 12)

ix. The draft principles are a useful starting point for discussing the requirements of a regulatory framework to address privacy challenges. However, some elements could be streamlined to improve clarity and relevance, for example, making Principle 2 an unambiguous statement that information should be treated as personal information by default, and amending Principle 7 to reflect the reality of securing meaningful, informed consent of all occupants of relevant vehicles. (Question 13)