SINTEF A27830 - Unrestricted

Report

Needs and challenges concerning privacy risk management within Intelligent Transport Systems

Problem analysis in project PrivacyAssessment@SmartCity

Author(s)
Gencer Erdogan, Aida Omerovic, Marit K. Natvig, Isabelle C.R. Tardy

SINTEF ICT
Networked Systems and Services
2016-12-09

SINTEF IKT
SINTEF ICT

Address:
Postboks 124 Blindern
NO-0314 Oslo
NORWAY

Telefax: +47 22067350

Enterprise /VAT No:
NO 948 007 029 MVA

KEYWORDS:
Privacy risk
Smart City
Intelligent Transport Systems (ITS)
Risk management
Risk assessment

Report

Needs and challenges concerning privacy risk management within Intelligent Transport Systems

VERSION	**DATE**
1.0	2016-12-09

AUTHOR(S)
Gencer Erdogan, Aida Omerovic, Marit K. Natvig, Isabelle C.R. Tardy

CLIENT(S)	**CLIENT'S REF.**
SINTEF ICT	102012754
PROJECT NO.	**NUMBER OF PAGES/APPENDICES:**
102012754	30

ABSTRACT
There are many privacy concerns within Intelligent Transport Systems (ITS). On the one hand, end-users are concerned about their privacy-risk exposure when using ITS, while on the other hand, ITS providers need to claim privacy awareness and document compliance with regulations or face devastating fines. One approach to address these concerns is to use methods specifically developed to assess privacy risks of ITS. The literature lacks such methods, and the complex and dynamic nature of ITS introduces challenges that need to be properly addressed when assessing privacy risks. In this report, we carry out an empirical study in order to identify needs and challenges concerning privacy risk assessment of ITS. Broadly speaking, the main challenges are related to real-time assessment of privacy risks to (1) inform end-users about exposed privacy risks, and (2) help ITS providers asses privacy-compliance risks, as well as to identify privacy risks at an implementation level.

PREPARED BY	SIGNATURE
Gencer Erdogan	Gencer Erdogan
CHECKED BY	SIGNATURE
Fredrik Seehusen	
APPROVED BY	SIGNATURE
Bjørn Skjellaug	

REPORT NO.	**ISBN**	**CLASSIFICATION**	**CLASSIFICATION THIS PAGE**
SINTEF A27830	9788214059182	Unrestricted	Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION
0.1	2016-11-01	Final draft to QA
0.2	2016-11-11	Corrections after QA
1.0	2016-12-09	Final version after QA

Table of contents

1 Introduction

The European ITS Directive (EU Directive 2010/40/EU) [4] defines Intelligent Transport Systems (ITS) as "systems in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport". The directive emphasizes that ITS covers all transport modes (road, sea, rail, and air).

As pointed out by the definition above, ITS is used by many different user groups. Users of public transport services and road users such as drivers, bikers and pedestrians use ITS in travel planning, to book transport services, to buy tickets (eTicketing) and so on. Hietanen [7] and Spickermann et al. [23] describe the transition from the multitude of different transport services to Mobility as a Service (MaaS) where "a customer's major transportation needs are met over one interface and are offered by a service provider". ITS services in the context of MaaS may for example support the use of public transport alone or door-to-door transport facilitated by combinations of public transport, city bikes, taxis, car sharing and, in the future, autonomous vehicles.

Transport authorities use ITS for traffic management to reduce congestion, emissions, accidents, and fatalities. This includes ITS for traffic control and acquisition and dissemination of traffic information. Back-end and road-side systems interact with each other, with actuators such as light signals, and with sensors such as optical sensors for automatic number plate recognition, sensors for speed registration, inductive loops for detecting vehicles, etc. All these systems, actuators, and sensors enable a variety of ITS services such as automatic speed control, road charging, and calculation of travel time.

The car industry is the driving force in the foreseen transition from driver assistance towards autonomous vehicles supported by Cooperative ITS (C-ITS) [2]. In C-ITS, systems on board vehicles exchange data with systems in other vehicles as well as other external systems, e.g. systems for traffic control. Vehicles broadcast data about their properties, heading, planned route, speed, accelerations, breaking, etc., and receive similar data from other vehicles. A common, real-time, situational awareness is thereby established, and more or less autonomous vehicles can make decisions on how to operate based on this awareness.

As pointed out by Psaraki et al. [19] and Vandezande et al. [26], there are many privacy concerns within ITS solutions due to the wide-spread data registration, exchange of data between systems, and monitoring/tracking of persons and vehicles. Much of this data originates from connected persons and connected things associated with persons (e.g. connected vehicles). Thus ITS may directly or indirectly compromise the identity of persons, their location, plans, and activities. Aggregated data may also show patterns in behavior, who a person interacts with, preferences, etc. Moreover, for a citizen, privacy represents a condition for his/her trust and service adoption. In addition, service providers in general have to fulfill strict privacy requirements defined by the recent EU Regulation 2016/679 [5]. Non-compliance with this regulation, which applies from May 2018, will according to the regulation result in fines up to 20 million EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year [5]. In light of all these privacy concerns, there is a need for additional measures to ensure sufficient and adequate safeguards to the user's privacy [26]. One measure is to use methods specifically developed to assess privacy risk of ITS. Such methods are essential for an ITS service provider to be able to claim privacy awareness and to document compliance with regulations.

However, the literature lacks methods that specifically assess privacy risk of ITS, and the complex and dynamic nature of ITS introduces challenges that need to be properly addressed when assessing privacy risk of ITS. Privacy risks are in general assessed by making use of general Privacy Impact Assessment (PIA) methods typically based on standards such as ISO 27005, NIST SP 800-30, ISO 29100, and ISO 22307, and are mainly developed and carried out at a governmental level [28]. These methods are often too generic and carried out at a high-level of abstraction, and they need to be specialized towards ITS services. In this report, we provide a state-of-the-art and a detailed account of a realistic case on ITS, and report on findings from interviews and a workshop with experts, and finally analyze our findings to identify needs and challenges within privacy risk assessment of ITS.

The remainder of this report is organized as follows. In Section 2, we first present the findings and then the needs and challenges identified based on our findings. In Section 3, we provide the research questions we will focus on in the project PrivacyAssessment@SmartCity to address the needs and challenges identified in Section 2. In Section 4, we describe the research method applied in PrivacyAssessment@SmartCity to address the research questions in Section 3 and to develop and evaluate an approach to assess privacy risks of ITS. In Section 5, we conclude.

2 Findings and identified needs and challenges

As illustrated by the activity diagram in Figure 1, we identified needs and challenges based on data collected from three parallel streams of activities: identify state of the art, study a realistic case on ITS, carry out interviews and a workshop with relevant stakeholders. In this report, we use the term stakeholder to collectively refer to ITS providers, end-users, or other relevant parties that may use or provide ITS services.

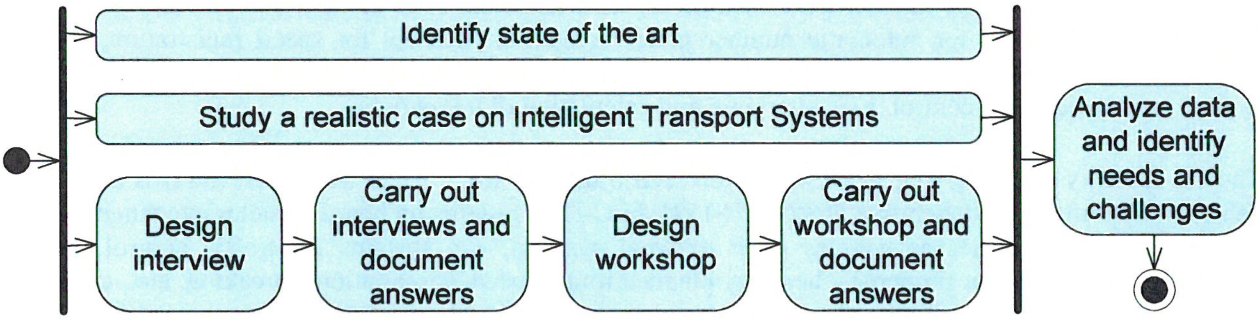
Identify state of the art
Study a realistic case on Intelligent Transport Systems
Design interview
Carry out interviews and document answers
Design workshop
Carry out workshop and document answers
Analyze data and identify needs and challenges

Figure 1: Research approach conducted to identify needs and challenges concerning privacy risk assessment

In order to obtain an overview of the problem domain we face within privacy risk assessment of ITS systems, we identified the state of the art within privacy impact assessment methods, privacy practices within ITS, and privacy within wireless technologies. This was carried out in terms of an initial mapping study. Initial mapping studies are typically carried out to obtain a high-level picture, and are carried out prior to systematic literature reviews which are highly focused compared to mapping studies [13]. In the mapping study, we used search engines such as the ACM Digital Library [43] and Google Scholar [44] to find relevant literature. For privacy impact assessment methods we used the search strings "privacy risk assessment", "privacy impact assessment", "privacy risk assessment within/in/of/for", and "privacy impact assessment within/in/of/for". The last two search strings were divided in four strings each by splitting the string with respect to "within/in/of/for". For privacy practices within ITS and wireless technologies we used a similar approach focused on their respective domains. The search strings were not strictly predefined and were also selected based on search results.

We analyzed a realistic case on ITS to obtain better understanding of privacy challenges specifically within ITS. In order to represent a real-life ITS system, we built the case based on concepts defined in ARKTRANS, which is a multimodal ITS framework architecture [17]. ARKTRANS provides a common view of the transport domain for all transport modes (road, sea, rail, and air), and it may be used as a template to establish ITS solutions.

