TECHNOLOGY AND THE HEAVY VEHICLE NATIONAL LAW

TCA SUBMISSION TO THE NTC'S HVNL REVIEW

NOVEMBER 2019

Contact

Transport Certification Australia
Level 6, 333 Queen Street
Melbourne VIC 3000

Phone: + 61 3 8601 4600
Email: tca@tca.gov.au
Website: www.tca.gov.au

TECHNOLOGY AND THE HEAVY VEHICLE NATIONAL LAW

TCA SUBMISSION TO THE NTC'S HVNL REVIEW

Transport Certification Australia Ltd
T: +61 3 8601 4600
E: tca@tca.gov.au
W: www.tca.gov.au

ABN 83 113 379 936

Document Details

Title:	Technology and the Heavy Vehicle National Law
Version	Final
Version Date	17 July 2019
Custodian	Gavin Hill, General Manager, Strategy and Delivery

Document History

Version	Date	Description and summary of changes
1.0	November 2019	Final version for submission

TCA page numbering convention: for ease of digital readability and referencing the cover is page 1.

Contents

Appendices

Executive Summary

Telematics and related intelligent technologies have, over the last decade, become an integral element of the heavy vehicle sector by supporting contemporary business approaches to achieve regulatory, productivity and safety outcomes.

The reliance on these technologies cannot be underestimated and, arguably, represents one of the most significant developments since the *Heavy Vehicle National Law Act 2012* (the HVNL) was first introduced.

The transformation has been so profound that some stakeholders within the heavy vehicle industry have made statements to TCA such as:

- "Telematics and data are now central to our business, and how we conform with the HVNL (and other laws)"
- "We've become so reliant on technology that we couldn't run our business without it"
- "Technology helps us deal with business and regulatory complexity"
- "With providers of systems and services now being such an embedded part of the transport and logistics chain, should they be assigned greater responsibilities in the law or be considered part of the chain of responsibility?"

These statements highlight the extent to which duty holders rely on technology and data to manage their conformance with the HVNL. However, technology providers are not captured within the HVNL. The HVNL could benefit from provisions that put positive obligations on technology providers to meet certain clear requirements to core duty holders in the chain of responsibility.

This creates an anomalous situation – with the exception of two particular use cases relating to the Intelligent Access Program (IAP) and the Electronic Work Diary (EWD) – the HVNL does not cover technology and data.

In an environment where the operation of heavy vehicles is being influenced by digital transformation, there is an opportunity to incorporate into the HVNL enabling provisions for technology and data which can:

- Define roles and responsibilities
- Ensure privacy-by-design
- Establish rights of consent, access to, and use of data
- Enable data to be fit-for-purpose for different requirements
- Enact appropriate assurance models
- Encourage data standardisation and interoperability.

A scenario from the not too distant future is presented in this paper (see Introduction) to both illustrate how reliant heavy vehicle operations are becoming on the effective use of technology and data, and also to illustrate the opportunities for further optimisation. The scenario is based on the use of an inter-connected framework which depends on business rules, definitions, defined roles, responsibilities and protections, data formats and other agreed elements to support the operation of inter-connected digital technologies and infrastructure.

Critical to these outcomes are the managed interactions and assurances (with clearly defined roles, responsibilities, accountabilities and rights) between the parties responsible for delivering accurate and reliable technology systems and services, which are demanded by parties in the supply chain.

This highlights the need for consistent legal provisions associated with the use of technology and data so that transport operators and other parties in the supply chain can meet their obligations under the HVNL and other related legislation (Workplace Health and Safety, privacy protection, surveillance devices, etc) in a digital environment.

Legislative considerations

Technology continues to develop rapidly and will continue to challenge the pace of legislative reforms. New technologies, business models and services are emerging. As far as possible, legislation should be agnostic of technology.

The HVNL should not prescribe specific technologies. Instead, it should enable technology to its fullest extent by incorporating provisions which:

- Provide opportunities for policy makers, program managers and duty holders to introduce innovative approaches to use technology and data to deliver upon the objects of the HVNL
- Offer consistency and certainty to all stakeholders in the use of technology and data in the heavy vehicle sector
- Can accommodate the disruptive influences of new technologies, market entrants and business models
- Define clear roles, responsibilities and accountabilities for technology providers in the context of the objects of the HVNL
- Enable the use of existing technologies by transport operators for regulatory purposes where appropriate.

These same principles should ideally be applied beyond the HVNL and be part of a regulatory approach for data that is consistent across all road vehicles, and across modes that may need to interact. There is a need for a single assurance framework comprising multiple assurance model, to support the use of telematics for different purposes and to optimise outcomes. The framework needs to be able to provide differing levels of assurance depending on the use case and application and be able to better support existing and emerging technology deployments where appropriate.

Part of this framework needs to include the clarification of roles and responsibilities for different entities, and a clear separation of duties between entities where appropriate. Telematics data collection, analysis, and assurance functions would benefit from being separated from regulators and policy makers to build in the mechanisms for trust between all entities in the data ecology. The National Telematics Framework in essence provides an ideal platform to support regulatory, policy and operational outcomes.

Introduction

It is evident that technology and data will play an increasingly important role in the future operation of Australia's supply chains – allowing Australia to meet its growing freight task more safely and efficiently.

Industry are increasingly reliant on technology and the intelligence provided by data systems. The reliance on these technologies cannot be underestimated and, arguably, represents one of the most significant developments since the HVNL was first implemented.

As an indication of the transformative nature of technology on the industry, some stakeholders within the heavy vehicle industry have made statements to TCA including:

- "Telematics is now central to our business, and how we conform with the law"
- "We've become so reliant on technology that we couldn't run our business without it"
- "Technology help us deal with business and regulatory complexity"
- "With providers of systems and services now being such an embedded part of the transport and logistics chain, should they be considered part of the chain-of-responsibility?"

