

6 July 2018

Our ref: D18/133809

Automated Vehicle Team
National Transport Commission
Level 3/600 Bourke Street
Melbourne VIC 3000

Dear Automated Vehicle Team,

Safety Assurance for Automated Driving Systems: Consultation Regulation Impact Statement

The Office of the Victorian Information Commissioner (**OVIC**) is pleased to provide a submission to the National Transport Commission (**NTC**) in relation to the Safety Assurance for Automated Driving Systems Regulation Impact Statement (**RIS**).

Established in September 2017, OVIC is the primary regulator for information privacy, data protection and freedom of information for the state of Victoria. As Information Commissioner I have a strong interest in matters that affect individuals' privacy, as well as the security of public sector data. One of my functions under the *Privacy and Data Protection Act 2014* (**PDP Act**) is to make public statements in relation to such matters.

In principle, OVIC supports the NTC in its preference for Option 4 of the proposed legislative options, including the development of a legislative safety assurance system which would include new legislation, mandatory self-certification, a regulatory agency responsible for administering automated vehicle safety and ongoing primary safety duty. OVIC supports the requirement to be placed on Automated Driving System Entities (**ADSEs**) to provide a Statement of Compliance demonstrating how each principle-based safety criteria have been managed before the Automated Driving System (**ADS**) can be introduced into the Australian market.

However, within this safety assurance system it is important that the potential risks inherent in collecting significant amounts of data, including personal information, are duly recognised. Given the frequent and escalating privacy and data breaches of recent times, it is arguable that privacy now more than ever warrants a stronger degree of scrutiny, rather than a weaker one. The emphasis attributed to these risks appears to have diminished significantly since many of the previous NTC papers, culminating in the explicit removal of privacy as a criterion within the Statement of Compliance to be required of ADSEs.

This submission outlines my office's views on the RIS, highlighting the concerns we have about the potential privacy impacts on individuals, as well as the inclusion of protective data security considerations.

Privacy Considerations

OVIC acknowledges that the NTC “considers the privacy of personal information collected and held by ADSEs is already broadly covered by the APPs”, and that privacy is “not specifically a safety issue.” Yet, the importance of an obligation on ADSEs to maintain the privacy of users should not be underestimated, nor should the indirect safety implications of mishandling data (including personal information). The potential harm from ADS-related privacy breaches still ought to be considered within this scheme. For example, privacy breaches could result in the loss, theft or inappropriate access to personal information, which can have implications beyond the use of ADSs in areas such as, but not limited to: identity fraud; access to location data within the context of domestic and family violence cases; and the inappropriate use of data for marketing purposes.

Further, while OVIC agrees that “private sector access to and use of data is a significant societal issue that is much broader than automated vehicle policy and regulation,” this is not a sufficient reason to disregard privacy as a consideration when introducing ADSs into the Australian market. The introduction of ADSs and the corresponding legislative response is one of the first instances in which the government is seeking to regulate widespread use of artificial intelligence technology. As such, this is an important opportunity to set the standard in this space, and to ensure that privacy and protective data security are properly considered throughout the process. Beyond this, the NTC itself has noted in previous papers that information privacy is essential to increasing customer confidence, trust and public perceptions.¹ It is clear that physical safety is not the only consideration that the public will take into account when it comes to adopting this technology.

The explicit exclusion of privacy as a criterion within the statement of compliance appears to reflect the shift in US policy from the *Federal Automated Vehicles Policy 2016*, to *Automated Driving Systems 2.0*, which also removed privacy as a criterion in the most recent Guidance for the US market. OVIC suggests that some important recent international policy trends indicate that sentiment may be shifting in favour of stronger privacy regulation such as the General Data Protection Regulation (GDPR) which came into effect in the European Union in May 2018, as well as the California Consumer Privacy Act of 2018. Aside from the clear benefit of aligning itself with the highest denominator of privacy standards, embracing robust privacy protections is an important factor in order for Australia to be competitive in international markets.

Recommendation

OVIC respectfully recommends that the NTC reconsider its position on excluding privacy as a consideration to be addressed in a Statement of Compliance, and thus include the ability of an ADSE to demonstrate compliance with the *Privacy Act 1988 (Cth)* and the Australian Privacy Principles (APPs) as an additional obligation to the 11 safety criteria. A clear demonstration of this could be achieved by requiring ADSEs to complete a Privacy Impact Assessment.

