EXPANDING ENFORCEMENT HORIZONS
Government access to heavy vehicle data – the privacy challenges of tomorrow and a legislative-framework solution

Graduate of the University of Melbourne, Australia, with a Bachelor of Arts and Bachelor of Laws. Previously advised the Australian Taxation Office, UK Department for Transport and the Victorian Department of Transport, with a background in the development of regulatory policy. Joined the National Transport Commission in 2012.

James Williams
Manager Policy (Compliance and Technology)
National Transport Commission
Melbourne, Australia
jwilliams@ntc.gov.au

Abstract

Intelligent transport systems (ITS) have the potential to improve heavy vehicle regulatory compliance and road safety, productivity and environmental outcomes, and to support cooperative approaches between carriers and regulators. Fundamental to ITS is the generation and exchange of data.

A growing policy challenge is the extent to which this valuable repository of information should be accessible for enforcement. The voluntary uptake of ITS is anticipated to be low unless there are clear privacy protections and certainty of treatment by public authorities.

This paper proposes a legislative-policy solution and articulates the Australian vision for a regulatory framework for heavy vehicle ITS. The framework is intended to recognize the higher probability of detection inherent in ITS from a natural justice perspective, while providing national policy certainty and utilizing international ITS standards to support manifold compliance and enforcement approaches.

Key Words: heavy vehicle, compliance and enforcement, intelligent transport system, ITS, privacy, Australia, Compliance Framework for Heavy Vehicle Telematics, ISO 15638.

1. Today's problem

In Australia, a number of measures, including fatigue and mass management and Chain of Responsibility obligations on third parties, have contributed to a reduction in crashes involving heavy vehicles.[1] This is echoed in road safety statistics where the road toll in a number of countries between the 1960s and the mid-2000s has reduced with a number of interventions including seat-belts and random breath testing. However, as these measures reach maximum effect, and traffic volumes increase, level or increased death and injury rates are forecast[2] without new or improved measures being introduced.

From an occupational perspective, truck driving in Australia is by some measures the most dangerous occupation. Between 2007 and 2012, transport- and storage-related fatalities equated to 11.41 fatalities per 100,000 workers – almost five times the national rate of 2.29 fatalities per 100,000.[3]

Recent crash causation analysis suggests that in the ten years to 2012, 37 per cent of fatalities involving a heavy vehicle were the fault of the heavy vehicle.[4] Fatigue, speed and unroadworthy vehicles are commonly referenced as causes of heavy vehicle crashes that are not the fault of a third party.[5] These are often the symptoms of underlying pressures and market demographics, including low barriers to entry and a highly competitive market.

Carriers have varied attitudes towards compliance, driver monitoring and the value of technology.[6] NTC research also indicates low levels of education amongst heavy vehicle drivers, with reported difficulties comprehending complex rules (such as fatigue).[7] Perceptions of inconsistent roadside enforcement can exacerbate disillusionment with the law and is a documented underlying contributory motivation for non-compliance amongst some drivers.[8] From an enforcement perspective, regulators seek improved levels of information to better distinguish safety and compliance levels and to better target enforcement. This in turn can improve industry perceptions of reasonableness and fairness.

The health impacts of a growing freight task[9] are exacerbated by increased urbanization adjacent to freight networks and high-density freight centers, such as port precincts.[10]

2. An ITS solution

Intelligent transport systems (ITS) typically comprise in-vehicle telematics, integrated in a system that captures, sends, stores and analyzes information electronically. The use of ITS varies from simple vehicle location information to advanced diagnostics and safety systems.[11] Developers are innovative and functionality has progressed from single-use devices to interactive and event-driven systems that are increasingly used to monitor, communicate, evaluate and respond to events, often in real time.[12] The market is also adapting to the development of tablets and smartphones, where a single platform may have multiple applications and be accessed on a range of devices. International standards are under

[1] A reduction in crashes has been observed with the introduction of the Heavy Vehicle National Law in 2008. See: NTC, *Heavy Vehicle Compliance Review* (2013), p. 37; BITRE (2011).
[2] BITRE (2014), p.3.
[3] Safe Work Australia, *Factsheet* (2014).
[4] Safe Work Australia (2014), p. vi.
[5] Safe Work Australia (2014); National Truck Accident Research Centre (2013).
[6] AMR (2013).
[7] The average education level attained by a heavy vehicle driver in Australia is between years 16 and 17; Australian Bureau of Statistics, *Job Outlook Information Sheet* (2012).
[8] NTC, Heavy Vehicle Compliance Review (2014).
[9] Department of Infrastructure and Regional Development (2014).
[10] Victorian Government (2013), p.27.
[11] AMR (2013).
[12] NTC, *Delivering a Compliance Framework for Heavy Vehicle Telematics* (2014), p.1.