Efficient, low cost sharing of data between large numbers of entities in a manner which benefits both private entities and the public good relies upon the use of a platform of business rules, data standards, definitions and other 'cyber-infrastructure' that are technology neutral but encourage interoperability of systems, technology and data.

TCA encourages this review to take a broad perspective and pursue a single coherent but flexible approach for the management and oversight of transport data and technology. This should also include access by government to data and requirements for compliance with national policy objectives surrounding procurement, policy and planning for technology. Some of the elements outlined in Chapter 7 of the HVNL are an appropriate starting point for regulating data and the entities involved in managing information collection, transmission and sharing (as outlined in appendix 1).

Data from a wide variety of connected transport systems will often exist as 'information streams' that interact with numerous devices, information systems and other data-streams and sources. This is particularly true when considering different policy areas included in the review of the HVNL. The privacy and security framework for connected information systems needs to support a holistic data architecture – from data generation through transfer, storage, sharing to use and potential destruction.

While the NTC's review is focused on the HVNL and therefore, heavy vehicles, the regulatory approach to data needs to be consistent across all road vehicles, and across modes that may need to interact.

The National Telematics Framework (NTF) evolved from the IAP operating model enshrined in the HVNL and includes the core elements of a platform. This includes a data dictionary, business rules for interaction, varying levels of assurance, agreements for participation and standardised data exchange formats.

Both through the work to co-design a best practice model for regulatory telematics, and through the review of the HVNL, TCA suggests consideration be given to the NTF and its components to be established in law. This will create certainty for investment in the technology sector, improve the resilience of the legislation over time, and avoids specifying particular programs or technologies.

TCA is currently implementing this approach through the delivery of the 16 initiatives approved in the 2018 business case to Ministers, *Enhancements to the Intelligent Access Program,* which expands the availability of applications and features with commensurate levels of assurance through the NTF platform.

This will drive efficiencies in systems and technology through the market, while also allowing flexibility in the level of assurance needed for data and supporting different approaches to using technology. Feedback from the telematics industry suggests that increased certainty of the NTF will improve consistency and drive increased confidence for them to invest in the market and develop innovative solutions.

This submission identifies opportunities for legislation to enable and support the adoption and use of technology for purposes that include, but are not limited to, enforcement and compliance.

The following scenario illustrates how digital transformation, coupled with enabling provisions in the HVNL, can lead to improved outcomes in the heavy vehicle sector.

Future-state scenario

The year is 2024, and the new HVNL has been enacted, enabling wide ranging technologies and changes to heavy vehicle access, accreditation and fatigue, and better supporting the use of fit-for-purpose data in improving efficiency and safety in heavy vehicle movements.

Leveraging technologies and digital business systems widely adopted across the heavy vehicle industry, transport operators and drivers now rely on in-vehicle systems and services offered by technology providers which contribute directly to the objectives of the HVNL to be achieved.

In this example, road managers, regulators, technology providers and other bodies worked together to establish a live, interactive permitting arrangement for restricted access vehicles. Using a combination of sensors and inputs, the vehicle's mass and configuration automatically determines allowable networks for each trip (with appropriate conditions) by interacting with on-line accessing systems to:

- provide turn-by-turn directions for drivers to achieve high levels of compliance
- allow certain larger vehicles to book routes (i.e. for Over Size, Over Mass movements)
- provide in-vehicle warnings about upcoming roadworks or restrictions such as speed or limitations on multiples vehicles crossing a bridge
- optimise journeys by accessing real-time information from on-road and off-road sources

The need for permits is significantly reduced, reducing waiting time for the vast majority of vehicles, with only highly specialised loads will need a permits officer to review the application.

Depending on conditions set by road managers or regulators, the vehicle's operator may share its data for aggregation with other vehicles, to assist road managers with road planning and forward investment decisions, or for regulatory compliance purposes.

Information sourced from off-road sources, such as ports, intermodal facilities or distribution centres is made available in a standardised way so that drivers receive real-time information. Real-time alerts may also communicate emergency events or upcoming road works, where alternate routes on permitted routes can be optimised.

Because of the flexibility provided through the law to manage driver fatigue, the driver is able to keep travelling without incurring a breach, and the fatigue monitoring technology can validate that the driver is not fatigued and is able to continue safely to their destination, in the event of an unexpected incident on their travel journey.

Combined with electronic systems to manage driver fatigue, the technology will identify suitable areas for the driver to rest and optimise the route and travel times to suit while providing greater flexibility on work and rest periods.

In order to secure that outcome, significant work is required. These outcomes are dependent on a complex interlay of operational, technical and data-driven activities. The HVNL should enable these outcomes by providing clarity and certainty to all parties involved in the provision of technology services which involve the use of data to and from vehicles.

Much of this work relates to data sharing. In TCA's experience, highly prescriptive requirements in law for the use of technology will be unsustainable when translated into practice for technology suppliers. This is also likely to slow investment in, and be a barrier to, adoption of innovation by technology providers.

The new HVNL should enable, but not prescribe, the use of technology to achieve the desired outcomes.

Within the current HVNL, Chapters 6 and 7 enable the use of telematics to demonstrate compliance with specific aspects of the law. However, beyond these specific aspects, the HVNL remains silent on the role of technologies, technology providers and the collection, transmission, storage and retention of data for other purposes which relate to the HVNL.

This is not breaking new ground. The HVNL already contains provisions for technology and data in Chapters 6 and 7. But these provisions do not extend more broadly to the use of technology and data for other purposes (despite the extensive use of data-collecting technologies across the heavy vehicle industry).

The review of the HVNL provides an opportunity to recognise the important roles responsibilities, and accountabilities of technology providers and data in achieving positive outcomes in line with the objectives of the HVNL.

