Designing Privacy-Aware Intelligent Transport Systems: A roadmap for identifying the major privacy concepts

Christos Kalloniatis[1], Dimitris Kavroudakis[2], Amalia Polidoropoulou[3] and Stefanos Gritzalis[4]

[1,2,3,4] **University of the Aegean, Greece**

Abstract

Intelligent Transport Systems (ITS) play a key role in our daily activities. ITS significantly improve mobility offering a variety of services to a vast amount of users that increase on a daily basis, as more and new services are introduced. These services are based on advanced Information and Communication Technologies (ICTs) and rely strongly on connectivity and computing resources. However, technical vulnerabilities of the technologies used in ITS, as well as the increase in users' awareness has brought security and privacy concerns to the forefront. This paper aims at identifying a set of privacy concepts that provide the bases for designing trustworthy ITS services identifying possible threats and users privacy concerns. A key contribution of the paper is a roadmap that presents in detail how for every ITS function corresponding privacy concepts can be realized for overcoming specific threats and users' privacy concerns in a smart city context.

Keywords: Intelligent Transport Systems, Security, Privacy, Threats, Privacy Properties, Services, Design, Software Engineering

Introduction

Intelligent Transport Systems (ITS) play an important role on contemporary smart cities by allowing for smart solutions such as information services provision; management of transport flows; traffic and vehicle surveillance; intelligent revenue systems; and intelligent infrastructure that allows for connectivity/communication (V2I, V2V). Privacy is a key component of smart cities as ITS affect a number of citizen's activities. For example, travelers generate massive quantities of detailed individual/ activity/ travel/ location information through a variety of channels (payments, subscriptions, social media, mobile Apps, internet cookies, etc.). This increases the exposure as well as the possibility of inappropriate use of individual information, raising severe concerns on data privacy, protection and security. The value of privacy in the context of mobile devices and mobility has been discussed in the work of Antoniou and Polydoropoulou (Antoniou et al., 2015). There is a trade-off that needs to be considered as additional personal information can improve quality of services but on the other hand this may lead to violation of users' privacy.

This paper attempts to shade light in the aspects of ITS which may be vulnerable to privacy violations and will contribute to the debate about ITS adoption by smart cities. Section 2 provides a brief overview of Intelligent Transport Systems and their significant role in Smart Cities. Section 3 presents the privacy properties a modern ITS should realize in order to provide trustworthy services to its users. The privacy properties are suggested after a clear discussion and linkage between the ITS main functional characteristics, technical functional services, indicative solutions used widely for the implementation of these services, thirteen identified privacy threats and respective privacy concerns expressed in the literature regarding the use of ITS services and their impact on users' privacy. Our previous work on cloud computing assisted a lot in the identification of the respective privacy properties since the nature and architecture of cloud environments are very similar to the ITS environments. Section 4 identifies a number of privacy requirements that ITS systems should implement for raising the users' trustworthiness. Section 5 concludes the paper and highlights directions for further research.

Smart Cities and Intelligent Transport Systems

Smart cities

The concept of smart urban spaces originated from the time when cities started facing problems of efficiency in sectors such as transport, health and environment. Smart cities are cities that utilise information and technologies for effective and intelligent usage of resources resulting in cost and energy savings, improved quality of life and reduced environmental footprint (Cohen, 2011). The concept of smart city is not static but rather a process by which cities become more liveable, resilient and responsive to new challenges. Recently a rising number of papers address issues regarding smart cities. Neirotti et al. (2014) present current trends in Smart City initiatives. Kramers et al. (Kramers et al., 2014) explore ICT solutions for reduced energy use in cities. Al-Hader et al. in (Al-Hader et al., 2009) discuss about development and monitoring of smart-city infrastructure. Nuaimi et al. in (Nuaimi et al., 2015) analyse applications of Big Data to smart cities while Batty in (Batty, 2013) and Goulias in (Goulias, 2015) set the case for big data in smart cities and city planning. Kavroudakis in (Kavroudakis, 2015) presents a methodology for constructing micro-data for smart decision-making. Furthermore, in (Kavroudakis et al., 2012, 2013) Kavroudakis et al. demonstrate the use of spatial microsimulation approaches for understanding population inequalities for smart policy evaluation in a smart city context.

ICT & Mobility

The rapid advances of Information and Communication Technologies (ICT) over the last decade as well as the introduction of mainstream mobile devices pushed innovation and smart solutions in cities across the world. That advances help overcome restrictions over space and time, while enabling faster and efficient transmission of data and information.

Smart mobility approaches are key components of smart cities. Actuators (sensors) measure, sense and observe transport conditions in any part of a city. Advanced communications allow people and systems to be interconnected and interact in entirely new ways. Finally, intelligent analytics are used to offer fast and accurate responses to changes and optimize future conditions.

Social networks and social media are also a vital part in gathering information regarding mobility in urban areas. Recent research focuses on social networks and detection of transportation information social network effect on travel choices (Goulias et al., 2015; Kamargianni et al., 2014; Lee et al., 2015; Ueno et al., 2012) uncovering patterns of inter-urban trips and spatial interaction based on "check-in" data (Kamargianni et al., 2014; Lee et al., 2016; Liu et al., 2014).

Smart Cities, Privacy and Security

Smart City and Intelligent Transport Systems

ITS development over the last decades has been based on the rapid evolution of information technologies, which include processing capabilities, availability of hardware and communication technologies. Contemporary IT approaches contribute towards real time monitoring and real time adjustments in a transportation network. Also, with the use of data mining and predictive modeling it is possible to estimate (to a certain extent) transportation flows and congestions. Recently, with the advances of Internet of Things (IOT) and the v*ehicle-to-vehicle* (V2V) communication systems, vehicles are able to communicate to each other sharing information regarding safety. The very same technologies could be used for sharing of congestions which make the vehicle part of an ITS as a producer/consumer of data and information in a smart city context.

