TECHNICAL REPORT

ISO/TR 17427-7

First edition
2015-11-01

Intelligent transport systems — Cooperative ITS —

Part 7: Privacy aspects

Systèmes intelligents de transport — Systèmes intelligents de transport coopératifs —

Partie 7: Aspects relatifs à la vie privée

Reference number
ISO/TR 17427-7:2015(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 ..... **iv**
Introduction ..... **vi**
1 Scope **1**
2 Terms and definitions **1**
3 Abbreviations and acronyms **2**
4 How to use this Technical Report **2**
4.1 Acknowledgements 2
4.2 Guidance 3
4.3 ITS and 'Privacy' 3
4.4 C-ITS 'Privacy' issues 4
4.4.1 General C-ITS 'Privacy' issues 4
4.4.2 Examples of vehicle tracking 6
4.4.3 Anonymity 6
4.4.4 Deployment models 8
5 C-ITS Actors and Privacy **9**
5.1 C-ITS and jurisdictions 9
5.1.1 United States 9
5.1.2 Europe 10
5.1.3 Australia 12
5.1.4 Other countries 14
5.1.5 International Standards 14
5.1.6 Privacy and governments 14
5.2 C-ITS and road operators/managers 15
5.2.1 Jurisdictions 15
5.2.2 'Core' systems 16
5.3 C-ITS and manufacturers 16
5.4 C-ITS information/application service providers 16
5.5 C-ITS, drivers and vehicle owners 17
5.6 Further reading 17
5.7 Aspects relating to probe vehicle information services 17
6 Policy questions and approaches **17**
6.1 Is specific regulation required for C-ITS? 17
6.1.1 Option 1: Continue current approach 17
6.1.2 Option 2: Privacy code 18
6.1.3 Option 3: Provide guidance on best practice 18
6.1.4 Option 4: Legislate C-ITS governance arrangements and use of information 18
6.1.5 Option 5: Legislate technical standards to protect privacy 18
6.1.6 Option 6: Match and copy mobile phone privacy measures 18
7 Summary of findings **19**
7.1 General 19
7.2 Principal opinions 20
7.3 Privacy — Private Sector 22
7.4 Privacy — Public Sector 22
Bibliography **23**

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 system' 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 architecture(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]

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.

Introduction

Intelligent transport systems (*ITS*) 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 its 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* 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 are used across *application*/service boundaries.

It will be immediately clear to the reader that such systems present the possibility to seriously compromise privacy, and must, and will, be strictly controlled by regulation and managed to prevent abuse of privacy by any party. The purpose of this Technical Report is to identify potential critical privacy issues that *C-ITS* service provision may introduce, to consider how to control, limit or mitigate such privacy issues, and to limit the risk of exposure to the financial consequences of privacy issues.

This Technical Report is a 'living document' and as our experience with *C-ITS* develops, it is intended that it will be updated from time to time, as and when we see opportunities to improve this Technical Report.

Intelligent transport systems — Cooperative ITS —

Part 7:
Privacy aspects

1 Scope

The scope of this Technical Report is as an informative document to identify potential critical privacy issues that *C-ITS* service provision may introduce; to consider strategies for how to control, limit or mitigate such privacy issues; and to give pointers, where appropriate, to standards deliverables existing that provide specifications for all or some of these aspect and to limit the risk of exposure to the financial consequences of privacy issues.

The objective of this Technical Report is to raise awareness of and consideration of such issues. 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 *IVS* (2.6) within the vehicle in the case of *C-ITS*, 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 providers instruction

2.3
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

[SOURCE: for example from the vehicle to an infrastructure managed system or from an infrastructure managed system to vehicle(s)]

2.4
core system
combination of enabling technologies and services that will provide the foundation for the support of a distributed, diverse set of *applications* (2.1), and *application* transactions which work in conjunction with 'External Support Systems' such as 'Certificate Authorities'

Note 1 to entry: the system boundary for the core system is not defined in terms of devices or agencies or vendors, but by the open, standardized interface specifications that govern the behaviour of all interactions between core system users

2.5
global navigation satellite system
GNSS
comprises 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

2.6
intelligent transport systems
IVS
hardware, firmware and software on board a vehicle that provides a platform to support *C-ITS* service provision, including that of the *ITS-station* (2.8) (ISO 21217), the facilities layer, data pantry and on-board 'apps'

2.7
in-vehicle system
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
ITS-station
entity in a communication network [comprised of *application* (2.1), facilities, networking and access layer components] that is capable of executing *ITS-S application* processes, comprised of an *ITS-S* facilities layer, *ITS-S* networking & transport layer, *ITS-S* access layer, *ITS-S* management entity and *ITS-S* security entity, which adheres to a minimum set of security principles and procedures so as to establish a level of trust between itself and other similar *ITS-stations* with which it communicates

3 Abbreviations and acronyms

ANPR automatic number plate recognition

EDR electronic data recorder

C-ITS cooperative intelligent transport systems, cooperative ITS

IPP information privacy principle

ITS intelligent transport systems (2.6)

IVS *in-vehicle system* (2.7)

NPP National privacy principle

TR technical report

V2V vehicle to vehicle

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 "*Cooperative ITS Regulatory Policy Issues*" and "*Cooperative Intelligent Transport Systems Policy Paper*" National Transport Commission, Australia. And this source is acknowledged and thanked.[1][17]

Contribution from various TCA (Transport Certification Australia) documents are acknowledged.

Contribution from the report of EC Project PRECIOSA is acknowledged.

Contribution from the US DoT document “CoreSystem_SE_SyRS_RevF” is acknowledged.

The review by the office of the European Data Protection Supervisor is acknowledged and thanked

4.2 Guidance

This Technical Report is designed to provide guidance and a direction for considering the issues concerning privacy associated with the deployment of *C-ITS* service provision. It does not purport to be a list of all potential privacy factors – which will vary according to the regime of the jurisdiction, the location of the instantiation, and to the form of the instantiation, nor does it provide definitive specification. Rather this TR discusses and raises awareness of the major issues to be considered, and provides guidance and direction for considering and managing privacy in the context of future and instantiation specific deployment of *C-ITS*.

4.3 ITS and ‘Privacy’

Privacy is the subject of National Regulation, but most countries have signed up to one or more of OECD, APEC and/or European Union principles for personal privacy.

The subject of how ‘privacy’ regulations affect *ITS*, the variations of ‘privacy’ regulations around the world, and general measures that *ITS* should adopt in respect of ‘privacy’ and *ITS* are dealt with in ISO/TR 12859.

