TECHNICAL REPORT

ISO/TR 17427-9

First edition
2015-11-01

Intelligent transport systems — Cooperative ITS —

Part 9: Compliance and enforcement aspects

Systèmes intelligents de transport — Systèmes intelligents de transport coopératifs —

Partie 9: Conformité et aspects relatifs à l'application

Reference number
ISO/TR 17427-9:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 204, *Intelligent transport systems*.

ISO 17427 consists of the following parts, under the general title *Intelligent transport systems — Cooperative ITS*:

— *Part 2: Framework overview* [Technical Report]

— *Part 3: Concept of operations (ConOps) for 'Core' systems* [Technical Report]

— *Part 4: Minimum system requirements and behaviour for core systems* [Technical Report]

— *Part 6: Core systems risk assessment methodology* [Technical Report]

— *Part 7: Privacy aspects* [Technical Report]

— *Part 8: Liability aspects* [Technical Report]

— *Part 9: Compliance and enforcement aspects* [Technical Report]

— *Part 10: Driver distraction and information display* [Technical Report]

The following parts are under preparation:

— *Part 1: Roles and responsibilities in the context of co-operative ITS architechtures(s)*

— *Part 5: Common approaches to security* [Technical Report]

— *Part 11: Compliance and enforcement aspects* [Technical Report]

— *Part 12: Release processes* [Technical Report]

— *Part 13: Use case test cases* [Technical Report]

— *Part 14: Maintenance requirements and processes* [Technical Report]

This Technical Report provides an informative consideration of 'Compliance and Enforcement Aspects' for Cooperative Intelligent Transport Systems (C-ITS). It is intended to be used alongside ISO 17427-1, ISO/TR 17465-1, other parts of the ISO 17465 series and ISO 21217. Detailed specifications for the application context will be provided by other ISO, CEN and SAE deliverables, and communications specifications will be provided by ISO, IEEE and ETSI.

Introduction

Intelligent transport systems (ITS) (2.7) are transport systems in which advanced information, communication, sensor and control technologies, including the internet, are applied to increase safety, sustainability, efficiency, and comfort.

A distinguishing feature of *'ITS'* are their communication with outside entities.

Some *ITS* systems operate autonomously, for example, 'adaptive cruise control' uses radar/lidar/and/or video to characterize the behaviour of the vehicle in front and adjust its vehicle speed accordingly. Some *ITS* systems are informative, for example, 'Variable Message Signs' at the roadside, or transmitted into the vehicle, provide information and advice to the driver. Some *ITS* systems are semi-autonomous, in that they are largely autonomous, but rely on 'static' or 'broadcast' data, for example, *GNSS* (2.6) based 'SatNav' systems operate autonomously within a vehicle but are dependent on receiving data broadcast from satellites in order to calculate the location of the vehicle.

Cooperative Intelligent Transport Systems (C-ITS) are a group of *ITS* technologies where service provision is enabled by, or enhanced by, the use of "live", present situation related, dynamic data/information from other entities of similar functionality [for example from one vehicle to other vehicle(s)], and/or between different elements of the transport network, including vehicles and infrastructure [for example from the vehicle to an infrastructure managed system or from an infrastructure managed system to vehicle(s)]. Effectively, these systems allow vehicles to "talk" to each other and to the infrastructure. These systems have significant potential to improve the transport network.

A distinguishing feature of *'C-ITS'* is that data is used across *application*/service boundaries.

It will be immediately clear to the reader that such systems present possibilities for 'Compliance and Enforcement'. However such issues are highly sensitive, bound closely with issues of personal privacy, and may have a major impact on the whole public acceptance of *cooperative ITS*.

Further Technical Reports in this series are expected to follow. Please also note that these TRs are expected to be updated from time to time as the *C-ITS* evolves.

Intelligent transport systems — Cooperative ITS —

Part 9:
Compliance and enforcement aspects

1 Scope

This Technical Report identifies potential critical compliance and enforcement aspects issues that C-ITS service provision may face or introduce; to consider strategies for how to identify, control, limit or mitigate such issues. The objective of this Technical Report is to raise awareness of and consideration of such issues and to give pointers, where appropriate, to standards deliverables existing that provide specifications for all or some of these aspects. This Technical Report does not provide specifications for solutions of these issues.