In the literature of Intelligent Transport Systems there is a growing number of applications regarding smart city services. These services include traffic monitoring (Kamijo et al., 2000) and management (Papageorgiou et al., 2003), congestion management (Gomez-Ibanez et al., 1994) , road usage charging (Jones, 2003) emergency response (Martinez et al., 2010), public information systems (Huber, 1995), smart parking (Polycarpou et al., 2013) and integrated traffic light management (Salama et al., 2010).

ITS as part of a smart city infrastructure, help citizens to make more informed choices regarding public transport, driving and navigation. Also, ITS contribute on the increase of a city's accessibility by providing means of ensuring availability and transport capacity when and where needed. There are also cases where ITS help planning for resilience against natural and man-made threats. ITS services contribute in decision-making and planning in a smart city context by making better use of existing transportation infrastructure and multi-modal planning within existing economic corridors. Mobility as a service is a central topic of smart city efforts as it uses best transport options for individual needs based on convenience, time-to-destination, sustainability and comfort (Kamargianni et al., 2016). In a smart city context, ITS appear to have an important role regarding smart mobility applications. These applications contribute towards connectivity, cooperation and automation of passengers, transportation means and infrastructure.

Intelligent Transport Systems Architecture

ITS architecture has some common elements with other contemporary IT systems such as Cloud computing. Some of these characteristics are the following:

a) *Agility*, which improves users' ability to re-provision technological infrastructure resources. In the ITS context this may be the re-usability of data management and analysis infrastructure which could be used by different agencies for a variety of analysis.

b) *Cost Reduction*, which is reduced since infrastructure is typically provided by a third party and does not need to be purchased for one-time or infrequent intensive computing tasks. Also, the cost of IT skills is lowered since in-house implementation is avoided (IDC, 2008). In the ITS context the decentralization of infrastructure provision help in reducing costs and is based on the idea that specialized agencies can offer better services than a central all-in-one agency.

c) *Virtualisation*, which is the basic technology used in cloud environments allowing servers and storage devices to be shared thus increasing utilization. Applications are usually being migrated from one server to another depending on the capacity and usage of the cloud providers' infrastructure. In the ITS context where traffic data and transportation flows generate substantial amounts of data, virtualization is a key concept for data storage and capacity efficiency reasons.

d) *Multitenancy*, which enables the sharing of resources and cost across a large pool of users allowing centralization of infrastructure, increment of peak-load capacity and systems' utilization and efficiency improvement (Hof, 2006). ITS require sharing of resources across users/agencies for efficient decision-making. Multitenancy could be a valuable aspect in a ITS as this could enable the sharing of resources for efficiency reasons.

e) *Reliability*, which is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery (King, 2008). In an ITS context, reliability is a key aspect as services continuity is important for reduction of system unavailability which may lead to potentially dangerous lack of information.

f) *Scalability* and *elasticity*, which support the on-demand provisioning of resources on a fine-grained self-service basis near real-time without users having to engineer for peak loads (Shawky et al., 2012). As cities grow, the number of potential users for an ITS is growing. Seasonality of transport flows due to unforeseen circumstances (natural or man-made) may also affect transportation flows. This elastic relationship between population and ITS ask for automatic scalability solutions of such systems. Scalability and resilience of ITS systems over time and geographical space is essential.

g) *Device and location independence*, which support users to access cloud services from anyplace through a web-browser regardless of the device they are using or the location they are accessing the service from (Farber, 2008). In an ITS context, users may access services from a variety of devices. It is important to provide equal opportunities to all citizens for information access regardless OS and hardware choices.

h) *Maintenance,* which is easier since there is no software installation on each user's machine and the services' sources are managed and updated from single third party.

The role of privacy in ITS

ITS Services and Technical Functionalities

Intelligent Transport Systems operations are based on distributed environments and usually insecure networks for exchange of information etc. Privacy threats in distributed environments have been discussed by many researchers since the nature of the network and the lack of confidentiality are usually the main challenges that generate the security and privacy implications.

In order to identify the privacy challenges in ITS first it is important to mention the main categories of user services an ITS is providing. Based on (Glancy, 1995) the following seven common areas exist which group the offered user services in ITS:

- *Travel and Transportation Management*, which includes services related to in route driver information, route guidance, traffic control, etc.
- *Travel Demand Management*, which includes services like Pre-Trip travel information, trip demand management and operations, etc.
- *Public Transportation Operations,* which includes public transportation management services, personalized public transit services, etc.
- *Electronic Payment*, which includes all services and supporting functionalities related to e-payment
- *Commercial Vehicle Operations*, which includes services like automated roadside safety inspection, hazardous materials incident response, etc.
- *Emergency Management*, which includes services like emergency vehicle management, emergency notifications, etc.
- *Advanced Vehicle Control and Safety Systems*, which includes mostly safety services like Collision avoidance, pre-crash restraint deployment, etc.

For implementing the aforementioned user services an ITS must satisfy and offer a number of functionalities in a more technical way. The aforementioned group of services may require the support of more than one of the following functionalities in order to be offered to the users. The main technical functionalities of an ITS are (Glancy, 1995) :

- *Traffic Surveillance*, which includes technologies that collect information for the traffic stream.
- *Vehicle Surveillance*, which includes technologies that collect information about the vehicle per se like location, speed, etc.
- *Inter-Agency Coordination*, which includes technologies for connecting the ITS parties with collaborative agencies like Police, Weather Stations, etc.
- *Payment Systems*, which includes technologies for enabling electronic transactions between the user and the provider
- *One-Way Mobile Communications*, which includes communication technologies that only, transmit information to mobile reception sites.
- *Two-Way Mobile Communications*, which includes technologies like the One-Way Mobile Communications but in this case it allows receipt of information from the remote sites as well.
- *Stationary Communications*, which include technologies that physically connect stationary sites.
- *Individual Traveler Information*, which includes technologies that through specific devices provide targeted information to users.
- *Message Displays*, which includes technologies that allow the broadcast of messages to multiple users, central signs etc.