Suffice to say, in summary that ISO/TR 12859 recommends that the conditions under which data shall be collected and held in support or provision of *ITS* services shall uphold all of the following principles:

a) Avoidance of harm	Recognize the interests of the individual to legitimate expectations of privacy, personal information protection; prevent the misuse of such information. Further, acknowledging the risk that harm may result; take account of such risk, and remedial measures should be proportionate.
b) Fairly and lawfully	Personal data obtained and processed fairly and lawfully.
c) Specified, explicit and legitimate purposes	Personal data collected for specified, explicit and legitimate purposes.
d) Explicit and legitimate and must be determined at the time of collection of the data	Purposes for which personal data are collected shall be determined at the time of the collection of the data and shall be explicit and legitimate at the time of collection of the data and use and subsequent of the data limited to the fulfilment of those purposes (or such others as are not incompatible with those purposes specified); All personal data collected shall be adequate, relevant and not excessive in relation to the purposes for which they are processed.
e) Not further processed in a way incompatible with the purposes for which it was originally collected	Personal data shall not be further processed or used in a way incompatible with the purposes for which it was originally collected.
f) Not be disclosed without the consent of the data subject	Personal data shall not be disclosed, made available or otherwise used for purposes other than those specified.
g) Adequate, relevant and not excessive in relation to the purposes for which they are collected	Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.
h) Accurate and, where necessary, kept up to date	Personal data shall be accurate and kept up to date; every reasonable step must be taken to erase or rectify inaccurate or incomplete data, having regard to the purposes for which they were collected.
i) Identification of data subjects for no longer than is necessary for the purposes for which the data were collected	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.
j) Restricted to those who have a demonstrable ‘need to know’	The use of personal data to be restricted to those who have a genuine need to know.

k) Clear and accessible	Personal information controllers shall provide clear and easily accessible statements about their practices and policies with respect to personal information that should include: a) the fact that personal information is being collected; b) the purposes for which personal information is being collected c) the types of persons or organizations to whom personal information might be disclosed d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information.
l) Security safeguards	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
m) Cumulative interpretation of multiple recommendations	In the development of *ITS* systems and standards, we are advised by legislators and lawyers that the recommendations cannot just be taken individually in isolation, but the combination of the recommendations may infer interpretations, this has significant implications. Lawyers often refer to this as 'cumulative interpretation'

4.4 C-ITS 'Privacy' issues

NOTE General privacy requirements are not dealt with further in this document, and the reader is referred to ISO/TR 12859 for further information on general aspects.

4.4.1 General C-ITS 'Privacy' issues

This Technical Report refers to the specific issues of privacy and privacy protection introduced by *C-ITS* service provision, the *C-ITS* environment, *C-ITS* data exchanges, and the date storage, mining and consolidation made possible by *C-ITS*.

In the introduction it was stated that a distinguishing feature of '*ITS*' are its communication with outside entities, and that a distinguishing feature of '*C-ITS*', is that data is used across *application* (2.1)/service boundaries. One can see that while *ITS* itself has to be very privacy aware, *C-ITS* has particular opportunity to compromise that privacy if not managed in a way to protect personal privacy. Furthermore, the use of data 'across *application*/service boundaries' runs the risk to conflict with the privacy regulations requirement "Not further processed in a way incompatible with the purposes for which it was originally collected ".

*C-ITS application*s rely on vehicles broadcasting signals to indicate their location, signals which are intended to be received and understood by a range of other devices. This raises a significant privacy issue: should *C-ITS* enable persons or organisations — either governments or private-sector companies — be able to locate and track specific vehicles? Clearly, without knowledge of the exact location and direction of movement of a vehicle, *application*s such as 'collision avoidance' nor even collision risk warnings', nor 'ice alerts' and other 'road obstacle' alerts would be possible. The risk for *C-ITS* consumers is that this information will be 'personal information' if their identity can be acquired or construed or is otherwise apparent. This is feasible if those that have access to location data can link the unique vehicle identifier (or series of identifiers) of the *C-ITS* signal to a registered vehicle and, in turn, to an individual (a registered owner). This information could be in real time (where the vehicle is presently located) or historic (where the vehicle was at a certain time on a certain day).

While the opportunities for improved road safety, traffic management and law enforcement are considerable, many individuals would not expect the movement of their private vehicle, and by extension themselves, to be plotted across the network by a government or a third party. This is a valid and legitimate concern and will require both government and industry to practice in good faith the privacy principles based on legal requirements, particularly in respect to the purpose of collection, data storage disclosure, and sharing of data.

The likelihood and significance of the privacy risk will depend on the extent to which the data is/are anonymised and the nature of the controls in place with respect to collecting the data and linking information to individuals. It will also depend on which bodies hold relevant data, (such as certificate information).

C-ITS is intrinsically linked to the movement and exchange of data, and cooperation among the various entities acquiring the information is often expected. In this situation, responsibilities need to be assessed in terms of security risks and possible threats to privacy, as some of the data will be purely situational or anonymous, while other data, either by itself or as part of multiple data sets, which independently can be purely situational or anonymous, taken together can provide personal information.

The definition of personal information is sufficiently broad to include location information if that information is about an individual whose identity is apparent or can be reasonably ascertained from that information. Australia, for example, succinctly defines personal information as *"information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.' (Privacy Act.1988).*[28]

Location information can be a very personal matter worthy of privacy protection, even if the movements and activities of an individual are within the law. In a report regarding surveillance activities; an Australian body, the Victorian Law Reform Commission, reflected on location information:

"The need to retain privacy in public places is sometimes concerned with the desire to keep particular information private. This information may relate to a person's political views, medical issues (such as attendance at an abortion clinic or a drug and alcohol treatment centre), and social matters (such as attendance at a gay bar). It is strongly arguable that people ought to be able to restrict access to information about themselves of this nature."

Consumers make choices that impact upon their privacy in many ways. For example, most people accept that certain location information can already be tracked, particularly through their mobile phone and location-based *application*s. They do so because of the advantages that these *application*s afford them, and – implicitly – because they trust the service providers to handle their personal information securely and responsibly. However, the ability for individuals to make this choice is important.

These privacy issues mirror a bundle of technology innovations that pose comparable risks, from ANPR to facial recognition technology. Privacy issues are also becoming increasingly cross-border in nature, due to the move towards cloud computing where personal information may be held anywhere in the world (or in multiple places).

In order to do responsibly manage these risks, and to avoid or minimize the risk of transgressing privacy and data security regulations, three general rules should ideally be observed regarding *C-ITS* data.

— With the exception of imminent safety of life *application*s (collision avoidance, ramp access, etc.), data should be anonymised before being sent to any third party.

— Data collected for imminent safety of life *application*s should be stored for only a very short period of time ,— the minimum necessary to achieve its task, and in any event no longer than 24 hours may be suggested.

— Unless determined by the jurisdiction to be for 'safety of life of others', those wishing to benefit from service provision where their personal data may be required for the provision of such service should specifically need to 'opt-in' to such services, acknowledge the use of their personal data in such service provision, and be advised how long such data are stored, and how to opt-out of such service provision.

Regardless of good intent, failure to observe these tenets is likely to cause friction with privacy regulators in most jurisdictions and may well result in the *C-ITS application* being prevented.

However, in order to achieve the life saving benefits of safety systems such as collision avoidance, ramp access, grade crossing warnings/control etc., some jurisdictions may want to *require* use of the *C-ITS* safety systems, as the lives, not only of the specific vehicle driver, but other road users, may be

compromised/risked if a driver can chose to opt-out of the *C-ITS* service provision. For example, in the US, NHTSA 05-14. "……*NHTSA will then begin working on a regulatory proposal that would require V2V devices in new vehicles in a future year, consistent with applicable legal requirements, Executive Orders, and guidance*."