There are also a number of ways that privacy could be more effectively represented within the existing criteria. This would help to ensure that ADSEs are meeting their privacy obligations under the *Privacy Act 1988* and the APPs, and to ensure that privacy is built-in throughout the design and development process, rather than as a compliance ‘check-box’ activity. Please see our suggestions below regarding how privacy might be more effectively incorporated into this system.

1. Sections C.3.1 and 4.4.1 on Data Recording and Sharing

OVIC is pleased to see that ‘Data Recording and Sharing’ has been included as an obligation on ADSEs in addition to the 11 proposed safety criteria. We recognise that the purpose of these additional obligations is primarily to manage liability for events such as road traffic law breaches and crashes, however there is much room under this requirement to also place emphasis on good privacy (and protective data security) practices.

¹ NTC, *Assuring the safety of automated vehicles*, Policy paper, November 2017, page 18

OVIC finds the use of the phrase “without limiting the data to be recorded and shared” under C.3.1 to be potentially misleading with regard to the privacy obligations of ADSEs under the *Privacy Act 1988* and the APPs that will, by their nature, place reasonable limits on the data to be recorded and shared. This could potentially be mitigated with a clear statement highlighting that compliance with the *Privacy Act 1988* and the APPs is essential when recording and sharing data that would be considered to be ‘personal information’.

Privacy is currently only mentioned in reference to the ability for individuals to receive data to dispute liability, however there are many more privacy factors to consider when managing data recording and sharing. In their current form, C.3.1 and 4.4.1 do not make any reference to the appropriate handling of data, such as limiting access to only those who require it and who are authorised, ensuring data is stored and disposed of securely, and only using it for the primary purpose for which it was collected. This section would benefit from highlighting these requirements.

OVIC understands that not all the data recorded and shared will constitute personal information, yet the potential to identify individuals from data created and collected by ADSs should not be understated. Care should be taken when handling data that contains personal information that has been ‘de-identified’, as there is a real risk of re-identification in instances where ‘de-identified’ datasets containing ADS data are shared beyond ADSEs (for example, for analytics purposes).

2. Section C.5.1 on Reporting Obligations

The NTC may wish to consider including other uses of data, such as the use of personal information for secondary purposes including targeted marketing, analytics, or information sharing for government purposes in the legislative reporting obligations under C.5.1. Further, it may be worth noting any privacy breaches that have occurred within this reporting requirement in addition to cyber vulnerabilities as already included. ADSEs would likely be required to report any such data breach to the OAIC under the Notifiable Data Breaches Scheme.

Cybersecurity considerations

OVIC is pleased to see that cybersecurity is included as one of the 11 safety criteria under the safety assurance system (4.3.10, C.1.10).

Cybersecurity is not a consistently defined term in industry and whilst work is being undertaken by standards committees to resolve this, it is important to define the term in this context. If cybersecurity only refers to attacks from the internet, then threats and vulnerabilities from other vectors may be missed when identifying design, organisational and operational risks (A.1 and A.2), and the resulting risk management plans.

The requirement placed on an ADSE to demonstrate “how it has designed and developed an ADS that minimises the risk of cyber intrusion” does not adequately emphasise the fact that protective data security entails much more than just external cyber threats. By placing focus solely on “cyber intrusion”, there is risk that the remaining security domains (physical, information, personnel) as well as governance, may be overlooked. For instance, attacks on “back-end servers of the ADS [that] could disrupt the whole automated fleet” may also be caused by a malicious insider, a misconfiguration from an administrator or an external attacker physically accessing the servers. With a focus on cybersecurity, as it appears to be inferred, these types of risk may not be taken into consideration.


The compliance and enforcement measures relating to safety assurance would benefit from expanding reporting of cybersecurity breaches to any breaches that either directly or indirectly impact on the in-service safety of the ADS.

Recommendation

OVIC respectfully recommends that the NTC clearly defines the use of the term “cybersecurity” within the context of ADSs, and that the requirement placed on ADSEs would benefit from expanding the scope to include all security domains, rather than limiting it to risks of “cyber intrusion.”

Thank you for the opportunity to provide comment on the RIS. OVIC is happy to provide further detail on any of these points and recommendations. I understand that the NTC is also currently analysing issues related to regulating government access to C-ITS and automated vehicle data. My office will be following this process with interest, and we look forward to providing comment on the NTC’s work in this area also.

Yours sincerely



Sven Bluemmel
Information Commissioner