Australian Government

Office of the Australian Information Commissioner

A national in-service safety law for automated vehicles

Submission by the Office of the Australian Information Commissioner

Elizabeth Hampton

Acting Australian Information Commissioner and Privacy Commissioner

17 December 2020

OAIC

Contents

Part 1: Executive summary

1.1 The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the National Transport Commission's (NTC) discussion paper on a national in-service safety law for automated vehicles.

1.2 The discussion paper seeks feedback on the content of a new national law for the in-service safety of automated vehicles in Australia, the Automated Vehicle Safety Law (AVSL). The AVSL will:

- establish a general safety duty on the entities responsible for automated driving systems (ADS)
- place due diligence obligations on ADS executive officers, and
- establish an in-service regulator to oversee the safe operation of vehicles on the road and ensure compliance by regulated parties with their duties.

1.3 When designing policy and law to regulate the collection, use and disclosure of personal information and sensitive information, it is important to ensure that an appropriate balance is struck between protecting privacy and protecting public safety. Any provisions or powers which authorise the handling of personal information must be necessary and proportionate to achieving the goal of ensuring the safety of automated vehicles in Australia.

1.4 Automated vehicles will collect a considerable volume of information, including personal and sensitive information, as part of their operation. The proposed AVSL will facilitate the collection, use and disclosure of relevant information from a broad range of stakeholders for the in-service regulator to fulfil its objectives. It is important for regulators and other stakeholders to understand the potential value of the personal information that will be collected through the operation of automated vehicles, particularly where this information is combined with other datasets.

1.5 The OAIC supports national consistency in relation to the protection of the right to privacy in the context of automated vehicles, including regulating the safety of these vehicles in Australia.

1.6 The below comments are intended to ensure that strong privacy protections, as well as robust accountability and oversight mechanisms, are achieved through the development of the AVSL.

Part 2: The OAIC and the requirements of the *Privacy Act 1988* (Cth)

2.1 The OAIC has regulatory oversight of the *Privacy Act 1988* Cth (Privacy Act), which sets out how Australian Privacy Principle (APP) entities (including most Australian Government agencies, and

all private sector and not-for-profit organisations with an annual turnover of more than $3 million) must collect, use and disclose individuals' personal information.[1]

2.2 The Privacy Act includes 13 legally binding APPs. The APPs set out standards, rights and obligations in relation to collection[2], use and disclosure[3], security[4], access to[5], and correction of personal information.[6] Sensitive information[7] is generally afforded a higher level of protection under the APPs, in recognition that inappropriate handling of sensitive information can have adverse consequences for an individual.

2.3 The proposed AVSL will establish an in-service regulator to oversee the safe operation of vehicles on the road and ensure compliance by regulated entities with their regulatory obligations. This regulator will require access to information about the operation of automated vehicles and regulated parties to effectively perform its role. This may include personal and sensitive information that identifies the driver of the car, the fall-back ready user, the owner, the remote driver and the occupants of the automated vehicle.

2.4 APP 3.1 provides that entities must not collect personal information unless the information is reasonably necessary for one or more of the entity's functions or activities. An agency's functions will be conferred either by legislation (including a subordinate legislative instrument) or an executive scheme or arrangement established by government.[8] The activities of an agency will be related to its functions. Implicit in these requirements is that agencies should only collect the minimum amount of personal information necessary for their functions or activities. The in-service regulator will need to consider whether collection of a broad range of information, including sensitive information, is reasonably necessary for, or directly related to, its functions or activities.

2.5 Additionally, the AVSL will also need to clearly set out any permitted uses and disclosure of personal information. APP 6.1 requires that agencies only use and disclose personal information for the particular purpose (the primary purpose) it was collected. Information may only be used or disclosed for another purpose (a secondary purpose) where the individual

---

[1] Personal information is defined in section 6(1) as any 'information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information is recorded in a material form or not'.

[2] See APPs 3, 4 and 5 (collection of personal information).

[3] See APPs 6, 7, 8 and 9 (use or disclosure of personal information).

[4] APP 11 requires an APP entity to take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

[5] APP 12 requires an APP entity that holds personal information about an individual to give the individual access to that information on request.