development to ensure systems architecture and ITS applications are interoperable and minimum standards of security and integrity are identified.[13] In parallel to these developments, regulators are developing intelligent risk assessment and benchmarking tools with the aid of ITS technologies.[14]

This paper is focused on the *regulatory* purposes of ITS – including the improvement of safety compliance or network utilization. ITS, including cooperative ITS (C-ITS), provide opportunities to improve heavy vehicle operations and compliance, with subsequent safety, productivity and environmental benefits.[15] However it is recognized that the quantification of these benefits is dependent on application choices and business methods.[16]

Two Australian examples illustrate how ITS can transform the heavy vehicle regulatory environment. The first is the Intelligent Access Program (IAP) which employs Global Navigation Satellite System (GNSS) to track vehicles in real time. IAP is a route compliance tool used by governments to protect network assets. Carriers participate to take advantage of Higher Mass Limits (HML) or to operate over-dimensional vehicles. Access to IAP data is legislated, and IAP is overseen by a government-owned entity that certifies and audits IAP service providers. IAP altogether bypasses roadside intercept processes: regulators receive non-compliance reports if an IAP vehicle is off-route but do not otherwise have access to the database of vehicle activity (constituting a privacy-by-design approach), while IAP demonstrates to communities that heavy vehicles are route compliant. IAP thereby provides a tool to balance heavy vehicle productivity with increased urbanization and asset protection.

The Electronic Work Diary (EWD) provides the second example. Analogous to the Electronic Logging Device (ELD) in the United States, the EWD is a voluntary alternative to a paper-based work diary to document Hours of Service. To date, an EWD has not been approved, but in 2013 an operational pilot reported the EWD is technically feasible and recommended that the system should be modelled on ISO standards to ensure that the EWD firmware is compatible with other regulatory and commercial applications. The adoption of GNSS and a cloud-based Remote Connection Access Framework, whereby roadside enforcement or audit investigations can remotely access EWD records, was recommended.

Like the ELD, the EWD is anticipated to have a transformative impact on heavy vehicle operations. It offers an alternative form of record keeping, but also provides drivers, carriers and regulators with more accurate, current and accessible information and, in turn, can improve fatigue compliance though the integration of record keeping with driver warning and fatigue management tools. GNSS functionality ensures that vehicles and drivers can be tracked remotely, while records will generally reach service providers within 15 minutes, thereby sharply increasing data currency.[17]

3. Tomorrow's Problem

Common to these initiatives are data hungry systems and applications that rely on vehicle tracking and a form of electronic surveillance. Information flows between drivers, vehicles, carriers, service providers and regulators is vital to the emerging ITS regulatory paradigm. By necessity, the probability of detection greatly increases, and the accuracy, currency and availability of the data escalates exposure to prosecution. Furthermore, the opportunities for, and scale of, misuse of the data – including data matching multiple sources – also increases. Location information can be a very personal matter worthy of privacy protection – as the

[13] ISO 15638 – TARV (2013).
[14] Observe the development of wireless roadside inspections and Compliance Safety Accountability (CSA) program (FMCSA, USA).
[15] E.g. see Transport Certification Australia (2013).
[16] National Transport Commission, *Discussion Paper* (2013).
[17] Transport Certification Australia (2013).

location information of an individual can tell us about that person's political views, medical issues, and so forth.[18] ITS could also pin an individual to a time and place, with implications for criminal investigations. These scenarios are clearly a departure from the intentions of legislators and public authorities seeking heavy vehicle improvements.

The *perception* of misuse is itself a policy challenge: the European eCall initiative provides an example of the sensitivities of ITS, with the European Union publishing privacy factsheets to address concerns that the installation of eCall would result in the continuous tracking of people's location and the infringement of their private lives.[19]

To what extent are these issues dealt with by existing surveillance and privacy laws? The emergence of surveillance laws since the mid-1990s seek to prevent covert surveillance by governments, corporations or individuals, whether that surveillance is in the form of an image, audio or other form. However, surveillance laws do not generally apply if the subject consents to the surveillance, whether explicit or implied. Labor dynamics are expected to result in many drivers largely accepting electronic surveillance as a condition of employment, in which case the surveillance laws will not adequately address the data challenges.

