Office of the Victorian Information Commissioner

t 1300 00 6842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D18/143326

22 November 2018

Mr Marcus Burke
Director, Automated Vehicle Program
National Transport Commission
Level 3/600 Bourke Street
Melbourne VIC 3000

Dear Mr Burke

Submission in response to the Regulating Government Access to C-ITS and Automated Vehicle Data Discussion Paper

The Office of the Victorian Information Commissioner (**OVIC**) is pleased to provide a submission to the National Transport Commission (**NTC**) in relation to the *Regulating Government Access to C-ITS and Automated Vehicle Data Discussion Paper* (**the paper**).

OVIC is the primary regulator for information privacy, information security and freedom of information (**FOI**) in Victoria, and administers the *Privacy and Data Protection Act 2014* (**PDP Act**) and the *Freedom of Information Act 1982* (Vic) (**FOI Act**). As the Information Commissioner, one of my functions under the PDP Act is 'to make public statements in relation to any matter affecting personal privacy'. As such, I have a strong interest in matters relating to government collection, use and disclosure of information, in particular personal information. I note that 'Australia's information access framework' referred to in the Paper encompasses existing privacy regulation across Australia, which includes the PDP Act.[1]

This submission outlines my office's views in relation to the questions posed in the discussion paper. My comments are organised around the key themes we have identified in the paper. The key points of this submission are:

- Cooperative intelligent transport systems (**C-ITS**) and automated vehicle (**AV**) data should be treated as personal information by default.
- Strong privacy protections around C-ITS and AV data will help build community trust and confidence in governments' collection and use of this information; this can have a positive effect on public uptake of AV technologies.[2]
- The traditional, transactional model of consent is challenged in the context of government collection, use and disclosure of C-ITS and AV data, for reasons outlined below. It is also challenged by the volume, type and context of the data.

[1] As per the discussion paper, the term 'information access framework' is used in this submission to refer to the broader existing privacy protections and other legislation that provide government with the legislative authority to collect and use information. This framework encompasses privacy laws, government collection powers, and surveillance devices laws.
[2] Similar to the discussion paper, the term 'use' in this submission is intended to broadly cover use, disclosure and destruction or de-identification of information. However, it is important to note that 'use' within privacy law is a discrete concept to disclosure, destruction, and de-identification. The relevant terminology will be used where those concepts are discussed separately.

- Additional privacy protections are needed to address the privacy challenges posed by C-ITS and AV technologies.

- OVIC welcomes the NTC's reform Option 2.

General comments

1. OVIC welcomes the NTC's suggestion that the potential benefits arising from government access to C-ITS and AV data must be balanced with sufficient privacy protections for users. OVIC is of the view that strong privacy protections can enhance and achieve business objectives; this is particularly relevant in this context, where users' privacy concerns may pose a barrier to the uptake of C-ITS and AV technologies, as acknowledged in the paper.[3] Ensuring that strong privacy protections are in place prior to the widespread deployment of C-ITS and AV technologies can help to mitigate such concerns that users may have regarding government access to the data generated about them by these technologies, and build public trust and confidence in governments' collection and use of this data.

2. OVIC acknowledges that the paper is focused on the privacy issues and challenges of C-ITS and AV technologies. However, it is important to note that privacy is closely tied to security; strong privacy cannot be achieved without information security. When considering whether additional privacy protections are needed around government access and use of C-ITS and AV data, thought should also be given to the security of that data, as both privacy and security protections will be important for encouraging public acceptance of C-ITS and AV technologies. The security of vehicles and connected systems is also important and there are safety and consumer trust issues that must be considered in this regard.

3. Security considerations may also come into play where C-ITS and AV data is held by private sector providers, not just government bodies. As government regularly enters into contracts with private operators (for example, for toll roads and other physical and digital infrastructure), a consistent security standard for C-ITS and AV data should apply to both public and private entities. In Victoria, for example, this standard would be the Victorian Protective Data Security Standards, which also apply to private sector service providers or operators acting under State contract to the Victorian government.

4. Another factor to consider when developing a regulatory framework for C-ITS and AV technologies is the broader implications of government collecting and subsequently holding C-ITS and AV data. For example, where a government entity holding C-ITS and AV data is subject to freedom of information laws, that data could potentially be requested – and accessed – by the public (including individuals and private organisations) under applicable FOI regimes. This gives rise to the risk of C-ITS and AV data being used for a wide range of purposes beyond those for which it was initially collected by the government entity.

Community expectations and context

5. As outlined in the paper, government access to C-ITS and AV data can deliver public value through informing and enhancing government decision making. However, strong consideration must be given to the problems that government is trying to address in accessing this data (or at least certain pieces of data). Government collection and use of C-ITS and AV data should not occur simply because such data has been generated and is accessible; the necessity of collecting and using such data needs to be clearly identified and justified.

