



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: D19/940

16 August 2019

National Transport Commission
Public submission – Effective fatigue management
Level 3, 600 Bourke Street
Melbourne VIC 3000

Dear Heavy Vehicle National Law Review Team

Submission in response to Effective Fatigue Management Issues 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 *Effective fatigue management issues paper (the paper)*.

OVIC is the primary regulator for information privacy, information security, and freedom of information in Victoria. My office administers both the *Privacy and Data Protection Act 2014 (PDP Act)* and the *Freedom of Information Act 1982 (Vic)*. One of my functions under the PDP Act is to make public statements on matters that affect individuals' personal privacy. The relationship between technology and privacy in particular is of strong interest to OVIC.

This submission focuses on one particular theme we identified in the paper, namely the potential use of emerging and sophisticated technologies to improve fatigue management systems. A key point raised in this submission is that the public interest in using these technologies to improve road safety must be balanced against the public interest in protecting individuals' privacy.

Balancing public interests and community expectations

The paper provides two case studies of heavy vehicle operators using technology to manage fatigue risks – one system monitors drivers' alertness in real time through eye movements, using key facial features as reference points; and another system captures eyelid and head movements through motion-sensitive cameras.¹ Both case studies demonstrate the potential for monitoring and distraction detection technology to change unsafe driving behaviours, inform decisions about fatigue management policies, and improve road safety outcomes. The use of these technologies clearly has benefits, and as indicated in the paper, there is potential for their uptake to increase.

OVIC acknowledges that technology can play a significant role in effective fatigue management, and this should be reflected, and facilitated, in the new Heavy Vehicle National Law (**HVNL**). However, there is a need to ensure that the public interest in using these technologies to improve road safety is balanced against individuals' privacy rights. Monitoring and distraction detection technologies, such as those referenced in the abovementioned case studies, could potentially be considered privacy invasive given they

¹ Page 33 of the paper.

monitor and record drivers' physical and behavioural characteristics, and without the appropriate protections, the use of these technologies could potentially impact upon individuals' privacy.

User and community expectations therefore also need to be considered when developing a new HVNL that allows operators to 'use technology-based risk management systems that support their compliance'.² Although the use of such technologies may be enabled under legislation (be it the HVNL or other laws), this does not necessarily entail that individuals affected by these technologies (for example, drivers) will accept or be comfortable with it. Use of monitoring or detection technologies that does not align with user expectations can have an impact on trust between the operator and the user.

Further, the context in which these technologies is used should be taken into account. What is considered an acceptable or appropriate use of technology to monitor driver fatigue in one context may not be in another. For example, whether the use of a particular technology is acceptable or appropriate may depend on the distance travelled, similar to work diaries and record-keeping requirements, or the driving arrangement (solo drivers versus two-up drivers). OVIC encourages the NTC to take user expectations into account when designing fatigue management provisions in the new HVNL.

Function creep

The purpose for using monitoring and distraction detection technologies should be clearly defined to manage the risk of function creep, where the data collected or generated via such technologies (for example, the recorded footage) is used for other purposes beyond monitoring alertness or fatigue, that affected individuals would not have expected. OVIC considers that protections should be put in place to manage the risk of function creep, for example by establishing appropriate limitations around the access and use of this data (including by government organisations, such as law enforcement agencies).

Collection of personal and sensitive information

In certain circumstances, the use of technologies as part of an effective fatigue management system may attract obligations under the federal privacy law, the *Privacy Act 1988* (**Privacy Act**). Data collected, recorded, or generated from monitoring and distraction detection technologies may likely constitute personal information under the Privacy Act, and would therefore be subject to the Australian Privacy Principles (**APPs**). The APPs govern standards, rights and obligations relating to personal information, including its collection, use and disclosure. For example, the APPs impose requirements on organisations covered by the Privacy Act around how personal information is collected and used.³

There may also be potential for monitoring and distraction detection technologies to collect sensitive information under the Privacy Act. For example, if the scope of these technologies were expanded to verify drivers' identities using their biometric information (such as certain facial features captured via cameras, as described in the case study above), this could potentially involve the collection and use of sensitive information.⁴ In this instance, relevant provisions under the Privacy Act relating to sensitive information would apply, such as the need for individuals' consent (unless an exception applies),⁵ along with the corresponding requirements for this consent.

OVIC suggests that the NTC consider the potential for operators to collect personal and sensitive information via monitoring and distraction detection technologies, and whether the new HVNL should include additional protections around this type of information, particularly to address any inconsistencies in the applicability of privacy legislation (discussed below). For example, the NTC may wish to consider treating any personal information collected, recorded or generated from these technologies as sensitive

² Page 46 of the paper.