Complementing surveillance laws are privacy laws that would ensure that individuals are notified of the collection of their personal information and the purposes for which the information is used, including third party disclosure.[20] However, most privacy regimes make exceptions for enforcement activities, and while many public authorities have internal policies to manage and protect personal information,[21] they primarily relate to data the organization is responsible for collecting and holding, while data held on other databases, such as ITS service provider platforms, falls through the information protection gap.

The proper use of ITS, and clarity of enforcement purposes, is important for three reasons: 1) ITS that do not meet minimum standards of performance and security could generate inaccurate data that, used as evidence, could result in a miscarriage of justice. 2) The increased transparency of behaviour is open to abuse by officials who have the tools to target individuals without justification, or to zealously pursue small or incidental breaches. 3) Without certainty, carriers and drivers are less likely to adopt innovative ITS technologies.

When regulatory regimes that use ITS emerge at different times, a patchwork of standards and rule-settings can develop. A fragmented approach could result in conflicting regulatory requirements, leading to duplicated data capture and multiple in-vehicle devices. ITS could also impact equality before the law, as regulatory applications must be price-competitive or the cost to comply will disproportionately impact smaller carriers.

4. A legislative-policy solution

To address these policy issues, public authorities in Australia are legislating regulatory access to ITS data in a number of areas, in combination with a Compliance Framework for Heavy Vehicle Telematics. The objective of the framework is to ensure that the collection or access of heavy vehicle data is transparent, reasonable and proportionate.

4.1 Legislative response

There are a number of precedents in Australia for limiting the access and use of transport-related data by legislation. IAP has legislated privacy protections[22] and in Victoria licencing

[18] Victorian Law Reform Commission (2010) p. 44.
[19] European Commission, *Factsheet* "eCall – Do you have any concerns for your privacy? You shouldn't ..." (2014).
[20] E.g. Privacy Act 1988 (C'wlth), Schedule 1.
[21] E.g. Commissioner for Law Enforcement Data Security, *Standards for Victoria Police Law Enforcement Data Security* (2014).
[22] Heavy Vehicle National Law 2012 (QLD), chapter 7.

and registration information can only be used for defined purposes under the Road Safety Act.[23] A number of tolling regimes also limit routine police access to data.[24] In these examples, public authorities must generally obtain a judicial warrant to access data for purposes not related to the primary function of the relevant legislation.

In circumstances where ITS cannot be anonymous, or where the personal identity of the subject is *reasonably identifiable*[25] – for example because a trusted source must be verified to ensure system security, or for billing purposes – legislative controls can provide invaluable certainty that personal information will not be routinely accessed or scanned for non-compliance with other laws. In 2014, Australia announced amendments to EWD legislation to replicate IAP to the extent that a judicial warrant will be required for purposes outside the Heavy Vehicle National Law (HVNL); and Australia has endorsed a similar approach for C-ITS in the event that the basic safety message of C-ITS cannot be anonymized. Legislative controls could also go further – for example, access to EWD data could be restricted to fatigue purposes rather than the broader HVNL.

Legislation has also limited enforcement access or use of data. In 2014, Australia endorsed an allowance for drivers who exceed Hours of Service by a small amount.[26] The approach recognizes that small breaches with nominal fatigue impact may occasionally occur in good faith, and under the amendment being currently drafted, drivers will not incur a Minor Risk Breach if work time is exceeded by up to eight minutes.[27] The eight minutes cannot be accumulated, making it impractical to schedule as additional work time, but it also conveys to industry that regulators are seeking to utilize EWDs to improve compliance and safety outcomes, not to target small breaches.

This is a innovative approach in Australia, where, with notable exceptions,[28] allowances are rarely published or legislated. The fatigue risk and operational effectiveness of the approach will therefore be reviewed after two years of initial uptake by industry.

4.2 Framework response

It is not feasible to legislate every data collection scenario. The general approach taken in Australia has been to place legislative limits on the access to data for purposes *outside* the relevant law, but to apply policies to govern access, use and disclosure of data for purposes *within* the relevant law.

