26th Australasian Transport Research Forum
Wellington New Zealand
1-3 October 2003

The Elements of a Robust Electronic Compliance Monitoring System for Heavy Vehicles

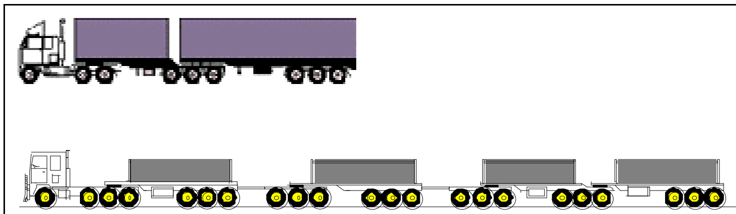
G Taylor
Queensland Department of Main Roads, Australia

J Opiola
Hyder Consulting, UK

1. INTRODUCTION

Like elsewhere in the world, Australian transport agencies[1] face a growing pressure to manage the access of heavy vehicles to the road network. Given that 96% of all road freight movements in Australia are carried by heavy vehicles [1], the forecast that road freight movements will almost double by 2022 [2] will see this pressure remain for the foreseeable future.

To manage this pressure Australian transport agencies have allowed the transport industry to operate more efficient, specialised, multi-combination vehicles (see Figure 1).



9 Axle B-Double: 25 m long max, mass 62.5 tonnes (68 tonnes with road-friendly suspension)

AAB Quad: 53.5 m long, mass 146.7 tonnes

Figure 1: Examples of Multi-combination Vehicles

This specialising of the road freight task has now reached such an extent in Australia that a project is underway to develop and introduce new national regulations for heavy vehicles based on key performance criteria for vehicles, road safety and the road system, with a view to augmenting current prescriptive-based regulations [3]. The aim of this work is to provide a nationally consistent means for industry to develop and introduce specialised heavy vehicles.

When operated as intended, these specialised multi-combination vehicles pose no more of a threat to roads, bridges and other road users than "normal" heavy vehicles. However, when these they operate "outside the envelope" (eg. travel at too high a speed, on the wrong route, or in the wrong traffic conditions) they can pose a much greater risk. To manage this risk, transport agencies impose operating conditions on these vehicles – restricting where, when and how they can operate.

[1] The term "transport agency" is used here in a specific sense, referring to agencies with road infrastructure and/or road transport regulatory responsibilities.

2. EXISTING COMPLIANCE ASSURANCE MECHANISMS

The traditional front-line tool used by transport agencies to ensure heavy vehicles comply with their operating conditions is on-road enforcement – which, in the main, means transport inspectors, though devices such as speed and red-light cameras play a role. Transport agencies have become increasing sophisticated in the deployment on transport inspectors in recent years:

- Drawing on weigh-in-motion (WiM) real-time and trend data, and other intelligence sources, to better target the time and place of heavy vehicle interceptions; and
- Equipping vehicles with portable computers and wireless data communications to enable access to registration systems and other compliance-oriented databases.

However, for all this sophistication, this on-road enforcement task is predominantly a sampling process – where a heavy vehicle (out of the thousands on the road) is intercepted at a certain time and day (out of all the hours in the week the vehicle is on the road), at a certain point on the road network (out of the tens of thousands of kilometres of road network) – dependent upon how the transport inspector is deployed. This fact tends to constrain the overall success of on-road enforcement as a deterrent to illegal behaviour. This fact is illustrated in Table 1, below.

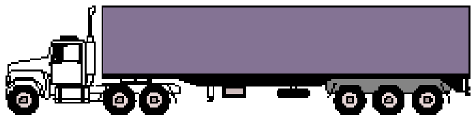
This table compares the estimated monthly level of heavy vehicle overloading in the state of Queensland (Australia) between July and December 2001 with the actual number of reported infringements for the same period [4]. Column (a) presents the total estimated number of illegal overloading events (or trips) by region, based on WiM data. Column (b) presents the estimated number of significant illegal overloading events (heavy vehicles more than 20% over the legal mass limit) by region, based on the same WiM data. Column (c) presents the total number of reported heavy vehicle infringements (caught by on-road enforcement) as a percentage of column (a). Column (d) presents the number of reported heavy vehicle infringements more than 20% over the legal mass limit as a percentage of column (b).