[3] On page 9 of the paper.

6. Government collection and use of C-ITS and AV data must also align with community expectations, which will play a part in public acceptance and uptake of these technologies – legislative protections alone will not determine what the public considers to be an acceptable collection or use of C-ITS and AV data. If the regulatory framework does not align with public expectations around government access and use of C-ITS and AV data, these technologies will not be met with community acceptance. Further, it should be recognised that community expectations are varied and can be determined by a number of elements, including cultural factors. What is considered by one group as an acceptable collection or use of C-ITS and AV data may not be acceptable to another group. This poses challenges in both policy development and policy implementation.

7. Similarly, the importance of context must also be considered. What is considered to be acceptable collection or use of C-ITS and AV data in one context may be considered unacceptable in another context. For example, community expectations around the collection of C-ITS and AV data from heavy vehicles may be different in comparison to the collection of that same data from private, individual vehicles.

8. Given the potential range of community expectations, the development of a regulatory framework for C-ITS and AV technologies should involve broad community and stakeholder consultation. Government access and use of C-ITS and AV data will affect various groups within the community in different ways, not just those individuals whose data is being collected by C-ITS and AV technologies. Community and stakeholder consultation will be important for informing acceptable and reasonable use of C-ITS and AV data that is in line with public expectations. Additionally, stakeholder consultation and engagement should not be a once-off occurrence; an effective engagement and change management strategy requires a continuous process of information sharing and feedback from stakeholders (including end users) and the organisations charged with leading reform relating to C-ITS and AV technologies.

Personal and sensitive information

9. OVIC supports the NTC's view that C-ITS and AV data will most likely amount to personal and sensitive information.[4] While not every piece of data generated by C-ITS and AV technologies may be directly identifying, OVIC believes that the potential for matching with other datasets can lead to the identification of individuals, particularly where this data is held by road and law enforcement agencies with access to a wide range of datasets and the technical capacity to analyse that data.[5] In particular, we wish to advise that methods for de-identification of unit-level records may not be sufficient to protect this data (see De-identification section below).

10. Given the potential for individuals to be identified, OVIC considers it best practice to treat all C-ITS and AV data as personal information by default, and strongly encourages this approach in the development of a regulatory framework.

11. Treating C-ITS and AV data as personal information by default offers assurance to users that their information will be protected under privacy legislation (where applicable), in addition to any privacy protections that may be enshrined in other laws (such as road transport laws). It also provides for consistency across organisations and jurisdictions, which may have different understandings as to whether C-ITS and AV data is or is not personal information. This creates the potential for confusion and inconsistency around what is or is not protected under privacy legislation.

[4] On page 3 of the paper.
[5] Ibid.

12. Further, treating C-ITS and AV data as personal information does not preclude it from being used or shared. OVIC accepts that such data can be used for purposes beyond anything that relates to individuals, or relies on the identification of individuals. However, treating C-ITS and AV data as personal information places important protections on the data that limit potential adverse effects on individuals.

13. As noted in the paper, whether C-ITS and AV data is considered sensitive information will vary across jurisdictions.[6] Under the PDP Act, sensitive information is a subset of personal information, and is strictly defined in Schedule 1. Biometric data that may be generated from biometric sensors in AVs, for example, would not be considered sensitive information under the PDP Act, but would be treated as such under the *Privacy Act 1988* (Cth), which has a broader definition of sensitive information.

14. As sensitive information is defined – and therefore protected – differently across jurisdictions, OVIC considers that there is value in having additional privacy protections around this type of information, particularly to address gaps in jurisdictions without existing privacy legislation. These protections should also be higher given the inherently sensitive nature of such information.

De-identification

15. OVIC agrees with the NTC's suggestion (outlined in page 18 of the paper) that it is difficult to irreversibly de-identify personal information. This assumption aligns with a report released by OVIC in May 2018 on the limitations of de-identification and its implications for the PDP Act.[7]

16. Some of the key points made in this report are that it is unlikely that a single technique can securely de-identify all types of data (in particular unit-record level information), and that there is an inherent risk of re-identification where unit-record level information is released in an open context, depending on the technique(s) used to treat the data and the auxiliary information available.

17. It is therefore OVIC's position that analysis of unit-record level data (as some C-ITS and AV data may be) is most appropriately performed in a controlled environment by data scientists. Where unit-level records are involved, it should not be made available where downstream governance of the data is not assured, for example as an "open" data set.

18. There would be value in developing a framework around the use (e.g. analysis) and disclosure of de-identified C-ITS and AV data. This should not be taken to mean that de-identified C-ITS and AV data cannot be used or disclosed, but rather that the risks arising from its use or disclosure (including the risk of re-identification) must be managed appropriately.

