

28 October 2019

Our ref: D19/5556

Heavy Vehicle National Law Review Team
National Transport Commission
Public Submission – Effective enforcement
Level 3, 600 Bourke Street
MELBOURNE VIC 3000

Dear Heavy Vehicle National Law Review Team

Submission in response to Effective Enforcement Issues Paper

The Office of the Victorian Information Commissioner (**OVIC**) is pleased to provide this submission to the National Transport Commission (**NTC**) in response to the *Effective enforcement issues paper (the paper)*, as part of its review of the Heavy Vehicle National Law (**HVNL**).

OVIC is the primary regulator for freedom of information, information security and information privacy in Victoria. My office administers the *Freedom of Information Act 1982* (Vic) and the *Privacy and Data Protection Act 2014* (**PDP Act**). As the Information Commissioner, one of my functions under the PDP Act is to make public statements on matters that affect individuals' privacy. The themes covered in the paper relating to technology and data to improve enforcement under the HVNL are therefore of interest to OVIC.

This submission focuses on some of the issues identified in the paper, in particular de-identification and data sharing. A key point raised in this submission is that while these activities can have benefits, entities need to be aware of the limitations and risks associated with data sharing and de-identification, and ensure that individuals' privacy is protected where such activities may be facilitated or encouraged in a new HVNL.

Data sharing

The paper highlights the importance of data, and data sharing, to improve the effectiveness of compliance and enforcement activities under the HVNL, however notes that the current law does not contain provisions for operators, regulators and governments to actively share data.¹

Balancing public interests

OVIC recognises that safe data sharing for the reasons above can be valuable, however where a new HVNL does enable data sharing, the purposes for which operators, regulators, governments and other relevant parties can share data should be clear in the legislation. Importantly, the public interest in sharing data for these or any other purposes should be balanced with the public interest in protecting the privacy of personal information, where such information may be involved in the data sharing. This balancing of public interests is expressly acknowledged in the PDP Act for example, where one of the objects of that Act is to

¹ On page 37.

‘balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector’.²

Community expectations

Additionally, any data sharing scheme under a new HVNL must be established in a way that aligns with community and stakeholder expectations. Given the complexity and range of actors regulated under the current HVNL, there will likely be diverse – and potentially conflicting – views about matters such as what data should be shared, how, for what purposes, and with whom. A data sharing scheme that considers and balances the potentially divergent expectations of a wide range of operators, regulatory and enforcement bodies, and governments can help build trust and may be more likely to be met with acceptance, as well as help overcome barriers to data sharing; for example, of operators being ‘reluctant to share data with regulators and governments because they’re uncertain about how it will be used’.³

Principles under privacy legislation

Some of the concepts underpinning many privacy laws including the PDP Act – reasonableness, necessity and transparency – may be useful for the NTC to consider and incorporate into data sharing provisions that may be included in a new HVNL. These principles aim to reconcile the interests of data subjects and data users; for example, one of the Information Privacy Principles (IPPs) in the PDP Act, which relates to collection, requires that an organisation must not collect personal information unless it is *necessary* for one or more of its functions or activities.⁴ OVIC is of the view that data sharing under a new HVNL should be permitted where it is necessary (or reasonably necessary) for a particular purpose or function, rather than, for example, because it would be convenient.

Another IPP under the PDP Act, relating to data quality, requires that an organisation must take ‘reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date’.⁵ Data sharing provisions under a new HVNL could incorporate a similar principle, which may help address one of the barriers to data sharing identified in the paper of organisations, being ‘afraid to share their data because it may be out of date, incomplete or contain errors’.⁶

Privacy and sharing data

The paper briefly touches on the different Commonwealth, state and territory privacy legislation that regulates the collection and handling of personal information.⁷ Given the complex regulatory environment in which the HVNL operates, where parties regulated or exercising functions under the HVNL may be subject to different privacy laws, further and close consideration will need to be given to the interaction between the HVNL and privacy legislation in a data sharing context.