	(a)	(b)	(c)	(d)
Region of Queensland	**Total per month**		**Percent caught**	**Percent caught more than 20% over**
	Over legal limit	**More than 20% over legal limit**		
Northern	4,260	120	1.00%	3.00%
Central	9,240	690	0.30%	0.70%
Southern	14,100	450	0.30%	0.90%
South-east	72,300	4,110	0.10%	0.12%
	99,900	5,370		

Table 1: Probability of Catching Overloaded Vehicles by Queensland Region, Jul to Dec 2001

As can be seen from column (c), on-road enforcement is catching between 'one in 100' and 'one in 1,000' illegal events. For significantly overloaded vehicles, the figures are a little better – column (d) – with on-road enforcement catching between 'three in 100' and 'three in 2,500' events.

As the percentage of specialised heavy vehicles in the vehicle fleet grows, the ability of on-road enforcement to maintain even theses figures will be under pressure. Unlike the standard Semi-trailer (see Figure 2), these specialised heavy vehicles do not operate under general access conditions – that is, they are not allowed on all public roads at any time.



6 Axle Semi-trailer: 19 m long max, mass 42.5 tonnes (45.5 tonnes with road-friendly suspension)

Figure 2: The standard 6-axle Semi-trailer, Australia's largest general access vehicle

This means that the transport inspector, having stopped and checked one of these specialised heavy vehicles, will not be able to assume that the vehicle's compliance with operating conditions has been the same over its entire trip. The simplest way of explaining this is to consider the question, "Having stopped a heavy vehicle that is route restricted at a point on that route, how does a transport inspector know that the vehicle has abided with its route restriction for its entire trip?" The only way our inspector can know this is to follow the vehicle – something that cannot be done with every one of the hundreds of specialised heavy vehicles that operate on the road every day.

This route restricted vehicle scenario becomes even more complex when time and mass restrictions are added to the mix. So it is becoming clear that the current sampling approach of on-road enforcement will not keep pace with the increasing complexity these specialised heavy vehicles bring to the transport task – a 'sharper' (more precise, smarter) tool is needed to better ensure these vehicles comply with their operating restrictions.

A scan of the activities of overseas transport agencies shows that there is a definite move towards implementing systems that automatically monitor the movement of individual heavy vehicles. In the USA, this implementation is focusing on linking that nation's extensive network of weigh-stations with heavy vehicles via dedicated short-range communication (DSRC) systems [5]. In Europe, work is progressing on both DSRC-based systems [6] and Global Positioning System (GPS) based systems [7].

It is this work on GPS-based systems that has fuelled a lot of interest in Australia – given its large physical area, its relatively low population density, and the fact that most of its 'vulnerable' road network (thin pavements, narrow carriageway, etc) is in quite remote areas where routine enforcement is most difficult. This interest has lead to a national project to explore the feasibility of introducing a national electronic compliance-monitoring (or e-compliance) regime for heavy vehicles based on this technology [8].

3. WHAT MATTERS IN ASSURING COMPLIANCE

In the development of any system, an articulation of its objectives is a key first step towards ensuring the system delivers what is required. For an electronic compliance monitoring (ECM) system, the obvious primary objective is the supply of evidence of compliance. If the system design were to take exception reporting rather than a continuous reporting approach, this objective would be better re-expressed as "looking for evidence of non-compliance". An example of this approach is red-light camera systems – they are designed to capture the exception (the vehicle running the red light) not the norm (all the vehicles that stop when they should).