To complement our results and observations from the state of the art and the ITS case, we conducted interviews and a workshop together with stakeholders ranging from governmental organizations to commercial software companies. The purpose of the interviews and the workshop was to gain knowledge about current practice related to privacy management in the government/industry, as well as expert viewpoints with respect to needs related to methods for assessing privacy risk. In total, we interviewed five experts, where each interview was carried out as an open-ended interview. During the interviews we asked the participants the seven questions listed in Table 1. The workshop was carried out some time after the interviews in terms of group work. In total, there were twelve participants in the workshop divided in two groups with six participants in each group. In the workshop, we focused more on the experience of the participants with respect to how they assess privacy risks, privacy challenges, and their thoughts about how methods to assess privacy risk would be helpful. We therefore asked each group in the workshop to discuss questions Q3, Q5 and Q7 in Table 1.

Finally, we collected and analyzed data obtained from the activities described above, and based on the analysis we identified needs and challenges within privacy risk assessment of ITS.

Table 1: Questions asked during interviews and the workshop

Q#	Question	Interview	Workshop
Q1	Have you experienced incidents related to privacy?	X	
Q2	How do you preserve privacy?	X	
Q3	How do you assess privacy risk?	X	X
Q4	How do you communicate privacy issues internally as well as externally (for example to customers / end-users)?	X	
Q5	What privacy challenges do you find relevant in current and emerging ICT services?	X	X
Q6	How is privacy an obstacle to develop new and useful services?	X	
Q7	How can methods to assess privacy risk be helpful?	X	X

2.1 State of the art

In this section, we present the state of the art related to privacy impact assessment (PIA) methods, and privacy practices within ITS.

2.1.1 Privacy impact assessment methods

Privacy impact assessment is basically a form of risk management conducted to manage privacy risks [27], [28]. This is typically carried out following a generic security risk management process such as ISO 27005 [9], but with a specific focus on privacy. PIA includes the identification of threats, vulnerabilities exploited by threats, and assets that may be harmed by threats which in turn cause privacy risks. We may divide PIA methods in two main groups: *general methods* and *domain-specific methods*. In the following, we describe the state of the art of PIA methods with respect to these two groups.

2.1.1.1 General PIA methods

General PIA methods are typically based on standards such as ISO 27005 [9], NIST SP 800-30 [16], ISO 29100 [10], and ISO 22307 [8]. General PIA methods are mainly developed and carried out at a governmental level, and there are in particular five countries that are in the leading position: Australia, Canada, New Zealand, United Kingdom, and the United States [28]. The methods provided by these countries are somewhat similar, but according to Wright et al. [28], they also have their differences as shown in Table 2.

Table 2: Differences between PIA methods by Australia (A), Canada (C), New Zealand (NZ), United Kingdom (UK), and United States (US) based on [28].

PIA features	**A**	**C**	**NZ**	**UK**	**US**
PIA guidance is targeted at government departments and agencies only.		X			X
PIA guidance is targeted at government departments and the private sector.	X		X	X	
PIA guidance envisages a PIA as a multi-disciplinary exercise.	X	X			X
PIA guidance puts emphasis on PIA as a process and not just preparation of the PIA report.	X	X		X	
PIA guidance explicitly encourages engaging external stakeholders in the PIA process.	X		X	X	
The PIA guidance puts primary emphasis on compliance.					X

The process in general PIA methods may be summarized in three overall steps [27]. In Step 1 the PIA is planned and the context is established. In Step 2 privacy risks are identified. Finally, in Step 3 risk treatments are identified and implemented. The purpose of Step 1 is to determine whether it is necessary to carry out a PIA (threshold analysis), identify and describe the target of analysis, and establish a team and a budget. The threshold analysis is carried out to introduce cost-effectiveness because PIA analyses are costly [27]. The purpose of Step 2 is to analyze the system target, in particular the information-flow, to identify and prioritize privacy risks. Stakeholders are typically included in this step. The purpose of Step 3 is to formulate risk treatments to be implemented by the system owner. A general recommendation is to verify treatments through a third party.

2.1.1.2 Domain-specific PIA methods

Domain-specific PIA methods can be regarded as specializations of the general PIA methods outlined above. Ren et al. [20] and Friginal et al. [6] provide approaches focusing on privacy risk within location-based systems. Ren et al. [20] provide an attack-tree based approach to identify and estimate privacy risks within Vehicular Ad Hoc Networks (VANETs), while Friginal et al. [6] suggest an approach to identify, estimate, and evaluate privacy risks within location-based systems in general. The process in the latter approach is in line with risk assessment in ISO 27005 [9].

Theoharidou et al. [25] and Tancock et al. [24] provide approaches focusing on privacy risk within cloud computing. Theoharidou et al. [25] adapt the process in general PIA methods outlined above to identify threats, vulnerabilities, and treatments that clients and providers should implement in order to achieve privacy compliance and accountability. Tancock et al. [24] provide a tool-based approach used in a cloud environment to identify privacy risks and compliance issues. The tool supports privacy risk analysts to identify and address privacy requirements for a given context.

Mylonas et al. [15] provide a user-centric approach to privacy impact assessment of Android apps. The approach is user-centric in the sense that qualitative risk estimation (i.e. impact and likelihood values) is based on answers collected from the end-user.

Knirsch et al. [14] provide a model-driven approach to assess privacy risks for smart grid applications. The approach is designed to assist system engineers to evaluate use cases in the smart grid in an early design phase. The output is a set of threats and privacy risks, where the risks are estimated quantitatively.

2.1.2 Privacy within Intelligent Transport Systems

According to Psaraki et al. [19] and Vandezande et al. [26], privacy and liability is one of the main concerns when ITS services are implemented since they monitor and track persons and vehicles. Vandezande et al. [26] conclude that privacy issues have to be handled when technology is specified. Standardization committees such as ISO TC 204, CEN TC 278 and ETSI TC ITS also follow privacy-by-design approach in their standardization work, for example for eTicketing, road charging and C-ITS services. However, all privacy concerns cannot be solved in this way.

Location based services may cause one of the main privacy risks, and Vandezande et al. [26] suggest these services should be disabled by default and manually activated by the users who will use them. Jureczek et al. [12] and Psaraki et al. [19] consider in particular location based services as a problem in fleet management systems which allow companies to track vehicles. Data from vehicles is also the concern in the threat analyses performed by Sato et al. [21], who also suggest methods for protection of privacy issues when vehicles play the role of sensors providing floating vehicle data. Jureczek et al. [12] propose techniques that blur trajectories according to the user's privacy profile. Jouvray et al. [11] address the problem of data exchange with third party service providers for charging of electric vehicles.

Øvstedal et al. [18] identify central factors to consider for privacy protection in a selection of ITS services in road transport. The ITS services may track the location of a person or vehicle, and the tracking at one single location interfere less with the privacy than tracking over a certain distance and continuous tracking. Speed control may measure the speed of a vehicle at one location, or the average speed over a distance. For road charging, vehicles may be tracked at a toll gate (one location) or by continuous tracking where the charging is calculated based on route and time data. The latter may also be realized without the exchange of detailed route data if the on-board system registers the length of a journey or calculates the costs and just exchanges data on journey length or incurred costs. Also for eTickeing the realization of the service affects the privacy. eTicketing services may be anonymous, or they may be linked to a person. The use of tickets may also generate data about the exact route used by the traveler. Pay-as-you-drive insurance and eCall services register the detailed situation or behavior of a vehicle or person. In traffic monitoring, vehicles may be registered at a single point, or they may be probe vehicles that are continuously tracked as addressed by Sato et al. [21]. It is also important whether a service is mandatory or optional.

Cincilla et al. [1] describe how Cooperative ITS (C-ITS) through broadcasting of information from vehicles may reveal sensitive information about the driver such as identity, residence, workplace, habits, etc. However, C-ITS also improve transport efficiency, safety and sustainability [3].

2.1.3 Privacy within wireless technologies

Wireless technology is the main communication infrastructure applied in Smart Cities in general, and therefore in ITS (ITS may be regarded as a special case of Smart Cities). In the following, we therefore review wireless technologies often used in Smart Cities as well as how they are related to ITS and privacy concerns.

2.1.3.1 Wireless technologies usage in smart cities

In a smart city, communication between people, between people and things and between the things themselves are increasingly important in volume and complexity. While communication between people often relates to communication between smart telephones or tablets involving mobile broadband functions, things can be as small as a sensor and traffic-modest. However, latency or reliability can be vital for these functions. Some applications will rely on personal data to enhance its service offer. The end user has ideally agreed to give away some personal data in exchange for a personalised service. However, with the proliferation of services in a smart city, personal data can be used by other applications than those originally thought. The type of personal data can range from knowing about the device, the location, the network used, to more sensitive data such as content, habits of the person, etc.

Knowing where the mobile devices such as smart phones are, allows commercial actors to tailor applications for the user. Localization is the key and can be performed by several techniques. Perhaps the best known is GPS, which, thanks to a number of satellites, can pinpoint your location at any time. This works well outdoors, but definitely not as well indoors. When the setting of interest is a mall, or public transportation, public or private WiFi can also be used. Other technologies based on Bluetooth can be used as well. Lately, beacons have received much attention.

In the following, we review some of the radio detection techniques and afferent limits. We also highlight new usage for beacons and applications and consequences as regards privacy.