2 Terms and definitions

2.1
application
app
software application

2.2
application service
service provided by a service provider accessing data from the in-vehicle system (within the vehicle), in the case of *C-ITS* (2.4), via a wireless communications network, or provided on-board the vehicle as the result of software (and potentially also hardware and firmware) installed by a service provider or to a service provider's instruction

2.3
compliance
assurance that equipment or a service behaves within a set of predetermined, declared and accepted parameters

2.4
cooperative ITS
C-ITS
group of ITS technologies where service provision is enabled, or enhanced by, the use of 'live', present situation related, data/information from other entities of similar functionality (for example, from one vehicle to other vehicle(s)), and/or between different elements of the transport network, including vehicles and infrastructure (for example, from the vehicle to an infrastructure managed system or from an infrastructure managed system to vehicle(s))

2.5
enforcement
regulatory measures to ensure observance with certain requirements

2.6
global navigation satellite system
GNSS
several networks of satellites that transmit radio signals containing time and distance data that can be picked up by a receiver, allowing the user to identify the location of its receiver anywhere around the globe

2.7
intelligent transport systems
ITS
transport systems in which advanced information, communication, sensor and control technologies, including the internet, are applied to increase safety, sustainability, efficiency, and comfort

2.8
jurisdiction
government, road or traffic authority which makes and enforce regulations

EXAMPLE Country, state, city council, road authority, government department (customs, treasury, transport), etc.

2.9
type approval
certificate of conformity granted to a product that meets a minimum set of regulatory, technical and safety requirements, generally, by regulation required before certain products are allowed to be sold

Note 1 to entry: Often called 'Homologation'.

3 Abbreviations and acronyms

ANPR automatic number plate recognition

C-ITS cooperative intelligent transport systems, cooperative ITS

ITS intelligent transport systems (2.7)

TR technical report

TTA Transport Ticketing Authority

4 How to use this Technical Report

4.1 Acknowledgements

Much of the inspiration for this Technical Report and its considerations and content originate from the reports l "Cooperative ITS Regulatory Policy Issues" and "Cooperative Intelligent Transport Systems Policy Paper" National Transport Commission, Australia. And this source is acknowledged and thanked. References [9] and [10].

Contribution from the European Commission project EETS is also acknowledged.

See Bibliography for further details.

4.2 Guidance

This Technical Report is designed to provide guidance and a direction for considering the issues concerning *compliance* (2.3) *and enforcement* (2.5) *aspects* associated with the deployment of *C-ITS* service provision. It does not purport to be a list of all potential *compliance* and *enforcement* aspects factors, which will vary according to the *application service* (2.2) being provided, the regime of the *jurisdiction* (2.8), the location of the instantiation, and to the form of the instantiation; nor does it provide definitive specification for the solution of these issues. Rather, this Technical Report discusses and raises awareness of the major *compliance* and *enforcement* aspects issues to be considered, and provides guidance and direction for considering and managing *compliance* and *enforcement* aspects in the context of future and instantiation specific deployments of *C-ITS*.

4.3 ITS and 'compliance and enforcement aspects'

Whilst they share the common framework of being regulatory measures, '*compliance*' and '*enforcement*' within the context of *C-ITS* are two very different, though in some cases closely linked, paradigms.

4.3.1 Compliance

Compliance is defined by the Oxford English dictionary as 'the state or fact of according with or meeting rules or standards'.

4.3.2 Enforcement

Enforcement is defined by the Oxford English dictionary as 'the act of compelling observance of or *compliance* with a law, rule, or obligation'.

4.3.3 Compliance and enforcement within the context of C-ITS

Within the context of *C-ITS,* the term '*compliance*' may therefore simply be applied to the assurance that equipment or a service behaves within a set of predetermined, declared and accepted parameters.

'*Enforcement*' may be considered to be regulatory measures to ensure observance with certain requirements.

While this at one end of the spectrum may imply that those who provide defective equipment or services (non-compliance) will face unpleasant consequences, so as to encourage them not to so by default, at the other end of the *spectrum enforcement* may also, and in a different paradigm, mean that specific *C-ITS* services, or information from *C-ITS* services, could be developed to penalise drivers that err from driving regulations.

4.4 C-ITS compliance and enforcement aspects issues

That *compliance*, and *enforcement* of *compliance*, for equipment and to defined systems specification is required is probably doubted by few, including drivers. Indeed, *compliance* assurance through certification (see ISO/TR 17427-11) and/or *type approval* (2.9) of equipment and *application* (2.1) systems, will help to provide confidence to drivers. *Type approval* regulations will also provide assurance to drivers. Such measures will normally therefore encourage the take-up of systems so approved.

However, particularly in a situation where the driver will have need or requirement to purchase equipment and/or subscribe to *ITS* service provision, to then find that this equipment will/may subsequently be used in *enforcement* measures to penalise him for violation of driving regulations will be a sure deterrent to dissuade him from buying/subscribing and using *C-ITS application services*. If the equipment is mandated, it will be a sure way to encourage the driver to switch the system off or otherwise disable it.

At some time in the future, if drivers become more used to being automatically controlled, or it becomes socially acceptable as a norm, the use of C-ITS systems for *enforcement* to driving regulations may become acceptable, but it seems highly likely that this is not the case at the time of developing this Technical Report.

Jurisdictions will therefore have to make a decision as to whether to try to enforce such measures to *enforce* regulations, which may well seriously affect their electability, or leave the choice of use to the market place. In this latter case, there is a high probability of drivers not using *C-ITS* systems, and the safety of life improvements, and improvements to the efficiency of the traffic system, achievable through the use of *C-ITS,* being lost as a result.