However, as experience with some other compliance monitoring schemes has demonstrated, safeguarding this evidence is not a trivial task. The introduction of tachographs in Europe has been accompanied by tampering to modify the data they record [9]. Australia has had similar experience with the introduction of speed limiters on heavy vehicles – recent articles on national television have demonstrated that they are open to tampering, and that the temptation to do so is quite real. It is acknowledged this Australian example is not compliance monitoring per se, but it demonstrates the universal problem of operator interference with devices that attempt to modify behaviour.

This leads to the realisation that non-compliance evidence must be delivered to the transport agency in a robust secure manner. From a technical perspective, this has two dimensions (the latter being the dominant):

- Ensuring the integrity of the equipment used (on-vehicle and elsewhere); and
- Ensuring the compliance data delivered to the transport agency is, as far as possible, irrefutable.

These dimensions cover a wide range of issues that will not be explored in great detail in this paper for the sake of brevity. However, by way of example, they include data security and audit trails in each step of the data's flow from the vehicle to the transport agency; and the task of managing vehicle, and even driver, identity. It must be emphasised that all the issues to do with integrity (of equipment) and irrefutability (of data) are best dealt with from a systemic viewpoint – with all the elements of the ECM system working together to ensure these two dimensions are adequately covered.

A commonly explored second-order requirement (objective) in the development of a system is ensuring it is as future-proof as practical. This would typically cover issues such as:

- Interoperability and the selection and use of open standards; and
- Ensuring the system had the capability and flexibility to add additional features and/or new services in the future with as little effort as possible.

With an ECM system, the issue of interoperability will become quite significant as the number of heavy vehicles using the system grows. This is because governments have an interest, especially in regulated markets, in minimising the potential for monopolistic practices by private sector product and service providers. To achieve this will likely require governments to be involved in more than just the selection of appropriate open standards. Standards provide a recognised framework for implementing a system, however it is the clear definition of systems interfaces and data definitions that ensure interoperability.

Another objective for an ECM system would be ensuring both transport agencies and the transport industry gain operational efficiencies through its use. This is a significant issue and is worthy of a separate paper just on its own. As it is more a business case issue than a technical one, it will not be covered in this paper.

4. CURRENT EXAMPLES OF E-COMPLIANCE

There are number of examples of successfully operating ECM regimes around the world. Several of them will be mentioned briefly here. The reader is referred to the references provided for further detail.

The Canadian state of Saskatchewan has been operating the “Rural Partnership Haul Program” [10] for a number of years. The Saskatchewan Department of Highways and Transportation partnered with International Road Dynamics Inc. to develop and implement an automated vehicle monitoring and audit system to meet the needs of the Saskatchewan Partnership Program. This program allows commercial carriers to operate larger and heavier truck configurations as long as they comply with the requirements of the program – using “road friendly” vehicle technologies, operating only on agreed routes, etc.

In January 2001, the Swiss Customs Authority introduced a “Heavy Vehicle Fee” (HVF) road-pricing scheme. This scheme is supported by on-vehicle and roadside equipment to simplify the calculation of associated charges and monitor operational compliance [11]. Two notable features of the on-vehicle equipment (OVE) used in this scheme are:

- The recording of “hidden files” accessible only to police and customs officials that, for example, cross-reference GPS data with from the vehicle’s tachograph; and
- A visual indicator on the outward facing side of the windscreen-mounted unit, which is used by on-road enforcement teams when stopping and checking vehicles.

The New South Wales Roads and Traffic Authority (NSW-RTA) in Australia has been operating a “Mobile Crane Concessional Benefit Scheme” since September 2001. This scheme provides operators of a certain class of mobile crane improved access in several large urban areas in New South Wales as long as a tracking device monitors the crane’s movements [12].

An assessment of these and other examples, and the material referenced in the preceding sections, has lead the authors to conclude that compliance monitoring is a task that must be dealt with from a systemic perspective – integrating technological and legal tools with on-road enforcement. It is not merely about collecting and verifying data. Flowing on from this, the authors conclude there are four broad elements to a successful ECM system. Each of these will be considered in turn in Sections 5 through 8.