- *Real Time Traffic Control*, which includes technologies that allow the control of the traffic flow in real-time through traffic signals, reversible lane designation etc.
- *Navigation,* which includes technologies for determining vehicle position in real time
- *Database Processing,* which includes technologies for data storage, handling and manipulation for sharing among other platforms.
- *Traffic Prediction,* which includes technologies for processing data in order to predict future traffic flows
- *Traffic Control*, which includes technologies for controlling actual traffic flows, rerouting due to incidents, optimal routes etc.
- *Routing,* which includes technologies for calculating the optimal routing for given drivers, vehicles, paths, etc.
- *In Vehicle Sensors,* which includes technologies for monitoring the vehicle status, performance, obstacle avoidance, etc.

Table 1 presents a matching of the aforementioned types of services with the service categories described above. Some indicative implementation examples are provided in the table as well in order to assist in the identification of the respective privacy properties that need to be addressed for designing trustworthy ITS services.

Privacy Threats in ITS

In our previous study (Kalloniatis et al., 2014) the identification of the major threats on cloud computing were identified. The applicability of the specific set of threats is examined in the context of ITS. The main conclusion is that ITS share the same threats as cloud services since they share almost the same architectural patterns and implementation solutions. This can be also verified via the majority of cloud-based services that provide ready-to-implement solutions for ITS and Smart Cities Systems in general. It is important to indicate that most of these threats are not ITS specific but have an impact on most cloud based or traditional distributed systems. We have focused however our discussion, of the identified threats, in the context of ITS. Thus, the last threat proposed in (Kalloniatis et al., 2014) regarding "Long-term viability" is not considered applicable in the ITS setting since it is not mandatory for the ITS to store users' data for long-term purposes based on the types of services offered. Thus, the considered threats for the ITS setting are the following:

- Threat #1: Abuse and Nefarious Use of ITS Services
- Threat #2: Insecure interfaces and APIs
- Threat #3: Malicious Insiders
- Threat #4: Shared technology issues
- Threat #5: Data Loss or Leakage
- Threat #6: Account or Service Hijacking
- Threat #7: Unknown Risk Profile
- Threat #8: Privileged user access
- Threat #9: Regulatory Compliance
- Threat #10: Data Location
- Threat #11: Lack of Data Segregation
- Threat #12: Lack of Recovery
- Threat #13: Investigate Support

Table 1. ITS Services, Technical Functionalities and Indicative Solutions

Service Categories	Management			Operations				
Technical Functionalities	Travel and Transportation Management	Travel Demand Management	Emergency Management	Public Transportation Operations	Electronic Payment	Commercial Vehicle Operations	Advanced Vehicle Control and Safety Systems	Indicative Solutions
Traffic Surveillance	x	x	x	x			x	Loop Detectors Machine Vision CCTV Vehicle Probes
Vehicle Surveillance			x		x	x	x	Weight-In-Motion Vehicle Location Vehicle Id Number Machine Vision
Inter-Agency Coordination	x	x	x	x	x	x	x	Wireless Comms LANs Data Protocols
Payment Systems			x		x		x	Automated Vehicle Identification Smart Cards Machine Vision
One-WayMobile Communications	x	x			x	x		Commercial Broadcasts Beacons Radio
Two-Way Mobile Communications			x	x	x			Cellular Phones Microwave Infrared Satellite
Stationary Communications			x	x	x	x	x	Fiber Optics Land Lines Radio
Individual Traveler Information			x		x	x	x	Info Kiosks Head-Up Displays Mobile Devices Audio-text Messages
Message Displays			x	x	x		x	Displays Audio Devices
Real Time Traffic Control	x	x	x	x	x	x	x	Optimized Traffic Signals CCTV Satellite Data
Navigation	x	x	x	x		x	x	GPS LORAN Local Beacons Cellular Triangulation
Database Processing	x	x	x	x	x	x	x	Data Base Software Computational Algorithms
Traffic Prediction		x			x			CCTV Algorithms for real time traffic prediction Satellite Data
Traffic Control	x	x			x			CCTV Algorithms for real time traffic monitoring Satellite Data

Service Categories	Management			Operations				
Technical Functionalities	Travel and Transportation Management	Travel Demand Management	Emergency Management	Public Transportation Operations	Electronic Payment	Commercial Vehicle Operations	Advanced Vehicle Control and Safety Systems	Indicative Solutions
Routing			x			x	x	Schedulers Algorithms for best path calculation Route Guidance Satellite Data
In Vehicle Sensors			x	x	x	x	x	Vehicle Monitoring Algorithms Driver Monitoring Algorithms GPS/Satellite Data for Vehicle location determination

Table 2 presents a matching between ITS privacy threats and service categories. Following the aforementioned logic of table 1, the mapping provided in section 2 assists on the identification of the most vulnerable service categories while in parallel a verification of the applicability of the identified threats is conducted. The combination of tables 1 and 2 will assist our goal of understanding the vulnerable ITS service categories along with the respective technical functionalities and the respective solutions in order to provide a more holistic suggestion of the proper privacy properties that need to be addressed per technical ITS functionality.