Similarly, OVIC suggests the NTC consider the different information security standards that may apply to entities collecting or generating information under the HVNL, and the implications for any data that may be shared under proposed data sharing provisions in a new HVNL. For example, information (including personal information) collected by Victorian law enforcement bodies and road authorities in the course of exercising compliance and enforcement functions under the HVNL, and which are covered by Part 4 of the PDP Act, may be subject to different security standards compared to similar information collected by equivalent bodies in other jurisdictions. Information protected to a certain level in one participating state may therefore be afforded a different level of protection when shared with an entity in a different state, where that entity may be subject to different privacy or security standards.

² Section 5(a), PDP Act.

³ Ibid.

⁴ Information Privacy Principle 1 (Collection), Schedule 1 of the PDP Act.

⁵ Information Privacy Principle 3 (Data Quality), Schedule 1 of the PDP Act.

⁶ Page 37 of the paper.

⁷ On pages 20 – 21.

Level of data being shared

In its 2017 report into data availability and use, the Productivity Commission stated that ‘a key issue in balancing access and trust is consideration of the level of data required for different uses’.⁸ Relevantly, the Productivity Commission gave the example of near real time data that identifies individuals (or businesses) as carrying the highest risks to privacy and security, noting that this level of data, ‘while useful for the enforcement of some regulations (for example, traffic speed limits)... is generally not currently necessary in order to obtain most of the benefits of data use’.⁹

Should the new HVNL facilitate data sharing, OVIC recommends the NTC carefully consider the level of data that would be appropriate for the different purposes for data sharing that the HVNL may enable. For example, unit-level record information that identifies individuals may not be necessary for data sharing conducted for the purposes of informing future planning and maintenance under the HVNL. While the paper does appear to recognise that sharing personal information is not always necessary, in encouraging the sharing of de-identified information,¹⁰ OVIC notes that de-identification is not a panacea to the potential privacy risks raised by data sharing that involves identifying information. These concerns are discussed further in the following section.

De-identification

The paper outlines four draft regulatory principles to guide the development of a new HVNL, one of which states that the ‘...sharing of de-identified and aggregated data should be facilitated and encouraged to inform non-regulatory decision making’.¹¹ In relation to de-identification specifically, the paper notes that ‘if proper de-identification techniques and re-identification risk management procedures are used, re-identification becomes difficult’.¹²

While robust de-identification techniques and risk management procedures are critical and can mitigate re-identification risks to an extent, it is OVIC’s view that successfully de-identifying personal information – particularly unit-record level data – to the point where it is permanent or cannot be re-identified, is likely to be impossible.¹³ Determining the likelihood of re-identification for any given dataset (for example, through data matching) is a key challenge as it is often difficult, if not impossible, to know what auxiliary information is available to the third parties with whom de-identified data is shared, particularly where it is shared openly in a public release context. OVIC’s work and experience in this area has highlighted the challenges and risks that can arise from the open release of unit-record level datasets, and we strongly encourage the NTC to carefully consider the potential implications for individuals’ privacy were a new HVNL to facilitate and encourage sharing of de-identified information.¹⁴

Notwithstanding the complexities of de-identification, it is not OVIC’s intention to dissuade entities from using de-identification techniques to enhance privacy; however, it is critical that operators, regulators, governments and other parties sharing de-identified personal information under a new HVNL for purposes such as improving compliance, enforcement and policy design, understand the challenges and limitations of de-identification, particularly in an open release context.

In OVIC’s experience, individuals and entities that lack an understanding of these challenges and limitations may fail to implement proper or adequate safeguards to protect the information under the belief that de-identification is ‘safe’. Where a new HVNL does facilitate the sharing of de-identified information, the NTC

⁸ Productivity Commission, *Data Availability and Use: Productivity Commission Inquiry Report, Overview and Recommendations*, No. 82, 31 March 2017, p. 12, available at <https://ovic.vic.gov.au/wp-content/uploads/2018/08/Submission-to-New-Data-Sharing-and-Release-Legislation-issues-paper.pdf>.