4.4.1 Private vehicles

The issues and potential effects were summed up in the US Privacy Policy Framework:

"were a National..... (*C-ITS*).....Program to be proposed that would use ...(*C-ITS*)..... as a surveillance tool for law *enforcement* purposes, '*concerns with regard to privacy and civil liberties would be raised by the public and its representatives and advocates, which would threaten the implementation of such a Program. The primary purposes of ....(C-ITS)...are to enhance transportation safety and mobility through improving driver situational awareness, to help avoid and/or mitigate crashes and to use technology to optimize anonymous traffic monitoring and control strategies. The program is being developed, and policy-makers are making decisions, with these purposes in mind. To expand the program beyond these purposes to include punitive uses of the....(C-ITS) system for enforcing traffic or other laws would cast doubt regarding the true intent of the initiative. If a National Program were used to facilitate or automate enforcement, many would likely seek ways to disable the ....(C-ITS)... communications system on their vehicles, or to purchase or retain an older, non-equipped vehicle. This would negatively impact not only their safety, but also the safety of other road users, because a ....(C-ITS)....-disabled or non-equipped vehicle and would no longer be sending or receiving safety data.*'" [14]

A further consideration is that there will be a long period during which more technologically advanced cars share the road with those that do not have *C-ITS* devices. Does *compliance* and *enforcement* activity need to take a different approach to these different groups? Would more advanced cars be held to a higher standard (because their breaches could potentially be more easily detected) and will this discourage the take-up of advantageous technology? Some stakeholders already report public concern that they could be fined for speeding based on roadside detection of *C-ITS* signals from the vehicle,[9] and there seems to be widespread fear of misuse.

As an example, police in Washington have set up a 'net' of ANPR detectors, tracking movements around the city, which have apparently moved from initially capturing wanted criminals or unregistered vehicles to a range of other purposes.

"Police also have begun using them as a tool to prevent crime. By positioning them in nightclub parking lots, for example, police can collect information about who is there. If members of rival gangs appear at a club, police can send patrol cars there to squelch any flare-ups before they turn violent. After a crime, police can gather a list of potential witnesses in seconds.

Beyond the technology's ability to track suspects and non-criminals alike, it has expanded beyond police work. Tax collectors in Arlington bought their own units and use the readers to help collect money owed to the county. Chesterfield County, in Virginia, uses a reader it purchased to collect millions of dollars in delinquent car taxes each year, comparing the cars on the road against the tax rolls".[22]

There have also been some examples in the US of private use, for example, by banks searching for delinquent borrowers.[23]

It seems clear that in respect of the private car driver, *enforcement* would likely be a disincentive to take-up of the technology. Do limits need to be placed on the use of data from safety systems in order not to penalise those who take them up? The principle that *ITS* policy should '*be consistent with broader transport network objectives*' needs to be taken into account in considerations of the use of *C-ITS* technology for *enforcement*.

Most concerns centre around keeping of information about members of the public who have not committed an offence. Many existing systems such as point-to-point are explicitly designed not to retain information if there is no suspected offence, in order to avoid this concern. Regimes are in place to limit the use of data from other systems, such as tolling. Surveillance device legislation in various states provides rules around the use of tracking devices, including for *enforcement* purposes.

In addition, there is a question over how *C-ITS* data would be used in the aftermath of a crash. Data could be captured within the vehicle or elsewhere within the system (e.g. by a roadside unit). There may be value in making this data available in order to analyse crash causation, which could be extremely valuable in helping to set appropriate speed limits on particular stretches of road or improve road infrastructure. However, this data could also be used to convict a driver, for example, of negligent driving. If historical data is retained then this could also be used (e.g. to show that a driver had a history of driving in a reckless manner).

There may be potential to counter-weight the increased surveillance made possible by *C-ITS* with incentives and rewards for its use where compliant behaviour is demonstrated (for example, reduced insurance costs).

While the advent of *C-ITS* provides opportunities for *compliance* and *enforcement*, it may be far more beneficial, rather than seek to use these *enforcement* opportunities, to promote opportunities to assist drivers in achieving *compliance* with road laws, for example, through intelligent speed warnings, which can assist and encourage drivers to keep to the speed limit, or by physically speed control at risk or danger zones (such as school crossings, blind spots, etc.) using the justification and incentive that the technology helps prevent violation of regulations and therefore assist avoiding enforcement and its penalties.

4.4.2 Commercial vehicles

It is important here to separate out private road usage from commercial road usage. For, while *enforcement* of private vehicle drivers may prove unpopular, *enforcement* that commercial vehicles respect the road rules is likely to be very popular with the population at large, and regulatory control is far more accepted in the commercial vehicle sector.

Automatic reporting, and in some cases control, by *C-ITS application* systems, can also be very popular with fleet operators, because it may allow better and less bureaucratic access to the road network, especially for large vehicles. For example, many of these opportunities have already been tested and are in growing use in Australia, under its 'Intelligent Access Programme' (IAP).