Table 2. Matching Privacy Threats with ITS Service Categories

	Travel and Transportation Management	Travel Demand Management	Public Transportation Operations	Electronic Payment	Commercial Vehicle Operations	Emergency Management	Advanced Vehicle Control and Safety Systems
Threat #1: Abuse and Nefarious Use of ITS Services	x	x					x
Threat #2: Insecure interfaces and APIs	x	x		x			
Threat #3: Malicious Insiders				x	x		
Threat #4: Shared technology issues	x				x	x	x
Threat #5: Data Loss or Leakage	x	x					
Threat #6: Account or Service Hijacking				x		x	x
Threat #7: Unknown Risk Profile	x	x	x				
Threat #8: Privileged user access				x	x		
Threat #9: Regulatory Compliance	x	x		x			
Threat #10: Data Location	x	x	x	x			
Threat #11: Lack of Data Segregation	x	x					x
Threat #12: Lack of Recovery		x		x	x	x	
Threat #13: : Investigate Support	x	x	x		x		

Privacy Concepts

As indicated above, it is important to identify the set of security and privacy properties that are related to ITS environments. In our previous works we have identified a number of security and privacy properties for traditional and cloud-based systems (Gritzalis et al., 2006; Islam et al., 2012; Kalloniatis et al., 2005, 2008, 2009, 2014). The aim in

this section is to examine the applicability of those in the ITS context based on the analysis conducted before.

The properties described below can be implemented in both traditional distributed systems as well as cloud-based systems. Since ITS can be deployed in both environments the list of potential privacy properties is formed by both domains. The list of the privacy concerns are mentioned below. A detailed description on the meaning of each privacy concern is presented in (Kalloniatis et al., 2005, 2008, 2009, 2014).

)a Isolation, refers to the complete seal of user's data inside the ITS deployment environment.

)b Provenanceability, refers to a Virtual Machine's (VMs) provenance mapping.

)c Traceability, refers to the ability, for the data to be traced or not by the user.

)d Availability, refers to the ability to support continuous service as per the agreement and reduce the factors that can break such continuity such as security attacks (for example DoS attacks), physical disasters and/or hardware failure.

)e Integrity, refers to the ability to avoid clients' data unauthorized modification.

)f Confidentiality, refers to the data communication in the multi-tenant environment of the ITS.

)g Transparency, refers to the ITS providers in order to be completely clear about their procedures and functions.

)h Intervenability, refers to the fact that users should be able to process their data despite the ITS architecture.

)i Accountability, refers to the fact that, all service providers in an ITS should provide information anytime about an incident.

)j Identification, refers both to the protection of the user that accesses a resource or service within the ITS as well as the user's data stored in the ITS. Also, examines that only authorized people may have access to those data.

)k Authentication, is necessary to ensure that only eligible users have access to various services.

)l Authorisation, refers to the fact that users' private data should only be accessed by authorized users.

)m Data Protection, ensures that every transaction involving personal data is realized according to the organization's privacy regulations and Directive 95/46/EU (EU Directive, 1995) regarding the processing of personal data and the free movement of such data.

)n Anonymity, means the state of being anonymous or virtually invisible, and having the ability to operate online without being tracked (Cannon, 2004). Therefore, anonymity is the ability of a user to use a resource or service without disclosing his/her identity (Fischer-Hübner, 2001).

)o Pseudonymity, is the user's ability to use a resource or service by acting under one or many pseudonyms, thus hiding his/her real identity. However, under certain circumstances the possibility of translating pseudonyms to real identities exists.

)p Unlinkability, expresses the inability to link related information (Cannon, 2004) . In particular, unlinkability is successfully achieved when an attacker is unable to link specific information with the user that processes that information.

)q Undetectability and Unobservability. The property of undetectability expresses the inability to detect if a user uses a resource or service. A. Pfitzmann in (Pfitzmann, 1993, Pfitzmann et al., 2010) defines undetectabilty as the inability of the attacker to sufficiently distinguish if an item of interest exists or not. Unobservability protects users from being observed or tracked while browsing the Internet or accessing a service.

In table 3 a link of the identified properties with the ITS technical functionalities is presented. Specifically, the authors examined the technical characteristics of every technical functionality and based on the coverage of every privacy concept described above the following matching was accomplished. This will assist the analysis in the following section for identifying which ITS related privacy concerns are affected by which technical functionalities generating specific privacy issues that need to be resolved when implementing ITS services.

Table 3. Matching ITS Functionalities with Privacy Concepts

Privacy Concepts / Technical Functionalities	Isolation	Provenanceability	Traceability	Availability	Integrity	Confidentiality	Transparency	Interveanability	Accountability	Identification	Authentication	Authorisation	Data Protection	Anonymity	Pseudonymity	Unlinkability	Unobesrvability
Traffic Surveillance	x	x	x	x	x	x		x	x		x	x	x	x			x
Vehicle Surveillance	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Inter-Agency Coordination			x	x													
Payment Systems	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
One-Way Mobile Communications	x	x	x		x	x	x	x	x	x	x						
Two-Way Mobile Communications		x	x		x	x	x	x	x	x	x	x	x	x	x	x	x
Stationary Communications				x													
Individual Traveler Information		x			x	x	x	x	x	x	x	x	x	x	x	x	x
Message Displays	x	x	x		x				x								
Real Time Traffic Control							x	x	x	x	x	x	x				
Navigation	x		x														
Database Processing		x			x	x	x	x	x	x	x	x	x	x	x	x	x
Traffic Prediction		x			x	x		x	x				x			x	x
Traffic Control	x	x			x	x	x	x	x	x	x	x	x	x	x	x	x
Routing	x		x							x	x						
In Vehicle Sensors																x	

Privacy Concerns in ITS

One of the main challenges in building trustworthy services is to make users trust the software they use through the establishment of secure and privacy-aware technologies that will provide sufficient protection over possible threats on the respective services. In order to identify the proper privacy concepts that developers need to address for raising users privacy, the previous sections describe the main functionalities and threats on a modern ITS and how the suggested privacy concepts satisfy the technical functionalities arised. However, for establishing a more concrete analysis and verification of the aforementioned concepts it is necessary to identify and match the actual users' privacy concerns from the use of ITS services along with the identified privacy concepts.