One of the trends with the network evolution towards 5G is to include Internet of Things (IoT) needs, resulting in more communication and control networks, where people and things will be connected. This is illustrated in Figure 1. The radio network proliferation can be both a solution and a new problem as far as security and privacy are concerned.

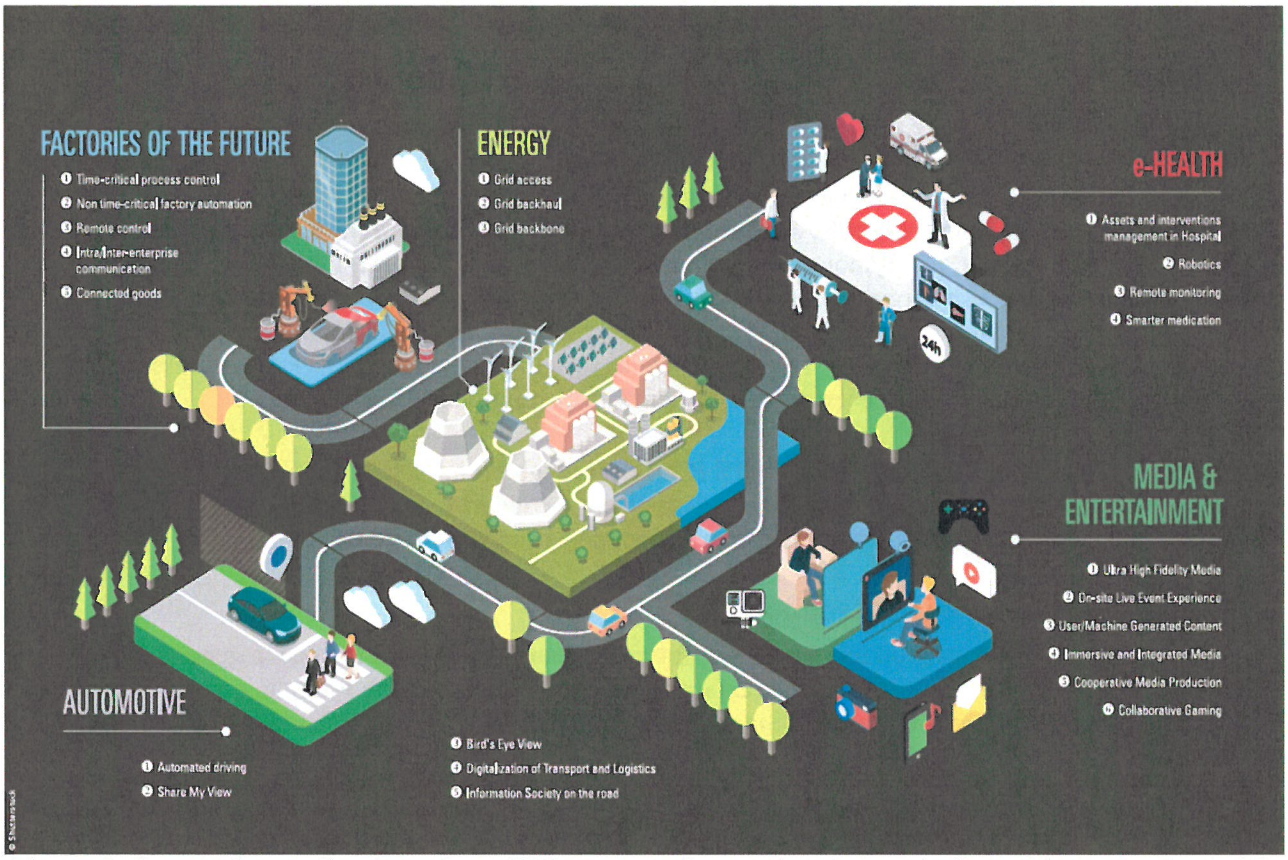
FACTORIES OF THE FUTURE
❶ Time-critical process control
❷ Non time-critical factory automation
❸ Remote control
❹ Intra/Inter-enterprise communication
❺ Connected goods
ENERGY
❶ Grid access
❷ Grid backhaul
❸ Grid backbone
e-HEALTH
❶ Assets and interventions management in Hospital
❷ Robotics
❸ Remote monitoring
❹ Smarter medication
24h
MEDIA & ENTERTAINMENT
❶ Ultra High Fidelity Media
❷ On-site Live Event Experience
❸ User/Machine Generated Content
❹ Immersive and Integrated Media
❺ Cooperative Media Production
❻ Collaborative Gaming
AUTOMOTIVE
❶ Automated driving
❷ Share My View
❸ Bird's Eye View
❹ Digitalization of Transport and Logistics
❺ Information Society on the road
© Shutterstock

Figure 2: Smart city applications, from "5G empowering vertical industries", a white paper from 5G-PPP, EU, 03/2016.

Addressing different needs have given rise to a proliferation of radio networks of different kinds, with different technical requirements and business models. All radio systems are subject to the same fundamental propagation laws that relate data rate, transmit power and range. Compromise will favour either one of these parameters, but not all together. Table 1 shows a simplification into three categories, with examples of relevant radio technologies classified according to the parameters mentioned above.

Table 3: Summary of possible wireless technologies.

	Applications and services	Relevant radio networks	Main characteristics
1	Mobile broadband communications	3GPP: 2G, 3G, 4G, WiFi	High data rates, relatively high transmit power
2	IoT communications (verticals, monitoring, control, security...)	WiFi, bluetooth, WirelessHart, ISA100	Short range, low data rate, low-complexity (relatively high data rates for WiFi).
		LPWAN; Dash-7, SigFox, LoRa, LTE-M	Compromise: larger range, low power.
3	Detection, tracking	Any of the above + beacons (often bluetooth-based)	Short range.

As mobile services allow an always-on connection to Internet while on the move, they also allow analytics of the users' needs. Metrics and statistics of apps can help to target advertising and enhance services. Tracking a large number of applications (about 30 apps on average on every smartphone) on a smart phone opens the door for the analysis of the user or a group of users in a common area where one or the other wireless network is deployed. However, wireless networks are particularly vulnerable as they allow potential eavesdropping in private arenas as well as public places where the networks are open.

Each radio network has its control and data channels. In the control part, authentication and access scheme depend on actual standard. Every radio network will broadcast its identity, usually from the base station/ access point. GSM networks came in a poor light with regards to privacy as false base stations became available on the market. End devices can communicate with these false base stations [36]. This can be detected in an unusual handover procedure with change of cell ID or location area code.

In more recent radio techniques, and in particular UMTS and LTE, a mutual authentication and stronger encryption have been introduced. This makes eavesdropping from a false base station more difficult.

The GSM vulnerability illustrates the potential dangers of a radio network. More generally eavesdropping can reveal

- A signal, a transmission exists at a particular frequency
- The location of an end-device
- The waveform, which technology (GSM, UMTS, LTE, WiFi)
- Any combination of the above

2.1.3.2 Range and data rate considerations

One of the most common methods for detection is the level of received signal. The combination of frequency band, channel width, transmit power, modulation, and data rate will contribute to define range of acceptable reception-coverage. Figure 3 shows a comparison of some wireless techniques used or planned for smart city services.

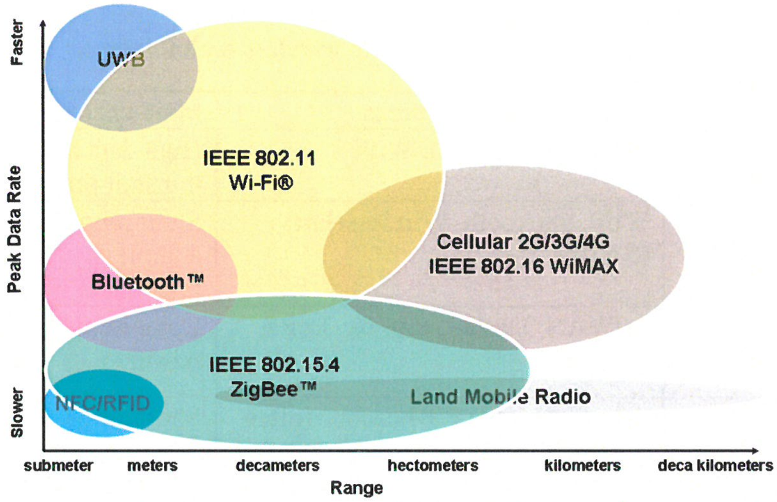

Figure 3: Comparison of some common wireless mobile, broadband and IoT techniques.

2G (GSM)/3G (UMTS), WiFi and Bluetooth are most common and available on all smartphones. Many have extra capabilities to 4G (LTE). The aforementioned technologies can be used for detecting an end-terminal. Hereafter we will focus on two cases: WiFi and Bluetooth, and in particular their potential range that defines the zone where eavesdropping will be possible.

2.1.3.3 WiFi and Bluetooth characteristics

The data rates between WiFi and Bluetooth are different as shown in Figure 3, but there is some overlap in range as the latest versions of Bluetooth allow for higher power, hence larger range. Depending on the propagation conditions and possible interferences, the following ranges can be assumed:

- WiFi (IEEE 802.11n): 50-200m, typical range is 70m indoor, while 200m outdoor.
- Bluetooth (IEEE 802.15.1 a): 1-100m. Bluetooth Smart has an extended range over 100m thanks to increased transmit power.

Both standards (WiFi and Bluetooth) use unlicensed spectrum (2.4 GHz and 5 GHz bands), also known as industrial, scientific, and medical – ISM. In unlicensed bands, interferences are more likely to occur, resulting in unreliable, unstable service, but its attractiveness relies in the fact that the spectrum is free, and the roll-out process is straightforward and swift.