[6] APP 13 requires an APP entity to take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.

[7] Sensitive information is a subset of personal information and is defined as information or an opinion about an individual's racial or ethnic origin, political opinions or membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices or criminal record, as well health information, genetic information, biometric information and biometric templates. See section 6(1).

[8] *APP Guidelines*, Chapter 3: APP 3 — Collection of solicited personal information, paragraph 3.10, https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-3-app-3-collection-of-solicited-personal-information.

consents to the use or disclosure, or where another exception applies, such as where the disclosure is required or authorised by law[9] or where the disclosure is authorised under the law enforcement exception in APP 6.2(e).

2.6 APP 11 requires an entity to take active measures to ensure the security of the personal information it holds, and to actively consider whether it is permitted to retain personal information. Given the nature of information that will be collected by the in-service regulator in the course of its functions, the reasonable steps required for compliance with APP 11 are likely to be significant.

2.7 APP entities also have obligations under the Notifiable Data Breaches scheme to notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved.[10] This requirement to notify individuals of eligible data breaches goes to the core of what underpins good privacy practice — transparency and accountability. This requirement will also ensure that individuals are given the opportunity to take action to mitigate any risks resulting from a data breach experienced by the in-service regulator.

2.8 These provisions ensure that the collection, use, disclosure and security of personal and sensitive information by the in-service regulator protects the privacy of individuals engaging with this technology.

Part 3: Access to personal information by the in-service regulator and information exchange with other regulators and agencies

3.1 There are two broad categories of information that the in-service regulator will require access to:

i. information about the parties involved in the automated vehicle's operation, and

ii. information about the operation of the automated vehicle.

3.2 This may include collection of personal and sensitive information that identifies a range of individuals, including the driver of the automated vehicle, the fall-back ready user, the owner, the remote driver and the occupants of the vehicle.

3.3 Information may be required about who was in control at a point in time (the automated driving system or a human), the level of automation engaged, speed and brake information as well as information about circumstances that may have caused or contributed to an incident (for example, in-cabin camera information or biological or health sensor information to assess the behaviour of the driver/occupants.). Where this information constitutes sensitive

[9] See APP 6.2(b).

[10] See Part IIIC of the Privacy Act. See also 'About the Notifiable Data Breaches scheme': https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme/

information (including health information) a higher level of privacy protection applies under the APPs.[11]

3.4 This information may be required to be collected by the in-service regulator from ADSEs, the first-supply regulator, registration and licensing authorities, law enforcement agencies (both federal and state and territory), the National Heavy Vehicle Regulator, private and public road managers, remote drivers and regulators outside transport systems (such as WHS, consumer safety and competition and corporations' governance regulators).

3.5 The discussion paper notes that the in-service regulator will need clear legislative authority to collect, use and disclose personal information to other agencies that is reasonably necessary for its functions and activities under the national law. It is also noted that the in-service regulator's management of personal information will need to comply with the APPs and that a Privacy Impact Assessment (PIA) will be undertaken before the NTC finalises the policy details of the AVSL.

3.6 It is anticipated that the in-service regulator will require access to information, including personal information, to effectively perform key compliance and enforcement functions under the AVSL including:

- monitoring, investigating and enforcement
- collaborating with other agencies and regulators
- accreditation and regulatory approvals
- developing standards, and
- crash investigation.

3.7 Similarly, other entities may be required or authorised to collect, use or disclose personal information including ADSEs and state and territory government agencies.

Part 4: Coverage under the Privacy Act

4.1 The discussion paper poses two options for legislative implementation of a national AVSL:

- a complementary law approach, or
- state and territory applied law, whereby laws to regulate the in-service safety of automated vehicles could be made entirely in state and territory legislation.

4.2 The discussion paper also notes that the privacy implications of the collection, use or disclosure of personal information may need to be managed differently depending on the legislative implementation model adopted. It is noted that under a state and territory applied law approach, state and territory legislation would apply to the collection, use and disclosure of personal information under the AVSL.

[11] For example, see APPs 3, 6 and 7.

