



Australian Government

Office of the Australian Information Commissioner

Our reference: [D2018/015007](#)

Ms Helen Tsirlina
National Transport Commission
Level 3/600 Bourke Street
Melbourne VIC 3000

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

Dear Ms Tsirlina,

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the *Regulating Government Access to C-ITS and Automated Vehicle Data Discussion Paper* (discussion paper).

The discussion paper outlines the context and privacy challenges of government access to data generated by cooperative intelligent transport system (C-ITS) and automated vehicle (AV) technology. It recognises that the adoption of C-ITS and AV technologies will likely lead to a significant increase in the volume of personal information and sensitive information handled, and that this would raise community concerns around privacy. Consequently, the National Transport Commission's (NTC's) preliminary recommendation is to adopt broad principles, which would inform a framework for regulatory privacy protections specific to C-ITS and AV data. The OAIC acknowledges the consideration that has been given to the potential privacy challenges associated with C-ITS and AV data and the role that privacy protections will play in ensuring community trust and the long term success of these technologies.

By way of overall comment, public support for projects that significantly increase governments' capability to access information depends on a number of factors, such as the purpose and security of the information being held, and on the level of choice and control afforded to individuals in how their information is used and by whom. In addition, robust accountability and oversight mechanisms are essential to ensuring the success and sustainability of initiatives involving new personal information handling practices.

The OAIC is therefore supportive of introducing a set of broad principles to address the privacy challenges identified, to the extent that these provide privacy enhancements to the existing regulatory landscape.¹ Option 2 involves agreeing broad principles on limiting government collection, use and disclosure of AV information. This option provides the

¹ As discussed below, adopting specific legislation is consistent with international developments in regulating AV and C-ITS.

flexibility to develop legislative privacy protections as the regulatory landscape for C-ITS and AV technologies matures, and the information flows between data sharing participants, and beneficial uses of C-ITS and AV data, becomes clearer.

The below comments are intended to ensure that strong privacy protections, as well as robust accountability and oversight mechanisms, are embedded in any recommendations made by the National Transport Commission (NTC).

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

The OAIC has regulatory oversight of the *Privacy Act 1988* Cth (Privacy Act), which set 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 handle, use and manage individuals' personal information.

The Privacy Act includes 13 legally binding APPs. The APPs set out standards, rights and obligations in relation to collection², use and disclosure³, security⁴, access to⁵, and correction of personal information.⁶

The discussion paper references the APPs and their State/Territory equivalents, and discusses matters particularly relevant to APP 3,⁷ which relates to collection, and APP 6,⁸ which relates to the use and disclosure of personal information. Information on how these APPs apply in practice is set out below.

APP 3.1 provides that agencies must not collect personal information unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities. As outlined in the OAIC's *APP Guidelines*, an agency's functions will be conferred either by legislation (including a subordinate legislative instrument) or an executive scheme or arrangement established by government.⁹ The activities of an agency will be related to its functions. Under APP 3.1, an agency must also be prepared to justify collection as

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 required 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 Discussion paper, Chapter 5, *Government collection of information generated by vehicle technology*, p.42.

⁸ Discussion paper, Chapter 6, *Government use, disclosure, de-identification and destruction of information generated by vehicle technology*, p.55.

⁹ *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>.

‘reasonably necessary’.¹⁰ Implicit in these requirements is that agencies should only collect the minimum amount of personal information necessary for their functions or activities.

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 consents to the use or disclosure (consent is discussed in further detail below), or where another exception applies, such as where the disclosure is required or authorised by law,¹¹ or where the disclosure is authorised under the law enforcement exception in APP 6.2(e), discussed further below.

Broad observations on Option 2 draft principles

The draft principles within Option 2 are intended to inform a framework for privacy protections specific to C-ITS and AV data. As mentioned, we recognise the benefit of a flexible, principles-based approach at this early stage of the implementation of C-ITS and AV technologies. In my view, Option 3 (in relation to C-ITS data) or Options 3 or 4 (in relation to AV data) could also be considered as information flows and their purposes become clearer, to address any areas of heightened privacy risk.