The IAP is a certified intelligent transport system recognized in law and developed in partnership between all Australian road agencies. The IAP has been operational since 2008. The IAP was developed by Australian Governments in response to current and emerging policy challenges, including the following:

— a growing population, public and private transport and freight task;

— community expectations about the use, availability and safety of the road network;

— road safety through the interaction of people, vehicles and infrastructure;

— sustainability and environmental impact in managing greenhouse emissions;

— security and associated responses in transport.

In common with many countries, Australia faces constrained infrastructure budgets, being impacted by an ever increasing maintenance demand, including in urban areas a declining ability to build new infrastructure. At the same time there are expectations of increased and unrestrained mobility of people, goods and assets including, pressure from the road transport industry to permit operation of larger, heavier vehicles. Increases in freight volumes have been higher than truck travel growth rates because of the trend towards larger trucks and higher payloads. Heavier articulated trucks are replacing small rigid trucks. Along with freight issues, Australia is facing challenges in increasing traffic congestion resulting from the interaction of demand and lack of capacity in the movement of people, goods and assets; road safety issues through the interaction of people, vehicles and infrastructure and a drive to dramatically decrease road casualties; sustainability and environmental impact issues in managing greenhouse emissions; security and associated responses in transport. Whilst traditional reforms have served Australia well, authorities required smart solutions to move forward. The IAP is an effective, efficient, non-intrusive approach that delivers unparalleled assurance and productivity gains.[20]

One of the many benefits of the IAP is its ability to accurately monitor *compliance*. In turn, road authorities and the road transport industry will have new opportunities to optimize vehicle operations safely, efficiently and productively. Another important feature of the IAP is its ability to combine regulatory and commercial fleet management services.

For further information on The Intelligent Access Program, its "Overview Guideline" provides an explanation of the IAP and the role of program participants.[21]

According to Transport Certification Australia (TCA), IAP brings several benefits:

— to *Jurisdictions*;

— to Transport Operators;

— to Government and Road Agencies.

To *jurisdictions* because the ability of the IAP to accurately monitor vehicle *compliance* provides a new set of opportunities for road authorities and the road transport industry to optimize heavy vehicle operations in terms of safety, efficiency and productivity; to transport operators to negotiate improved road access.

In Australia, the IAP provides an opportunity for transport operators to achieve productivity gains, better turnaround times and increased profits. It also creates the possibility for a transport operator to develop an advantage over competitors. If a transport operator is enrolled in the IAP and a direct competitor is not, the enrolled operator may be able to deliver a better service to their customers. To road authorities, a means to better manage transport obligations for the growing transport demands. Freight owners are increasingly relying on the IAP to fulfil their obligations under 'Chain of Responsibility' legislation. With the IAP, freight owners have the assurance that their transport operators are complying at all times with the conditions set by relevant road agencies.

The Australian IAP provides for more productive and compliant heavy vehicle operations that promote sustainable road infrastructure, improve road safety and reduce environmental effects. The IAP will help to reduce damage to the road infrastructure and allow road agencies to focus their *enforcement* activities in more efficient areas and with greater flexibility.[21]

The IAP provides restricted access and over-dimension vehicles with improved access to Australia's road network. In return, their *compliance* with approved access conditions is monitored using satellite-based tracking technology and GSM/UMTS communications. This provides Roads and Maritime Services and the community with greater assurance that the right heavy vehicles are operating on the right roads.[20]

In the Australian IAP, an in-vehicle unit is installed by a certified IAP service provider. The unit will automatically record the date, time, and position of any heavy vehicle that is non-compliant with the access conditions on the IAP permit. Information about any non-compliant travel may form the basis of an investigation by Roads and Maritime Services. The IAP is mandatory for access and provides enhanced route access for several types of commercial vehicle, including: vehicles operating under higher 'Mass' Limits, B-Triples and AB-Triples, Quad Axle Group Permit Scheme vehicles and other 'road trains', high risk mobile Cranes, etc. The electronically measured 'mass' pressure that the axles of a vehicle exert on the road pavement is also being used using *ITS* technology to control and manage access of certain classes of 'equipped' vehicles to control and manage their access to parts of the road network. Equipped and electronically monitored vehicles have greater access to the road network. This is managed in accordance with ISO 15638-12. Work diaries have been mandated for commercial vehicle drivers in Australia for many years, but the paper based system is administratively cumbersome, and disliked by the Administrations, fleet operators and drivers alike. It is being replaced by an 'electronic work diary' system, operated in accordance with ISO 15638-11. Heavy goods vehicles are also closely monitored for speed violations, this is now increasingly achieved using *ITS* technology in accordance with ISO 15638-16.

The issue is important from a road user perspective but also has a potentially significant impact on road agencies' structure and resourcing.

The conclusion that can be drawn is that, at this point in time, the use of *C-ITS* for *enforcement* of the commercial freight network brings many advantages and seems likely to be politically acceptable, whilst the use of *enforcement* for private vehicles is fraught with both political acceptability and privacy obstacles.