Two aspects of interferences, noise and collision, will disturb a service. Noise is caused by a physical blockage for instance and the interesting signal is difficult to extract from the rest of the noise, but interference is also caused by different transmitters trying to access the system and get a channel concurrently. In order to avoid collisions, frequency hopping techniques are used to mitigate poorer performances when several WiFi or Bluetooth systems are co-located.

2.1.3.4 An experience with WiFi-based detection

In the project Åtot (which was a User-driven Research based Innovation (BIA) project), detection was used to track bus passengers, and allow the bus company to gather and analyse the number of passengers and the travel patterns of passengers to get input to the public transport route planning process. The idea was to avoid expensive cameras on board buses and rely instead on the WiFi network cards of different end-devices like smart phones that most passengers carry. The parameters that can be detected include the received power, channel number and time between transmitted (and detected) packets.

A Kismet [45] system was used. Kismet is an 802.11 wireless network detector, sniffer and intrusion detection system. It works with wireless card supporting raw monitoring mode and can sniff 802.11 b/a/g/n traffic. Kismet detects data traffic by collecting packets.

The experience from early measurements from the project indicate that the detection can be carried out to levels in general higher than the sensitivity levels expected, as the network card employed misses some low level packets. The detections tests were carried out in different environments like a home and an exhibition hall. Detected levels were above -55dBm, corresponding to a free range of up to 50 m.

This indicates that an off-the-shelf detector installed in a bus can detect the WiFi signals from the smart phones on board, but most likely not the signals from smart phones outside the bus but in its vicinity. This is because buss windows and doors are the only electromagnetic propagation openings and the signals emitted from inside the bus are likely to be largely attenuated, and therefore most likely undetected, when coming from smartphones located outside.

This method seems adequate for passenger count. Indeed the issue was not to detect several packets coming from one smartphone but to know how long this unit has been on board the bus before being detected and how time was elapsed between the last detection and the time when the person left the bus.

In the project, several solutions to avoid intruding passengers' privacy have been considered, including

- Anonymizing the MAC address, through shortening or cryptography techniques
- Use of pseudonym and changing regularly (e.g. once a day)
- Separation and control of domains (e.g., invoicing)
- User can see and delete the data retrieved

2.1.3.5 Beacons

Beacons are small, cheap broadcasting units and are deployed by different commercial actors, particularly in public places such as malls, public transport stations, etc. Beacons are a one-way system. They broadcast their identity and use Bluetooth Smart [38], [39]. Beacons come in different shapes. Some commercial examples are shown in Figure 4.

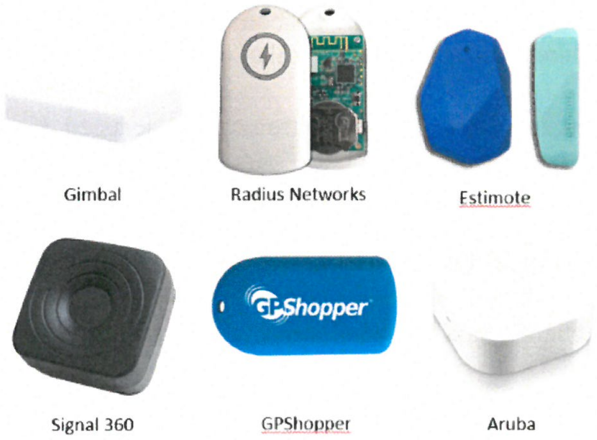

Figure 4: Beacon examples.

Bluetooth Low Energy (BLE, marketed as Bluetooth Smart) focus is on data, excluding voice. It differs from the earlier versions of Bluetooth as it addresses a specific need of many Internet of Things applications, namely, a low duty cyle (bursty, not thirsty applications) and low signalling levels in order to save energy from battery-operated devices where batteries should last for several years. BLE beacons sleep most of the time, waking up only to broadcast an advertisement.

The 2.4GHz spectrum for Bluetooth extends from 2402MHz to 2480MHz. LE uses 40 1MHz wide channels, numbered 0 to 39. Each is separated by 2MHz. Channels 37, 38, and 39 are used only for sending advertisement packets. The rest are used for data exchange during a possible connection. This is shown in Figure 5. During BLE advertisement, a central device scanning for beacons listens to those channels. Should there be interference from another Bluetooth or WiFi channel, it is possible to hop to another advertisement channel. Since BLE has a low latency down to 6 ms, compared to previous versions, it is well adapted to advertisement channels. In fact, a random delay can be added in order to reduce the probability of packet collisions and improve robustness.

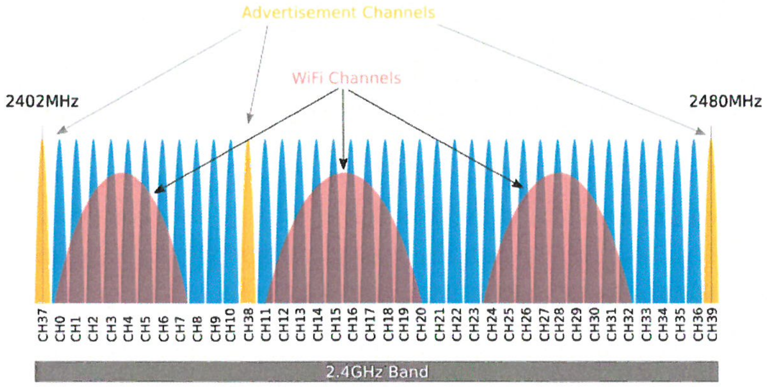

Figure 5: Bluetooth channel plan (from [46])

Many telecommunication operators allow the reading of the beacon identity. Beacons allow the smart phone of an end-user to locate itself, as whenever the smart phone comes near the beacon an app will generate an alert. This however relies on a couple of actions from the user. He/she must previously have downloaded the appropriate app, and allowed for location retrieval and enabled Bluetooth on the phone. The result is that on a sheer physical side, the smart phone is tracking the beacon, not the opposite. Another consequence is that the battery of the smart phone is likely run out faster than that of the beacon.

The denser the beacons are placed, the more precise location can be deduced. Using beacons technology give companies insight in customers' pattern of movement. Commercial actors can then know about the smart phone location and which store or even which segment of the store it is located. Special products or deals can be highlighted on your phone and guide your shopping experience. Such a mall example can be envisaged also in public transportation like in train stations or airport where the passenger is guided.

The systems will interact and exchange data with each other and receive data from "things" in their vicinity – provided there is wireless coverage - to be able to provide value added services and smart functionality to their users. While the original thought for beacons was that an entity - say a transport company - would use their own beacons to enhance their service, the beacon apps opens for reading also others' beacons. In addition, the applications previously installed on the phone may be updated to read beacons in the vicinity. By default, these apps can have a beacon reading function, which basic functionality will be to give information about the beacons read, i.e., the location of the smart phone. The beacon app extends the physical location of the Bluetooth coverage to a common register where other applications can potentially make use of private data.

An example of proximity detection and beacon application is shown in Figure 6.