Some of the privacy protections included in the draft principles are that: ‘additional privacy protections will likely be needed to appropriately limit the collection, use and disclosure of C-ITS and automated vehicle information to specific purposes’ (Principle 3), ‘to the extent possible, additional privacy protections for C-ITS and automated vehicle information should be legislative’ (Principle 4), and principles that provide for obtaining individuals consent (Principle 7) and the regular review of privacy protections (Principle 8).¹²

The OAIC is broadly supportive of legislating for enhanced, harmonised 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, and the suggested approach aligns with this goal.¹³ However, it is important that the principles do not derogate from the obligations of the Privacy Act, and the APPs in particular. A number of the draft principles generally align with certain APPs and with the OAIC’s advice in applying them. For example, Principle 2 notes that ‘government entities should err on the side of caution and consider treating C-ITS and AV information as personal information.’ This is consistent with the OAIC’s advice in the *APP Guidelines* that ‘where it is unclear whether an

¹⁰ *APP Guidelines*, Chapter 3: APP 3 — Collection of solicited personal information, paragraph 3.18, <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-3-app-3-collection-of-solicited-personal-information>.

¹¹ See APP 6.2(b).

¹² Discussion paper, p.5.

¹³ Privacy Act s 2A

individual is ‘reasonably identifiable’, an APP entity should err on the side of caution and treat the information as personal information.’¹⁴

While the discussion paper focuses on the collection, use and disclosure of C-ITS and AV information, and transparency of those processes, it does not address risks associated with security of information (APP 11), its accuracy (APP 10), and access to, and correction of, that information (APPs 12 and 13). The OAIC would welcome further information about whether any privacy risks have been considered in respect of these matters and how these might be addressed.

Further, the OAIC understands that the draft principles will involve participants that are covered by privacy laws in different jurisdictions. These include Federal, State and Territory agencies, some of which are subject to privacy laws with similar requirements to the Privacy Act.¹⁵ In addition, some of these participants will be subject to the Australian Government Agencies Privacy Code, which commenced on 1 July 2018.¹⁶ The draft principles appear to be designed to address this fragmentation and draft Principle 4 states that, to the extent possible, additional privacy protections should be legislative. However, it remains unclear how additional legislative protections will interact with existing Commonwealth, State or Territory privacy laws and complaint handling and enforcement powers under those frameworks. The OAIC suggests that this be clarified as this initiative progresses.

Further consideration could also be given to privacy challenges relating to consent, law enforcement, de-identification, and accountability and oversight as outlined below.

Consent

Draft Principle 7(b) suggests that government agencies consider obtaining consent from users for the direct collection of C-ITS information. Consent is central to personal autonomy and to individuals’ trust in entities’ handling of personal information. When individuals feel a sense of personal control over the uses of their data, they are more likely to be supportive and confident about those uses.

Requiring an individual’s consent before collecting sensitive information and when handling personal information for a secondary purpose are a key privacy protection in the Privacy Act.

¹⁴ *APP Guidelines*, Chapter B: Key concepts, paragraph B.94, <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts>. Also refer to OAIC’s guide, *What is personal information?*: <https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information>. The concept of ‘personal information’ is broad, and in most cases, whether or not information is personal information will be a straightforward question. However, in some cases it may not be as clear, and the answer will depend on the context and circumstances. Where there is uncertainty, the Office of the Australian Information Commissioner (OAIC) encourages entities to err on the side of caution by treating the information as personal information, and handle it in accordance with the Australian Privacy Principles (APPs).

¹⁵ For more information about State and Territory privacy laws, see <https://www.oaic.gov.au/privacy-law/other-privacy-jurisdictions>.

¹⁶ Further information about the *Australian Government Agencies Privacy Code* is available on the OAIC’s website at: <https://www.oaic.gov.au/privacy-law/australian-government-agencies-privacy-code/>

The OAIC has published advisory guidelines (the *APP guidelines*) which address some of the key challenges and issues in seeking consent.¹⁷ For example, the APP guidelines discuss:

- the four key elements of consent — consent must be voluntary; consent must be current and specific; the individual must be adequately informed before giving consent; and the individual must have the capacity to understand and communicate their consent (paragraph B.35)
- the limited circumstances in which use of an opt-out mechanism to infer consent may be appropriate (paragraph B.40)
- the potential for the practice of bundled consent to undermine the voluntary nature of consent (paragraphs B.45 – B.46)
- the assessment of whether an individual has capacity to consent (paragraph B.52 – B.58).