4.4.3 Surveillance devices

C-ITS may be impacted by surveillance device legislation in various *jurisdictions*. Surveillance regulations vary, but are present in most *jurisdictions*, set out conditions for law *enforcement* agencies to use surveillance devices to track locations and to listen to conversations.

Certain potential *C-ITS applications* (for example, using *C-ITS* to measure individual vehicle trips in order to manage traffic flows) may inadvertently be captured by this legislation. This has reportedly been the reason that some *jurisdictions* have not used technology to track 'Media Access Control' (MAC) addresses of Bluetooth devices to measure trip times.[9]

Surveillance devices that track vehicle activities may also fall within various state legislations in different *jurisdictions*. Under many privacy protection laws, the person under surveillance, or person controlling the object being tracked, must provide their consent to that surveillance.[24] For example, in Western Australia, the Surveillance Devices Act 1998 (WA) legislates that:

A person shall not attach, install, use, or maintain, or cause to be attached, installed, used, or maintained, a tracking device to determine the geographical location of a person or object without the express or implied consent of that person or, in the case of a device used or intended to be used to determine the location of an object, without the express or implied consent of the person in possession or having control of that object.[25]

A tracking device means any electronic device capable of being used to determine or monitor the geographical location of a person or an object. This is sufficiently broad to include vehicle movements, and is likely to capture vehicle tracking by state or territory road managers for the purposes of managing traffic flows. Without trying to influence the decisions made by a *jurisdiction*, *jurisdictions* need to examine their legislation to make sure that it is adequately worded and that their legal requirements in respect of *C-ITS* are clear and explicit.

Point of purchase (or sign-up) is perhaps the appropriate time in which agencies usually obtain individuals' consent to track their vehicles for traffic management purposes. However, as with privacy, individuals should be made aware of the implications of consent and arrangements should be in place to ensure that the tracking devices do in fact only track those vehicles where consent has been obtained.

Further, in many *jurisdictions*, and for sound reason, telecommunications interception regulations prohibit the interception of, and other access to, telecommunications, except where authorized in special circumstances or for the purpose of tracing the location of callers in emergencies (or by warrant for state security). The application of these regulations are usually limited to communications as they travel across the communications network, and *C-ITS* communications are perhaps unlikely to be captured, but, again, without trying to influence the decisions made by a *jurisdiction*, and bearing in mind the use of collection, collation and use/re-use of data in the *C-ITS* paradigm, *jurisdictions* need to examine their telecommunications interception legislation to make sure that it is adequately worded and that their legal requirements in respect of *C-ITS* are clear and explicit, and that *C-ITS* service provision is not accidentally trapped by a legislation written in a different era.

4.4.4 Comparative systems

4.4.4.1 'Automatic Number Plate Recognition' (ANPR) technology

If signals from individual vehicles are able to be tracked, the system will have similarities to ANPR technology. A Queensland study into the use of ANPR recommended that safeguards and controls governing the use of automatic number plate recognition technology be clearly articulated in enabling legislation, and should prescribe the following:

— access to data collected by ANPR devices is restricted to authorized agencies and users;

— the collection and retention of personal information is limited to that which is necessary to achieve clearly articulated purposes;

— data relating to vehicles not found to be committing an offence shall be cleansed nightly from devices to minimize the possibility of security breaches;

— data shall be transported securely between devices and repositories and stored with high-security encryption and digital signatures;

— security systems shall be subject to regular audits to ensure they are adhered to;

— should additional and compelling public interests be served in the future by new *applications* of ANPR, these should only be pursued after public consultation and scrutiny by Parliament the misuse of ANPR data attracts severe penalties;

— affected individuals have access to a complaints scheme to seek redress if their rights are abused.[26]

Similar recommendations may need to be examined in relation to *C-ITS* technology if detection devices are used for *compliance* purposes, in particular ensuring that data is used for stated purposes, is secured correctly and that there are appropriate offences for misuse. The role and organisational independence of Certification Agencies will play an important role in such management. See also ISO 17427-9.

4.4.4.2 Automatic toll collection

Perhaps the closest automatic data collection systems relating to vehicles are automatic toll collection systems.

EETS is the European Electronic Toll Service, a relatively recent European initiative for harmonization of road tolling across the European Union. Reference [28] states *"EETS provision requires to process large numbers of transactions with appropriate security mechanisms against data loss and corruption as well as data privacy breaches."*

EETS enables *"Identification of an EETS Providers' contract on the basis of a license plate: This could be a kind of broadcast communication to EETS Providers supporting this service to ask whether an identified license plate belongs to a service contract of these EETS Providers. This supports the identification of EETS Users where no OBE communication could be established.*

Compliance with European and local privacy legislation shall be ensured."[28]

Although how such *compliance* is assured is not specified.