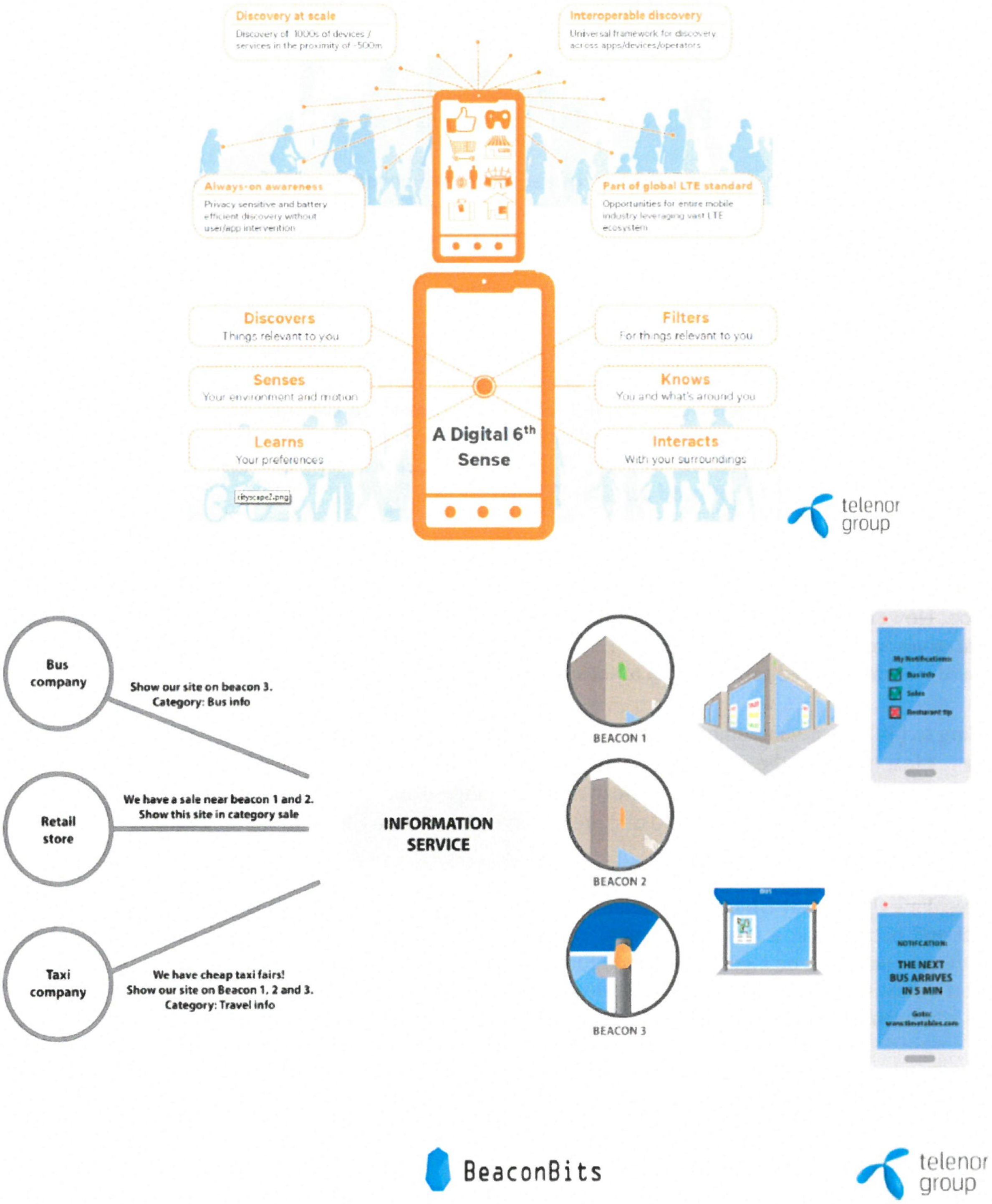
Discovery at scale
Discovery of 1000s of devices / services in the proximity of ~500m
Interoperable discovery
Universal framework for discovery across apps/devices/operators
Always-on awareness
Privacy sensitive and battery efficient discovery without user/app intervention
Part of global LTE standard
Opportunities for entire mobile industry leveraging vast LTE ecosystem
Discovers
Things relevant to you
Senses
Your environment and motion
Learns
Your preferences
A Digital 6th Sense
Filters
For things relevant to you
Knows
You and what's around you
Interacts
With your surroundings
cityscape2.png
telenor group
Bus company
Show our site on beacon 3.
Category: Bus info
Retail store
We have a sale near beacon 1 and 2.
Show this site in category sale
Taxi company
We have cheap taxi fairs!
Show our site on Beacon 1, 2 and 3.
Category: Travel info
INFORMATION SERVICE
BEACON 1
BEACON 2
BEACON 3
My Notifications:
Bus info
Sales
Restaurant tip
NOTIFCATION:
THE NEXT BUS ARRIVES IN 5 MIN
Goto: www.timetables.com
BeaconBits
telenor group

Figure 6: Beacon Bit, the beacon app from Telenor.

Beacon Bits app is built using ContextHub platform, which makes it easy to develop beacon-enabled apps. Indeed, the Beacon Bits app can broadcast as a beacon or locate beacons, which will turn the phone into a beacon or beacon locator. It can be used by developers to develop a beacon app although they actually do not own actual beacons.

Beacon actors allow for a wider usage of beacons. While the original thought for beacons was that an entity - say a store or transport company - would use their own beacons to enhance their service, the beacon apps opens for reading also others' beacons. In addition, the applications previously installed on the phone may be updated to read beacons in the vicinity. By default, these apps can have a beacon reading function, which basic functionality will be to give information about the beacons read, i.e., the location of the smart phone.

The beacon app extends the physical location of the Bluetooth coverage to a common register where other applications can potentially make use of private data. The case of beacons and beacon applications highlight the challenges occurring when services of common interest come in the way of personal data protection. The beacon applications in particular can propagate personal data to other applications than the one originally accepted by the user.

While there are applications of common interest for the society, these do not usually have the financial means to protect usage by a single beacon operator / owner. Instead, the advertising industry has benefits from reading the smart phone positions, register different interests and combine this accumulated data into a tailored advertising offer. Beacon applications' lack of security and restriction to a particular beacon owner does not appear to be quite open information. It makes it difficult to take educated decisions about giving away personal data in order to get good services [37].

2.1.3.6 Applicability of WiFi and Bluetooth networks to ITS

Wireless networks are enablers to many applications at home or on the move, and ITS applications are no exception. However, wireless networks are quite vulnerable as far as privacy is concerned, since they allow potential eavesdropping within their range. Exposed data that can be retrieved include the transmission, the location of transmitter, and can range up to the content of the transmission.

According to [40], intra-vehicular wireless channels have several properties such as

- Most (90%) of the coherence bandwidth at 2.4 GHz is around a few MHz
- The coherence time of the intra-car channels range from 2.5 to a few hundred seconds
- Very large path loss (over 80 dB) are observed between a transmitter and a receiver located in two different compartments

These results indicate that Bluetooth channels in particular may be well adapted as they feature low-power, low-cost and occupy just a few MHz bandwidth. Although BLE was not originally designed for vehicular applications, it seems to be a good candidate for the ITS services as it includes both a star topology approach and a broadcasting mode, giving several physical possibilities to a specific application. Specific carrier-sensing approach has also been described [41], in order to facilitate the detection of weak beacon signals.

As far as C-ITS is concerned, regional initiatives and standardization processes have already started. For example in Europe and USA, a first common release of the standard [42] has been published. This is based on IEEE 1609 on the service advertisement and messaging protocols. Work is still on-going to harmonize single-hop and ad-hoc protocol sets from IEEE 1609 and ISO TC204 (WG16). What is remarkable in this context is the use of ad-hoc communication means that there is no centralized entity that can gather information; the information flows from vehicle to vehicle within a range of about 100m in an urban environment. The MAC address can also be shortened and therefore made anonymous. The Cooperative Awareness Message (CAM) gives information on the vehicle type, position, heading, speed, and acceleration. It also makes the vehicle anonymous through a length information in dm, not cm, which does not allow the precise vehicle brand and model recognition. At last, the certificate is changed on a daily basis.

Altogether, the different approaches concur to protect personal data of the drivers, in spite of the C-ITS concepts relying primarily on a collective data gathering effort.

At last, privacy by design may consider going for higher frequencies and defining closed groups for a particular application. Indeed, millimetre-wave systems will, by design, enhance privacy as these are high frequency radio waves that are intended for short distances. In LTE systems, the indoor version of LTE includes in its standard the possibility of defining a closed group of users (e.g., family members and the related devices). Limiting the access to a network to a given list of MAC addresses would reinforce privacy. However, most smartphones and ITS devices make use of public networks when on the move.

2.2 Understanding privacy challenges within ITS based on a realistic case

Different target groups use ITS services for different purposes. To obtain a holistic understanding of privacy challenges within ITS, we need to view the usage of ITS from the perspective of various target groups. In this section, we look into relevant target groups and provide an example case on ITS to illustrate the complex privacy challenges. The ARKTRANS framework [17] provides a functional decomposition of the transport domain into the following sub-domains according to the generic roles of the stakeholders involved.

- ITS for Transport Service Clients support transport demands, travel planning, booking of transport services, journey execution and access to travel information.
- ITS for Transport Service Providers support the provision of transport services, e.g. public transport services, taxi services, parking services and charging services for electric cars. One focus is to manage relations with Transport Service Clients to support booking, ticketing and information provision. Another focus is to manage the operations delivering the transport services (transport operations, charging of electric vehicles, etc.) and the associated use of resources (fleets of transport means, personnel, parking slots, chargers, etc.).
- ITS for Drivers target on-board control and support, and include systems for driver assistance and safe driving such as automated and built-in ADAS (Advanced Driver Assistance Systems) and C-ITS, systems mounted in the car (e.g. tags for road charging), and other systems for driver support (e.g. built-in or portable navigation systems) and systems providing data.
- ITS for Traffic Management contribute to the best possible utilization of the transport network by providing support for vehicle and traffic data acquisition, traffic management planning, traffic monitoring, traffic control, and transport demand management (e.g. road charging to reduce the traffic).

It is important to notice that one actor may have several roles and thereby use several categories of ITS. For example, a traveler planning and getting travel support is a Transport Service Client. On the leg between his home and the train station, the traveler may be a Driver. Finally, while driving his car, the traveler may offer to share his car via a car sharing service and thereby take the role as Transport Service Provider. Similar to the above, one system may fulfill several purposes and belong to several ITS categories. A portable navigation system may be ITS for Transport Service Clients as well as ITS for Drivers.

2.2.1 Example case on ITS

Figure 7 illustrates a realistic example on ITS. The ITS services considered in our case are interconnected via wireless communication. In the case, we follow "Joe" and consider potential situations where his personal data is exposed to privacy risks while using ITS services. Joe has a Travel Companion App on his mobile phone. This app supports Joe when he switches between several roles: Joe makes use of ITS for Drivers when driving his electric car, ITS for Transport Service Providers when offering to share his car, and ITS for Transport Service Clients during travel planning and execution. There are also other apps on Joe's phone, one of these, the "Vicious App", eavesdrops to collect and sell information about Joe. For example, it may collect signals from beacons. Beacons are small and inexpensive broadcasting units that use Bluetooth to allow the smart phone of an end-user to locate itself.