This places difficult dilemmas to the jurisdiction (that will be a matter of National decision, not an ISO TR).

(Past regulated analogies include things like the use of direction indicators, brake lights, safety belts, traction control systems, etc.)

4.4.2 Examples of vehicle tracking

Vehicle tracking technology is widely utilized around the world today. Many telematics systems include a level of tracking, for example, to provide emergency assistance or to track stolen vehicles. Vehicle tracking technology is also a common component of commercial freight management systems, and many modern 'SatNav' systems provide traffic information based on data submitted from other vehicles, and recipient vehicles therefore also provide their location data so that the service company can analyse traffic conditions and advise those in or approaching problem spots.

Telematics are increasingly used for insurance and crash-liability purposes. Systems may record information regarding driving style, including speeds, distances, time of day and harsh braking events. While offering safety benefits for drivers, and cost benefits (lower insurance premiums etc.), telematics devices are also capturing driver behaviour and vehicle location information.

Infrastructure providers also utilize vehicle-tracking technology in a range of circumstances. Enforcement agencies have applied ANPR technology for many years to track vehicles through point-to-point systems or mobile units, while tolling systems record certain vehicle information for the purposes of road user charging. In some countries (such as Australia), vehicle tracking technology is also required for certain types of commercial vehicles in return for access to the transport network and management of vehicles using the transport network. These systems typically have stringent controls in place to govern the collection, use, access and disposal of information.

Some stakeholders have suggested that, due to the significant vehicle tracking which already takes place, and because most vehicle users carry cell phones that either enable them to be tracked, or at the least identify which communications cell they are linked to, additional information collection through *C-ITS* is likely to have a minimal impact. However, all technologies that have an impact on privacy require a risk assessment and systems appraisal to ensure compliance with the privacy principles, and as has been seen above, the law, though it may vary to some extent from jurisdiction to jurisdiction, is demanding in most countries of the world in respect of personal privacy protection.

To consider any potential threat to privacy caused by *C-ITS*, it is necessary to consider two aspects in a little more detail:

— the extent to which *C-ITS* data will be anonymous;

— the deployment model for *C-ITS*.

4.4.3 Anonymity

While this paper is intended to focus on the policy principles and not specific technologies, the privacy issues will to some extent be framed by the technology solutions implemented and in particular the extent to which *C-ITS* signals generated by vehicles can be anonymised. This is critical given that the surest way to protect privacy is not to gather the personal information in the first instance.

International standards for *C-ITS* are in development. A focus of these standards needs to be that *intelligent transport systems* (2.6) will be developed with a 'privacy by design' objective. There may, however, be limitations on whether true anonymity can be achieved. For security purposes, vehicles are likely to be required to have a form of security certificate (similar to those for secure websites) in order to ensure that signals are legitimate and prevent false signals being generated. While security certificates

for drivers or vehicles are still under development, it is expected that these will need to be authenticated by a certification authority to ensure that false signals are not recognized within the system.

Further, many safety of life *C-ITS applications* (such as collision avoidance, ramp access, etc.) require timely and precise positional, directional and speed data in order to perform their critical safety of life objectives; other systems (such as obstacle and road condition alerts) work efficiently if they are targeted only to vehicles in or approaching specific locations/direction of travel. Both of these examples and others require location and positioning data, and that former group of services needs to target messages to specific (therefore identified) vehicles.

This means that, much like providing details to purchase a mobile phone, individuals – personally or through vehicle registration – will likely need to identify themselves in some way to gain access to the system. This creates a unique identifier, or collection of identifiers, that can potentially link a vehicle's activity to a vehicle registration number or individual license number. Whilst the intention is to make the signals generated by vehicles anonymous, there may remain the ability to trace, via the certification authority, these identity numbers back to an individual. In fact there may be a need to do so, if individuals within the system need to be penalised for misuse of devices (for example, hacking a device so that it broadcast an incorrect signal). These issues will also feed into decisions around governance, such as which body should act as the certification authority and whether this needs to be separated from road authorities.

Indeed the *C-ITS* paradigm may be compared to mobile telecommunication services. Private mobile telecommunication network providers collect personal information from subscribers (customers) to establish accounts. These providers link communications data (calls, SMS, Internet access for third party *applications*) from subscriber devices to the individual subscriber accounts for billing purposes. In linking the communications data to an individual, the communications data becomes "personal information" and hence its collection, use, disclosure and handling are governed by Privacy Principles under existing privacy regulations. Specific privacy legislation is therefore not required.[38]

This is the approach that has already been taken in a number of *C-ITS* initiatives to date, namely to acknowledge the privacy implications and build the initiative within them rather than re-inventing for each initiative. Indeed, it is quite dangerous to even ask this question without the context of the specific *C-ITS application* defined. It is the data to be collected and the underlying policy intent that will define the use and disclosure of personal information not simply a 'cross-cutting' technology such as *C-ITS*.[38]

In 2011, the Canadian Information and Privacy Commissioner of Ontario published a paper that considered the privacy implications of Wifi and MAC addresses. The discussion paper discusses the privacy challenges associated with MAC addresses and makes the following suggestions:

— privacy is predicated on providing individual mobile device users with personal control, alongside openness and transparency on the part of the provider;

— in no case should the MAC address of an individual's mobile device be collected or recorded without the individual's consent;

— privacy by design is now the international standard for privacy and should be used by engineers to ensure privacy is embedded in the systems architecture; the potential for possible unintended uses should form part of the privacy risk analysis;

— Wifi protocols should seek to randomize MAC addresses or ensure privacy through a proxy-like method of assigning addresses; innovative solutions will be required to change the existing model of using persistent MAC addresses that remain uniquely bound to a mobile device.

Industry does not necessarily agree that an IP or MAC address will always constitute personal information, and it has been observed that:

A MAC address or an IP address information is rarely going to be in and of itself information about an identifiable individual in the sense of having a precise connection and being directly related to an identifiable individual. But it is the context of how the MAC address or IP address is combined with other information (or could be reasonably be combined with other information) that has privacy advocates concerned.

Further work needs to be undertaken to establish whether communications media such as Wifi or Bluetooth can provide *C-ITS* functionality without it being possible for an entity to link the unique address to the identity of the owner.

In the event that the individual 'owner' of a *C-ITS* signal can be reasonably identifiable, the privacy principles outlined in this report will always apply.

As stated above, the issues are not just the choice and privacy of the driver. Some jurisdictions may want to *require* use of the *C-ITS* safety systems, as the lives, not only of the specific vehicle driver, but other road users, may be compromised/risked if a driver can chose to opt-out of the *C-ITS* service provision, depriving others of vital, life-saving information, and this places difficult dilemmas to the jurisdiction (that will be a matter of National decision, not the advice of an ISO TR).

As with ANPR technology, the privacy regulators of many jurisdictions rule that vehicle registration numbers, when collected by government authorities with the means to link those numbers to individuals' names and addresses, are likely to be personal information. This principle extends to *C-ITS* and regulators around the world are likely to come to the same opinion. The question will be whether the broadcast identity number can be linked back to an individual, either directly or through a process or data mining or matching. At the same time, if a service provider collects a vehicle's unique number but has no method to match that number to a vehicle registration or individual, then it is not the collection of personal information.