Australia is therefore developing the Compliance Framework for Heavy Vehicle Telematics. To be finalized this year, the framework is widely supported by industry and will provide certainty in national enforcement policy. This approach departs from previous policy responses to technology developments, as it is intended to support multiple enforcement approaches across State regulators and police agencies, and is not application or technology specific. For example, the framework will be equally applicable to current regimes, such as EWDs and IAP, in addition to future regulatory areas, such as road pricing and intelligent risk classification systems. The framework will have three components: framework principles (**Appendix A**), a

[23] Road Safety Act 1986 (Vic); however, this is unique in Australia – most road agencies rely on generic privacy laws to regulate the access and management of licencing and registration data.
[24] E.g. Melbourne City Link Act 1995 (Vic); CityLink privacy code.
[25] Whether or not the data is "reasonably identifiable" is the threshold test in Australia's Privacy Act 1988 (C'wlth).
[26] National Transport Commission, EWD Final Policy Paper (2014).
[27] A driver who exceeds work time by 5 minutes in the first period of work may only exceed work time by up to 3 minutes for the rest of the 24-hour period, unless the driver makes up for the five minutes at a later time in that day. The quantum of 8 minutes is based on fatigue advice and seeks to ensure equity with drivers who use written record keeping methods and round work and rest time in 15 minute periods.
[28] E.g. the Road Safety Act 1986 (Vic), s 78, provides that Point-to-Point speed cameras that measure distance over time and are highly accurate must round speed down to the next whole number. This is a 1-2% allowance, comparative with 8 minutes in a 12 hour work day.

common dataset and a resource for regulators and industry to improve compliance and enforcement using ITS technology.

4.2.1 Framework principles

Adopting the framework, States with responsibility for road safety will be bound to framework principles to protect carriers and drivers from unreasonable or intrusive data collection. In addition, the framework will establish minimum standards for ITS when used for compliance or enforcement purposes.

One of the criticisms of ITS has been the steady and piecemeal growth in data collection without community consensus on the role of government and "big data." [29] In many respects, this remains an ongoing discussion and a principles approach has been adopted so that, as a minimum, government access to ITS data is transparent and accountable.

Privacy and protection of information: principles 1 to 4 will bind public authorities to privacy and information principles aligned with the Australian Privacy Principles.[30] This is a major step in Australia where enforcement activities are effectively exempt from privacy legislation. Today, enforcement agencies can collect, share and receive personal information without requiring the individual to be aware that this information is being collected or disclosed for enforcement purposes. Current practices are legal but hardly a meritorious or persuasive when governments are seeking to build a co-operative pact with industry to drive the voluntarily increase of ITS. Furthermore, it is arguable that mandatory ITS would only increase the importance of being transparent about enforcement activities using ITS data.

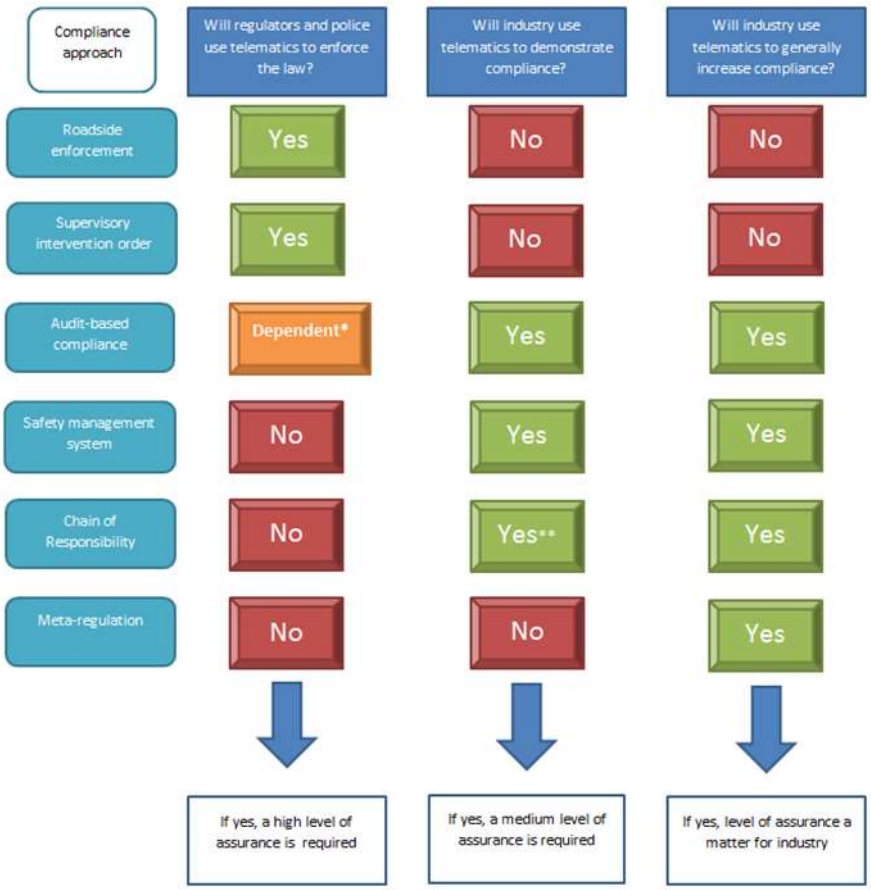
Compliance and enforcement: principles 5 to 7 consider the use of ITS in the context of compliance and enforcement. Under the framework, regulatory policies must not only be clear about the purpose for which ITS data is collected and used, but enforcement must be reasonable and proportionate. Concerns that enforcement will be neither reasonable or proportionate remains the greatest hurdle to uptake by carriers and drivers in Australia, particularly in relation to the treatment of small breaches. We saw in the earlier discussion that a key response has been the unprecedented decision to legislate an allowance in the law for EWDs – this approach is reinforced in the principles, which will have a much broader application and not be specific to EWDs or fatigue. It is critical that drivers are not unfairly targeted because they use regulatory ITS application, or that public authorities use ITS to focus on petty or small breaches. Rather, ITS should provide an increased evidence base to identify patterns of behaviours and to enable public authorities to develop intelligent, risk-based analyses and to target high levels of noncompliance. In turn, drivers and carriers will be able to demonstrate compliant behaviour, thereby increasing the incentive to use ITS by the way in which public authorities approach the technology for enforcement purposes.