The data flows in the context of C-ITS and AV technology are likely to be complex, and this presents challenges for obtaining genuine consent from individuals. To build public trust in these technologies, careful consideration must be given to how individuals can exercise choice and control over their personal information – particularly, how individuals can be given notice of, and exercise meaningful consent to the collection, use and disclosure of their information.

The 39th International Conference of Data Protection and Privacy Commissioners (ICDPPC) 2017 *Resolution on Data Protection in Automated and Connected Vehicles* provides useful recommendations in this regard.¹⁸ The Resolution calls on all relevant parties (including public authorities, vehicle and equipment manufacturers, and providers of data driven services) to ‘fully respect the users’ rights to the protection of their personal data’, and urges them to, among other things:

- provide granular and easy to use privacy controls for vehicle users enabling them to, where appropriate, grant or withhold access to different data categories in vehicles
- provide technical means for vehicle users to restrict the collection of data
- develop and implement technologies for cooperative intelligent transportation systems in ways that enable vehicle users to inhibit the sharing of positional and kinematic data while still receiving road hazard warnings
- provide vehicle users with privacy-friendly driving modes with default settings.

¹⁷ Available at: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/>.

¹⁸ Available at: <https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-data-protection-in-automated-and-connected-vehicles-.pdf>.

It is equally important to acknowledge that in some circumstances, where the key elements of consent cannot be satisfied, it will not be appropriate to obtain an individuals' consent to particular information handling practices. For example, this may be the case where the use or disclosure of data is necessary to ensure road safety or proper functioning of a vehicle.

Where it is not appropriate to obtain consent in particular circumstances, a commensurate increase in oversight, accountability and transparency is required to balance individuals' expectations of privacy and other public interest objectives.

Law enforcement collection, use and disclosure of C-ITS and AV data

The discussion paper outlines a particular concern with the breadth of law enforcement agencies' powers to collect, use and disclose personal information obtained through C-ITS and AV technologies, including through the application of the general law enforcement exception in APP 6.2(e).¹⁹ Further, the discussion paper makes reference to potential new law enforcement powers to access information in order to determine whether an automated vehicle system or the human driver was in control of the vehicle in the event of a breach of a road traffic law or crash.²⁰

To build and maintain public trust, a balance must be struck between the legitimate objective of enhancing agencies' access to data for enforcement purposes and potential privacy impacts on individuals. This has been demonstrated recently through the broad community debate in relation to the My Health Record (MHR) system, which has evidenced community concern about the extent to which Australian Government agencies should be able to access data for secondary purposes, and in particular for purposes related to law enforcement. The objectives of the MHR are evidently different from initiatives concentrated on C-ITS and AV technology; however, there is potential for similar community concerns to arise should governments' (including law enforcement agencies) powers to collect, use and disclose personal information expand.

Draft Principle 5 may be useful in striking an appropriate balance between privacy and law enforcement objectives. Draft Principle 5 suggests that additional privacy protections should specify the C-ITS information covered, the specific purposes for which it may be used, and the parties to whom any specific purpose limitations apply.²¹ This may include carefully

¹⁹ Discussion paper, p. 49. APP 6.2(e) is aimed at enabling APP entities to cooperate with an enforcement body where it may have personal information relevant to an enforcement related activity of that enforcement body. Under this APP, an APP entity must reasonably believe that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body (see *Privacy Amendment (Enhancing Privacy Protection) Bill 2012 Explanatory Memorandum*, p.80). An entity must have a reasonable basis for the belief, and not merely a genuine or subjective belief. It is the responsibility of the entity to be able to justify its reasonable belief. See Chapter 6: APP 6 — Use or disclosure of personal information, *APP Guidelines*, clause 6.59, <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-6-app-6-use-or-disclosure-of-personal-information>.

²⁰ Discussion paper, p. 46.