Key Factors for Consideration

A consistent, harmonised and integrated policy and legislative approach is needed to accommodate the use of technology and data in the transport industry.

The HVNL should move beyond the current 'problem-specific' approach by creating a coherent, consistent approach to transport technology and its use across regulatory, commercial, safety and policy purposes.

TCA regards the establishing of a trusted ecosystem for data sharing essential to achieve the policy and other goals sought through the HVNL review. The key elements necessary for the wide-spread utilisation of an efficient, low cost, widely trusted technology platform include the factors below.

Clearly defining roles and responsibilities

Key points:

- Technology providers are now an embedded part of the heavy vehicle industry, and the broader logistics sector
- Trust in the data sharing framework requires protection of privacy beyond the privacy principles, and obligations for entities handling data
- The assignment of roles and responsibilities may be influenced by the levels of assurance sought by regulators and road managers as consumers of analysis, and the relationship with alternative assurance models for technology providers and transport operators
- Duty holders in the 'chain-of-responsibility' rely on the accuracy, reliability and services offered by technology providers to conform with the objects of the HVNL
- Duty holders under the chain of responsibility could also benefit from technology providers being given clearly defined roles, responsibilities and accountabilities within the HVNL
- Transport operators should be able to benefit from the sort of protections offered in Chapter 7 of the HVNL for other uses of technology.

Whether the purpose of technology is for the management (commercial- or regulatory-based compliance) of speed, fatigue, route, mass, vehicle dimension, maintenance, or driver readiness-for-duty, there needs to be clear definitions about the respective roles and responsibilities between:

- Data generators
  - Devices that generate data about vehicles, their surroundings, the behaviour of the driver, transport operator, or other duty holder. This data could be either private, personal or commercial in nature.
- Data collectors & transmitters
  - Technology providers should have obligations in terms of data requirements and levels of assurance, but this should be technology agnostic and based on the minimum necessary assurance to achieve the end purpose.
- Data stores and aggregators
  - Entities that manage raw data should have obligations to not reveal information that could potentially identify personal, private or commercially sensitive data.
- Consumers of analysis and reporting.
  - For the purposes of the HVNL, this is generally government agencies seeking insights or regulators performing compliance and enforcement.

In a similar way to the concept of 'chain-of-responsibility' in the HVNL, each of these parties perform specific roles in the management of data collected for the purposes of conformance with the HVNL.

Moreover, each of these entities are relied upon by duty holders to achieve the objectives of the HVNL (as illustrated in the case study below). The review provides an opportunity to establish provisions in the new HVNL which recognise the importance of these parties to other duty holders in the HVNL.

Clearly defining roles and responsibilities – Use case example:

John relies on his technology providers to conform with his responsibilities under the HVNL.

John benefits from the clarity the HVNL provides on the roles, responsibilities and accountabilities of technology providers because the HVNL contains provisions which include:

- Roles
- Responsibilities
- Obligations and procedures for transport operators and drivers
- Powers, duties and obligations of technology providers
- Models for achieving assurance appropriate for use that are clear and transparent, and that John can rely on.

The provisions mean that John obtains assurance that his technology provider understands their legal obligations under the HVNL and that the provision of those services is consistent with the objectives of the HVNL.

The responsibilities of John's technology providers extend to the management of privacy provisions (see 'Privacy-By-Design').

The HVNL already provides guidance on how to manage the roles, responsibilities, relationships and protections between these parties.

An area of particular complexity is the use of transport operator managed telematics monitoring devices and systems for regulatory purposes. TCA is working with road managers, transport operators and service providers in relation to the use of transport operator managed telematics systems for low level-of-assurance applications. There is the potential for this to be seen as a form of operator accreditation, which may need to be considered through the NTC's work on operator accreditation more broadly.

Creating and protecting clear duties and obligations with a separation of duties from policy makers and regulators for data collection and management to prevent inappropriate use of data for undisclosed purposes should be a key element of the future regulatory framework. Because of the current governance arrangements, strong communication and regulatory provisions such as Chapter 7 of the HVNL,

TCA is one of a small number of 'trusted entities' with whom transport and logistics companies are willingly share data on a voluntary basis. Trust in data sharing and de-identification is critical in the emerging cooperative transport ecology, and that trust should ideally be protected by more stringent obligations (and penalties) than the existing privacy principles in order to facilitate data sharing.

In terms of technology, TCA suggests identifying the characteristics of different entities (in a similar manner to the HVNL's treatment of the chain of responsibility entities) and setting appropriate responsibilities to reinforce the outcomes desired in terms of increased regulated and voluntary sharing of connected vehicle/device data.

As Illustrated in diagram 1, there are clusters of functions within a data transmission stream including data generation, collection, storage, analysis and reporting. One entity might occupy multiple functions and should therefore have all relevant duties. Additionally, some duties likely relate to the level of assurance or purpose of the data (for example privacy and security obligations should be commensurately higher for highly personal data compared to basic aggregated movement data).