Transparency is a common theme in the framework and is germane to the legislated eight minute allowance. Enforcement must not only be reasonable and proportionate, it must be *seen* to be the case. The framework therefore focuses on providing carriers and drivers with clarity of enforcement policy, including the treatment of small breaches.

Minimum standards: principle 8 of the framework has regard to minimum standards expected of ITS when used for regulatory purposes. The key test is: *will the ITS application be used for compliance, or enforcement, or for another purpose?* This question taps into an ongoing debate in Australia and elsewhere on whether carriers' systems and devices should be used for enforcement purposes. This remains an issue regardless of whether Australia adopts centralized and government-administered certification, or self-certification coupled with an audit regime

[29] NatRoad submission to the NTC Telematics Discussion paper (2013); available on the NTC website.
[30] Privacy Act 1988 – Schedule 1

(the preferred approach in the U.S.A. for the ELD[31]). On the one hand, carriers seek to optimize legacy systems that can integrate regulatory and commercial applications. Carriers are also concerned about additional costs to purchase and maintain regulatory ITS. On the other hand, public authorities are cautious of relying on data for evidentiary purposes that may not meet minimum standards of security, tamper-evidence and trust. The framework therefore differentiates ITS used for enforcement from ITS used to demonstrate or increase compliance, or for other commercial purposes. The minimum standards methodology is outlined in **Figure 1.**



* Level of assurance is dependent on extent to which audit-based schemes are subject to roadside enforcement.
** This is not an indication that telematics should be mandatory to meet Chain of Responsibility obligations. Telematics is only used to demonstrate legal compliance under Chain of Responsibility if parties in the chain choose to adopt telematics.

Figure 1. Methodology to determine the assurance required of an ITS application[32]

The methodology aims to ensure public authorities only set minimum standards for a high level of assurance when they have an enforcement stake in the data. The level of confidence required in the performance of the system is dependent on the requirements of policy and the compliance or enforcement approach taken, rather than the application:

- *Will the data be used by regulators and enforcement agencies to enforce the law?* If so, governments should seek a *high level* of assurance. This could require a regulatory approvals process (such as EWD) or certification (such as IAP).
- *Will the data be used by industry to demonstrate legal compliance?* If so, governments should seek a *medium level* of assurance. This could require common standards to be

[31] United States Department of Transportation, *Electronic Logging Devices and Hours of Service Supporting Documents* (2014).
[32] National Transport Commission, Discussion Paper (2013).

adopted with increased penalties for non-conformance, increased system auditing, third-party record keeping or a reverse onus of proof.

- *Will the data only be used by industry to generally increase compliance levels?* If so, the level of assurance is a matter for industry.