²¹ Discussion paper, Draft Principles, p. 5

considering the types of offences that may justify intrusions on individuals' privacy through increased disclosures to law enforcement. To the extent possible, additional privacy protections could also state the kind of personal information that may be disclosed to relevant law enforcement agencies. Additional oversight, accountability and transparency mechanisms may also help to ensure ongoing community support in the event of increased disclosures to law enforcement agencies.²²

De-identification

The discussion paper includes the assumption that 'it is difficult to irreversibly de-identify personal information'.²³ In addition, it notes that 'requirements for public sector agencies to de-identify or destroy personal information are unlikely in practice to greatly reduce the amount of personal information held by government.'²⁴ Accordingly, the draft principles do not specifically suggest that entities use de-identification, anonymisation or pseudonymisation measures.²⁵ Additionally, draft Principle 7 refers to aggregating any C-ITS information collected, which would likely increase the risk of individuals becoming identifiable within a dataset due to the richness of C-ITS information, including vehicle location and patterns of movement.

De-identification can be a valuable tool allowing the utility of data to be maximised while preserving individual privacy. It is an important risk management exercise that should be applied as an additional layer of privacy protection, wherever practical. The OAIC encourages the NTC to consider the circumstances in which de-identification, anonymization or pseudonymisation (where de-identification or anonymization is not feasible), may be appropriate to minimise the amount of personal information collected and handled in the context of C-ITS and AV data.²⁶

Whether personal information is de-identified will necessarily depend on context. Information will be de-identified where the risk of an individual being re-identified in the data is very low in the relevant release context.²⁷ To de-identify effectively, entities must consider not only the data itself, but also the environment the data will be released into. Both of these factors will inform which techniques and controls are necessary to de-identify the data, while ensuring it remains appropriate for its intended use. The OAIC has produced various resources in the area of de-identification which may be useful, including co-

²² For example, the My Health Records Act 2012 was recently amended to limit access of personal information through imposing warrant requirements

²³ Discussion paper, p. 18

²⁴ Discussion paper, p. 58

²⁵ Discussion Paper, p. 5

²⁶ Relevantly, the ICDPPC's *Resolution on Data Protection in Automated and Connected Vehicles*, urges parties to 'utilize anonymization measures to minimize the amount of personal data, or to use pseudonymization when not feasible'.

²⁷ For these reasons, it is important to be aware that open data environments are really only appropriate for information that is either not derived from personal information, or information that has been through an extremely robust de-identification process that ensures - with a very high degree of confidence - that no individuals are reasonably identifiable, and that no re-identification could occur.

authoring with CSIRO/ Data 61 the *De-identification Decision-making Framework*²⁸, which provides detailed guidance on the factors that should be considered to ensure de-identification is carried out effectively and in compliance with the Privacy Act, as well as a guidance sheet on the *De-identification of data and information*.²⁹

Accountability and oversight

It is unclear from the discussion paper what mechanisms will be in place to monitor compliance with any legislated principles. In addition, the paper does not appear to discuss accountability, complaint and redress mechanisms for alleged privacy breaches. While the OAIC appreciates that this may not be within the scope of this initial discussion paper, having in place robust accountability and oversight mechanisms for responsible information privacy management will be essential to ensure the success and sustainability of this initiative. The OAIC would be pleased to further explore these important privacy safeguards with the NTC as this initiative progresses.

Privacy by design

The OAIC welcomes and supports the discussion paper's focus on building a privacy regulatory framework to support Australians' confidence in the handling of C-ITS and AV data. In addition, the OAIC suggests that the NTC continue to promote a privacy by design approach in any recommendations it makes.

Privacy by design is about finding ways to build privacy into projects from the design stage onwards and is a fundamental component of effective privacy protection. It positions entities to take a risk management approach, where privacy risks are identified and mitigated in the early stages of any project or initiative. APP 1.2 enshrines a privacy by design approach to privacy protection by requiring entities to embed APP compliance into their information practices, procedures and systems.