5. THE FIRST ELEMENT OF E-COMPLIANCE: ON THE VEHICLE

ECM begins with the vehicle to be monitored. This typically means that in/on the vehicle there are:

1. Sensors to monitor the operating parameter of interest. This can range from a GPS for position and time, to on-board weighing equipment.
2. A processing unit to collect, store, manage and possibly make decisions on this sensor data.
3. Some form of data transmission sub-system. This can be some form of wireless transceiver[2] or a smartcard / chipcard interface.
4. A means of uniquely identifying the vehicle, and perhaps even the driver, to the rest of the ECM system.
5. A simple and unambiguous means of identifying if the OVE is operating correctly.
6. A means of either manually or automatically validating the data being stored in the processing unit mentioned in point #2. This can be achieved by cross-referencing the output of one sensor with that of another (point #1).

[2] Such as a DSRC device, a GSM/GPRS modem or a Bluetooth interface.

The following table suggests ways in which the on-vehicle part of an ECM system meet the requirements outlined in Section 3.

Suggested Requirements
A. As much as possible, the OVE should be supplied as a single integrated unit – covering data transmission (eg. GSM mobile phone), data storage, computing and sensor interpretation (eg. GPS receiver hardware, odometer pulse counter). • This would minimise the potential for operator interference. • The on-vehicle equipment used in the Swiss HVF scheme has taken this approach [13]. • Another, somewhat more obscure, example is the integrated satellite communications / GPS tracking units (referred to as "Sat C" terminals) used on ships operating on the shore side of Australia's Great Barrier Reef [14].
B. The OVE should visually declare the status of itself and the vehicle to those outside the vehicle. • This measure allows transport inspectors to easily determine if the OVE is not operating properly, or the vehicle is not complying with its operating conditions. • As mentioned in Section 4, the Swiss HVF scheme uses a visual status indictor (made up of an array of LED's) that, for example, shows whether or not an attached trailer has been declared. • In the Hong Kong electronic road pricing (ERP) trials, a LED was mounted on the outside of the test vehicles. This LED received a signal from an independent source – a FM or digital radio service – that generated a flashing sequence at random if the OVE was operating properly. If this was not the case, the LED defaulted to a continuous "on" state. The LED was located near the vehicle's number plate, allowing the video enforcement system to capture both at the one time.
C. The central on-vehicle unit has a unique permanently stored identifier, which is separate to the identity of the vehicle it is on and that used by any data transmission sub-system. • This allows attempts to surreptitiously move the equipment or identity between vehicles to be detected. This deals with the problem some existing commercial systems have, were the unit and vehicle identity is linked to phone number of the GSM modem used in the unit … allowing a simple swapping of a SIM to manipulate identity.
D. Data moved out of the vehicle, by whatever means, is secure and has an audit trial. • This begins the chain of evidence that, should, ultimately ensure the data that enters the transport agency's hands is irrefutable – that the agency can authenticate the identity of the vehicle in question, and the vehicle operator cannot repudiate the data. • The Swiss HVF unit stores records on a chipcard in an open format with an encrypted checksums – thus attempts to change the data are detected.
E. The status of the sensors and their connection to the central on-vehicle unit should be monitored, if possible validated, and reported. Ideally this can be done by cross-referencing data from sensors external to the central on-vehicle unit, with that from sensors inside the central unit. • This tamper-detection measure would flag potential operator interference and complements the physical tamper-proofing measures used in the design and manufacture of the equipment. • The "Sat C" terminals mentioned above log and report power-on events and the connection / disconnection of the GPS antenna. • The Swiss HVF unit uses the DSRC link to turn it on and off at border crossing. Once on,

	the distance data from the connected tachograph is recorded for charging purposes. Both these events are compared with data from a GPS inside the unit and discrepancies recorded in the "hidden files" mentioned in Section 4. Additionally, other sensors inside the unit determine if it is operating properly, if the vehicle is running, if the vehicle is moving, and if there is a trailer attached. Again discrepancies are recorded in the "hidden files". Customs auditors can examine these files to determine if the driver committed, or attempted to commit, fraud.