Other compliance approaches, including Chain of Responsibility and voluntary industry schemes, are not focused on infringements or other forms of enforcement and do not have the same prosecutorial emphasis. When regulators shift from roadside enforcement to carriers and other parties demonstrating their compliance (e.g. through audit-based schemes) the evidentiary dynamic naturally shifts as these parties take on greater responsibility to demonstrate their compliance. It becomes less incumbent upon regulators to ensure a minimum evidentiary standard is met.

At the heart of this approach, a higher system standard is warranted when ITS is explicitly used for enforcement – notably roadside enforcement where fines are issued based on the evidence before the Authorized Officer – because if the system was not of sufficient quality, this could result in incorrectly identified breaches and the miscarriage of justice. Establishing higher minimum standards also increases certainty within the judicial process.

Net efficiencies: principle 9 relates to regulatory efficiencies. ITS policies should aim to ensure net safety and efficiency outcomes for both industry and the community. The work of the NTC further identified that regulatory applications could generate very high returns if used to underpin intelligent, risk-based targeting of high noncompliance and rebalancing roadside enforcement and audit-based compliance approaches.

Application of the principles: principle 10 of the framework seeks to ensure that the principles will be consistently applied to future regulatory policies and programs. Initial analysis indicates that IAP, the only regulatory application using ITS in Australia today, has legislation, processes and policies that are consistent with the framework.

4.2.2 Common data set

Over the last decade, telematics has shifted from proprietary, single-purpose devices, such as the digital tachograph, towards dynamic, multi-purpose and open standards platform-based ITS that use remote and cloud technology. In consultations with industry, the NTC has identified that there is likely to be an ongoing need for basic, stand-alone ITS solutions that only perform a core regulatory function, particularly for those carriers that are owner-drivers or have fleets with small vehicles numbers and therefore do not have, or do not perceive to have, operational requirements that would benefit from integrated systems. Nonetheless, a growing carrier market is anticipated to benefit from the adoption by governments of a *common dataset* that enables the generation of data from a single unit to be used for both commercial and regulatory purposes. This could reduce carrier costs while providing the tools to improve operational efficiency and compliance. The integration of electronic record keeping, for example, has the potential to improve compliance with work and rest hours, and enable "regulatory time" to be dynamically aligned with real-time driving schedules.

A market-driven approach has been adopted in a number of instances by governments looking to service providers and innovators to develop solutions.[33] The framework applies international standards, notably 15638:2013 *Intelligent transport systems - Framework for collaborative Telematics Applications for Regulated Commercial Freight Vehicles* (TARV), to ensure that a common platform can host regulatory and commercial applications. **Figure 2** illustrates how

[33] E.g. Transport Certification Australia (2013) and United States Department of Transportation, *Electronic Logging Devices and Hours of Service Supporting Documents* (2014).

common data from a single system can be used for different regulatory and commercial purposes.

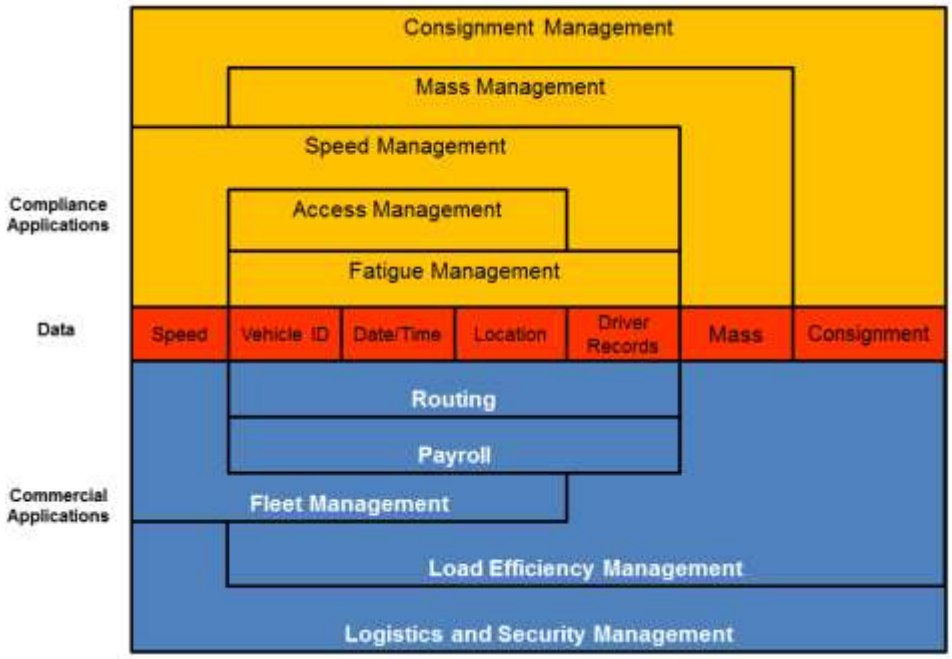


Figure 2: Typical data elements by heavy vehicle application[34]