In (Glancy, 1995) an empirical identification of a list of ten users privacy concerns regarding ITS is presented. For verification purposes, the specific list of concerns was validated with fifty students of the "Information Security" class of University of the Aegean. The results from this short validation process were encouraging since all concerns mentioned during the interviews by the students could be classified in these ten items. The list as it is presented in (Glancy, 1995) is the following:

a) *PC#1: ITS applications can be used invisibly to track a targeted individual's movements from place to place*, mainly expressing users' concerns about the role of ITS as a way to perform real-time surveillance to citizens not only by Law Enforcement Agents and Public Organizations, but also from private investigators, etc.

b) *PC#2: ITS applications can be used automatically to collect comprehensive information about when and where every person travels*, mainly expressing experienced IT users who understand that while the data collected through an ITS are neither too personal or too impersonal, indeed there is a possibility that upon combination may lead to travel patterns for a specific person, etc.

c) *PC#3: ITS will create a computerized personal travel profile which will be used to make decisions about an individual, as well as to predict and to manipulate the individual's future choices about transportation and other matters*, mainly expressing users concern that ITS-generated profiles will threaten privacy since they may substitute the person herself and this faulty image may lead to a disjunction that can be damaging psychologically.

d) *PC#4: ITS applications can aggregate, or connect up, stored information about an individual's travel patterns with other information regarding that individual*, mainly expressing the concern that various providers of the ITS gather information that independently may seem privacy aware for the users but their combination may lead to serious privacy inventions.

e) *PC#5: ITS applications can use or disclose information about an individual's travel history or profile in ways which may both reflect him or her and affect his or her future opportunities and choices*, mainly expressing the concern that ITS will label its users like "Die hard driver", "Eco-friendly", etc. and these labels may affect the personal or professional live of every individual.

f) *PC#6: ITS can manipulate individual decisions about modes, times and destinations of travel by means of route guidance, traffic congestion information, persuasion and advertisements of products and services*, mainly expressing the concern of users receiving unwanted advertising information and manipulation by the ITS traffic management system in route suggestions, etc.

g) *PC#7: ITS monitoring and reporting of vehicle and operator conditions can be used to override individual travel decisions*, mainly expressing the users' concern regarding driver surveillance systems which will be able to decide which functions the driver will be able to use based on his behavior, tiredness, etc.

h) *PC#8: ITS can take over control of vehicle or transit operations by means of intelligent automated systems, which substitute ITS control for control by an individual*, mainly expressing the concern of future autonomous systems where in some parts of the route it will be mandatory for the driver to "hand over" the control to an Automated System where for safety reasons will guide the vehicle in specific zones thus overriding individual's control. The privacy relation is that some users feel their privacy being violated in the sense of overriding their choices, decisions and controls.

i) *PC#9: Government agencies can use ITS to collect, manipulate and disclose information about individual travellers and to control their travel by means of government-controlled automated systems*, mainly expressing the users' concern that ITS will provide public organization and government with individual's data regarding traveling habits, preferred destinations, etc.

j) *PC#10: Private entities, especially large corporations, will use ITS to collect, to manipulate and to disclose transportation information about individuals and use ITS to take over control of travel*, mainly expressing the concern that large private organizations will handle users' data for invading their privacy and/or for profitable and commercial reasons without users providing their consent or even knowing that this action is indeed happening.

The matching of the aforementioned privacy concerns with the privacy concepts described previously is presented below. The goal of this matching is mainly the validation of the completeness of the set of privacy concepts identified as a way to capture beside the technical functional requirements users' concerns as well. Table 4 presents the matching of the aforementioned concepts.

Table 4. Matching Users' Privacy Concerns with Privacy Concepts

Privacy Concepts / Privacy Concerns	**Isolation**	**Provenanceability**	**Traceability**	**Availability**	**Integrity**	**Confidentiality**	**Transparency**	**Interveanability**	**Accountability**	**Identification**	**Authentication**	**Authorisation**	**Data Protection**	**Anonymity**	**Pseudonymity**	**Unlinkability**	**Unobesrvability**
PC#1	x				x	x		x	x			x	x	x	x		
PC#2	x		x	X			x		x	x				x		x	x

Privacy Concepts / Privacy Concerns	Isolation	Provenanceability	Traceability	Availability	Integrity	Confidentiality	Transparency	Interveanability	Accountability	Identification	Authentication	Authorisation	Data Protection	Anonymity	Pseudonymity	Unlinkability	Unobesrvability
PC#3	x	x			x	x		x	x			x					
PC#4					x								x		x		
PC#5					x	x			x	x					x		
PC#6		x	x			x	x	x	x		x	x		x	x	x	x
PC#7	x	x			x					x		x					
PC#8		x	x					x	x					x	x	x	
PC#9		x	x	x	x	x	x										
PC#10	x	x		x	x	x	x	x	x		x	x	x	x	x	x	

Discussion

One of the main contributions of this work is the identification of the relationship between Technical Services and Threats. This is crucial as it can be used by system designers as a roadmap during design phase for conceptualizing possible ITS threats and associate these threats with functionalities offered by such a system. This linkage offers the opportunity for testing a system against 13 categories of threats. Table 5 depicts the relationship between 13 threats and 16 technical functionalities of an ITS system.

Furthermore, the 15th column of this table indicates the associated privacy concerns (from the user's side of view) with technical functionalities of an ITS. The last column of the table depicts the privacy concepts associated with each privacy concern. This four dimensional relationship depicted in Table 5, offers a unique association between vital concepts of ITS privacy by linking technologies, threats, user's concerns and concepts. For example the first ITS technical functionality "Traffic Surveillance" is associated with threats: 1,2,4,5,6,7,9,10,11,12 and 13. This functionality appears to be associated with users privacy concerns: PC1, PC2, PC9 and PC10 which are then associated with the following concepts: Isolation, Integrity, Confidentiality, Interveanability, Accountability, Authorisation, Data Protection, Anonymity, Pseudonymity, Traceability, Availability, Transparency, Identification, Unlinkability, Unobesrvability, Provenanceability and Authentication. Systems designers could focus only on specific ITS functionalities and address user's concerns by implementing the associated privacy concepts.