New privacy challenges

19. OVIC recognises that the paper focuses on the new privacy challenges posed by C-ITS and AV technologies; however, it is important not to diminish or overlook the existing privacy challenges arising from the technologies used in current vehicles. The use of technologies such as sensor input units, navigation systems and microphones will likely become more widespread, and will only contribute further to the volume and breadth of information that may be collected by government.

---

[6] On page 33 of the paper.

[7] A copy of the report, *Protecting unit-record level personal information*, is available on the OVIC website.

20. In addition to the new privacy challenges raised in the paper – including the generation of new types of information, and a greater breadth and depth of collection – there is also potential for function creep. Without the appropriate protections, there is a risk that C-ITS and AV data collected by government for one purpose (such as traffic management or road safety) may be used for another purpose that individuals would not have expected.

Information access framework

21. The current information access framework in Victoria, specifically in relation to existing privacy regulation (namely, the PDP Act) could allow for the broad collection of C-ITS and AV data by government where that information is necessary for its functions or activities, including where it is necessary for law enforcement purposes in certain circumstances. Similarly, there is potential for broad use and disclosure of C-ITS and AV data, particularly for law enforcement agencies that are exempt from a number of provisions contained in the Information Privacy Principles (**IPPs**) under the PDP Act, including IPP 2.1, which places limitations around the use and disclosure of personal information.[8]

22. The existing privacy protections in Victoria are therefore unlikely to be sufficient to address the new privacy challenges identified in the paper,[9] particularly for law enforcement collection and use of C-ITS and AV data and moreover, in light of organisations' growing capacity to link data (in terms of access to more datasets and their technical ability to perform data matching).

23. Accordingly, OVIC is of the view that reform and guidance is required to limit government collection and use of C-ITS and AV data to what is necessary and reasonable, noting the importance of community expectations and context to these notions of necessity and reasonableness. While the right to privacy is enshrined in Victoria's *Charter of Human Rights and Responsibilities Act 2006* (**the Charter**), and information privacy protections are offered under the PDP Act, reform would be valuable to address the privacy challenges raised by C-ITS and AV technologies.

24. Legislative reform would also be valuable for ensuring consistency around government access to C-ITS and AV data, particularly as privacy and other relevant legislation (for example, road transport, surveillance etc.) differs across jurisdictions. A regulatory framework would ensure that users experience a consistent standard of privacy protection regardless of in which state they are using AVs.

25. However, regardless of the resulting regulatory framework, government organisations need to ensure that they have the legislative authority to access and use C-ITS and AV data, whether under enabling legislation or privacy law. Further, access and use of this data must be in accordance with other obligations, such as the Charter in Victoria.

Reform options

26. OVIC is of the view that establishing principles to inform legislation is a good starting point for reform, and therefore supports Option 2 for both C-ITS and AV technology. We also agree that, notwithstanding the overlap between C-ITS and AV technology, separate options for addressing the privacy challenges posed by these two technologies is reasonable, given that both technologies can operate independently of each other.

[8] Section 15 of the PDP Act.
[9] As outlined on pages 29-31 of the paper.

27. We understand that at this stage, there is no view as to whether state-based legislation will be amended or if a national law will be created to regulate government access to C-ITS and AV data (if Option 2 is the preferred option). However, the benefit of principles to inform legislation is that they can do so regardless of whether it is state or federally-based, or whether new legislation is created, or existing laws amended.

28. OVIC is also mindful that framing consent in a legal manner is unlikely to address the challenges of managing public expectations; any principles need to be expressed clearly and succinctly, in a way that can be easily understood by members of the public.

29. While OVIC supports the idea of principles to inform legislative change, there is scope to improve the principles outlined in the paper. Further, given the relationship between privacy and security, we recommend that security protections also be considered as part of the principles, and legislative reform more broadly.

30. We also suggest that the draft principles promote embedding privacy enhancing practices in governments' access and use of C-ITS and AV data. This may entail, for example, a recommendation that government organisations collecting or intending to collect C-ITS and AV data complete a Privacy Impact Assessment prior to doing so. This will allow organisations to assess the privacy implications of their collection and handling of C-ITS and AV data, and help to ensure that privacy obligations under relevant legislation(s) are being upheld.

Draft principles

31. Principle 2 of the draft principles states that government entities should 'err on the side of caution' and treat C-ITS and AV data as personal information, unless there are 'legitimate reasons not to do so.' As noted above, OVIC strongly encourages that all C-ITS and AV data is treated as personal information by default, as best practice. We recommend providing clarification as to the 'legitimate reasons' for not treating the data as personal information, as this may be interpreted differently by organisations, resulting in different standards of protection being applied.