Taking a privacy by design approach supports the overall objectives of the NTC's project on C-ITS and AV data, and would reduce privacy risks for entities in a number of ways:

- limiting the amount of information collected and held to that which is necessary for the performance of its functions and activities
- ensuring robust processes are in place to ensure information is destroyed or de-identified when it is no longer needed³⁰

²⁸ Available at: <https://www.oaic.gov.au/agencies-and-organisations/guides/de-identification-decision-making-framework>

²⁹ Available at: <https://www.oaic.gov.au/agencies-and-organisations/guides/de-identification-and-the-privacy-act>

³⁰ APP 11.2 requires APP entities to take such steps as are reasonable in the circumstances to destroy or de-identify information when the entity no longer needs the information for any purpose for which it may be used or disclosed under the APPs – provided the information is not contained in a

- ensuring appropriate security controls are in place to reduce the risk of a data breach
- building public trust through clear and meaningful notices and information about how information is handled, including how it is used and disclosed
- developing granular and easy to use privacy controls for individuals where this is practicable.

Privacy impact assessments (PIAs) are an important tool that can support the privacy by design approach. As of July 2018, all Australian Government agencies have been required to conduct a PIA for ‘high privacy risk’ projects or initiatives involving new or changed ways of handling personal information.³¹ The OAIC recommends that PIAs continue to be used throughout the development and implementation of regulatory frameworks for C-ITS and AV data. A PIA is a systematic assessment of a project that identifies the impact that it might have on the privacy of individuals and sets out recommendations for managing, minimising or eliminating that impact. The OAIC has developed the *Guide to undertaking privacy impact assessments*³² and an eLearning course on conducting a PIA³³, which aim to assist entities undertaking a PIA.

International regulatory developments

The international data privacy regulatory community is taking a keen interest in C-ITS and AV enabled vehicles. As mentioned above, in 2017 the ICDPPC published a *Resolution on Data Protection in Automated and Connected Vehicles*, which urged relevant parties to ‘fully respect the users’ rights to the protection of their personal data and privacy and to sufficiently take this into account at every stage of the creation and development of new devices or services.’ The resolution outlines 16 actions and activities which parties are urged to undertake to achieve this.

More recently, in March 2018, the European Union (EU) Parliament adopted a resolution on a European strategy on Cooperative Intelligent Transport Systems which emphasised that smart vehicles should comply fully with the General Data Protection Regulation (GDPR) and related rules.³⁴ The GDPR applies extraterritorially, to entities offering goods and services in

Commonwealth record or the entity is required by an Australian law, or a court/tribunal order, to retain the information.

³¹ Refer to: <https://www.oaic.gov.au/privacy-law/australian-government-agencies-privacy-code/>

³² Available at: <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments>

³³ Available at: <https://www.oaic.gov.au/elearning/pia/topic1.html>

³⁴ Refer to: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2018-0036+0+DOC+XML+V0//EN&language=en>


the EU, or monitoring the behaviour of individuals in the EU. The OAIC has published a resource to assist Australian businesses to understand the new requirements of the GDPR.³⁵

The regulatory frameworks and tools that are emerging internationally in response to C-ITS and AV technologies may provide valuable lessons for Australia in the near future.³⁶ Key themes under consideration internationally, particularly around transparency, choice and control for individuals in the context of C-ITS and AV data, resonate with Australians' privacy expectations, and the goals of the NTC within this project on government access to C-ITS and AV data.

The OAIC notes that developing an appropriate Australian privacy framework for C-ITS and AV data will require ongoing engagement with stakeholders from across government, the private sector, members of the public, and others. We look forward to continued engagement with the NTC on this issue.

If you would like to discuss these comments or have any questions, please contact Sophie Higgins, Director, Regulation and Strategy Branch, on +61292849775 or email sophie.higgins@oaic.gov.au.

Yours sincerely,



Angelene Falk
Australian Information Commissioner
Privacy Commissioner

6 December 2018

³⁵ Available at: <https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation>

³⁶ For example, in January 2018, Canada the Standing Senate Committee on Transport and Communications released a report on its study of the regulatory and technical issues of automated and connected vehicles
<https://sencanada.ca/content/sen/committee/421/TRCM/Reports/COM_RPT_TRCM_AutomatedVehicles_e.pdf>.

In 2017, the House of Lords Science and Technology Committee in the United Kingdom also published a report which set out recommendations for the Government in making policy and investment decisions in relation to autonomous vehicles
<<https://publications.parliament.uk/pa/ld201617/ldselect/ldsctech/115/115.pdf>>.