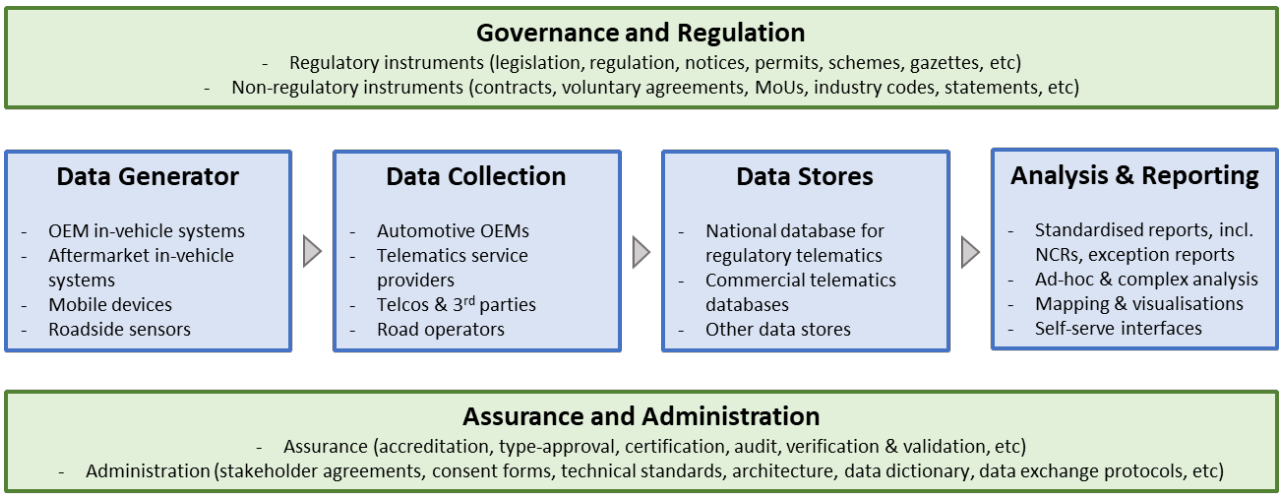

Diagram 1: Entities and roles in the transport data ecosystem

Regulatory instruments can not only establish obligations and rights for entities (such as those in the data chain) but can also establish bodies under legislation to perform certain duties. Examples of this currently in the HVNL include the National Heavy Vehicle Regulator administering the law for heavy vehicles, and TCA administering telematics assurance functions and applications.

Similarly, as illustrated in Diagram 1, it is important to have cross-cutting assurance and administrative functions along the entire data chain, based on the standards and framework necessary for efficient and secure data sharing. These include the common interoperability and standardisation requirements such as data formats, data dictionary, minimum data fields, optional data fields, functional and technology specifications for different levels of assurance, and international standards. For the NTF, these are agreed nationally, and administered by TCA.

Privacy-By-Design

Key points:

- Technology service providers are central to the collection, transmission, storage and protection of data
- The HVNL should incorporate strong privacy protection principles for the management of data collected from vehicles, as already offered in Chapter 7
- Privacy-by-design cannot be dealt with through a ‘one-size-fits-all’ approach, but a set of principles and safeguards which cater for:
  - different uses of technology for different purposes
  - different assurance models.

Privacy-by-design is a pre-requisite for any discussion about the collection, transmission, storage and use of data.

The original IAP model, developed in consultation with Privacy Commissioners, recognised that the use of data collected can be highly invasive, and that stronger safeguards than those incorporated into existing privacy frameworks were needed for the use of telematics.

The need for strong privacy protections were further reinforced when, during 2012, financial penalties were introduced into the HVNL for breaches of privacy in relation to the collection, access, use, protection and disclosure of data collected through the Intelligent Access Program (IAP). In 2014 TISOC agreed to these penalties being further increased (from $6,000 to $20,000), which is reflected in the current version of the HVNL.

Privacy-By-Design – Use case example:

Petra uses technologies to manage driver behaviour, and the management of fatigue. Petra's drivers have expectations that data about them is managed with an appropriate level of privacy and security and is not used in any way that could have an adverse effect on them.

Moreover, Petra and her drivers know that technology providers who are transmitting and storing private and sensitive information about individuals are bound by the obligations and privacy protections of the HVNL.

This means that all private and sensitive data collected is legally protected and the technology providers have a positive obligation to develop and offer services which reflect the law. TCA (as the data store and analysis provider for certain applications) also has obligations about the protection and use of data.

Stakeholders in the heavy vehicle sector continue to place an understandably high premium on privacy. They seek assurance that data collected is only for its intended purpose through consent mechanisms.

This is especially true for those at the upper end of the compliance pyramid (as illustrated in the diagram in the NTC's paper Efficient Enforcement). Operators who have decided consciously or unconsciously not to comply with the law, or who would rather not comply are likely to take steps to actively avoid monitoring. Anecdotally, this might include removing monitoring devices from vehicles, and could certainly include using older vehicles with no monitoring capabilities.

At the other end of the spectrum, operators that actively seek to comply are also generally utilising vehicle data to improve their operational performance and driver safety, and may be open to sharing data to better target strategic compliance efforts, improve planning and investment and benefit industry and the community.

Trust in data sharing and de-identification is critical in the emerging cooperative transport ecology. Learnings from the existing regulatory telematics environment highlight that this trust must be protected by more stringent obligations (and penalties) than the existing privacy principles.

The framework of roles outlined above, coupled with appropriate legislative obligations would protect the privacy of individuals and operators by only collecting and disclosing data for individual telematics applications in accordance with disclosed intended purposes. As an example of how this works currently, there are penalties in Chapter 7 of the HVNL which apply to TCA, service providers and governments for the misuse of data collected through the IAP.

As a result, the HVNL includes strict privacy management provisions on TCA and Service Providers, with financial penalties for breaches of these provisions. The review of the HVNL presents an opportunity to extend these provisions to other uses of technology, to provide safeguards for duty holders in the law.

Over time, demonstration of this framework has resulted in heightened trust and higher uptake.

This legislation necessarily goes far further than the privacy principles and enshrines specific legislative obligations (and penalties) on those who participate in the framework – primarily in relation to protection of data privacy, but also in reporting of tampering and other acts or omissions.

TCA regards the existing provisions in Chapter 7 of the HVNL as a starting point for a regulatory framework for protecting transmissible data, and the basis for the National Telematics Framework. This includes:

- Establishing the approval framework and body(ies) for technology
- Creating offences to discourage falsifying information or illegal release of information
- Requiring basic reporting of malfunctions and other critical events
- Protecting data collected under the schemes, especially where it could be considered personal
- Establishing the key allowable uses of information collected under the legislation.