At issue is how easily, if at all, a *C-ITS* vehicle signal can be linked to a particular individual. In the event that genuine anonymity is not attainable, consideration should be given as to how privacy can otherwise be ensured.

4.4.4 Deployment models

The privacy impact of *C-ITS applications* will vary depending on the deployment model introduced for *C-ITS*. At a broad level, three options are available.

— **Opt-in model** – where consumers must explicitly purchase, or opt for *C-ITS applications* and, as part of this consumer choice, they accept the consequent privacy implications as part of the contract or access terms and conditions. While this approach may result in a lower take-up of *C-ITS*, and a smaller realization of the safety benefits of the technology, the opt-in model is the most privacy-friendly option.

— **Opt-out model** – where consumers purchase a vehicle and *C-ITS* would be operational by default, but with the ability to be switched off. Whilst this approach is likely to result in a higher uptake of *C-ITS* and consumers are still empowered to make decisions, they may not be as aware of their available choices and the resultant privacy implications.

— **Mandatory model** – where all new vehicles in the future are built with *C-ITS* and, potentially, all older vehicles are required to be retrofitted with *C-ITS*. This approach would provide the greatest safety benefits, but the privacy implications of *C-ITS* would become of much greater significance for the community, and the implementation issues, especially with regard to the existing fleet, would be very difficult.

In the event that *C-ITS* safety *applications* are incorporated into the mandated vehicle construction requirements (currently an option being considered in USA and Russia), they would effectively become mandatory as such features cannot generally be switched off or opted out of.

Opt-in and opt-out models are premised on consumers being able to make informed choices, which may not always be the case. A recent survey (see Reference [4]) in the US indicated that, while it did not stop consumers purchasing the technology, consumers are concerned about their location being tracked through their mobile phones, and that they do not feel they are given sufficient information about the use of this information. A separate report (see Reference [5]) concluded that *'privacy policies are hard to read, read infrequently, and do not support rational decision making*.' It found that, read in full, the number of online privacy policies that an average user encounters would require some 25 days a year to read.

In the limited circumstances where consent may be required under either opt-in or opt-out methods (for example, to disclose personal information for a secondary purpose), thought must be given to how a consumer will give their consent, which could be at the point of purchase (or sign-up) of either the *C-ITS* hardware or individual *application*s.

Subject to further consultation, technology and standards development, the opt-in model provides choice to the consumer and therefore is likely to be the most feasible approach to introducing *C-ITS* service provision into most markets. This method will significantly help mitigate the privacy risks. At a later stage, jurisdictions may consider mandate in respect of some specific service provisions, where this can be nationally justified.

However any changes to the adopted approach (such as a move towards mandating *C-ITS*) should include a re-evaluation of *C-ITS* compliance with the privacy principles.

5 C-ITS Actors and Privacy

5.1 C-ITS and jurisdictions

Despite the similarity of strategic policies and trade agreements, there can be no one global recommendation in respect of privacy, in that National and Regional jurisdictions have different perspectives, particularly concerning the balance between personal privacy and the safety of citizens. The sections below, identify some of the issues in the major trading regions of the world.

5.1.1 United States

At the time of developing this Technical Report, the US Department of Transportation is conducting a *C-ITS* pilot with a view to assess regulatory options, including mandatory *C-ITS* in new vehicles, and the department has funded the RITA 'Connected Vehicle' program. A recent statement from the US Department of Transportation, NHTSA 05-14, "*U.S. Department of Transportation Announces Decision to Move Forward with Vehicle-to-Vehicle Communication Technology for Light Vehicles*". "*….The U.S. Department of Transportation's (DOT) National Highway Traffic Safety Administration (NHTSA) announced today that it will begin taking steps to enable vehicle-to-vehicle (V2V) communication technology for light vehicles. This technology would improve safety by allowing vehicles to "talk" to each other and ultimately avoid many crashes altogether by exchanging basic safety data, such as speed and position, 10 times per second.*

"Vehicle-to-vehicle technology represents the next generation of auto safety improvements, building on the life-saving achievements we've already seen with safety belts and air bags," said US. Transportation Secretary Anthony Foxx ….

……. The safety applications currently being developed provide warnings to drivers so that they can prevent imminent collisions, but do not automatically operate any vehicle systems, such as braking or steering. NHTSA is also considering future actions on active safety technologies that rely on on-board sensors…….

…….. NHTSA will then begin working on a regulatory proposal that would require V2V devices in new vehicles in a future year, consistent with applicable legal requirements, Executive Orders, and guidance."

US DoT RITA has recommended nine privacy principles for 'connected vehicles', with a strong emphasis on anonymity *'secured, in part, through technical methods designed and built into [the system].'*

These privacy principles propose limitations on the use of information, which are relevant for discussions of compliance and enforcement issues. The US also has "existing legislation in the form of the Drivers Privacy Protection Act, which strictly governs the use and release of information by State motor vehicle authorities." Consent is not a feature of the proposed US privacy principles. A Mobile Device Privacy Bill has been introduced in the US Congress, proposing that all mobile phone data collection requires explicit user consent. The Bill has not, however, progressed at this stage.

The US Congress is also currently considering legislation that would make Event Data Recorders (EDRs), the equivalent of black boxes in aircraft, mandatory in new vehicles from 2015.

However, outstanding questions regarding ownership of EDR data remain. There are privacy concerns over how data in such devices might be used and who would have access to it. Currently the US sets minimum standards for EDRs and requires that manufacturers disclose to owners the existence of an EDR in the drivers' manual. However, these devices typically only retain the last few minutes/seconds before an incident. Whilst these devices are not strictly part of *C-ITS*, they are likely to play a part in monitoring the performance of the technology. There is also a growing trend overseas to use similar devices, measuring driving style and performance, for insurance purposes.

The US Supreme Court recently found in *United States v Jones* that the surreptitious use of GPS trackers on vehicles without a warrant by enforcement agencies was unconstitutional, although the court was split on whether this was because the placement of the GPS tracker constituted a search, or because the action impinged on expectations of privacy. A subsequent case, however, found that tracking location via mobile phone records was constitutional as the subject *'did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone.'* This apparent inconsistency between vehicle tracking and mobile phone tracking has received some criticism.

5.1.2 Europe

The privacy implications of *ITS* have been a strong focus within the European Union. The 'Privacy Enabled Capability in Cooperative Systems and Safety Applications '(PRECIOSA) project has developed guidelines aimed at ensuring that cooperative systems can comply with future privacy regulations and protect the location-related data of individuals.

PRECIOSA recommends:

(5.2.1) Privacy Analysis

Privacy analysis should allow for the evaluation of privacy protection properties at design time. Several different stakeholders perform privacy analysis. Consequently, every type of stakeholder has its own perspective, purposes, and privacy criteria. The purposes of the privacy analysis may include setting up privacy requirements to define privacy conformance system behaviour, evaluating systems to detect privacy leakages, to calculate metric values which serve as indicators for describing the privacy risk of using such systems, and checking whether an entity's behaviour conforms to a given set of privacy requirements.