This unique 4 dimensional association may offer a structured roadmap which could enable a more systematic approach on satisfying privacy issues and the use of their associated technologies. The list of technical functionalities is not exhausted but offers a general categorization of a number of contemporary ITS functionalities.

Thus, the final matching produced from the aforementioned analysis makes a useful tool for the software engineers to easily identify, which are the threats that need to be resolved for every category of ITS service they wish to implement, which are the users' privacy concerns that are raised for the specific services and which privacy technical concepts needs to be fulfilled for satisfying users and systems privacy requirements. Software developers will require to choose the best implementation techniques for providing the intended functionalities of the ITS respecting the identified privacy concepts. Criteria such as cost, complexity, etc. can be established for the selection of the most appropriate ICTs but this part is out of the scope of this paper.

Table 5. A Roadmap for Identifying Privacy Concepts for ITS Services

Technical Functionalities	Threat #1	Threat #2	Threat #3	Threat #4	Threat #5	Threat #6	Threat #7	Threat #8	Threat #9	Threat #10	Threat #11	Threat #12	Threat #13	User Privacy concerns	Technical Privacy Concepts
Traffic Surveillance	**x**	**x**		**x**	**x**	**x**	**x**		**x**	**x**	**x**	**x**	**x**	**PC1 PC2**	Isolation, Provenceability, Traceability, Availability, Integrity, Confidentiality,

Technical Functionalities	Threat #1	Threat #2	Threat #3	Threat #4	Threat #5	Threat #6	Threat #7	Threat #8	Threat #9	Threat #10	Threat #11	Threat #12	Threat #13	User Privacy concerns	Technical Privacy Concepts
														PC9 **PC10**	Interveanability, Accountability, Authentication, Authorisation, Data Protection, Anonymity, Unobservability
Vehicle Surveillance	**x**	**x**	**x**	**x**		**x**		**x**	**x**	**x**	**x**	**x**		**PC1** **PC2** **PC10**	Isolation, Provenceability, Traceability, Availability, Integrity, Confidentiality, Interveanability, Accountability, Authentication, Authorisation, Data Protection, Transparency, Identification, Anonymity, Pseudonymity, Uninkability, Unobersvability
Inter-Agency Coordination	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**PC9** **PC10**	Traceability, Availability
Payment Systems	**x**	**x**	**x**	**x**		**x**		**x**	**x**	**x**	**x**	**x**		**PC4** **PC9** **PC10**	Isolation, Provenceability, Traceability, Availability, Integrity, Confidentiality, Interveanability, Accountability, Authentication, Authorisation, Data Protection, Transparency, Identification, Anonymity, Pseudonymity, Uninkability, Unobersvability
One-Way Mobile Communications	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**PC9**	Isolation, Provenceability, Traceability, Integrity, Confidentiality, Transparency, Interveanability, Accountability, Identification, Authentication
Two-Way Mobile Communications		**x**	**x**	**x**		**x**	**x**	**x**	**x**	**x**		**x**	**x**	**PC1** **PC2** **PC9** **PC10**	Provenceability, Traceability, Integrity, Confidentiality, Transparency, Interveanability, Accountability, Identification, Authentication, Authorisation, Data Protection, Anonymity, Pseudonymity, Unlinkability, Unobservability
Stationary Communications	**x**	**x**	**x**	**x**	**x**	**X**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**PC5**	Availability
Individual Traveler Information	**x**	**x**	**x**	**x**	**x**	**X**		**x**	**x**	**x**	**x**	**x**	**x**	**PC1** **PC2** **PC4** **PC9** **PC10**	Provenceability, Integrity, Confidentiality, Transparency, Interveanability, Accountability, Identification, Authentication, Authorisation, Data Protection, Anonymity, Pseudonymity, Unlinkability, Unobservability
Message Displays	**x**		**x**	**x**		**x**	**x**	**x**		**x**	**x**	**x**	**x**	**PC7**	Isolation, Provenceability, Traceability, Integrity, Accountability
Real Time Traffic Control	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**PC9** **PC10**	Transparency, Interveanability, Accountability, Identification, Authentication, Authorisation, Data Protection
Navigation	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**PC1** **PC2** **PC3** **PC5** **PC6** **PC10**	Isolation, Traceability
Database	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**PC3**	Provenceability, Integrity,

Technical Functionalities	Threat #1	Threat #2	Threat #3	Threat #4	Threat #5	Threat #6	Threat #7	Threat #8	Threat #9	Threat #10	Threat #11	Threat #12	Threat #13	User Privacy concerns	Technical Privacy Concepts
Processing														**PC4** **PC9** **PC10**	Confidentiality, Transparency, Interveanability, Accountability, Identification, Authentication, Authorisation, Data Protection, Anonymity, Pseudonymity, Unlinkability, Unobservability
Traffic Prediction	**x**	**x**	**x**		**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**PC4** **PC5** **PC9** **PC10**	Provenceability, Integrity, Confidentiality, Interveanability, Accountability, Data Protection, Unlinkability, Unobservability
Traffic Control	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**PC1** **PC2** **PC9** **PC10**	Isolation, Provenceability, Integrity, Confidentiality, Transparency, Interveanability, Accountability, Identification, Authentication, Authorisation, Data Protection, Anonymity, Pseudonymity, Unlinkability, Unobservability
Routing	**x**		**x**	**x**		**x**		**x**			**x**	**x**	**x**	**PC1** **PC2** **PC3** **PC4** **PC6** **PC7**	Isolation, Traceability, Authentication, Identification
In Vehicle Sensors		**x**	**x**			**X**	**x**	**x**	**x**	**x**		**x**	**x**	**PC8**	Unlinkability

Requirements for a Methodology to Support Security and Privacy Analysis in ITS

Following the analysis conducted before regarding the identification of the service categories and technical functionalities of an ITS along with the respective privacy threats, privacy concerns and privacy concepts, we proceed on the identification of a number of challenges that should be considered for integrating the identified privacy concerns in the design analysis of an ITS system. These challenges are:

- Challenge 1: Organisational and user's needs should be identified in order to have a clear understanding of the respective privacy issues that need to be considered when designing privacy-aware ITS systems
- Challenge 2: Different ITS technical functionalities require different privacy properties.
- Challenge 3: A clear association should be supported between analysis and design.
- Challenge 4: Different providers offer different mechanisms to support privacy properties.
- Challenge 5: It is important to have a clear association between properties, threats and mechanisms.