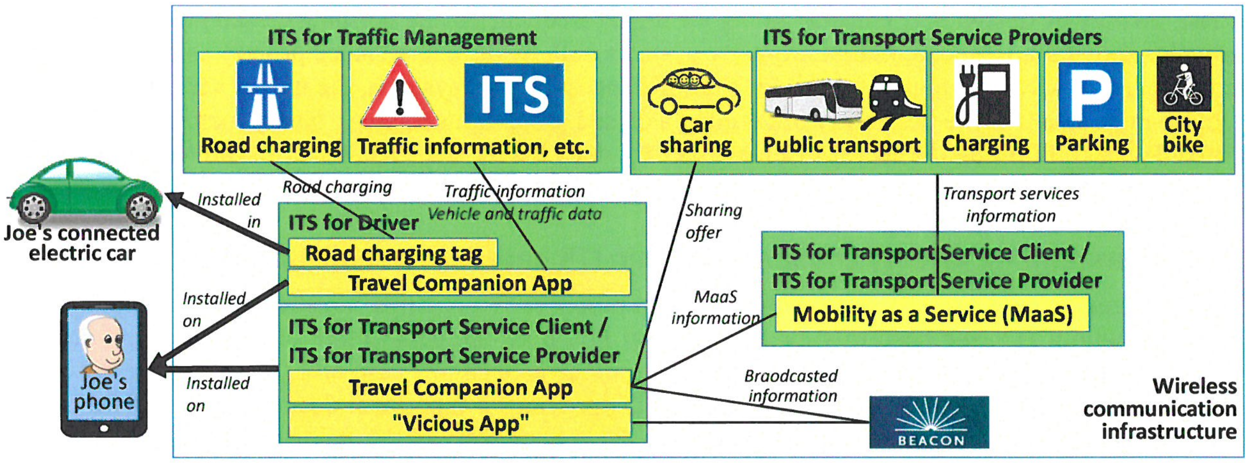
ITS for Traffic Management
ITS
Road charging
Traffic information, etc.
ITS for Transport Service Providers
Car sharing
Public transport
Charging
Parking
City bike
Joe's connected electric car
Installed in
Road charging
Traffic information
Vehicle and traffic data
ITS for Driver
Road charging tag
Travel Companion App
Sharing offer
Transport services information
ITS for Transport Service Client /
ITS for Transport Service Provider
Mobility as a Service (MaaS)
MaaS information
Installed on
Joe's phone
ITS for Transport Service Client /
ITS for Transport Service Provider
Travel Companion App
"Vicious App"
Installed on
Broadcasted information
BEACON
Wireless communication infrastructure

Figure 7: Example case on ITS.

When Joe makes use of ITS for Transport Service Clients, the Travel Companion App interacts with the MaaS Provider to find the best possible travel alternative and to get support during the travel. MaaS (Mobility as a Service) is a single point of contact for transport services covering the whole journey. The journey may be composed of many legs and services offered by different service providers, but Joe only interacts with the MaaS provider that composes and offers the complete journey for just one payment. Thus, from Joe's perspective, the MaaS provider is a Transport Service Provider while Joe is the Transport Service Client. However, in order to compose a journey for Joe, the MaaS provider must send requests to the individual services (public transport, charging, parking, etc.) and in that case takes the role as Transport Service Client.

When Joe drives his car, the Travel Companion App supports navigation based on real-time traffic information. Both the road charging tag and the Travel Companion App support road charging. The former interacts with toll stations, while the latter reports data on actual road use (distance, locations, time, etc.) to support price calculations. Table 4 describes potential usage scenarios and related privacy risks in the context of our case.

Table 4: Potential scenarios and related privacy risks.

Potential scenario	**Privacy risk examples**
When Joe prefers to travel by public transport, the Travel Companion (TC) App uses Joe's preferences to request a door-to-door journey. He receives possible travel plans and selects a plan with a shared car to the train station that matches the arrival time of the train, and on arrival to the city center, a city bike is available for the last leg.	• The TC App communicates Joe's preferences and transport demands to MaaS. Preferences, routes and other data may be stored for later use by MaaS to build a prole of Joe's travel patterns. • The car sharing service matches Joe with a driver. For safety/security reasons, their identities are stored.
In train stations, the TC App gets information on special offers from beacons. The same happens when Joe picks up the city bike.	• The Vicious App also detects beacon signals and thereby Joe's location. His travel patterns are tracked, and he receives customised offers.

When the train is delayed, the TC App guides Joe on a bus journey with several transfers. Joe is tracked, and his patterns are used in the planning of public transport services.	• If Joe travels by bus often, and there are few other passengers following the same route, it may be possible to identify Joe and to find a pattern.
When Joe travels by car, the TC App uses a car sharing service to match Joe with other drivers. Joe receives a 70 % road-charging discount when he drives and shares an electric car. The parking service detects Joe when he arrives at and leaves work, and TC App organises the payment.	• Same as above with respect to car sharing. • The link between Joe and other drivers is registered. • To receive the discount, data on car sharing must be exchanged and stored. • Joe is also tracked by the parking provider, included the time he spends at work.
Joe's car is registered by road-side equipment, and information is delivered to the road-charging agency. The information is also used in calculations of travel times and travel patterns.	• Timestamps, locations and distances are tracked.
Assume Joe goes exercising after work, and that this information is stored in Joe's calendar. The TC App may use this information to book an electric car charger close to the gym in advance. Such pre bookings support demand side load balancing in the grid, and Joe will get a 5% charging discount.	• Use of calendar information is convenient, but Joe's plans are exposed in advance and may be sold to others, used in marketing, etc. • Pre-booking is convenient for both Joe and the service provider, but data must be stored, and charging patterns may be discovered.

Table 4 is by no means complete, but it illustrates different situations where the Travel Companion App and the MaaS service provider have access to and may store detailed data on Joe's life. The motivation may for example be to learn about Joe's preferences and habits and thereby provide customized user support. However, data can also be used for purposes that Joe is not aware of, and by analyzing Joe's data, it is possible to generate information on how Joe drives according to speed limits, his routines, where he goes shopping, where he spends time, etc. The Vicious App may, if Joe's phone uses wireless technology such as Bluetooth, detect signals from beacons and track Joe regardless whether the app has access to location information or not.

2.3 Results from interviews and workshop

In this section we summarize the results obtained from the interviews and the workshop. The answers to the questions are given according to the order in Table 1. Moreover, in each interview, as well as in the workshop, we signed a non-disclosure agreement with the interviewee. Because of this, the answers are presented in an aggregated manner to avoid disclosing the identity of each interviewee. The summary for questions Q3, Q5, and Q7 include results obtained from the interviews as well as the workshop. The respondents in the interviews did not participate the workshop and vice versa, but they all were experts in the domain.

Q1 Have you experienced incidents related to privacy? In general, respondents pointed out that privacy-related incidents currently do not occur often, but that emerging ITS services such as MaaS and C-ITS will bring complex privacy issues, in particular privacy risks related to tracking. In terms of specific incidents, one respondent reported on leakage of privacy data from approximately 40'000 vehicles due to poor categorization of privacy-related and non privacy-related information, while another respondent reported on social engineering incidents. The remaining three respondents did not report on specific privacy incidents.

Q2 How do you preserve privacy? Privacy is preserved by following general privacy-by-design recommendations and guidelines. However, the most commonly used techniques are to anonymize and pseudonymize data. These techniques are regarded as useful and effective, but they are often carried out in an ad hoc manner. Current recommendations and guidelines are helpful to obtain general directions for how to preserve privacy, but the respondents highlight the need for techniques to identify privacy-related issues and requirements early in the development phase, as well as the need for processes to check compliance with the recent EU Regulation 2016/679 [5].

Q3 How do you assess privacy risk? Privacy risks are mainly assessed using in-house check lists. In addition to check-lists, one respondent develops use-cases which in turn are analyzed to identify potential privacy risks. Moreover, one respondent pointed out that although check lists are developed and put into action by the management, there are no processes to check whether the intended target group, such as developers, document and address identified privacy risks. Two respondents pointed out that privacy risk assessment must be carried out in a systematic way as an integrated phase of the development life cycle, in order to identify privacy risks early in the development. With respect to responses collected from the workshop, most answers align with aforementioned results. However, four respondents in the workshop represented large organizations and used more rigor approaches to assess privacy risks. In particular, these large organizations have employees positioned as Data Protection Officers managing the assessment of privacy risks by making use of general privacy impact assessment methods, developing and analyzing detailed data flows, carrying out code-reviews focused on privacy, and employing in-house routines for classifying privacy-related data.

Q4 How do you communicate privacy issues internally as well as externally (for example to customers / end-users): In general, privacy risks are considered and communicated at the business level (by managers). One respondent pointed out that this is done in an ad hoc manner. All respondents pointed out that the challenge is to communicate privacy risks at low-level of abstraction, for example to developers, in order to properly address privacy risks in the services provided. One respondent mentioned that developers sometimes perceive this top-down communication of privacy risk as a distraction because they have to focus on management tasks rather than development tasks. Another factor is that privacy risks at business level often use legal language, which makes it more difficult to understand and address at implementation level. With respect to external communication, the main channel used is web-pages and references to standards and regulations. In addition, two respondents communicate privacy risks externally (to end-users and ITS-providers) by writing newspaper articles and holding public seminars.

Q5 What privacy challenges do you find relevant in current and emerging ICT services? Privacy challenges mentioned by all respondents are the increasingly large volume of data being logged, real-time tracking, and less anonymity, e.g. broadcasting unencrypted privacy-related information in the context of C-ITS. Another challenge is how to make privacy-sensitive services consent-based in an easily understandable manner by end-users because privacy policies are mainly defined in terms of long legal texts, and often ignored by users [22]. End-users have to easily understand what they consent to. Different regions have different privacy-related laws and regulations. A challenge in this respect is to assess whether a service comply with the law/regulation in question. In particular, it will be challenging to assess whether current and legacy systems comply with the new EU Regulation 2016/679 [5]. Moreover, systems neither provide an overview of the information stored about an end-user nor enable end-users to delete this information in an easy way. Interestingly, with respect to responses collected from the workshop, most respondents regarded privacy as a major obstacle limiting potential business opportunities such as MaaS and other advanced ITS services. The participants highlighted that emerging privacy-sensitive applications must be consent-based in exchange to better and more advanced services. The workshop-respondents also pointed out that emerging applications will need to collaborate and exchange privacy-related data between each other, which in turn may violate privacy policies because different applications have different privacy policies.