The need for privacy-by-design is becoming more critical with the advent and use of technologies which are capable of collecting data about drivers and their attentiveness, fitness for duty and other potential measures in the future as technology advances.

Consideration needs to be given to appropriate regulatory, technical and operational safeguards are in place to give confidence to drivers that data being collected about them – by a third party technology providers and data consumers – is being managed in line with privacy principles, and the expectations of stakeholders.

Consideration should also be given to existing workplace surveillance laws, and the interplay between these laws and the HVNL.

Establish rights of consent, access to and use of data

Key points:

- The HVNL should provide clear provisions that government does not own private vehicle or driver data, and clarify the accountabilities associated with data (including its protection and disclosure) in what is an increasingly complex exchange of data from multiple origins to multiple destinations
- Data access and use conditions are currently addressed in Chapters 6 and 7 of the HVNL for specific uses of technology, but these do not extend more broadly to other technology uses which relate to conformance with the HVNL
- Potential ambiguities and conflicts associated with the use and management of data need to be contemplated.

Clarity of the rights of access to data is a necessary consideration for the HVNL, and links to the need for clear roles and responsibilities in the supply chain of technology and data collection, as well as privacy-by-design protections.

The HVNL already provides guidance in Chapters 6 and 7 over access rights to data from vehicles monitored under regulatory applications including clear obligations to only disclose data in compliance with the HVNL and other laws.

However, the rights to access and use data for other purposes – which is being collected for purposes to manage conformance with the HVNL, or for other commercial or private purposes – are not catered for in legislation.

Establish rights of consent, access and to and use of data – Use case example:

David's technology providers collect a lot of data from his vehicles and drivers. Data collected from David's vehicles and drivers has commercial value.

Although this data is captured, transmitted and stored by third party technology providers, David benefits from the clarity in the HVNL that establishes that his data cannot be used for purposes he hasn't consented to.

Transport operators and drivers benefit from unambiguous consent mechanisms that come from clearly defined data ownership and access rights provisions in law and a privacy-by-design data chain. This allows David to have certainty over the collection, use, and access of his data.

With the increasing reliance on third parties to provide technologies (which collect, transmit and store data), the HVNL needs to provide clarity to duty holders about the rights of access to data, as well as the storage, retention and destruction of data (which relates to the earlier section on roles and responsibilities).

The HVNL should also provide clarity to the technology sector, which is rapidly moving to an environment where data are being merged (even those within the confines of a vehicle) with other data, where amalgamated data are being created.

In this environment, tranches of data are being merged together and repurposed, which – without appropriate governance and regulatory safeguards – has the potential to expose transport operators and drivers.

Enable data to be fit-for-purpose for different requirements

Key points:

- Data from different sources will have different levels of accuracy and integrity
- Knowing the quality of your data is essential for duty holders and regulators to make appropriate decisions, commensurate with the level of assurance of the data chain
- The HVNL should provision for different levels of assurance based on the intended use of technology and data.

Telematics and connected vehicles generate and transmit data with varying levels of accuracy, tamper evidence, malfunction reporting and a wide variety of other factors. Where government seeks certain outcomes from the use of analytics based on telematics data, certain levels of assurance may be required to be established.

Different levels of assurance should drive appropriate levels of data quality, and the use of data for relevant purposes.

The HVNL already provides a framework for the provision of high-integrity data which can be used as prima-facie evidence (with certificate-based evidence) in Chapter 7. However, not all data collected from vehicles (or derived from other sources and used by technologies in vehicles) demands this level of assurance.

For instance, road managers across Australia are moving towards the use of data that can be used for policy and planning, and where necessary, for education and follow-up compliance activities. Data for this purpose does not demand the same levels of integrity or assurance as that is currently provided in the HVNL.

Nevertheless, the HVNL should incorporate provisions that enable different grades of data to be used commensurate with its intended use.

Enable data to be fit-for-purpose for different requirements – Use case example:

Sarah's transport operation relies heavily on data. Sarah's vehicles generate data and consume data from multiple sources.

Sarah has high expectations of the data collected from her vehicles. This is because she depends on the accuracy, integrity and reliability of data collected by her technology providers to conform with the HVNL.

Because Sarah demands high levels of assurance, she uses technology providers who are independently assured.

Sarah also relies on data from road managers, regulators, port operators and distribution centres to optimize journeys, by balancing productivity, travel times and fatigue management requirements.

Sarah knows that not all data is of equal quality. That is why she works with her technology providers to differentiate between data that is "advisory" in nature, and data which is "safety critical".

Sarah's drivers are better able to make informed decisions based on the journey information delivered through her technology provider.

Legislation should have the head of power to define levels of assurance (and assurance requirements) in subordinate instruments. This allows the development of a single coherent but flexible approach for the management and oversight of transport data and technology. The current levels of assurance under the NTF are outlined in the break-out box below.

What are the levels of assurance of the NTF?

Assurance Level 3: Applications at this level have the governance, oversight, system integrity and device reliability that creates the ability for TCA to issue a certificate of evidence for a court prosecution, that would stand alone as evidence of wrongdoing. These certificates of evidence can be challenged, but prosecutors are able to rely upon these certificates as prima facie evidence of the facts of the data. At level 3, TCA provides the assurance, certifying service providers, type-approving devices, auditing participants in the data supply chain, and oversighting and collecting the data for analysis.

Assurance level 2: Applications at this level have a lighter level of governance, auditing and oversight, but will generally use certified service providers and type-approved devices, so the quality of data remains robust – albeit without the certificate-based evidence offered by Assurance Level 3. TCA type-approves any devices sold by third parties for use at this level, but (depending upon road manager policies) there is the option for a transport operator to have their own commercial/operator system approved by TCA for use within a level 2 application. This introduces some complexities in governance and policy, as explored in the 'Can I be my own service provider' break out box.