To support the above challenges, a set of requirements that an analysis and design methodology should support is defined. It is worth mentioning that this list does not include requirements that are required from any software systems methodology, such as for example being clear and structured and include well-defined concepts and stages, but only focuses on a list of requirements related to modeling and analysis of privacy related concerns. The identified requirements are:

- Requirement 1: The methodology should include concepts from both ITS and organization areas such as actor, organizational goals, dependencies, infrastructure, information management, portability, application during the analysis for the development of ITS system. This supports understanding of organizational and user needs for

establishing a privacy-aware ITS service (response to Challenge 1);

- Requirement 2: The methodology should provide techniques to select appropriate privacy properties and respective techniques for every technical functionality. The selected functionalities shall support organizational needs, requirements and shall address the identified threats and risks. Selection of ITS services needs to analyse the different service categories considering all constraints and portability of organizational data or infrastructure into the distributed ITS environment (Response to Challenge 2).
- Requirement 3: The methodology should enable the usage of a defined set of concepts and notations during the analysis and design process, to support a unified analysis and a clear connection between requirements analysis and design solutions (Challenge 3).
- Requirement 4: The methodology should allow developers to evaluate potential providers. The selection should be based on degree of satisfaction of requirements, mechanisms, and organizational needs and the selected ITS services (Challenge 4).
- Requirement 5: The methodology should consider relevant privacy properties, threats, and risks and be able to identify appropriate measures and mechanisms to control privacy threats and risks and satisfy the privacy properties (Challenge 5).
- Requirement 6: The methodology should provide mechanisms to clearly identify a linkage between privacy issues, users' needs and relevant threats and properties. To support an easy facilitation of such linkage we have identified, in Table 5, an association between privacy issues, and the threats and concepts we have presented in the previous sections. Although we do not claim the list to be extensive nor final, we believe it can be used as a starting point and be modified and/or extended as required (Challenge 5).

Conclusions and future steps

Modern ITS technologies are designed for improving peoples' everyday lives by providing innovative services for improving the safety, efficiency and mobility of surface transportation. However, as ITS services evolve so do the amount of personal data collected in order for the providers to offer improved and more personalized services to citizens and also to attract more potential new users. In parallel there is a great amount of stakeholders, providers, public agents and private organizations that have great interest on the quantity of data generated from the ITS services either for direct or indirect purposes related to citizens. Citizens on the other hand do enjoy innovative services but their awareness from the use of ICT services regarding privacy has also increased the past decade thus their concerns about security and privacy play an important role when selecting which services they will trust to use.

The specific paper moves on this direction by providing a roadmap to software engineers for designing trustworthy services in ITS environments. This is achieved through a clear linkage among ITS technical functionalities, threats within the functionalities, users' privacy concerns and specific privacy concepts. The roadmap was progressively introduced by conducting an analysis and linkage of specific categories initially beginning from the categories of services, through their connection with potential threats and identification of privacy concepts and their relationship with user privacy concerns. This led to a four dimensional table which can be used by software engineers in order to identify the specific privacy concepts that need to be implemented for a given ITS service, risk and user concern. As a secondary aim this paper provided an initial set of requirements that modern ITS should realise and include in their development process.

In future research, we aim to enhance these privacy concepts in work on privacy requirements in the engineering field in order to develop a holistic approach for modeling privacy-aware ITS services. The identification of proper implementation techniques that could assist in the realization of the specific privacy concepts in the ITS context is also an issue for future investigation towards the goal of trustworthy implementation of ITS services.

References

Antoniou, C., Polydoropoulou, A., 2015. The Value of Privacy: Evidence From the Use of Mobile Devices for Traveler Information Systems. Journal of Intelligent Transportation Systems 19, 167–180.

Al-Hader, M., Rodzi, A., 2009. The smart city infrastructure development & monitoring. Theoretical and Empirical Researches in Urban Management 87.

Batty, M., 2013. Big data, smart cities and city planning. Dialogues in Human Geography 3, 274–279.

Cannon, J.C., 2004. Privacy: what developers and IT professionals should know. Addison-Wesley Professional.

Cohen, B., 2011. Smart Cities. Disponible on-line en: http://www. boydcohen. com/smartcities. html (consultado el 8