Table 2: Suggested Requirements for On-vehicle Equipment

There is large number of commercially provided services that could form the basis for an ECM system. However, focusing on the issue of interoperability, there is work on several fronts that is relevant to ECM systems.

There are a number of European initiatives underway that could lead to the development of international standards in fields akin to ECM:

- Within the International Organisation for Standardisation (ISO) there is work on the development of an interface standards for electronic fee collection (EFC) applications using both DSRC and a combination of GPS and mobile phone networks [15].
- The German autobahn heavy vehicle tolling system, which has been awarded a consortium comprising of DaimlerChrysler, Deutsche Telekom, and Cofiroute.
- Currently underway in the UK, both Department for Transport's DIRECTS project and the recently announced HM Treasury "Lorry Road User Charging" program will require OVE.

There is the potential for all these programs to produce a unit that meets the currently emerging CEN and ISO standards being driven by ERTICO (the European ITS Association) in Europe. Though this work is focused on ERP, it has the potential to define the core building blocks necessary for an ECM system.

There are also three industry-driven initiatives that are worthy of mention under the banner of interoperability – Motorola's mobileGT platform [16], ACUNIA's Open Telematics Framework [17] and the Telematics Forum [18]. The first two represent multi-company alliances implementing in-vehicle (and in ACUNIA's case, back-end systems) to a set of agreed specifications. The Telematics Forum is similar, but with financial underwriting from the European Union (EU) and the support of ERTICO. Interestingly all these initiatives support (or aim to) the application interface standard published by the Open Services Gateway Initiative [19]. As with the ISO work, these initiatives have the potential to define the core building blocks necessary for an ECM system.

It should be said here that the above paragraphs obliquely demonstrate, to the best of the authors' knowledge, that an interoperable ECM system is yet to be demonstrated anywhere in the world – let alone one based on agreed open standards.

6. THE SECOND ELEMENT OF E-COMPLIANCE: ON THE ROADSIDE

As articulated in Section 3, the primary objective of an ECM system is the delivery of evidence of non-compliance in a robust manner. One common engineering approach to ensuring a robust overall system is the use of redundant sub-systems, allowing the results from one sub-system to be validated against that of another.

This is one of the main reasons emerging ECM systems around the world incorporate roadside equipment – to provide validation data. There are a number of examples of how these ECM roadside sub-systems are evolving:

- The NSW-RTA has a gantry-based "Safe-T-Cam" system that uses licence-plate recognition (LPR) technology to identity heavy vehicles at strategic points on the road network [20]. This allows vehicle travel times to be computed, which can be compared with driver's log-book details to identity excessive driving hours and speeding.
- Queensland Main Roads is developing an integrated infrared digital image capture and weigh-in-motion system. This will allow potentially overloaded vehicles to be uniquely identified, providing independent evidence that can trigger regulatory audits by transport inspectors.
- In its review of New Zealand's "road-user charging" (RUC) regime for heavy vehicles, Transfund (the New Zealand road funding agency) identified the need for converting WiM sites into full "roadside monitoring sites" to gather validation and enforcement data [21].

The need for the type of roadside system discussed above has grown to the degree that the private sector has developed and is marketing commercial systems. The "Integrated Roadside Operations Computer" (IROC) from International Road Dynamics (IRD) of Canada is a recent example [22]. This particular system (for the US market) integrates WiM screening, vehicle/driver/carrier credential checking and truck inspection station operations.

The other reason ECM systems incorporate roadside equipment is to provide a mechanism for capturing the data transmitted by the on-vehicle equipment. This, of course, is dependent on the design of the system – the use of some form of DSRC sub-system would necessitate the incorporation of roadside transceivers. The use of "wide area" wireless communications (such as GSM) would, of course, reduce the need for (and capital cost of) roadside equipment, but the downside would be the possible increase in the system's operational (ie. communications) costs.