32. With respect to Principle 5, OVIC suggests that additional privacy protections should also clarify the circumstances around when government can collect C-ITS and AV data; that is, when it may or may not be reasonable or acceptable to collect this data. This will assist in limiting the C-ITS and AV data collected by government to that which is necessary; collection minimisation is a key tenet underpinning most privacy laws around the world, including the PDP Act in Victoria.

33. Given the risks associated with de-identification, OVIC supports the destruction – rather than de-identification – of C-ITS and AV data, as outlined in Principle 6b. We also support a stronger position towards these privacy protections and those outlined in Principle 5, and are of the view that they should be a requirement rather than simply a 'consideration', as expressed in the paper. In particular, it should be a requirement to provide notice to both drivers *and* passengers about any government collection and use of C-ITS and AV data (Principle 6a). Providing notice is critical for enabling individuals to exercise their information privacy rights, as well as setting the public's expectations around secondary use and disclosure of that information.

34. OVIC also suggests that the notion of obtaining consent from users as per Principle 7b be reconsidered, for reasons detailed below. We also consider that providing individuals with the opportunity to opt out of government collection and use of their C-ITS and AV data may pose additional challenges – for example, this could have implications on the integrity of the data that road agencies, for example, rely upon for traffic management or planning if C-ITS and AV data is collected from some vehicles but not others.

35. Finally, OVIC welcomes Principle 8 and the need to regularly review privacy protections for C-ITS and AV data. This is particularly relevant given that these technologies are still nascent and will only become more advanced and widespread with trials and testing.

Consent

36. Principle 7b of the draft principles relates to the issue of consent, and proposes that government consider obtaining consent from users for its collection of C-ITS and AV data. In OVIC's view, this is problematic for many reasons. As outlined in the paper, the volume, breadth and depth of C-ITS and AV data that could potentially be collected, and the range of purposes for which this data may be used, can be extensive. Moreover, given that these technologies are still in the early stages of being designed, developed and implemented, it is difficult to truly foresee the full extent of government access and use of C-ITS and AV data.

37. Without this information, it will be challenging for users to accurately undertake a risk-benefit analysis that is inherent in consent models underpinning privacy legislation in Australia. This traditional, transactional model of consent relies on the notion of meaningful consent which has a number of elements, including that consent must be informed. If users (and passengers) do not know the extent of government collection of their C-ITS and AV data, or do not understand how that data will be used and the implications in providing their consent, or the ways in which that data might be combined with other data sets and the impacts that might have, it is unlikely that they will be able to provide informed consent.

38. Meaningful consent also needs to be voluntary – that is, individuals must be free to exercise genuine choice. If a user does not consent to government collection or use of their C-ITS and AV data, what is the alternative? This issue is particularly relevant in relation to data captured by external cameras; while this type of data is already captured (for example, via CCTV and dashboard cameras), the breadth and depth of this type of collection will likely increase, as noted in the paper.

39. Another element of consent is that it must be given by a person with capacity. There may be some instances where users do not have the capacity to give consent for their C-ITS and AV data to be collected. Consent must also be current and specific, which may similarly give rise to potential issues, such as how consent will be updated or renewed into the future.

40. While consent could be obtained in a legal sense, for example via lengthy all-purpose user agreements, the question as to whether it is meaningful remains. Further, other passengers in C-ITS and AV vehicles present an additional challenge to this model of consent, as they may not have provided their own agreement. The difficulty in executing such an agreement for every 'driver' and passenger seems almost incomprehensible.

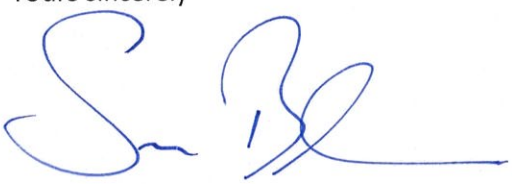
41. Given the challenges and issues involved with obtaining meaningful consent (from both users and passengers), OVIC suggests that rather than relying on consent, government ensures it has the legislative authority to collect C-ITS and AV data, and establish strong privacy protections to protect that information. This approach is consistent with a growing global trend moving away from consent-based models towards the establishment of minimum standards for protecting the privacy of personal information.

Thank you for the opportunity to comment on the paper and the matter of government access to C-ITS and AV data. OVIC will continue to follow the progress of the NTC's broader reform program with interest.

I have no objection to this submission being published by the NTC without further reference to me. I also propose to publish a copy of this submission on the OVIC website, but would be happy to adjust the timing of this to allow the NTC to collate and publish submissions proactively.

If you have any questions about this submission, please contact Adriana Nugent, Assistant Commissioner – Policy at Adriana.Nugent@ovic.vic.gov.au.

Yours sincerely



Sven Bluemmel
Information Commissioner