The guide only states *"Data protection authorities may define policies for the security and privacy in a toll charging environment."* and *" The role related to the provision of the toll service is responsible of providing the basic artefacts, mechanisms, organization structures, and information transfer tools needed to run an EFC system.*

Responsibilities related to this role include:..... — implementing and adhering to the security and privacy policies for the toll systems"[28]

The EETS guide also offers the following:

— *Operating enforcement, including:*

.....

— *handling enforcement cases while protecting the privacy of the actors having taken the role as driver;*

— *implementing and adhering to the security and privacy policies for the toll charging environments"*[28]

The EETS guide has a specific section on *enforcement* which state:

"6.2.2. Enforcement

The scope of enforcement covers detection, chasing and prosecution of toll violations. Enforcement would appear to operate most effectively through national enforcement systems.

This guide considers liability questions between a Toll Charger and an EETS Provider in the case of an offending vehicle covered by a valid EETS contract. Enforcement authorities should be able to determine

whether an offending vehicle is an 'EETS vehicle' and therefore covered by the payment guarantee of the responsible EETS Provider (see Article 7(2) of Decision 2009/750/EC). Annex II to Decision 2009/750/EC foresees a direct communication link between the EETS on-board equipment and the fixed or mobile roadside enforcement equipment for real-time compliance checking transactions."[28] (our underline).

This therefore addresses even more starkly the *enforcement* v privacy issues that face *C-ITS*, but provides no solution.

"DIRECTIVE 2004/52/CE on Interoperability of Electronic Fee Collection Systems in Europe: Recommendations on enforcement (including cross-border enforcement) for the European Electronic Toll Service. Prepared by: Expert Group 3: EFC enforcement working to support the European Commission DG TREN" back in 2005, offers the following:

"*However, the reality is that in some countries, it is not possible to remove the lifting bars as public authorities have not yet given operators the authority to implement the Compliance and Enforcement measures necessary to recover payments due."*

It is significant that the word "privacy" does not appear at all in this Directive and "Data Protection", manages only one reference in the Directive:

"*Ideally, it would be advisable to keep such black lists as up-to-date as possible and constantly available for consultation by TSP's. The Expert Group also recognise that creating and maintaining such lists at a European level may raise significant legal and data protection issues which will need to be addressed*."

EETS also faces and confronts the issues regarding the movement of vehicles across *jurisdiction* boundaries, and the need for data within a different *jurisdiction*:

"6.2.3. Cross border enforcement

The considerations below show that cross-border enforcement mechanisms cannot be included in the arrangements for EETS; to do so would go beyond the scope of Directive 2004/52/EC.

Where it has not been possible for enforcement authorities to stop a vehicle which is registered in another country and has committed violations, whether they relate to toll violations, speeding offences or any other form of infraction, raises questions of how sanctions are taken against those vehicles from other countries. In general, sanctions can only be exercised by identifying the vehicle using its registration mark and identifying the keeper through the national vehicles record of its country of origin.

The extent to which it is possible to obtain this information varies between Member States. In some Member States, the national registration authorities are relatively willing to release information; in others there are considerable legal difficulties in obtaining such information and in particular transferring it to foreign entities, especially where those entities are in the private sector.

The matter is further complicated in the case of tolling infractions by the fact that the nature of the offence may be either civil or criminal, depending on the national legal status of the toll. For example, where the duty to pay toll is directly based on a legal act, as in Austria, or the charge is a tax the sanction concerns public law and where it is a toll based on private law the redress is likely to be civil, as in Spain. This means that there may be questions of convention rights with enforcement regimes' establishment.

The availability of cross-border enforcement is important to Toll Chargers for the implementation of free-flow systems, considering the potential difficulties to recover the tolls due in the absence of such a mechanism. Keeping barriers may then be a Toll Charger's preferred option in comparison to beefing up enforcement systems with e.g. additional roadside enforcement equipment. Smaller toll domains (bridges/tunnels) might decide to implement the possibility of proceeding offences inside their own network to avoid extra costs and/or toll evasion."

This seems to indicate that EFC has a similar, but more extreme, problem to that of *C-ITS enforcement*, but, as yet, no solutions.

5 What are the key compliance and enforcement aspects issues

5.1 General

5.1.1 Application to C-ITS

One approach that appears to make practical sense is to separate collection and storage of vehicle activity from the entity that holds the information linking the unique identifier to a vehicle registration number or other *C-ITS* identifiers.

In circumstances where this information is required by law enforcement bodies, a warrant, or similar *jurisdiction* regulated process would be required, and privacy principles adhered to, in accordance with the regulations of the *jurisdiction*. In this scenario, personal information would be tightly controlled around one entity that is not engaged in day-to-day *C-ITS* activities, thereby minimising the privacy risk exposure of *C-ITS*.

Whether location information can be linked back to an individual whose identity is apparent will become more important as *C-ITS* develops beyond speed and direction information. Advanced *application*s in the future could require much more information, conceivably including the following:

— number and placement of occupants, to allow vehicles to minimize the impact on drivers and passengers if collisions cannot be avoided;

— license information, to determine whether the driver is subject to particular restrictions, for example, in relation to speed restrictions for learner drivers;

— registration information, for *compliance* checks and tolling;

— vehicle class/weight/volume/mass;

— vehicle driving behaviour;

— etc.