If the OVE contains a "wide area" wireless communications sub-system, it could be used as a secondary means of both identifying its location as well as provide a link to the roadside monitoring/enforcement equipment. With communications protocols such as GSM/GPRS, 3G or TETRA, a mobile unit will generally have overlapping contact with several towers (base-stations that connect to the landline communications network). These digital communications protocols use this information in their normal functioning to identify the closest and most powerful link over which to transmit. If this information was recorded and mapped to the road location, a parallel source of data could be generated to localise the vehicle on a segment of the road network.

Further, several new 3G and other wireless communications protocols support a mobile-to-mobile communications links – as opposed to the normal mobile-to-tower communications links. These mobile-to-mobile links could be used to communicate directly with roadside equipment. Such a technique would function much like a DSRC link without the additional hardware and cost.

On the interoperability front, there has been significant investment into developing interface standards for DSRC-based systems – driven mainly by the worldwide demand for electronic fee collection (EFC) systems. GSM-based systems are also starting to receive some attention – the work of ISO's Technical Committee 204 on "Traffic and Traveller Information Message via Cellular Networks" is an example [15].

The last, but most important element, of the roadside element of an ECM system is the enforcement camera. While any one of several techniques may be used to communicate between the roadside and the vehicle, these will only work if the vehicle OVE and the Roadside equipment are functioning properly. If the OVE is non-operational, or tampered with, or disconnected, or removed, the only means to identify the vehicle is through a video camera source. This video image capture must also be capable of distinguishing the designated class of vehicle from all the others on the road at that specific site. The enforcement camera is an essential part of the overall ECM system and can also be integrated with other ECM data to help positively identify non-compliant behaviour.

7. THE THIRD ELEMENT OF E-COMPLIANCE: THE DATA CENTRE

The data centre[3] plays a key role in an ECM system. As there is a lot of mainstream IT material on this subject, this section will simply point out the four main roles of a data centre from the ECM perspective and the implications one can draw from these roles.

Firstly, the data centre is a repository. It is here that the data collected from 'on-vehicle' and the roadside is held. As this repository serves a potentially significant compliance task, the security of equipment that underpins the data centre and the data itself are crucial. As mentioned in Section 3, this can mean addressing issues such as:

- Managing physical access to the computers that hold the data – for example housing them in a lockable room;
- Managing electronic access to the database that holds the data – this covers user authentication (from password through to biometrics) and permissions levels (eg. editing rights); and
- Ensuring the database used maintains audit trails of who accesses the data when and changes what.

The potential size of an ECM repository should not be underestimated, as it may have to hold a large volume of image data, vehicle track data, monitoring site data, etc. The data centre for the NSW-RTA Safe-T-Cam system, for example, processes upwards of 10 Terabytes of data [23].

Part of the repository function would likely involve the aggregation of the collected data. This aggregated data would provide a valuable base for a transport agency's network and road asset planning activities.

Secondly, the data centre is most likely the place where data from 'on-vehicle' is correlated with that from the roadside. This is where the key purpose of an ECM system's roadside element (discussed in Section 6) comes to fruition: validation. The roadside data is used to

[3] This term is used very broadly here, as the 'data centre' can range from a stand-alone personal computer to a mainframe-based system.

independently validate, or refute, the data collected from the vehicle. The management of vehicle identity is central to achieving this in an unambiguous way. This is why the on-vehicle equipment needs some mechanism for passing the vehicle's identity to the roadside equipment (as mentioned in Section 5).

Thirdly, the data centre will also be the likely place where a telephone support centre and help desk will be located to help answer questions and provide an interface to both users and fleet managers. The administrative functions necessary to run a system of this magnitude should not be overlooked. The recording of OVE serial numbers for new vehicle installations, the replacement of damaged or malfunctioning units and the call for service of suspect units to operators are just a few of the support activities that must be managed and the data centre presents the logical location for these functional requirements.