According to the Privacy Impact Assessment (PIA),[21] *the purpose of the privacy analysis process is to create privacy-aware design specifications. The PIA process takes the perspective of legal authorities and project managers. The results of PIA are privacy requirements that take into account privacy regulations, privacy laws, and project requirements adapted to the application domain. These results are at a conceptual level which does not reflect technical interdependencies.*

Formal methods for privacy analysis are mostly based on languages which describe technical systems. The purpose is to provide a formal defined vocabulary to avoid ambiguity, to make domain assumptions explicit, to prove properties of a solution, and to explore the design space. Different languages (mostly logic based) and mechanisms (e.g. model checking or system simulations) exist which can be used to provide (semi) automatic evaluation and verification of systems. Technical privacy requirements involve system-specific properties but often fail to integrate high-level privacy requirements that include privacy regulations or stakeholders' interests.

Current research activities focus on improving existing mechanisms of privacy analysis, and some of them try to integrate the different perspectives into a holistic approach. Such approaches try to create a privacy recognition cycle which in one direction injects privacy criteria into a system, while the opposite direction evaluates system behaviour and properties to calculate privacy indicators, as seen in Figure 1.

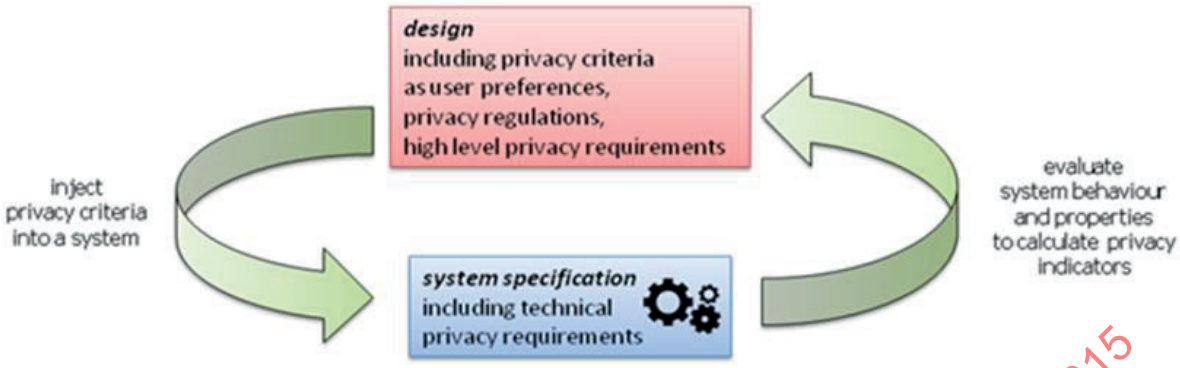

Figure 1 — (Preciosa): Privacy Recognition Cycle

To adequately implement privacy criteria of different stakeholders, high level privacy criteria (described in the language of stakeholders as data subject and data controller) must be translated into technical requirements which can be analysed and implemented by formal methods and tools such as PETs. Currently, the process of translating high level requirements (such as the results of a Privacy Impact Assessment) into technical requirements is poorly understood. There exist several challenges to translate descriptions from one language into another because the languages address different purposes and thus have different techniques of expression and focus on different aspects. Thus, while performing the translation process, some details of the original description are often lost. Such effects must be taken into consideration with the guarantee that they do not affect the intended purposes. To address these challenges, promising approaches create a shared understanding of the privacy domain by creating standard definitions in form of models and ontologies. We may use these standards to extend the existing analyses by integrating requirement engineering mechanisms, best practices, design patterns, and other well-understood techniques.

Privacy Evaluation

Privacy evaluation must take place at least at three levels.

— A user-centric vision must be provided which will allow the end user to have an understanding of possible privacy profiles and to evaluate whether it matches his own preferences. This will involve initiatives for creating public awareness and initiatives for defining and standardising profiles, with the notion of default values in order not to harass users with too many on-the-spot warnings.

— An engineering-centric vision where existing ICT-based systems can be evaluated. This involves evaluating the process, i.e. verifying that systems are designed with the right methodology. Further privacy protection profiles could also be defined, and evaluation could ensure that a given implementation conforms to well-established profiles. A specific problem that needs to be addressed is incremental evaluation, i.e. how to evaluate individual subsystems and then evaluate the integration of these systems.

— A business stakeholder vision where the roles of the data controller and the data processors must be clearly analysed and evaluated. The problem here is the transfer of liability between stakeholders.

On top of this is the problem of privacy metrics. There is no general consensus how the level of privacy experienced by a person should be quantified and measured. This would be a pre-requisite for comparing different approaches and evaluating if investments in privacy protection are well spent.

PRECIOSA recommends a model based engineering approach.

— Privacy analysis could involve a formal verification process, leading to some proof-related artefacts. An artefact is an artificial product or effect observed in a natural system, especially one introduced by the technology used in scientific investigation. For instance, a relevant artefact for embedded systems is time or a resource constraint.

— An engineer could carry out the Privacy by Design process sketched above, leading to privacy by design artefacts.

— An *ITS application* engineer could apply his own *application* development process.

— Vertically, MDE would ensure the integration consistency of the artefacts.

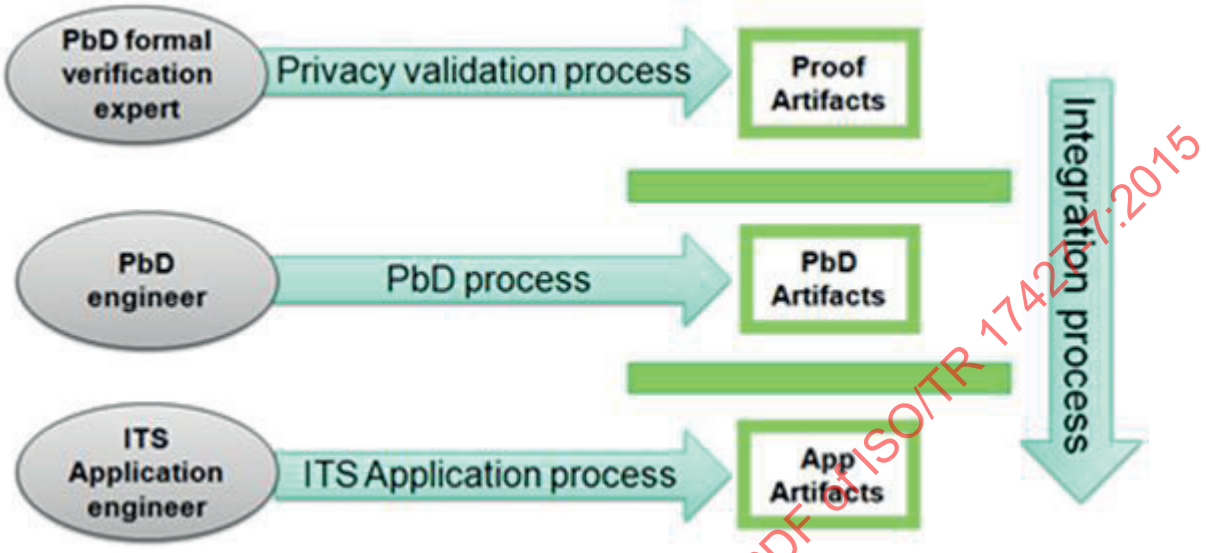

Figure 2 — (PRECIOSA): Model-Driven Engineering Vision

The European Union Directive setting out the framework for *ITS* deployment includes specific provisions for both privacy and liability. Article 10 concerns privacy and directs Member States to ensure that personal data are protected against misuse, including unlawful access, alteration or loss. The use of anonymous data are encouraged, where appropriate, and personal data shall only be processed when it is necessary for the performance of *ITS applications* and services.