³ For more information, refer to the Office of the Australian Information Commissioner's *Australian Privacy Principles guidelines*, available at <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/>.

⁴ Under the Privacy Act, sensitive information includes 'biometric information that is to be used for the purpose of automated biometric verification or biometric identification', s 6(1).

⁵ APP 3.3, Schedule 1 of the Privacy Act.

information as best practice, which would afford it stronger protections under the Privacy Act and may better align with community expectations, given the nature of the information.

Interaction with privacy legislation

The interaction of the HVNL with privacy legislation, namely the Privacy Act, needs to be further considered when developing the new HVNL, especially given the potential for monitoring and distraction detection technologies to become more widespread amongst operators. This is particularly pertinent as the Privacy Act applies to private organisations with an annual turnover of more than \$3 million;⁶ instances may therefore arise where a small operator using such technologies may not be covered by the Privacy Act, compared to a larger operator similarly using these technologies that may be covered by the Act.

The application of the Privacy Act to heavy vehicle operators may therefore vary, resulting in inconsistent privacy protections in the collection, use and disclosure of data collected via monitoring and distraction detection technologies. OVIC therefore suggests the NTC consider this potential gap in the operation of privacy law when designing the new HVNL, and if appropriate, include safeguards to ensure operators using these technologies are subject to consistent obligations to protect individuals' privacy, regardless of whether the operator is covered by the Privacy Act or not.

Adopting a privacy enhancing approach

OVIC encourages an approach towards the development of a new HVNL that upholds human rights, including the right to privacy. For example, this could be achieved by promoting a Privacy by Design approach to ensure privacy is considered and built into the adoption and use of monitoring and distraction detection technologies.

A common way of operationalising a Privacy by Design approach is by conducting a privacy impact assessment (PIA), which is a useful process designed to assist organisations to analyse a program or project's impact on individuals' information privacy. Conducting a PIA would be beneficial for operators to identify potential privacy risks arising from the use of monitoring and distraction detection technologies, and develop risk mitigation strategies to address those risks.⁷ The new HVNL could encourage the use of PIAs, for example in regulations.

OVIC also encourages establishing appropriate limitations around the access and use of data collected and generated via these technologies. This includes potential access by third parties, such as government entities (for example, regulators and law enforcement agencies) or other private bodies such as insurers. Ensuring there is a consistent approach towards the collection and use of this data by third parties is important, given different privacy regimes may apply to those parties. For example, if a law enforcement agency in Victoria were to collect recorded footage from an operator, that footage would be afforded different privacy protections compared to that same footage being collected by another law enforcement agency in another state.

As noted earlier, establishing these limitations around data access and use can help to address the risk of function creep by ensuring the data collected and generated via these technologies is not used for purposes beyond those for which it was initially intended (with exceptions).

⁶ The APPs apply to APP entities (s 15 of the Privacy Act). 'APP entity' means an agency or organisation (s 6(1)) of the Privacy Act). Section 6C of the Privacy Act provides a definition of 'organisation'.

⁷ For more information about privacy impact assessments, refer to OVIC's template and accompanying guide, available at <https://ovic.vic.gov.au/privacy/for-agencies/privacy-impact-assessments/>.

Automated vehicles

The paper states the need to consider the potential of automated vehicles (AV) when drafting the new HVNL.⁸ In the NTC's previous discussion paper *Regulating government access to C-ITS and automated vehicle data*, the NTC noted that it 'considers that data produced by C-ITS and automated vehicle technology will most likely be personal information and sensitive information, especially where held by road agencies and law enforcement agencies'.⁹ OVIC suggests that the NTC again consider the potential for AVs – specifically in the heavy vehicle context – to generate data that could amount to, or reveal, personal information, whether as part of its review of the HVNL, or its broader reform program in relation to AVs.¹⁰

Thank you for the opportunity to comment on the issues paper. OVIC will continue to follow the progress of the HVNL review with interest, and we look forward to reading the remaining issues papers in relation to this review.

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

Yours sincerely



Sven Bluemmel
Information Commissioner

⁸ Page 46 of the paper.

⁹ Page 3 of the NTC's Discussion paper *Regulating government access to C-ITS and automated vehicle data*, September 2018.

¹⁰ See OVIC's *Submission in response to the Regulating Government Access to C-ITS and Automated Vehicle Data Discussion Paper*, available at <https://ovic.vic.gov.au/privacy/submissions-and-reports/submissions/>.