Assurance level 1: Applications at this level are essentially self-assured. TCA will accept data from any enrolled participant, as long as the data conforms to basic data format and quality requirements. In general, applications at this level aim to collect large quantities of data from large numbers of vehicles, and this data would only be reported at an aggregated and de-identified level. Level 1 assurance applications aim to manage low level risks – where the task itself is largely unknown and vehicle movements across the network, at certain times of day, or across particular assets needs to be monitored, but the risk from individual vehicles is low and vehicles and operators do not need to be identified.

Establishing the ability to create different levels of assurance and requirements for determining fitness-for-purpose of data in law will create certainty for investment in the technology sector, improve the resilience of the legislation over time, and avoids specifying particular programs or technologies. This should be based on clear requirements such as (for example) type-approval of devices and or certification of systems to meet broad levels of assurance, rather than based on different requirements for specific applications, as illustrated below.

Appropriate assurance models

Key points:

- The HVNL should consider a single framework that supports multiple assurance models commensurate with the provision of technology services, and the intended use of data collected from those technologies
- Chapters 6 and 7 currently incorporate separate assurance models for technologies for specific uses in relation to the HVNL
- Different assurance models may be appropriate for different circumstances
- Assurance models may be linked to transport operators.

As outlined in the previous sections, assurance is key to providing data and analysis that is fit-for-purpose. Whether a road manager wants to know about general usage of the network, or a regulator is prosecuting an operator for regulatory breaches, data needs to meet the requirements of that use – and assurance is key to achieving that.

Assurance can be at different levels (as demonstrated in Break-out box 6 above) and can also be via different assurance models. TCA supports the new legislation providing a head of power for assurance at multiple levels, as well as through different models as appropriate.

Appropriate assurance models – Use case example:

Sharon has invested heavily in technologies over the last decade and they are an integral part of her accreditation.

Road managers and regulators have allowed the use of Sharon's technologies for higher productivity access and flexible future working arrangements because the technology meets the expected levels of assurance outlined in the legislation and supporting documents.

This is because Sharon's technology is managed through her accreditation and business systems in such a way that road managers and regulators derive the level of assurance required to offer higher productivity access arrangements.

In addition to different assurance levels, the NTF accommodates different assurance models depending on:

- Policy design and objectives
- Technical and operational risks
- Operating paradigms.

The nature of regulatory telematics applications is influenced by the interaction between a regulatory telematics application and an accompanying regulatory program. The distinction is important. A regulatory telematics application relates to the provision of telematics services by technology providers. A regulatory program relates to the legislative, policy and operational design of a government initiative (which may utilise telematics) to deliver a public outcome.

The form of a telematics application is therefore directly influenced by the needs of the government program. As a comparative example, the legislative, policy and operational design of the IAP access application (and for the corresponding arrangements within government of utilising intelligent access as a government policy/program) differs markedly from the policy and operational design of the Road Infrastructure Management program (and the corresponding policy/program to manage drivers from operating a vehicle when under the influence).

The HVNL already accommodates different assurance models – in this case for the IAP and Electronic Work Diaries (EWDs). The NTC's review of the Best Practice Model for Regulatory Telematics is expected to consider the appropriateness of multiple assurance models, and we encourage the HVNL review to include this consideration in legislative design.

Furthermore, beyond the realm of telematics, the HVNL also offers differentiated assurance models for the National Heavy Vehicle Accreditation Scheme (NHVAS) in what could be considered as a 'distributed' or 'federated' assurance model) and the Performance Based Standards (PBS) Scheme. The PBS Scheme is an example of a more centralised assurance model with only one approving authority.

As an example of how this might operate in practice, TCA currently provides services (through the NTF, but not under the HVNL) in assuring taxi cameras, alcohol interlock devices, bus routes and school bus contracts, and has developed a specification to support reform in the charging of vehicles for road use.

Another factor that should be considered, is whether the new law should recognise transport operator (industry-led) accreditation within the assurance framework. TCA suggests that other policy arenas have successfully utilised this approach through a head of power for recognition of standards and approval systems that meet the requirements of an accrediting or approving body. Again, these requirements should be driven and determined by the ultimate use of the application.

Can I be my own service provider?

Level 3 applications are based on a separation of responsibilities, whereby the person collecting data can't 'mark their own homework'. Under IAP at Level 3, a Service Provider may be required to testify in court to the robustness of their system during a prosecution against a transport operator (customer). Service providers are also required to undertake data analysis– comparing data received against conditions laid out by road managers to identify non-compliances. For certificate-level court evidence, it is likely inappropriate for a transport operator to be their own service provider. This is fundamentally a policy choice by road managers, and TCA has explored options for minimising this risk. TCA does not, however, recommend that transport operators with their own systems should be their own Service Provider at level 3.

In contrast, at level 1, we fully expect many participating transport operators to run their own systems (although many will purchase the service from a certified service provider). Data at this level is likely not evidentiary quality and will usually be associated with applications that only report aggregated and de-identified data. This data is useful because of the size and diversity of the data pool, rather than because of the quality of any particular data stream.

The current design of the level 2 applications assumes certified service providers and type-approved systems, but with the acceptance of other systems at the discretion of road managers (upon advice from TCA as to the compliance of any particular system).

This also allows drivers to move between different vehicles and transport operators fitted with fatigue monitoring systems so that data "follows the drivers" seamlessly.

Data standardisation and interoperability

Key points:

- Data standardisation and interoperability is essential for the adoption of technology, minimising effort and costs as well as the seamless connection of technologies
- The HVNL should ideally avoid any form of prescription in this area but could instead reference subordinate instruments to enable standardisation and interoperability which could evolve over time and respond to changes in technology and business models.