The European Data Protection Supervisor issued an opinion on the EU draft directive which noted the importance of identifying who the data controllers will be to ensure that privacy and data protection considerations are implemented at all levels of the chain of processing. The opinion also stressed the importance of establishing principles of 'privacy by design' and data minimization, ensuring that the personal data processed through interoperable systems are not used for further purposes that are incompatible with those for which they were collected.

Further, a new data protection study was launched in December 2011 aiming to assess the importance and impact of data protection and privacy aspects in the areas and actions of the '*ITS* Action Plan' and '*ITS* Directive'. The final report of the study is yet to be completed.

5.1.3 Australia

Privacy principles in Australia are governed by a mix of Commonwealth and State laws and regulations. While there are relevant differences across Commonwealth and State-based privacy principles that are explored below, the treatment of privacy is largely consistent across jurisdictions with a principles based approach adopted. In general,

— Commonwealth agencies are subject to the Commonwealth Information Privacy Principles (IPPs),

— most private sector organisations are subject to the National Privacy Principles (NPPs) under Commonwealth legislation, and

— State agencies are subject to their respective State privacy regimes, generally contained in State-based IPPs.

The NPPs will be particularly relevant to *C-ITS* given that this is an industry-led development, but State-based privacy principles will apply to State road agencies.

The Privacy Act distinguishes between personal information collected by private sector organisations and personal information collected by public sector agencies. The NPPs apply to private sector organisations and the IPPs apply to public sector agencies and are the federal equivalent of State-based IPPs. As a general rule, a Commonwealth or Australian Capital Territory (ACT) agency would apply the IPPs under the Privacy Act, while State-based public sector agencies would apply their own privacy legislation; private sector organisations – regardless of which Australian jurisdiction they operate in – would generally apply the NPPs.

A notable exception, however, is when a private sector organization is undertaking the collection of personal information under contract, or on behalf of, a State-based public sector organization. In this circumstance, the State-based IPP may apply rather than the NPPs. This will be relevant in a number of circumstances in the area of transport. Public-private partnerships for toll roads, for example, have raised challenging issues over whether privately operated roads are subject to Commonwealth or State jurisdiction.

Importantly, if the collection of personal information by an agency or organization is within the law and is necessary to undertake its functions, the privacy principles do not prevent that collection and use, but set out guiding principles in the way in which that personal information is collected and used. There are 10 NPPs that regulate how private sector organisations manage personal information. They cover the collection, use, disclosure and secure management of personal information. They also allow individuals to access that information and have it corrected if it is wrong:

— An organization must not collect personal information unless the information is necessary for one or more of its functions or activities.

The privacy principles do not prescribe under what conditions or circumstances the collection of personal information is necessary. Therefore what can be collected, as opposed to how the information is collected or used, is very broad in scope given that private sector organisations self-assess what personal information is required to undertake any of its functions or activities:

— At, or before, the information is collected, the organization must take reasonable steps to ensure that the individual is made aware of
  - the identity of the organization and how to contact it,
  - the fact that he or she is able to gain access to the information,
  - the purposes for which the information is collected,
  - the organisations (or the types of organisations) to which the organization usually discloses information of that kind,
  - any law that requires the particular information to be collected, and
  - the main consequences (if any) for the individual if all or part of the information is not provided.

This is considered in Australia to be an essential privacy principle, for only by being aware that this information is being collected about him or her can an individual seek to access, correct or challenge the collection of that information.

The organization must collect the personal information directly from the individual or, if not, take reasonable steps to ensure that the individual is aware of the matters listed above.

For *C-ITS*, point of purchase (or sign-up) is considered to be probably the most logical juncture for organisations collecting or accessing personal information to inform the individual that they are doing so.

Consent by the individual of the collection of personal information for a primary purpose, whether express or implied, is not required by the NPPs. Where the personal information has already been collected for another reason (the primary purpose), a private sector organization may nonetheless use

or disclose personal information for certain secondary purposes. For example: if the secondary purpose is related to the primary purpose of collection, then the individual has consented, or if the personal information is used for direct marketing, public health or law enforcement.

5.1.4 Other countries

Summaries may be added at a later date.

5.1.5 International Standards

In 2009, the International Organization of Standardization (ISO) released ISO/TR 12859, a Technical Report that summarizes international privacy requirements (standards and legislation) which will affect intelligent transport systems.

5.1.6 Privacy and governments

5.1.6.1 Introduction to the issues

The Information Privacy Principles (IPPs) adopted by the regulations of jurisdictions, regulate the collection, use, disclosure, security and access of personal information by public sector entities, including police and road agencies. While terminology and form vary from jurisdiction to jurisdiction, the general approach across jurisdictions is consistent. Namely, a public sector agency must not collect personal information unless the information is collected for a lawful purpose that is directly related to a function or activity of the agency, and the collection of the information is reasonably necessary for that purpose.

The challenge for policy makers is that not every jurisdiction has these additional privacy protections, so they cannot be uniformly relied on in an internationally consistent approach, and as vehicles are mobile and can move between jurisdictions, *C-ITS* is intrinsically international.

It also remains to be determined the extent to which road agencies' roles and responsibilities in relation to *C-ITS* will overlap with registration, licensing and enforcement functions, the handling of *C-ITS* certification or other *C-ITS* identification data, by, or under the control of the same Government department, would be a cause for concern in respect of privacy protection.

5.1.6.2 Surveillance laws and the privacy principles

The applicability and inter-relationships between the various privacy regimes and the surveillance laws that have been introduced across jurisdictions can be complex and require further explanation. Put simply, privacy laws do not set limits on, or define, what can be collected. Under the privacy laws the collection must simply be "not unlawful," or "not unfair" or "not unreasonable" or required to undertake the legal task. While the phrasing changes in each jurisdiction, it is clear that most privacy laws are concerned with what happens to the personal information once it is collected – for example, how it is used and secured, who it is disclosed to and how it is discarded. The surveillance laws, on the other hand, are not focused on what is done with the personal information once it is collected, but on the legality of the collection itself. The surveillance laws of a jurisdiction therefore serve as a gateway to ensure that a device is not used for covert surveillance purposes. In this sense, the privacy and surveillance regimes are complementary.

Further to this, surveillance laws can be separated into two distinct groups: (a) laws which set out conditions for jurisdiction enforcement agencies to use surveillance devices to track locations and to listen to conversations (see 5.1.6.1), and (b) laws which are much broader and prohibit covert surveillance of any person and by any public or private entity.

One of the challenges for *C-ITS* is that, once the data exists, if it can be legally accessed by an enforcement agency it is for the courts to determine whether the data is relevant and reliable and therefore admissible. Policy-makers must therefore understand the circumstances in which governments could legally access the *C-ITS* data today. The evidentiary value of the data is/are also to be determined.