The application of privacy principles and surveillance laws to *C-ITS* is dependent on the extent to which the information collected is anonymous and whether the deployment model is opt-in, opt-out, or mandatory.

Clearly, for *enforcement* to succeed, a link between the violation and the offender, and therefore the offender's personal information, is required. However, by the use of identification by security certificate, with the link between certificate reference and user known only by the certificate issuer, and not known to the *enforcement* agency, the amount of personal data directly available to the *enforcement* agency is limited, and the conditions of access to that data (via the certification authority) can be more strictly controlled. Clearly, in *jurisdiction*s where vehicle registration data is made readily available, this problem is more severe.

5.2 International approaches

5.2.1 United States

To provide assurance to the public about the uses of *C-ITS* information, the US 'Intellidrive' project has proposed a set of limitations on the use of *C-ITS* information, including Limit 4, which states:

*"No specific information about an individual or vehicle shall be … used for law enforcement or investigation purposes without a valid warrant (or its equivalent). However, anonymous data may be collected and used by law enforcement to, for example, assist traditional law enforcement efforts or to analyse transportation problem locations. Specifically, the National VII (*read C-ITS*) Program shall not be used by law enforcement for:*

— *recording real-time video or voice of vehicle occupants, or*

— *associating precise vehicle identification numbers (VIN) with times or locations, or*

— *off-board control of vehicle driving or manoeuvring functions."*

5.2.2 Europe

Compliance and *enforcement* was not specifically included in the EU's *ITS* Action Plan and *enforcement* action is complicated by the nature of the EU, with *enforcement* agencies based in the different member states. Nonetheless, the use of *C-ITS* information for *enforcement* has not been specifically excluded at this stage. The office of the European Data Protection Supervisor will no doubt take close interest in these issues.

5.2.3 Australia

There is as yet no direct address of *C-ITS* issues in Australian state or federal law. But measures are enacted locally.

5.2.3.1 Myki

For example, the 'Myki' Public Transport Ticketing System in Victoria records location information of public transport users, which may be linked to personal information for certain types of tickets. In regard to the disclosure of information, the Victorian Transport Ticketing Authority (TTA) states in its privacy policy:

Apart from disclosures connected with administration of the new ticketing system and Transport Act enforcement, TTA will only provide personal information about Myki customers to other third parties, including law *enforcement* agencies, in the following circumstances:

— *where TTA is required to do so by law, e.g. in response to a warrant or subpoena;*

— *where TTA reasonably believes that the disclosure is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of one or more people;*

— *where disclosure is necessary for the purposes of complaint handling, such as disclosure to the Public Transport Ombudsman or the Privacy Commissioner;*

— *where the disclosure is requested in writing by the individual concerned;*

— *where an authorized police officer certifies in writing that the disclosure is reasonably necessary for the enforcement of the criminal law;*

— *in connection with investigating or reporting suspected unlawful activity detected by TTA or its contractors;*

— *in exceptional circumstances - to intelligence agencies; the Australian Security Intelligence Organization (ASIO) or the Australian Secret Intelligence Service (ASIS).*[9]

The TTA has also developed 'Guidelines for disclosure of personal information by the Transport Ticketing Authority' setting out criteria and procedures for disclosure of personal information.

5.2.3.2 Melbourne CityLink

CityLink is a toll road which utilizes ANPR technology and collects personal information from and about motorists. CityLink is governed by the Melbourne City Link Act. Under the Act, a motorist who drives on CityLink without a valid pass may receive an infringement notice and *enforcement* procedures remain in the hands of Victoria Police.[9]

CityLink has implemented a privacy code, and additional legislative privacy protection has been created under the Melbourne City Link Act. The Act requires that information collected by CityLink, including the names, addresses, licence plate numbers, activities and infringements of motorists, remains confidential. Disclosure is only legal in defined circumstances, namely to relevant agencies such as

police and road agencies for specific purposes, including infringement notices, criminal investigations and to enforce certain road safety laws. Penalty units apply, not only to CityLink for illegal disclosure, but to relevant agencies if the records are subsequently misused.[9]

This is an example of governments applying specific legislative instruments to restrict the use of personal information and to ensure against function creep in a commercial environment that coexists with genuine state requirements to access information for *enforcement* and road safety purposes. The intended outcome is that motorists will be confident that their personal information is secure and used only for the purposes intended by the Act.[9]

5.2.4 Other countries

To be added later.

6 Policy questions and options

In most *jurisdictions*, the use of *C-ITS* information for *compliance* and *enforcement* purposes is not currently explicitly regulated. However, the use of this information for *compliance* and *enforcement* purposes (assuming it is technically possible to do so) may create a significant disincentive to consumers (citizens) to use this technology. This would be an unfortunate outcome if it led to the loss of the benefits of *C-ITS*. Nonetheless, there are legitimate scenarios where *enforcement* agencies may need to access data; the question becomes whether limits and controls need to be put around the use of this data. For the commercial sector, there appears to be a very workable trade-off between benefits in administration and access traded off against automatic *enforcement*.