⁹ Ibid.

¹⁰ Refer to draft regulatory principle 4, page 40.

¹¹ Draft regulatory principle 4.

¹² On page 36.

¹³ See, for example, Office of the Australian Information Commissioner, *Publication of MBS/PBS data: Commissioner initiated investigation report*, March 2018, p. 4, available at: <https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/publication-of-mbs-pbs-data>.

¹⁴ See, for example, OVIC’s report *Protecting unit-record level personal information*, May 2018, available at <https://ovic.vic.gov.au/wp-content/uploads/2018/07/Protecting-unit-record-level-personal-information.pdf>.

may wish to consider whether it is appropriate for the updated legislation to include privacy-enhancing measures, such as requiring entities to adopt access controls or use secure research environments to provide an additional layer of protection, in addition to de-identifying personal information before it is used or shared.

Further, given public release of de-identified information may not always be a safe option – depending on the techniques used and the auxiliary information available, and inability to guarantee downstream uses of the de-identified information – OVIC suggests the NTC consider whether a new HVNL should limit data sharing of de-identified information to sharing between relevant or prescribed entities only, rather than also facilitating the release of de-identified information (particularly unit-level information) in an open context. Enabling sharing of de-identified data between authorised parties only, in controlled environments and with appropriate safeguards, would minimise the risk of re-identification. The ‘five safes’ framework for managing data risk is useful in those controlled environments, but it cannot be made to work effectively with unrestricted open data.

Use of technology and data to underpin compliance and enforcement

OVIC acknowledges that technology and data can play a valuable role in driving effective compliance and risk-based enforcement under the HVNL, as outlined in the paper. However, as noted in a previous submission to the NTC, the use of technologies that have the potential to collect or generate personal information, or be privacy invasive (for example, monitoring and distraction detection technologies), should be carefully considered, and where appropriate, privacy and security safeguards put in place to protect any personal and sensitive information that may be collected, used or disclosed.¹⁵

The data collection and management provisions in the current HVNL in relation to the Intelligent Access Program (IAP) serve as a good starting point or model for the use of technologies for regulatory purposes. As outlined in the paper, these provisions require data collected under the IAP to be necessary for the purpose for which it is collected, restrict how and when IAP information can be shared, and prescribe how information is to be collected, stored and destroyed, amongst other requirements.¹⁶

In principle, OVIC would welcome similar provisions for the generation, collection, handling, use and disclosure of personal information where technologies are involved for regulatory purposes; however, OVIC agrees with the recommendation noted in the paper that a technology-neutral approach should be adopted, rather than legislating for a particular technology.¹⁷ This is similar to the PDP Act, which adopts a technology-neutral and non-prescriptive approach to privacy regulation, allowing Victorian public sector organisations to apply the IPPs in a flexible way to suit their unique operating environment. Having separate standards for the management of personal information with respect to each specific technology that may be used for compliance or enforcement (or other regulatory purposes more broadly) would create an unnecessarily complex regulatory environment and could potentially cause confusion for entities, who would need to comply with potentially different standards for each different technology. Legislating for specific technologies would also likely not be feasible given the fast pace with which technologies are developed and adopted.

Thank you for the opportunity to engage with the NTC’s review of the HVNL, and to comment on this issues paper. OVIC continues to follow the progress of the HVNL review with interest, particularly in relation to the issues discussed in this paper. OVIC also looks forward to reading the final issues paper relating to this review, *Other policy matters*.

¹⁵ See OVIC’s *Submission in response to Effective Fatigue Management Issues Paper*, 16 August 2019, available at <https://ovic.vic.gov.au/privacy/submissions-and-reports/submissions/>.

¹⁶ On page 28.

¹⁷ On page 38.

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 me or my colleague Tricia Asibal, Policy Officer at tricia.asibal@ovic.vic.gov.au.

Yours sincerely 

Sven Bluemmel 
Information Commissioner