Whether those circumstances will be a disincentive to consumers, which in turn would reduce uptake and curb the attainable safety benefits is a significant, and as yet unanswered, question.

Privacy by design, and where practicable, anonymisation, remain the primary safeguards. What the community is prepared to accept in return for increased safety and productivity (including reduced congestion) is, however, a factor that legislators also need to take into account when trying to establish a balance between personal privacy and benefit to the community.

If individuals can be identified in some way via the data message broadcast by *C-ITS*, jurisdictions should consider legislative provisions to limit access to *C-ITS* information for enforcement purposes. Such provisions should set out the circumstances in which police, or another enforcement agency, should seek an access warrant by court order to obtain *C- ITS* information, in addition to information sharing provisions, and establish a procedure and conditions for the issue of such warrants. Legislation could also explicitly state in what circumstances a warrant is not required by an agency (e.g. for non-enforcement purposes, such as traffic management, provided appropriate safeguards are in place).

5.1.6.3 Surveillance device legislation

The definition of a surveillance tracking device is largely consistent across jurisdictions. But as a general rule, the surveillance laws will not apply if the subject of the tracking device, or the person controlling the object being tracked, provides his or her consent.

Surveillance Devices legislation differs from jurisdiction to jurisdiction, but typically 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.*"

The variations between the jurisdictions are small but notable. For example, in some jurisdictions, the prohibition on the installation, use and maintenance of a tracking device does not apply when the tracking device is for a lawful purpose; while in other jurisdictions *'require that a person must not knowingly install, use or maintain a tracking device to determine the geographical location of a person or a vehicle or thing without the express or implied consent of the owner, or a person in lawful possession or control, of that vehicle or thing.*' However, in some jurisdictions there is no explicit nor specific legislation in place to cover these aspects.

Where a 'privacy by design' approach that anonymises *C-ITS* signals is not feasible, alternative means to establish implied or express consent should be investigated. In circumstances where identification data and location data can be matched without the consent of the owner, it is clear that this information could be used to track the location of individuals and would be in direct contravention of surveillance laws. It is argued that community acceptance of *C-ITS* will be significantly reduced if the surveillance laws are amended to exempt *C-ITS* in such a way that undermines the spirit and intent of those laws.

Consent to use pre-existing technologies (such as an IP or MAC address) will be particularly challenging given that the owner of a *C-ITS* device could be any person in the vehicle – not necessarily the driver – and the IP or MAC address could be accessed without an *application* to enable *C-ITS* functionality (which could have provided an interface to secure consent from consumers).

5.2 C-ITS and road operators/managers

5.2.1 Jurisdictions

Jurisdictions should explicitly consider privacy impacts on drivers in any decision relating to institutional arrangements for *C-ITS*. Regardless of current good intent, history has shown that jurisdictions can be coerced into misuse of data held concerning its citizens. As a preventative measure, but also to make public acceptance more easy to achieve, any entity that manages and stores unique identifiers should be separate from agencies which hold licensing and registration.

5.2.2 'Core' systems

A critical factor driving the conceptual view of the 'Core System' and the entire '*connected vehicle-highway system*' environment is the level of trustworthiness between communicating parties. A complicating factor is the need to maintain the privacy of participants, but not necessarily exclusively through anonymous communication. From the US perspective, the 'Core System' is planning anonymity into the trusted exchange of data, using the existing privacy principles (VII Privacy Policies Framework version 1.0.2) as guidelines, and balancing privacy against security and safety.

While 'Core System' are being planned for anonymity – privacy by design, they are also providing a foundation from which to leverage alternative communications methods for non-safety *applications*. These alternatives are typically available on the market today and the levels of anonymity and privacy inherent to these systems are typically governed by agreements between communication providers and consumers. So, while privacy is not compromised for an individual, what happens between that individual and their communication provider (e.g. 3G service provider) very well may compromise privacy. Some *application* providers may require personal information in order to function which would require the *application* user to opt-in to use that *application*.

See also the following:

ISO/TR 17427-2, *Intelligent transport systems - Cooperative ITS — Framework Overview*

ISO/TR 17427-3, *Intelligent transport systems - Cooperative ITS — Concept of operations (CONOPS) for Core systems*

ISO/TR 17427-4, *Intelligent transport systems - Cooperative ITS — C-ITS Minimum system requirements and behaviour for core systems*

5.3 C-ITS and manufacturers

C-ITS equipment providers and system designers will need to make clear any limitation on information being provided and may need to ensure that commercial features do not conflict with safety features. They will need to respect the provisions summarized in 4.3, and respect local privacy regulations. In particular, vehicle instruction manuals and any documentation needs to be clear and explicit, written in terms comprehensible to most people, and not buried among other general provisions. Where opt-in or opt-out provisions are made, they must be clear and simple to follow and make selection, and must not be part of a 'bundle' of provisions accepted en-bloc, where the privacy opt-in or opt-out acceptance and procedures are not explicit and clear to the user.

5.4 C-ITS information/application service providers

The private sector is already harnessing personal information for commercial *ITS* purposes. For example, navigational systems are available on the market that provide consumers with live traffic updates based on the consolidation of the location and speed of other users of the commercial *application*. In these situations, consumers voluntarily opt-in to a commercial *application* and thereby agree to share their personal information for these purposes, and providers must handle their personal information in compliance with existing privacy regulations.

Applications based on *C-ITS* technology are likely to operate within the same privacy framework.

C-ITS application service (2.2) providers and information service providers will need to make clear any limitation on information being provided and may need to ensure that commercial features do not conflict with safety features. Their systems in operation will need to respect the provisions summarized in 4.3, and respect local privacy regulations. Where opt-in or opt-out provisions are made, they must be clear and simple to follow and make selection.

Where *C-ITS* is a requirement of a service provision (for example, car insurance), these issues must be made explicit to the user and a positive assent process undertaken (opt-in).

5.5 C-ITS, drivers and vehicle owners

While equipment and manufacturers have reasonably clear responsibilities, outlined above, the vehicle owner must also have the responsibility to appraise himself of properly declared opt-in or opt-out provisions.

The situation for drivers other than the owner of the vehicle is much less clear and needs more attention. For vehicles under contracted hire, this will presumably be made clear in the rental contract, although how this is not lost in the many provisions of contract agreements needs to be addressed.

In the case of a vehicle driven by a relative or acquaintance of an owner, the position is much less clear. Presumably, by borrowing a vehicle he/she assents to the conditions that that vehicle is normally driven under. Though this probably needs to be clarified in law.

Also, ridiculous as it may sound, the position of a thief who steals and drives away a vehicle may also need to be clarified in law. It would be unfortunate if, through lack of clarity in the law, a thief, apprehended because a *C-ITS* system enabled the vehicle to be tracked and located by police, could claim in his/her defence that as he/she had not assented to the vehicle that he/she had stolen being tracked, providing personal information via the *C-ITS* system had violated privacy regulations, thereby violating his/her privacy, so a judgement against them would be based on inadmissible evidence.