Following this approach, location data only needs to be collected once, but can be used by the carrier to improve commercial outputs (such as routing and fleet management) and to increase compliance (such as network access management).

TARV utilizes system providers to hold the data (not public authorities), a wireless interface and remote connection access. Australia supports international standards such as TARV, and the framework is an opportunity to incorporate the TARV model into future policies and programs. IAP, for example, provides network managers with non-compliance reports if a carrier's HML vehicle drives off the agreed route – but agencies do not have access to the database of vehicle movements and cannot analyse the data for breaches of other laws.

One of the benefits of TARV as an ISO standard is the structured process to ensure development, maintenance and harmonization with other standards. Further, to facilitate interoperability, Transport Certification Australia (TCA) is working with the NTC to develop a data dictionary as a key component of the common dataset.[35] The data dictionary will assist in the exchange of information across systems by standardizing data types (such as numeric, text or binary data). Each system may implement its own method of data management, provided that the interface adheres to the agreed definitions. Common data dictionary interfaces include the vehicle identification number, time stamping and location (latitude, longitude and altitude).

Importantly, the adoption of TARV and an integrated approach to regulatory and commercial applications does not mean that public authorities can access all the data generated by an integrated system. Indeed, adopting a privacy-by-design approach, data interfaces can be siloed so that public authorities can only access data that is relevant to the enforcement task. This

[34] National Transport Commission, Telematics Final Policy Paper (2014); courtesy of Transport Certification Australia.
[35] Transport Certification Australia, "TCA to develop telematics data dictionary" *Media Release* (2014).

approach explicitly enables invaluable aggregation of anonymized data for planning and investment purposes.

4.2.3 Guidance for enforcement agencies and regulators

Section 2 identified opportunities to improve compliance and enforcement outcomes with ITS solutions. ITS have the potential to underpin improved roadside enforcement and alternative approaches to traditional forms of enforcement, including audit-based compliance and safety management system approaches. In Australia, with the introduction of Chain of Responsibility obligations for other parties in the transport chain that impact the actions of carriers and drivers, ITS can also provide information to help parties demonstrate reasonable steps were taken to meet their legal duties. Further, there are opportunities to utilize ITS data to better evaluate non-compliance in the context of carrier operations and normative behaviours. An example of a responsive approach to compliance can be seen in the sophisticated comparative analysis of driver and carrier behaviour in the United States, with the development of intelligent profiling, industry benchmarking and risk assessment, notably with the development of Wireless Roadside Inspection (WRI) and the Compliance Safety Accountability program overseen by the United States Department of Transportation.

Given that the road freight task continues to increase as traditional enforcement resources decline,[36] the framework will provide guidance to facilitate better use of ITS solutions to improve responsive regulation, audit-based schemes, safety management systems, Chain of Responsibility and industry-led and operated schemes that increase compliance above minimum regulatory requirements.

ITS opportunities should also be recognized in targeted policies and programs. For example, as regulators develop and introduce guidelines to carriers and other organizations on how to manage Chain of Responsibility obligations, or as pre-exiting programs such as accreditation schemes are renewed, the identification and promotion of ITS solutions will be critical.

5. Conclusion

Jurisdictions can proactively recognize and respond to the compliance and enforcement opportunities and privacy challenges of harnessing ITS to improve heavy vehicle operations. The optimum approach depends on existing legislation and policy factors, including whether applications are voluntary or mandatory, and the driving issues for key stakeholders.

A clear legislative-policy framework may underpin transparent, reasonable and proportionate access to ITS data: this approach does not have to limit or frustrate enforcement activities, but, in a cooperative approach with industry, can ensure certainty of enforcement and "no surprises" for carriers and drivers. The process of consultation and developing a policy framework is also an opportunity for the community to explore and debate what level of government access to industry data it deems to be reasonable, and in what circumstances.

[36] National Transport Commission, *Heavy Vehicle Compliance Review* (2013), p. 38.