Q6 How is privacy an obstacle to develop new and useful services? Respondents were concerned about the high fines announced by EU Regulation 2016/679 [5] and they pointed out the challenging trade-off between "complete" privacy versus providing useful services. For example, a service to predict collisions in C-ITS requires all nearby vehicles to publicly broadcast their speed, direction, and location. One respondent often experience that privacy requirements demanded by the government are not possible to implement without negatively affecting the usefulness/intended purpose of the service.

Q7 How can methods to assess privacy risk be helpful? Respondents mentioned that methods to assess privacy risks would help balance the trade-off between "complete" privacy versus useful services by facilitating guidelines to reason about acceptable and not acceptable privacy risks. Moreover, a method would be useful to consider privacy risks throughout the complete value chain, which may in turn facilitate internal revisions with respect to privacy. Governmental and industrial organizations need proper methods to assess privacy risks because many applications collect a very large amount of data which is difficult to categorize as privacy-related or not privacy-related data. Methods will also be useful to assess compliance to laws and regulations. Moreover, it was explicitly pointed out that the privacy risk assessment method must be a part of the organizational risk assessment strategy, carried out using a continuous "privacy life-cycle approach", and capable of suggesting treatments to privacy-risks within ITS. This is because the nature of services within ITS, including the way they use and exchange privacy-related data, evolve in an unpredictable manner.

2.4 Summary, needs and challenges

ITS services are very dynamic with respect to how they are used and by whom, what technology they are based on, as well as how they manage data. In general, ITS services are used by end-users to get travel assistance, as well as to plan and carry out journeys. On the other hand, ITS providers collect data from end-users, and the providers may also combine data from several services to provide even more useful value added services. The data may be collected and processed in a manner completely oblivious to the end-user, which in turn may expose end-users to privacy risks related to tracking and monitoring. For example, generate information about how an individual end-user drives according to speed limits, daily routines of the individual, where the individual goes shopping, and whom the individual meets at a certain time and location.

Within ITS, end-users are exposed to privacy risks, while ITS providers are exposed to privacy-compliance risks.

End-users need to be informed and be aware of exposed privacy risks caused by ITS services. Moreover, due to the highly dynamic and complex ecosystem of ITS services, end-users need to be informed about privacy risks in real-time, and based on that decide whether or not to use the service in question.

ITS providers need to identify privacy risks of the services at implementation level early in the development phase, obtain a privacy risk picture of ITS services in real-time, and to properly assess privacy risk with respect to compliance with privacy laws and regulations - in particular compliance with the recent EU Regulation 2016/679 [5].

Privacy risks are in general assessed by making use of general Privacy Impact Assessment (PIA) methods. These methods are often too generic and carried out at a high-level of abstraction, and they need to be specialized towards ITS services. To the best of our knowledge, there are two domain-specific PIA methods for ITS services [20], [6]. These approaches are useful for assessing privacy risk of ITS services at business level, but they lack two important features. First, they do not facilitate real-time privacy risk assessment of ITS services. Second, they mainly facilitate privacy risk assessment from the provider point of view, and do not include assessment from the end-user point of view.

To summarize:

- There is need for practically useful tool-supported methods for real-time privacy assessment of ITS services to:
    - Inform end-users about exposed privacy risks caused by ITS services in real-time.
    - Help ITS providers assess privacy-compliance risks of their services in real-time.

Moreover, this means that the methods need to facilitate privacy risk assessment from the perspective of end-users, as well as from the perspective of ITS providers.

- ITS providers need methods and techniques to identify privacy risks at design and implementation level to properly implement privacy-risk measures. The methods and techniques should also show a clear link between high-level privacy risks at business level, and low-level privacy risks at implementation level.

3 Research questions and success criteria

Based on findings from the empirical work presented in Section 2, the main research questions in PrivacyAssessment@SmartCity project are the following:

- RQ1: How can we identify and manage privacy risks in smart city solutions? What privacy-relevant requirements should be posed to the smart city solutions, providers and customers?
- RQ2: How can privacy-awareness of smart city solutions be evaluated and validated in real-time? What kind of methods and decision support is needed for this?
- RQ3: How can we develop and offer useful and pragmatic principles/guidance for privacy management of the smart city solutions?

In this section, we identify success criteria for a method to assess privacy risks of ITS. We motivate each success criteria **SC** with respect to information obtained in Section 2.

Concerns and risks related to privacy are perceived differently depending on whether it is viewed from the perspective of a provider or an end-user. The state of art privacy practices within ITS identify the ability of services to track, locate, and identify individuals as major privacy risks for end-users. Some of the stakeholders we interviewed have similar concerns. To mitigate these risks, the literature provides possible risk-treatments, as indicated in Section 2.1.2. However, as pointed out in our case on ITS (see Section 2.2), emerging ITS applications need to broadcast and process data in a public manner to provide useful services (Mobility as a Service, and Cooperative ITS). On the other hand, providers need to comply to strict privacy regulations or face devastating fines [5]. As pointed out by the stakeholders we interviewed, this is perceived as a risk to business opportunities. In short, end-users need to assess how much privacy-related information they are willing to share, or in other words how much privacy-risks they are willing to take, in return for services, while providers need to assess whether they comply with privacy regulations and at the same time still able to provide services. Thus, the method must facilitate privacy risk assessment on behalf of providers as well as end-users.

SC1: The method must facilitate privacy risk assessment on behalf of providers as well as end-users.

End-users are interested in obtaining a correct picture of their privacy-risk exposure based on choices they make. For example, when agreeing to a privacy policy. On the other hand, providers are interested in obtaining a correct risk picture of their systems and services to check whether they comply with privacy regulations. In both cases, not having a correct picture with respect to privacy risks may lead to serious consequences. For example, an end-user may be harmed by malicious people tracking and locating him or her, while a provider may end up in a lawsuit and shut down the business. When assessing privacy-risks, it is therefore important not to leave out any relevant risks in order to obtain a correct risk picture.

SC2: The method must support the identification of relevant privacy risks.

To the best of our knowledge, the majority of current methods assess privacy risks at a high-level of abstraction (that is, at business level) and suggest treatments accordingly (see Section 2.1.1). However, current privacy practice within ITS indicate that privacy issues have to be handled when technology is specified and developed (see Section 2.1.2). Moreover, as pointed out by experts we interviewed, there is a gap between high-level privacy risks identified at business level and their corresponding low-level risks at implementation level. We need to bridge this gap to support developers understand and identify privacy risks at implementation level, which in turn helps developers to implement appropriate risk treatments, and thereby address privacy risks from a bottom-up approach.

SC3: The method must facilitate the transition from high-level privacy risks (i.e., business level) to low-level privacy risks (i.e., implementation level).

As pointed out in Section 2.1.1, conducting privacy risk assessments is costly. In particular, the mobility aspect of ITS (see Sections 2.1.2, and 2.2) introduces an extra dimension of complexity, which must be considered in a privacy risk assessment. This will inevitably add to the already costly assessment process. General methods address the cost of assessing privacy risks by carrying out a threshold analysis. Similarly, we need to make sure that privacy risk assessment of ITS is carried out in a cost-effective manner.

SC4: The method must be cost-effective.

The mobility aspect of ITS demands real-time assessment of privacy risks. As explained in Sections 2.1.2 and 2.2, privacy-related data is exchanged, processed, and stored dynamically by different actors to provide various real-time ITS services. This, in turn, means that privacy risks within ITS may occur dynamically and in real-time. For example, the continuous tracking of Joe's journeys as explained in Section 2.2. The method must therefore take this dimension of mobility into account and thereby support real-time privacy risk assessment.

SC5: The method must support real-time privacy risk assessment.

As discussed above, privacy is perceived and assessed differently by different stakeholders. Moreover, as explained in Section 2.2, ITS services are used by a number of different stakeholders for different purposes. This means that the method must provide appropriate guidelines to assess privacy risks depending on the stakeholder carrying out the assessment. In addition, these guidelines must be comprehensible by the relevant stakeholders. In other words, the method must provide appropriate and comprehensible guidelines to relevant stakeholders carrying out the assessment.

SC6: The method must provide appropriate and comprehensible guidelines to relevant stakeholders carrying out the assessment.

For the same reason as for requirement SC6, the method must also produce output that is appropriate and comprehensible to relevant stakeholders. For example, ITS-service providers would probably be interested in a detailed output that represents identified privacy risks in terms of likelihood of occurrence and their consequence on privacy, while an end-user would probably be interested in a simple qualitative indication on whether his or her privacy-risk exposure is "high, medium or low", where the meaning of high, medium, and low is predefined. Thus, success criterion SC7.

SC7: The method must produce output that is appropriate and comprehensible to relevant stakeholders.

4 Research method

Given the scope of this project, and the desired results from the work initiated by this project, we mainly conduct research according to the technology research method. In the following we first give an overview of the technology research method, and then we give an overview of evaluation strategies to evaluate an artifact, and finally we explain how we apply the research method in this project.