5.6 Further reading

Further considerations on general aspects concerning privacy can be found at

http://www.oecd.org/sti/ieconomy/privacy.htm

5.7 Aspects relating to probe vehicle information services

In 2010, the International Organization of Standardization (ISO) published ISO 24100, an International Standard that specifies the basic rules to be observed by service providers who handle personal data in probe vehicle information services, and the reader with specific interest in probe data and its use in ITS is advised to read this document

6 Policy questions and approaches

6.1 Is specific regulation required for C-ITS?

A threshold question is whether any further regulation is required to protect personal information collected by *C-ITS*. Internationally required privacy principles (see above) would appear to sufficiently meet this objective in the first instance, although there may be some complexity in the implementation of *C-ITS* in particular circumstances, particularly where *C-ITS* is required by legislation of the jurisdiction. Other options could also be examined, including industry codes, guidelines or education campaigns.

It will be necessary to determine to what extent anonymity can be built into each and every instantiation of a *C-ITS application*, in particular the signals generated by private vehicles. This is both a technical and policy question: the breadth and limitations of the technology will shape and determine the appropriate policy response.

The following options are proposed for discussion by jurisdictions and those instantiating *C-ITS* service provision. It is noted that a combination of approaches may be recommended

6.1.1 Option 1: Continue current approach

Existing privacy principles have been in place for a number of years and have already been applied to a wide range of technologies. *C-ITS* is about the provision, exchange and use of data to perform a service for a service recipient (see ISO 17427-1). The laws regarding data protection have been established in most countries for many years. There is nothing that singles out the privacy aspects of *C-ITS* data as being

technically any different from the privacy aspects of any other data. Some stakeholders have suggested that these principles can readily be applied to *C-ITS applications*, and that industry and government can manage the impact on privacy of individual products and services that may be offered. However this could result in inconsistent implementation and potentially negative perceptions of *C-ITS* technology.

6.1.2 Option 2: Privacy code

Privacy codes – approved by a privacy commissioner – could be introduced by jurisdictions to amend the principles as they relate to a specific sector; creating an effective exemption without changes to privacy laws. It may be that moving to using codes of practice would provide more flexible industry-specific options. Such codes of practice would need to be recorded in a register of approved codes of practice. However, these have not always proven successful and have a number of important limitations, for example, State agencies in some jurisdictions may not be obliged to subscribe to them.

Further, until the system technology specification and governance arrangements are settled, it is not evident what a *C-ITS* Code would provide industry and consumers with a level of comfort that is not already provided by the existing privacy principles.

6.1.3 Option 3: Provide guidance on best practice

Working with privacy commissioners, *C-ITS* guidance material could be provided to governments and industry, including manufacturers, service providers, enforcement agencies and record keepers. This may also involve recommending that organisations conduct privacy impact assessments before implementing *C-ITS applications*. Utilizing best practice from within the transport technology sector, such as road tolling, guidance material could assist industry to understand how to apply the privacy principles. Guidance could include establishing purpose, information use and disposal practices, security, disclosure to third parties and secondary uses.

Guidance could also be provided on appropriate processes for gaining consent of individuals where required.

6.1.4 Option 4: Legislate C-ITS governance arrangements and use of information

To build confidence in the privacy and security of *C-ITS*, regulations could be introduced to fully separate collection and storage of vehicle activity (the *C-ITS* service provider) from the entity that holds information linking the unique identifier to a vehicle registration number or any other personal identifier. Such a governance arrangement would recognize that, for the most part, the identity of vehicles is not necessary for effective *C-ITS* and in circumstances where this information could assist with law enforcement activities a warrant, or jurisdiction specified procedure, would be required.

6.1.5 Option 5: Legislate technical standards to protect privacy

If Standards develop a 'privacy by design' approach that normally provides anonymity, then these technical standards could be incorporated into relevant transport legislation in order to guarantee their adoption and service provision where anonymity could not be guaranteed would be dealt with as exceptions, with specific privacy protection measures made explicit.

Enforcing standards of anonymisation, if feasible, will likely offer the best solution for protecting privacy.

6.1.6 Option 6: Match and copy mobile phone privacy measures

Cooperative ITS (2.3) messages will be sent via a range of media, including, and may be principally, especially in early years, via cellular telephone communications. 5,9 GHz will also be used, but in the early stages its use will be V2V and a limited number of hot-spots.

Cellular wireless communication (GSM, UMTS, E-UTRAN) are wireless technologies that are used globally, IEEE 802.16 and IEE 802.20 are wireless mobile broadband technologies that are also used in a widespread manner in many countries. Both are already covered by the requirement to comply to existing privacy regulations.

It would seem incongruous, impractical, and potentially legally challengeable if *C-ITS* wireless transmissions over cellular communications were subject to different privacy regulations that already exist for these wireless media.

The sixth option is therefore that the wireless communications aspects for *Cooperative ITS* privacy should therefore simply be aligned with those for any other cellular wireless communications, and that the '*application*' aspects are already covered by data protection laws in almost every country of the world.

This would require little or no new legislation, and simple statements as to these requirements in *C-ITS* standards.

7 Summary of findings

7.1 General

The seriousness of the privacy risk will depend on the anonymity of *C-ITS* signals and how readily (if at all) the unique identity for a signal could be linked back to an individual. If, for example, a road agency were able to link a unique identity (or collection of identities), via the certificate authority, to registration information and signals were being tracked by that road agency across the network, then this would represent a significant privacy issue. However, the standards and processes that govern these signals are still evolving, thus only qualified answers can be suggested at this stage.

The decision as to which, or which combination, of the privacy regulation strategic options (see 6.1) are appropriate will be a matter determined by the relevant jurisdiction and its governance. This Technical Report can only recommend that an absolute minimum would appear to be

a) adoption of 'privacy by design' in *C-ITS application service* system design,

b) anonymity should be the expected norm, and where this is technically or practicably not possible, then rules for privacy should be explicitly specified,

c) all privacy protection regulations should be respected (e.g. Avoidance of harm; Fairly and lawfully, Specified, explicit and legitimate purposes; Explicit and legitimate and must be determined at the time of collection of the data; Not further processed in a way incompatible with the purposes for which it was originally collected ; Not be disclosed without the consent of the data subject; Adequate, relevant and not excessive in relation to the purposes for which they are collected; Accurate and, where necessary, kept up to date; Identification of data subjects for no longer than is necessary for the purposes for which the data were collected; Restricted to those who have a demonstrable 'need to know'; Clear and accessible the fact that personal information is being collected including: the purposes for which personal information is being collected; the types of persons or organizations to whom personal information might be disclosed; the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information,

d) security safeguards: Cumulative interpretation of multiple recommendations-the recommendations cannot just be taken individually in isolation, but the combination of the recommendations may infer interpretations (see 4.3 for more detailed summaries),

e) wireless communications should at least adopt measures equivalent, and preferably at a minimum, the same as those regulating cellular wireless communications networks,

f) wireless communications should only be more stringent than (d) where the threat to privacy is identifiably greater than that for other data carried over cellular wireless communications networks,

g) application service privacy should be covered by the same data protection and privacy regulations as any other IT service, and

h) except where a jurisdiction mandates the installation of *C-ITS* service provision because of the societal and/or safety of life benefits, the user should preferably have the choice to 'opt-in' to