Through its administration of the NTF, TCA ensures regulatory telematics applications are standardised, harmonised, and interoperable across multiple legislative frameworks, policy areas and industry sectors (not just in relation to heavy vehicles or the HVNL). With the road and transport portfolio already well advanced in the use of telematics and related intelligent technologies to deliver public purpose outcomes, other portfolios across government can leverage the availability of an open technology market.

This platform approach enables a standardised approach to data collection, privacy management and security across policy areas and industry sectors and provides the assurance necessary for the technology market to develop (and support) technology applications for government initiatives and programs – irrespective of the portfolio area or industry sector from which telematics applications may emerge.

Data standardisation and interoperability – Use case example:

Gavin's transport operations depend on multiple technologies ranging from telematics devices embedded in vehicles, through to mass monitoring systems and nomadic fatigue management devices.

The new HVNL provides a head of power for an agreed set of data and data exchange requirements for technology providers offering technologies and services in the heavy vehicle industry. These become a common industry standard for services.

The HVNL's reference to agreed data definitions and exchange mechanisms benefits Gavin's transport business by allowing him to adopt new technologies as they become available without needing to incur unnecessary costs – or experience delays – by having to undertake technical integrations necessary to manage data formats and exchange arrangements.

The sharing mechanisms in portals or cloud-based networks are dependent on data standards and protocols so they can be shared effectively. Effort in standardising collection formats, definitions and data are in motion across national and international groupings. Work on creating data dictionaries to format transport data is being undertaken in USA, UK as well as in Australia.

Establishing an architecture for the data collection and dissemination is a vital role which tends to be adopted by governments across selected countries.

Interoperability is stressed in the formation of collaborative data portals within industry, for example: Architecture for European Logistics information Exchange (AEOLIX) formed in 2016 from a consortium of shippers, ports, technology companies, funded under the EU Horizon 2020 program, to provide a means to support data exchange between supply chain partners, without the need to develop multiple portals.

Technology such as telematics is used not just for compliance monitoring for trucks, but also across a range of regulatory and non-regulatory applications and across multiple transport modes. For a strong digital ecosystem to emerge, the data protection framework must simultaneously support service delivery, while also preventing the misuse of that data for inappropriate means, and work across artificial boundaries such as state borders and modes.

In terms of regulating for technology, it is also critical to ensure that the legislation supports uses which are both multi-modal and multi-vehicular (heavy and light, and both freight and passenger vehicles).

TCA supports increased national consistency between jurisdictions, by adopting the best elements of systems from across Australia. TCA regards the impact of inconsistent regulatory and policy approaches between jurisdictions to be a key factor in supressing industry investment in innovative technologies to improve safety, productivity and environmental impacts. In terms of the telematics industry, policy differences such as the adoption of regulatory telematics for different purposes has significantly hampered investment by fragmenting markets.

Emerging Technologies

While obvious, it cannot be overemphasised that technology is moving quickly.

Decisions are being made nationally and internationally that will significantly shape the future of technology, and potentially our transport system. The progressive shift to embedded and integrated telematics, cloud-based applications and services, automation and artificial intelligence , changes in business safety management systems, and increasingly ubiquitous sensory devices and data sharing (the ‘Internet of Things’) have the potential to rapidly change the efficiency, safety and governance of our transport system.

A new HVNL should be forward-looking, and to do so it needs to incorporate the concept of technology systems (rather than only devices or vehicles), multiple interacting entities with roles that may differ or overlap, and the ubiquity of personal data.

Technology can fundamentally transform the way regulation and compliance can be managed. For example, for decades, heavy vehicle driver fatigue laws have focused on long distance vehicles of over 12 tonnes, and compliance has been demonstrated through laborious recording of work and rest hours. Whether this has driven a change in the likely behaviour of drivers to lower their fatigue risk is debatable.

New technology offers the opportunity to detect the early signals of fatigue or its likely precursors. This in turn allows the development of risk-based legislation that regulates behaviour of drivers of any regulated vehicle (all vehicles over 4.5 tonnes, for example) who are impacted by fatigue. TCA has recently developed a specification and protocols for the sharing of fatigue-related data – opening the door for regulatory telematics-based systems to monitor, transmit and record the ‘fatigue risk status’ of a driver on the road.

Similarly, vehicle location has been monitored for years under certain regulatory applications, but now the mass, speed, time of day, time-on-task and other behaviours of vehicles and drivers can be quickly, cheaply and easily monitored and analysed – both in terms of individual vehicles, but more valuably, in terms of whole fleets of road users. This allows much greater utilisation of the network, and more importantly, increased road safety through reduced heavy vehicle journeys, as outlined in the case study below.

Policies to Extend the Life of Road Assets

Because of a historical lack of vehicle-specific data, road managers particularly have been forced to include significant safety margins in the design of roads and vulnerable assets such as bridges and culverts. The primacy of protection of public safety, and assurance of the lifespan of public assets has meant that, in the absence of accurate vehicle-based data, assets have been used to their full, safe capacity.

Australian standards for bridge assessment have recently been updated (AS 5100.7:2017) (SA, 2017). This revision incorporates the possibility to allow for increased flexibility and productivity for vehicles engaging in increased monitoring. The updated standard incorporates reduced traffic load factors for vehicles monitored through the IAP and On-Board Mass for the Ultimate Limit State (Koniditsiotis and Hill, 2018).

On-board mass monitoring, linked to regulatory telematics, can be a tool to support optimised infrastructure design and thus better 'sweat the asset', as well as being used for compliance and enforcement.

Other trends in telematics/technology include:

- telematics embedded in vehicles at factory fitment
- Extended Vehicle concept
- use of telematics in cyber physical systems (e.g. automated driving)
- over the air updates and machine learning
- a wide variety of fatigue and fitness for duty monitoring technology.