4.3 The Commonwealth Privacy Act continues to apply to APP entities regardless of whether a complementary or an applied law approach is taken. However, the Privacy Act does not apply to organisations with an annual turnover of $3 million or less, or to state and territory government agencies.

4.4 Most states and territories have equivalent privacy regimes which cover public sector agencies however some states and territories do not have their own privacy legislation.

4.5 We recommend that the collection, use and disclosure of personal information be covered by the Commonwealth Privacy Act to ensure consistent privacy protections are embedded as part of the in-service regulation of automated vehicles in Australia.

4.6 A complementary law approach would therefore be preferable where this option presents opportunities to achieve a nationally consistent framework with enforceable privacy protections.

4.7 We recommend that any entity which is not currently subject to privacy laws that is required or authorised to collect, use or disclose personal information, including sensitive information, under the AVSL, be covered by the Privacy Act.

4.8 Any entity – such as an automated driving system entity – that is exempt from the Privacy Act by virtue of the small business exemption, should opt into coverage of the Privacy Act under section 6EA.

4.9 Similarly, where a state or territory authority is not covered by privacy legislation, we recommend they opt into coverage of the Privacy Act under section 6F(1). This provision allows a state or territory authority to be prescribed as an 'organisation' under the Privacy Act in respect of certain acts or practices.

Recommendation 1
The collection, use and disclosure of personal information as required or authorised by the AVSL be covered by the Commonwealth Privacy Act to ensure enforceable privacy protections are embedded as part of the in-service regulation of automated vehicles in Australia. Any entity that is exempt as a small business operator should opt into coverage of the Privacy Act under section 6EA, and any state or territory authority that is not subject to privacy legislation should opt into coverage under section 6F(1).

4.10 The OAIC is pleased to see that a PIA will be undertaken by the NTC prior to finalising the policy details of the AVSL, and we suggest that the above recommendation be considered as part of the PIA.

4.11 We suggest that a PIA would be particularly helpful in assessing the privacy risks that may arise under a complementary law approach or a state and territory applied law approach and would usefully inform any decisions regarding the scope and implementation of a national AVSL.

4.12 A PIA could also usefully consider whether it would be beneficial for all state and territory authorities to opt into coverage of the Privacy Act, regardless of whether a relevant privacy law exists, in the interests of achieving a nationally consistent framework. There are differences and

gaps across state and territory privacy regimes including in relation to important privacy protections such as notifiable data breach obligations which would be overcome by nationally consistent coverage by the Privacy Act.

4.13 This would ensure that personal information is handled consistently regardless of which state or territory an individual resides in - or an entity operates in - and that the OAIC will have jurisdiction in the event that one of these exempted entities experiences a privacy incident.

4.14 National consistency and enforceable privacy protections will ensure that individuals can have trust and confidence in relation to the collection, use and disclosure of personal information by entities under the AVSL.

Part 5: Suggested privacy protections

The information exchange framework should be prescribed in legislation

5.1 Question 28 seeks views on whether a 'specific power authorising collection, use and disclosure of personal information is required in the national law and in state and territory legislation'.

5.2 Due to the volume and nature of the personal – and potentially sensitive – information that may be required to be collected, used and disclosed under the AVSL, we recommend that provisions authorising or requiring collection, use and disclosure of this information be prescribed in primary legislation.

5.3 Providing such detail in primary legislation would provide for greater public scrutiny and protect against collecting, using or disclosing personal information in ways that may not have been originally intended, or which may not be reasonable, necessary and proportionate in light of the relevant policy objectives.

Recommendation 2
An information exchange framework should be prescribed in legislation.

Provisions which permit or require the collection, use or disclosure of personal information should be clearly and narrowly expressed

5.4 We recommend that any provisions in the AVSL which authorise or require the collection, use and disclosure of personal information be clearly and narrowly prescribed, and that any categories of personal information to be collected, used or disclosed be clearly set out, paying due regard to the strengthened protections in the Privacy Act for certain types of personal information, including sensitive information and health information.

Recommendation 3
Provisions which authorise or require the collection, use and disclosure of personal information be clearly and narrowly prescribed, and any categories of personal information to be collected, used or disclosed must be clearly set out in primary legislation.