Finally, the data centre is where data analysis will occur. Once data from the different ECM sub-systems has been imported, 'cleaned' and matched up (ie. the above correlation process), it can be analysed to identify such things as:

- Compliance breaches;
- Potential equipment tampering; and
- Patterns of behaviour that can be brought to the attention of on-road enforcement staff (the transport inspectors mentioned in Section 2) – allowing them to be positioned where they are most likely to capture non-complying vehicles.

The importance of this analysis role should not be overlooked, as it provides a valuable source of intelligence. To achieve this, the data centre needs to support an appropriate set of data analysis and mining software tools.

8. THE FOURTH ELEMENT OF E-COMPLIANCE: ENABLING LEGISLATION

Though this is substantially a technology paper, there needs to be a brief acknowledgment of the importance of law (ie. Acts and regulations) to an ECM system. Ultimately, any transport agency has to act within the bounds of its jurisdictional legal framework – this is doubly so with the often confrontational tasks of compliance and enforcement.

It will be from enacted legislation that a transport agency draws the authority to do such things as:

- Demand or support the use of on-vehicle ECM technology;
- Identify the legal channels and judicial procedures for record keeping, evidence, defence procedures and levels of mandatory and discretionary fines;
- Empower its agents (most commonly its transport inspectors) to make sure the equipment is properly installed and operational – this can range from remote electronic checks to periodic physical inspections;
- Ensure that ECM data is admissible and recognised as accurate in a court of law;
- Impose penalties on non-compliant behaviour, based on the evidence of ECM data; and
- Impose penalties on proven cases of ECM equipment tampering and the falsifying of ECM data.

Indeed, in Australia there is work currently underway to move some of these concepts into transport law [24].

One of the challenges facing ECM systems is the supply of evidentiary-quality data. In most Australian applications, devices that measure quantities in a legally recognisable manner (eg. the taxi meter, the green grocer's scales) need to be certified for compliance with trade measurement legislation. This has yet to be achieved with GPS-based tracking devices and WiM equipment. In one Australian state, the way around this problem has been to give the transport agency the ability to inspect the records of the vehicle driver, the business operator and even the consignor of the goods for legal evidence of non-compliant behaviour [25] – these audits are triggered by the intelligence information gathered from sources such as an ECM system.

It is not just transport and trade measurement legislation that will impact on an ECM system. In Australia, privacy laws place constraints on the collection and use of personally identifiable information. Care needs to be taken to ensure an ECM system is implemented and managed so as stay within such constraints.

9. CONCLUSIONS

This paper has demonstrated that the traditional methods of ensuring heavy vehicles comply with their operating conditions will not keep pace with the increasingly complex road transport task. This realisation is motivating transport agencies to look at applying electronic compliance monitoring systems to the heavy vehicle fleet.

This paper has outlined the four elements of an electronic compliance monitoring system:

- Equipment on the vehicle;
- Equipment on the roadside;
- The data centre; and
- Enabling legislation.

Further, this paper has asserted that the whole electronic compliance monitoring system needs to work towards ensuring its own internal integrity and the supply of irrefutable evidence of non-compliant behaviour.

And finally, this paper has pointed out that the building blocks for each element of an interoperable electronic compliance monitoring system either exist or soon will.

10. REFERENCES

1. Australian Bureau of Statistics, *Survey of Motor Vehicle Use, Australia*. 2001, Australian Bureau of Statistics: Canberra. p. 44.
2. Commonwealth Department of Transport and Regional Services, *AUSLINK, Towards the National land Transport Plan (Green Paper)*. 2002, Commonwealth Department of Transport and Regional Services: Canberra. p. 117.

3. National Road Transport Commission, *Road Transport Reforms, Performance-based standards*. 2002, http://www.nrtc.gov.au/progress/reformsall.asp?reform=D01&lo=progress.