Proposed Legislative Design Principles

TCA notes that, in terms of a risk-based approach to regulatory design, technology can be a risk factor, a mitigating element, or part of the regulatory feedback loop that generates information for risk assessments.

The HVNL includes regulation for TCA and the IAP which includes a blend of both prescription and outcomes-based provisions, as well as semi-coregulatory elements (with TCA certifying private sector Service Providers to provide services for government schemes, in an open-market). The use of outcome and performance-based regulation for these sophisticated and highly changeable areas of the regulation is appropriate and supported by TCA.

TCA supports many of the principles outlined in the NTC issues papers. These regulatory design principles are fitting, particularly in terms of increasing the flexibility and variety of options for transport operators seeking to comply with the desired outcomes of the law.

As well as considering the above factors, TCA suggests the NTC consider the following legislative principles with regards to technology:

- **The law should be technology neutral, and support innovation and emerging technologies.**

  The law should enable and support adoption of new and emerging technologies for a range of purposes – not just hardwired to the Intelligent Access Program (IAP) and Electronic Work Diary (EWD).

- **Technologies and assurance requirements should be fit-for-purpose and should allow recognition of technologies already in use where appropriate.**

  Recognising technologies already used by transport operators where it is fit for purpose, with appropriate models of assurance is essential to boost the confidence that the use of technology enables compliance with the intent of the law. For circumstances where data is unlikely to be needed as prima facie evidence in a prosecution, lower levels of assurance are likely to be appropriate, with bring-your-own-device providing valuable 'big data' pools that are invaluable to planners and policy makers.

  The level of assurance for devices and systems should be matched to their ultimate use and may include assurance of devices (such as type-approval) and the robustness of back office systems (such as the current certification process).

- **Roles, rights and responsibilities for entities dealing with data should be clearly defined and key duties separated.**

  The data ecosystem is highly complex, but can be simplified into key roles, which should be paired to clear legislative obligations and rights where necessary. For lower assurance data, this should focus on data privacy rather than 'tamper-evidence', but the legislation should be clear about the responsibilities of entities for all levels of assurance and functions.

  Duties, responsibilities and rights of entities should be separate, to create a privacy-by-design ecosystem that encourages trust and supports increased data sharing and appropriate use. The NTF currently offers the building blocks to enable interoperable, efficient sharing, assurance and protection of data.

Conclusion

Telematics and related intelligent technologies are now a key part of the heavy vehicle regulatory framework, embedded in the majority of all vehicles. Transport operators now rely on technologies, and providers of technology to manage safety and compliance. The reliance on these technologies cannot be underestimated, and arguably represents one of the most significant developments in the decade since the HVNL was first implemented.

Although technology providers are not duty holders under the HVNL (and it is beyond TCA's remit to comment on policy in this area) it does highlight the need for assurance to be offered to transport operators and other parties in the supply chain in the use of technologies to meet their obligations under the HVNL and other related legislation (Workplace Health and Safety, privacy protection, surveillance devices, etc).

TCA proposes the following simple principles be included in the regulatory design of the entire new HVNL:

- **The law should be technology neutral, and support innovation and emerging technologies.**
- **Technologies and assurance requirements should be fit-for-purpose and should allow recognition of technologies already in use where appropriate.**
- **Roles, rights and responsibilities for entities dealing with data should be clearly defined and key duties separated.**

TCA is particularly keen to assist in the development of a robust and trusted data sharing ecosystem and framework that is flexible, efficient, market-based, and broadly used, by:

- Clearly defining roles and responsibilities
- Establishing privacy-by-design
- Establish rights of consent, access to, and use of data
- Enabling data to be fit-for-purpose for different requirements
- Enacting appropriate assurance models
- Encouraging data standardisation and interoperability.

There is a need for a single assurance framework comprising multiple assurance model, to support the use of telematics for different purposes and to optimise outcomes. The National Telematics Framework in essence provides a platform to support regulatory, policy and operational outcomes.

APPENDIX

Existing Provisions of The Heavy Vehicle National Law ACT 2012

The *Heavy Vehicle National Law Act 2012* (HVNL) already provides a fit-for-purpose approach to managing privacy and data management. The National Telematics Framework (NTF, which is based on the core elements of chapter 7 of the HVNL) is a platform-based approach to technology that is agnostic of policy content, technology provider or other market-restricting requirements. The NTF is based on this operating model and broader policy principles for telematics that have broadly been endorsed at the Chief Executive and Ministerial level. This is an example of a very effective broader regulatory framework if extended to other types of data and other entities, as outlined below.

Chapter 7 of the HVNL currently contains an end-to-end data protection framework, with explicit obligations, requirements and penalties for breaching these obligations on all parties in the data 'chain'. In addition to clear allocation of responsibilities between parties and substantial penalties for releasing information contrary to the legislative requirements, the legislation outlines the circumstances in which data may be used for research and public good purposes.

It is important to note that Chapter 7 of the HVNL contains provisions which relate to both the 'IAP application', and the 'IAP operating model' – which was subsequently renamed the National Telematics Framework, which houses multiple telematics applications. The change of naming convention was essential to avoid confusion between the 'IAP application' and the 'IAP operating model'. However, this was only a half-way house until such time as further structural changes to the legislation could be implemented to distinguish this separation, and de-couple the provisions relating to the IAP application from the National Telematics Framework (IAP operating model). This way, common privacy and data management provisions which apply to all telematics applications, could be progressed by the NTC.

Chapter 7 provides the highest level of privacy protections, in recognition that telematics applications have – by their very nature – the ability to compromise privacy principles without appropriate regulatory, technical, intuitional and operational safeguards.

For instance, Chapter 7 includes specific provisions and penalties which relate to privacy protection and data management, including the role and function of TCA as the national administrator of the National Telematics Framework. In this context, the role of TCA is a critical privacy protection safeguard for telematics applications administered through the National Telematics Framework.