de agosto de 2014).
EU Directive, E.U., 1995. 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the EC 23.
Farber, D., 2008. The new geek chic: Data centers. CNET News 25.
Fischer-Hübner, S., 2001. IT-security and privacy: design and use of privacy-enhancing security mechanisms. Springer-Verlag.
Glancy, D.J., 1995. Privacy and intelligent transportation technology. Santa Clara Computer & High Tech. LJ 11, 151.
Gomez-Ibanez, J.A., Small, K.A., 1994. Road pricing for congestion management: A survey of international practice. Transportation Research Board.
Goulias, K.G., 2015. An Overview of GeoSimulation for Smart City Planning, Design, and Operations. In: Smart Cities Symposium. Presented at the Smart Cities Symposium, Faculty of Transportation Sciences, Prague, Czech Republic.
Goulias, K.G., Davis, A., hyun, L.J., Polydoropoulou, A., Tsirimpa, A., Tsouros, I., 2015. Measurement of sense of place and comparison with social media data in a Greek island. In: IMIC Conference. Presented at the IMIC Conference, Santorini.
Gritzalis, S., Kavakli, E., Kalloniatis, C., Loucopoulos, P., Gritzalis, S., 2006. Incorporating privacy requirements into the system design process: the PriS conceptual framework. Internet research 16, 140–158.
Hof, R.D., 2006. Jeff Bezos' risky bet. Business Week 13, 52–8.
Huber, P., 1995. Public Transport Information Systems in Munich. In: Steps Forward. Intelligent Transport Systems World Congress.
IDC, 2008. IDC eXchange » Blog Archive » Defining "Cloud Services" and "Cloud Computing."
Islam, S., Mouratidis, H., Kalloniatis, C., Hudic, A., Zechner, L., 2012. Model based process to support security and privacy requirements engineering. International Journal of Secure Software Engineering (IJSSE) 3, 1–22.
Jones, P., 2003. Acceptability of road user charging: meeting the challenge. Acceptability of transport pricing strategies 27–62.
Kalloniatis, C., Kavakli, E., Gritzalis, S., 2005. Dealing with privacy issues during the system design process. In: Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology, 2005. IEEE, pp. 546–551.
Kalloniatis, C., Kavakli, E., Gritzalis, S., 2008. Addressing privacy requirements in system design: the PriS method. Requirements Engineering 13, 241–255.
Kalloniatis, C., Kavakli, E., Kontellis, E., 2009. Pris Tool: A Case Tool For Privacy-Oriented Requirements Engineering. In: MCIS. p. 71.
Kalloniatis, C., Mouratidis, H., Vassilis, M., Islam, S., Gritzalis, S., Kavakli, E., 2014. Towards the design of secure and privacy-oriented information systems in the cloud: identifying the major concepts. Computer Standards & Interfaces 36, 759–775.
Kamargianni, M., Ben-Akiva, M., Polydoropoulou, A., 2014. Incorporating social interaction into hybrid choice models. Transportation 41, 1263–1285.
Kamargianni, M., Li, W., Matyas, M., Schäfer, A., 2016. A Critical Review of New Mobility Services for Urban Transport. Transportation Research Procedia, Transport Research Arena TRA2016 14, 3294–3303.
Kamijo, S., Matsushita, Y., Ikeuchi, K., Sakauchi, M., 2000. Traffic monitoring and accident detection at intersections. IEEE transactions on Intelligent transportation systems 1, 108–118.
Kavroudakis, D., 2015. sms: Microdata for Geographical Analysis in R. Journal of Statistical Software 68, 1–23.
Kavroudakis, D., Ballas, D., Birkin, M., 2012. Using Spatial Microsimulation to Model Social and Spatial Inequalities in Educational Attainment. Applied Spatial Analysis and Policy.
Kavroudakis, D., Ballas, D., Birkin, M., 2013. SimEducation: A Dynamic Spatial Microsimulation Model for Understanding Educational Inequalities. In: Tanton, R., Edwards, K. (Eds.), Spatial Microsimulation: A Reference Guide for Users, Understanding Population Trends and Processes. Springer Netherlands, pp. 209–222.
King, R., 2008. How cloud computing is changing the world. Business Week 4, 08.
Kramers, A., Höjer, M., Lövehagen, N., Wangel, J., 2014. Smart sustainable cities–Exploring ICT solutions for reduced energy use in cities. Environmental modelling & software 56, 52–62.
Lee, J.H., Davis, A.W., Goulias, K.G., 2016. Activity Space Estimation with Longitudinal Observations of Social Media Data. In: Paper Submitted for Presentation at the 95th Annual Meeting of the Transportation Research Board. Washington, DC.
Lee, J.H., Gao, S., Janowicz, K., Goulias, K.G., 2015. Can Twitter data be used to validate travel demand models? In: IATBR 2015-WINDSOR.
Liu, Y., Sui, Z., Kang, C., Gao, Y., 2014. Uncovering patterns of inter-urban trip and spatial interaction from social media check-in data. PloS one 9, e86026.
Martinez, F.J., Toh, C.-K., Cano, J.-C., Calafate, C.T., Manzoni, P., 2010. Emergency services in future intelligent transportation systems based on vehicular communication networks. IEEE Intelligent Transportation Systems Magazine 2, 6–20.
Neirotti, P., De Marco, A., Cagliano, A.C., Mangano, G., Scorrano, F., 2014. Current trends in Smart City initiatives:

Some stylised facts. Cities 38, 25–36.
Nuaimi, E.A., Neyadi, H.A., Mohamed, N., Al-Jaroodi, J., 2015. Applications of big data to smart cities. J Internet Serv Appl 6, 1–15.
Papageorgiou, M., Diakaki, C., Dinopoulou, V., Kotsialos, A., Wang, Y., 2003. Review of road traffic control strategies. Proceedings of the IEEE 91, 2043–2067.
Pfitzmann, A., 1993. Technischer Datenschutz in öffentlichen Funknetzen. Datenschutz und Datensicherung DuD 17, 451–463.
Pfitzmann, A., Hansen, M., 2010. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management.
Polycarpou, E., Lambrinos, L., Protopapadakis, E., 2013. Smart parking solutions for urban areas. In: World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on A. IEEE, pp. 1–6.
Salama, A.S., Saleh, B.K., Eassa, M.M., 2010. Intelligent cross road traffic management system (ICRTMS). In: Computer Technology and Development (ICCTD), 2010 2nd International Conference On. IEEE, pp. 27–31.
Shawky, D.M., Ali, A.F., 2012. Defining a measure of cloud computing elasticity. In: Systems and Computer Science (ICSCS), 2012 1st International Conference On. IEEE, pp. 1–5.
Ueno, K.S.S.N.K., Cho, K., 2012. Feasibility study on detection of transportation information exploiting twitter as a sensor.