4. Hollingworth, G., *Comparison of heavy vehicle infringements with estimated total overloading*, G. Taylor, Editor. 2002: Brisbane.

5. Faciane, T. and S. Radin, *Tracking State Deployments of Commercial Vehicle Information Systems and Networks*. 1998, US Department of Transportation, Intelligent Transportation Systems Joint Program Office: Cambridge, MA. p. 51.

6. Scientific American Newsletters, *Germany Seeks Bids to Toll Trucks on Autobahns*, in *The Intelligent Highway*. 2000.

7. Hamet, P., *Seeking information on INITIATIVE*. 2000, European Commission Directorate General for Information Society: Brussels.

8. Austroads Inc., *Austroads Intelligent Access Project*. 2002, http://www.austroads.com.au/iap.html.

9. Taylor, G., *Meeting with RAPP and FELA*. 2001, Queensland Department of Main Roads: Basel, Switzerland. p. 9.

10. Lang, A., et al., *Saskatchewan Rural Partnership Haul Program*. 2001, University of Saskatchewan, http://www.irdinc.com/english/html/tech_ppr/index.htm.

11. Swiss Federal Customs Administration, *HVF - in concrete terms*. 2000, http://www.zoll.admin.ch/d/steuern/lsva/infoe.htm.

12. Roads and Traffic Authority, *Introduction to the Mobile Crane Concessional Benefit Scheme*. 2002, http://www.rta.nsw.gov.au/frames/initiatives/e_f.htm?/frames/initiatives/e8&/initiatives/e8_c.htm&Mobile+Crane+Concessional+Benefits+Scheme&8.

13. FELA Management AG, *DSRC / GNSS-CN: The entire spectrum of tolling systems*. 2002, http://www.fela.ch/elektroniktelem/de/produkteprojekt/gebhrenerfassun/index.html.

14. Trainor, N., *The Great Barrier Reef Ship Reporting System*, G. Taylor, Editor. 2002, Australian Maritime Safety Authority: Melbourne.

15. International Organisation of Standardisation, *Technical Committee 204 - Transport Information and Control Systems*. 2002, http://www.iso.ch/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=4559.

16. Motorola Inc., *mobileGT Platform*. 2002, http://e-www.motorola.com/webapp/sps/site/overview.jsp?nodeId=02M0ylfWcbfM0yrBwp3h.

17. ACUNIA NV, *The ACUNIA Open Telematics Framework© (OTF)*. 2002, http://www.acunia.com/.

18. Telematics Forum, *The Telematics Forum*. 2002, http://www.telematicsforum.com/index.htm.

19. Open Services Gateway Initiative, *Implementation & Deployment Fact Sheet - Open Services Gateway Initiative (OSGI)*. 2002, http://www.osgi.org/.

20. Roads and Traffic Authority, *Introduction to Safe-T-Cam*. 2002, http://www.rta.nsw.gov.au/frames/initiatives/e_f.htm?/frames/initiatives/e5&/safety/c1a_c.htm&Safe-T-Cam&0.

21. Body, A., et al. *Transfund New Zealand's Plans for a Transport Information System and Electronic Road User Charges*. in *14th IRF World Road Congress*. 2001. Paris, France.

22. ITS America, *IRD IROC Enhances Weight, Credential and Safety Compliance Checks at Weigh Stations*. 2002, International Road Dynamics, http://www.itsa.org/itsnews.nsf/key/8622?OpenDocument.

23. RLM Systems Pty Ltd, *Safe-T-Cam™*. 2002, http://www.rlmsystems.com.au/compj_safetcam.asp.

24. National Road Transport Commission, *Road Transport Reform (Compliance and Enforcement) Bill*. 2002, http://www.nrtc.gov.au/progress/forcomment.asp?lo=progress.

25. Office of the Queensland Parliamentary Counsel, *Transport Operations (Road Use Management) Act 1995*. 1999, Queensland GoPrint. p. 264.