Privacy Impact Assessment

5.5 As the proposed AVSL will have impacts on individual privacy, we are pleased to see that a PIA will be undertaken to systematically consider the information access, use and disclosure proposals set out in the discussion paper. This is consistent with a privacy by design approach and will ensure that privacy risks are identified and mitigated in the early stages of this project.

5.6 A PIA is a systematic assessment of a project, which can assist in identifying potential impacts that a project might have on individuals, and sets out recommendations for managing, minimising or eliminating those impacts. The OAIC has published a Guide to undertaking privacy impact assessments[12], which may be helpful in this regard, as well as a PIA e-learning tool.[13]

5.7 We note that agencies are required to undertake a PIA for all high privacy risk projects, in accordance with s 12 of the *Privacy (Australian Government Agencies – Governance) APP Code 2017.*[14] A project may be a high privacy risk project if the agency reasonably considers that the project involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals.

5.8 We suggest that a PIA would usefully assist in identifying privacy risks and mitigation strategies in relation to the collection, use and disclosure of ADS-derived personal information, as posed by question 29. A PIA would also usefully assist in mapping out the relevant data flows that will arise as a result of the introduction of an in-service regulator, and in identifying and analysing any privacy risks inherent in a complementary law approach and a state and territory applied law approach to implementing the AVSL, including potential gaps in coverage of privacy protections.

Part 6: Government access to automated vehicle data

6.1 The discussion paper notes that in 2019 the Infrastructure and Transport Council endorsed 11 design principles for managing government access to, and addressing new privacy challenges of cooperative intelligent transport systems (C-ITS) and automated vehicle data.

[12] OAIC Guide to undertaking Privacy Impact Assessments: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/

[13] PIA eLearning tool: https://www.oaic.gov.au/s/elearning/pia/welcome.html

[14] Privacy (Australian Government Agencies – Governance) APP Code 2017: https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/australian-government-agencies-privacy-code/

6.2 It is intended that an information sharing framework will incorporate these 11 design principles, although we understand that it is not intended that these design principles be codified in the AVSL.

6.3 The design principles state that the laws and aligned standards for C-ITS and automated vehicles should:

i. balance 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 C-ITS and automated vehicle data

ii. be consistent with, and informed by, existing and emerging Australian and international privacy and data access frameworks

iii. embed access powers and privacy protections for C-ITS and automated vehicle data in legislation

iv. clearly define C-ITS and automated vehicle data in inclusive and technology neutral terms

v. align government entities' approach to managing C-ITS and automated vehicle data with the objectives underlying existing concepts of personal information

vi. 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

vii. recognise the importance of notifying users in plain English about government collection, use, disclosure and storage of C-ITS and automated vehicle data

viii. recognise that meaningful informed consent is important but provide avenues for government entities to balance individuals' expectations of privacy in alternative ways where obtaining such consent is not possible

ix. recognise the difficulty of irreversibly de-identifying C-ITS and automated vehicle data in many circumstances

x. support data security

xi. allow for regular review of privacy protections for C-ITS and automated vehicle data.

6.4 The OAIC is broadly supportive of enhanced, harmonised privacy standards for government agencies that handle C-ITS and AV data. In this regard, an object of the Privacy Act is to provide the basis for a nationally consistent framework to regulate privacy.[15] However, it is important that the principles do not derogate from the obligations of the Privacy Act, and the APPs in particular, and that they do not cause any confusion for regulated entities in relation to their privacy obligations.

[15] Section 2A(c) of the Privacy Act.

6.5 The APPs are binding legal principles which apply to regulated entities, and it is important to ensure that there is clarity and consistency for the regulated community in relation to their regulatory obligations.

Recommendation 4
There must be clarity and consistency for regulated entities in relation to their privacy obligations under the APPs, and in relation to the role of the design principles generally.

6.6 The OAIC welcomes the opportunity to engage further with the NTC as they progress this proposal.

6.7 If you would like to discuss these comments or have any questions, please contact Kellie Fonseca, Director, Regulation and Strategy Branch