References

AMR, *Reform Evaluation in the Road Transport Industry, 2012: Compliance and Enforcement, and Speed* (2013).

Bureau of Infrastructure, Transport and Regional Economics, *Fatal Road Crashes in Australia in the 1990s and 2000s: Crash Types and Major Factors*, Information Sheet 41 (2011).

Bureau of Infrastructure, Transport and Regional Economics, *Road Safety: Modelling a Global Phenomenon*, Research Report 141 (2014).

Department of Infrastructure and Regional Development, *Trends: Infrastructure and Transport to 2030* (2014).

ISO 15638-5, *Intelligent Transport Systems – Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV) – Part 5: Generic Vehicle Information* (2012).

ISO 15638-6, *Intelligent Transport Systems – Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV) – Part 5: Regulated applications* (2013).

ISO 15638-7, *Intelligent Transport Systems – Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV) – Part 5: Other applications* (2012).

National Transport Commission, *Cooperative Intelligent Transport Systems: Final Policy Paper* (2013).

National Transport Commission, *Cooperative ITS Regulatory Policy Issues* (2012).

National Transport Commission, *Delivering a Compliance Framework for Heavy Vehicle Telematics: Final Policy Paper* (2014).

National Transport Commission, *Developing a Compliance Framework for Heavy Vehicle Telematics: Discussion Paper* (2013).

National Transport Commission, *Electronic Work Diaries: Final Policy Paper* (2014).

National Transport Commission, *Heavy Vehicle Compliance Review: Consultation Draft* (2014).

National Transport Commission, *Preparing Australia for Electronic Work Diaries: Regulatory Issues Paper* (2013).

National Truck Accident Research Centre, *Major Accident Investigation Report* (2013).

Transport Certification Australia, *Final Report: Operational Pilot of Electronic Work Diaries and Speed Monitoring Systems* (2013).

Safe Work Australia, *Work-related fatalities involving trucks, Australia, 2003 to 2012* (2014).

Victorian Government, *Victoria the Freight State: The Victorian Freight and Logistics Plan* (2013).

Victorian Law Reform Commission, *Surveillance in Public Places Report* (2010).

Appendix A: Compliance & Enforcement Framework for Heavy Vehicle Telematics: Framework Principles

Principle 1: The access and use of telematics information must be consistent with Australia's international human rights obligations: public authorities must not apply or enforce laws, policies or programs in a discriminatory or arbitrary manner, and no one must be subjected to arbitrary or unlawful interference with his or her privacy.

Principle 2: When accessing telematics information for compliance and enforcement purposes, public authorities must be bound by privacy and information principles that are consistent with the Australian Privacy Principles – these principles should allow the aggregation of de-identified telematics data for research and planning purposes.

Principle 3: Information derived from telematics systems must only be accessed by public authorities for the regulatory purposes for which they were intended. For example, a telematics system installed only to meet regulatory requirements under the Heavy Vehicle National Law must not be accessed for any other regulatory, enforcement or investigatory purpose unless a court-issued warrant is obtained.

Principle 4: Each regulatory application must clearly identify to the user which organisation has responsibility for personal information generated by the telematics system, and which organisations may access or hold personal information derived from the telematics system.

Compliance and enforcement principles

Principle 5: Each regulatory application must set out:

- the purposes for which information will be collected
- which data will be accessed for these purposes
- the conditions under which this information will be sought.

Principle 6: Public authorities that use telematics information for a regulatory purpose must develop and implement policies based on reasonable and proportionate enforcement. The treatment of telematics information should have regard to patterns of behaviour and the higher probability of detection.

Principle 7: Enforcement polices in relation to the use of telematics information should be publicly released where it is appropriate to do so, and when the release of the enforcement policy does not pose a risk to the integrity of enforcement or regulatory policy.

Minimum standards of telematics

Principle 8: The performance standard of telematics used for regulatory purposes is a policy decision to be guided by the objectives of the regulatory application under consideration. Where possible, standards should support interoperability and facilitate multiple commercial and compliance applications. Telematics used for enforcement must meet evidentiary requirements.

Regulatory efficiencies

Principle 9: The use of telematics to improve compliance should aim, where possible, to ensure greater safety and efficiency for industry and public authorities.

Application of these principles

Principle 10: These principles should be consistently applied by public authorities across all participating jurisdictions. Public authorities should demonstrate and communicate to stakeholders why a departure from the framework principles is warranted.