It is clear that making privacy *compliance* an essential component of the approval process (opt-in or opt-out) is a crucial issue, and indeed requirement for the use of *C-ITS* by citizens.

As mentioned above, one means to make *C-ITS* enabled automatic control measures politically acceptable is to promote them on the basis that they help prevent the motorist from violating laws and therefore are a means to avoid enforcement penalties and their consequences.

6.1 Option 1: Continue current approach

Allow *jurisdictions* to develop their own procedures and processes. This will provide greater flexibility, but will likely lead to inconsistent approaches between *jurisdictions*. This will have particular implications for commercial vehicle fleets which regularly cross multiple *jurisdictions* in a journey. It will also present difficulties in respect of private citizens driving in multiple *jurisdictions*.

6.2 Option 2: Amend current road rules

Provide specific protection and regulation for *C-ITS* based information from use for *compliance* and *enforcement* purposes (potentially through legislation or policy). This could provide guidance that, except for control of commercial vehicles, such information should not be used as part of certain regular *compliance* and *enforcement* activities (e.g. generating infringements), but only as part of a court order or utilizing a specific process.

6.3 Option 3: Create guidelines or principles for manufacturers

Again linked to the privacy issues, guidance could be provided on the appropriate use and disposal of data to ensure against misuse. This would provide guidance on and encourage best practice, although it would not compel organisations to follow the same processes, and does not adequately deal with *enforcement* issues.

6.4 Option 4: Examine technology options as they develop

Other than a general awareness, it may still be too early to suggest or standardize guidelines for *jurisdictions*, although in federated countries, or associated groups of countries like the European

Union, or potentially NAFTA or APEC, resolution for these issues will have to be agreed in the near future if the safety of life and traffic system efficiency benefits *C-ITS* are to be realized.

7 Summary of findings

The principal findings of this Technical Report are the following:

a) *Compliance* and *enforcement* issues are linked to privacy issues in that both relate to the appropriate collection and use of data. In a similar way to privacy, the issue of *compliance* and *enforcement* centres on how information is collected and for what purposes it is used (see also ISO/TR 14827-7 for further consideration of these issues).

b) Ensuring that for *compliance*, the system is anonymised where possible, and is under strict and open control and management for *enforcement* and *compliance enforcement*, and that data are not kept any longer than absolutely required, and passed to a third party only in exceptional and strictly controlled circumstances, will assist in building the confidence of drivers.

c) Whilst it can be argued that '*if people aren't doing the wrong thing they have nothing to worry about*,' many members of the public will be concerned about stores of information being created about their travel patterns and driving behaviour, with the potential for almost continuous monitoring.[29]

d) The scope of the *compliance* and *enforcement* purposes that *C-ITS* data may be used for should be made clear to consumers. There needs to be strict rules in respect to security of the data at all points and restrictions on who can access the data.

e) *Compliance* issues can be ensured through the use of certification procedures (see ISO/TR 17427-11). The use of an institutionally independent and firewalled certification authority can make the conformance situation manageable and politically acceptable, whilst maintaining appropriate security.[29]

f) *Enforcement* cannot be made completely anonymous, but the separation of the managers of vehicle registration information and certificate management and issue is strongly advised. The use of an institutionally independent and firewalled certification authority can make the *enforcement* situation manageable and politically acceptable, whilst maintaining appropriate security.[29]

g) Ultimately any information once gathered can potentially be used in a court case; subpoenas can be used to access most forms of relevant information in the right circumstances (with rare exceptions such as client confidentiality for lawyers). However, there is a difference between information that could be gathered as part of a specific investigation and information that is constantly being monitored in order to issue infringements.[29]

h) Many *jurisdictions* are examining setting explicit limits on the collection and use of *C-ITS* data for *compliance* and *enforcement* purposes.

i) It will be important as part of building trust in systems likely to be primarily used for safety purposes, that *compliance* and *enforcement* does not become a disincentive to the uptake of systems. It would seem counterproductive to encourage the use of *C-ITS* for *enforcement* on citizens as this would significantly deter take-up and use of the technology, and lose the safety of life and economic benefit issues that *C-ITS* offers.

j) Just uncertainty in the treatment of *C-ITS* data for *compliance* and *enforcement* purposes may act as a disincentive to the take-up of technology and result in reduced safety and other benefits.

k) The use of *C-ITS* for *compliance* and *enforcement* in the commercial vehicle sector is not only much more politically acceptable, even attractive, to most parties, and may offer benefits that make it particularly attractive to fleet operators.

l) Regulatory *applications* should be considered separately from non-regulatory, safety advisory or commercial systems. For *applications* that do not have a primary regulation and monitoring function, the standard privacy provisions should limit access to data.[13]