The technology research method is iterative and motivated by the need for a new artifact, or the need to improve an existing artifact [29]. The researcher starts by identifying a set of requirements to the artifact. Depending on the artifact, the requirements may be identified from the viewpoint of existing users, potential/new users, as well as other stakeholders, such as people who seek to obtain economical gain by maintaining or selling the artifact. Then, having identified the requirements, the researcher aims to invent an artifact which fulfils the requirements. This is the step in which the researcher needs to be innovative and use his/her creativity and technical expertise. Finally, having developed the artifact, the researcher needs to evaluate the artifact to check whether it fulfils the requirements and thereby whether it satisfies the (potential) need. If the evaluation yields successful results, the researcher may argue that the artifact satisfies the need. If the results are negative, the researcher may try to adjust the artifact accordingly and reiterate the evaluation. Thus, the technology research method consists of the following three steps (see Figure 8).

- **Problem analysis**: The researcher captures a potential need for a new or improved artifact by interacting with possible users and other stakeholders.
- **Innovation**: The researcher tries to construct an artifact that satisfies the potential need. The overall hypothesis is that the artifact satisfies this need.
- **Evaluation**: Based on the potential need, the researcher formulates predictions about the artifact and checks whether these predictions come true. Predictions are evaluated/tested by making use of evaluation strategies (described in Section 4.1). If the results are positive, the researcher may argue that the artifact satisfies the need.

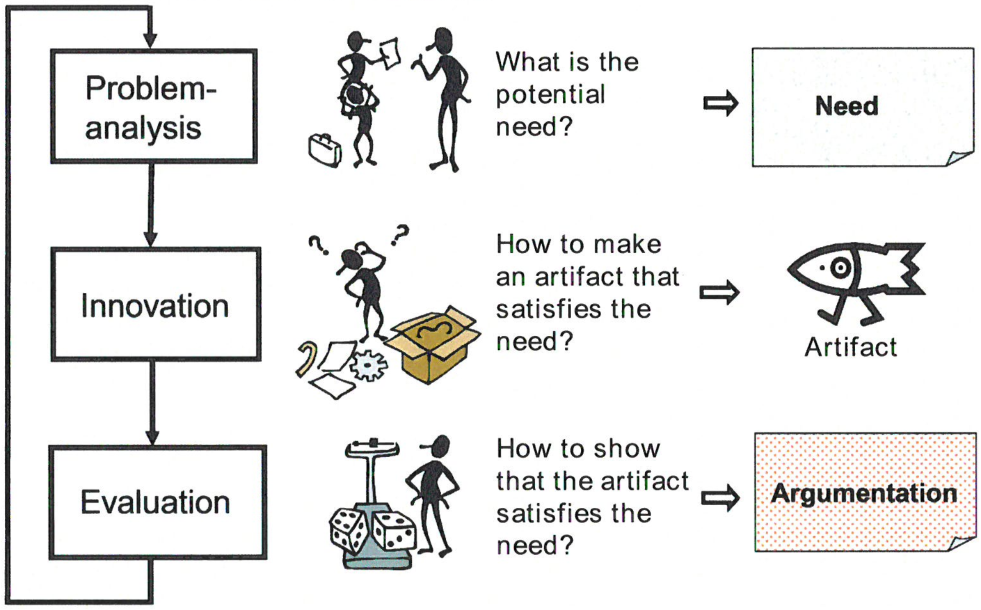
Problem-analysis
What is the potential need?
Need
Innovation
How to make an artifact that satisfies the need?
Artifact
Evaluation
How to show that the artifact satisfies the need?
Argumentation

Figure 8: The main steps in the technology research method (adapted from Solheim and Stølen [29]).

4.1 Evaluation strategies

According to McGrath [31], evaluation strategies are carried out to gather evidence to assess the degree of generality, precision, and realism of the artifact under evaluation. This is illustrated in Figure 9. Generality indicates that results are valid across populations. Precision indicates that the measurements are precise. Realism indicates that evaluation is performed in environments similar to reality.

When gathering a batch of research evidence, one is always trying to maximize the scores on generality, precision and realism of the prediction under evaluation. While it is most desirable to maximize all of these three qualities simultaneously, it is, however, an impossible act [31]. Broadly speaking, it is therefore important to consider factors such as the nature of the predictions (that is, whether the predictions address the generality, precision or realism of an artifact), the maturity of the artifacts addressed by the predictions, and the available resources (time, cost and people) when choosing evaluation strategies. In the following, we give an overview of the most common evaluation strategies.

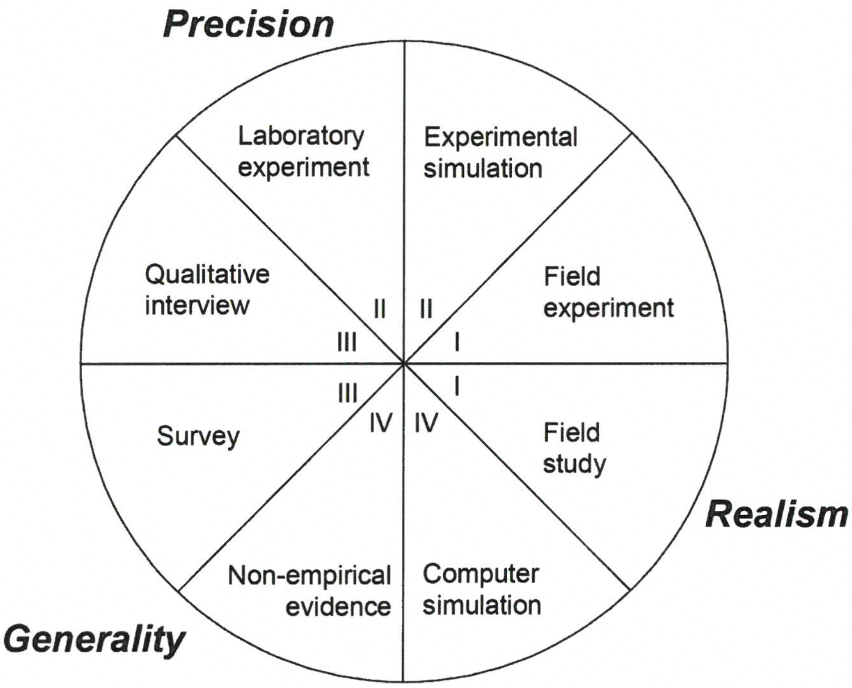

Figure 9: Evaluation strategies (adapted from McGrath [31]).

- **Field study** is a direct observation of "natural" systems, with little or no interference from the researcher. Field studies are strong on realism but lack precision and generality because they are difficult to replicate.
- **Field experiment** is similar to field study in the sense that it is an experiment carried out in a natural environment. However, in field experiments, the difference is that the researcher intervenes and manipulates a certain factor.
- **Experimental simulation** is a laboratory test simulating a relevant part of the real world.
- **Laboratory experiment** gives the researcher a large degree of control and the possibility to isolate the variables to be examined. It scores high on precision but lacks realism and generality.
- **Qualitative interview** is a collection of information from a few selected individuals. The answers are more precise than those of a survey, but cannot be generalized to the same degree.

- **Survey** is a collection of information from a broad and carefully selected group of informants. The information is typically collected via questionnaires or interviews. Surveys have a high degree of generality, however, they are less controlled than experiments and therefore lack precision. Moreover, the likelihood of bias on the part of the respondents may weaken the realism of a survey.
- **Non-empirical evidence** is argumentation based on logical reasoning. It scores high on generality, but low on realism and precision because it is not empirical.
- **Computer simulation** is operating on a model of a given system. This means that computer simulations are system-specific and therefore score higher on realism than non-empirical evidence, but lower on generality.

These eight strategies are further divided into the following four groups of pairs as shown in Figure 9.

I. The evaluation is performed in a natural environment.
II. The evaluation is performed in an artificial environment.
III. The evaluation is independent of environments.
IV. The evaluation is independent of empirical measurements.

In addition to the above evaluation strategies, Wieringa [32] and Zelkowitz et al. [33] point out the following additional strategies.

- **Case study** is an empirical inquiry that draws on multiple sources of evidence to investigate one instance (or a small number of instances) of a contemporary software engineering phenomenon within its real-life context, especially when the boundary between phenomenon and context cannot be clearly specified [34]. According to Yin [35], "a case study allows investigators to focus on a "case" and retain holistic and real-life perspective." For example, when studying a method for security testing, a software development life cycle, or organizational and managerial processes. The results of a case study can help determine to what extent an artifact is useful, comprehensible and scalable.
- **Literature review** examines existing publications related to a topic and a scope. The method is often used to identify the current state of art and state of practice within a field. Moreover, it may also be useful to confirm an existing hypothesis. However, a weakness with a literature search is that it may be biased in the selection of published works [33].
- **Expert opinion** is an evaluation strategy in which the design of an artifact is submitted to a panel of experts, who imagine how such an artifact will interact with problem contexts imagined by them and then predict what effects they think this would have [32]. However, this kind of validation is limited to the expert's understanding of the artifact under evaluation.
- **Technical action research** is the use of an artifact prototype in a real-world problem to help a client and to learn from this [32]. This is typically carried out as one of the last stages before an artifact moves from the "laboratory" to the real world.

Figure 10 illustrates how we plan to apply the technology research method. In terms of evaluation strategies, we have already carried out a case study, a literature review, and collected expert opinions based on interviews/workshops as documented in previous section. We plan to carry out a similar strategy in the next rounds of innovation and evaluation phases of the research process.

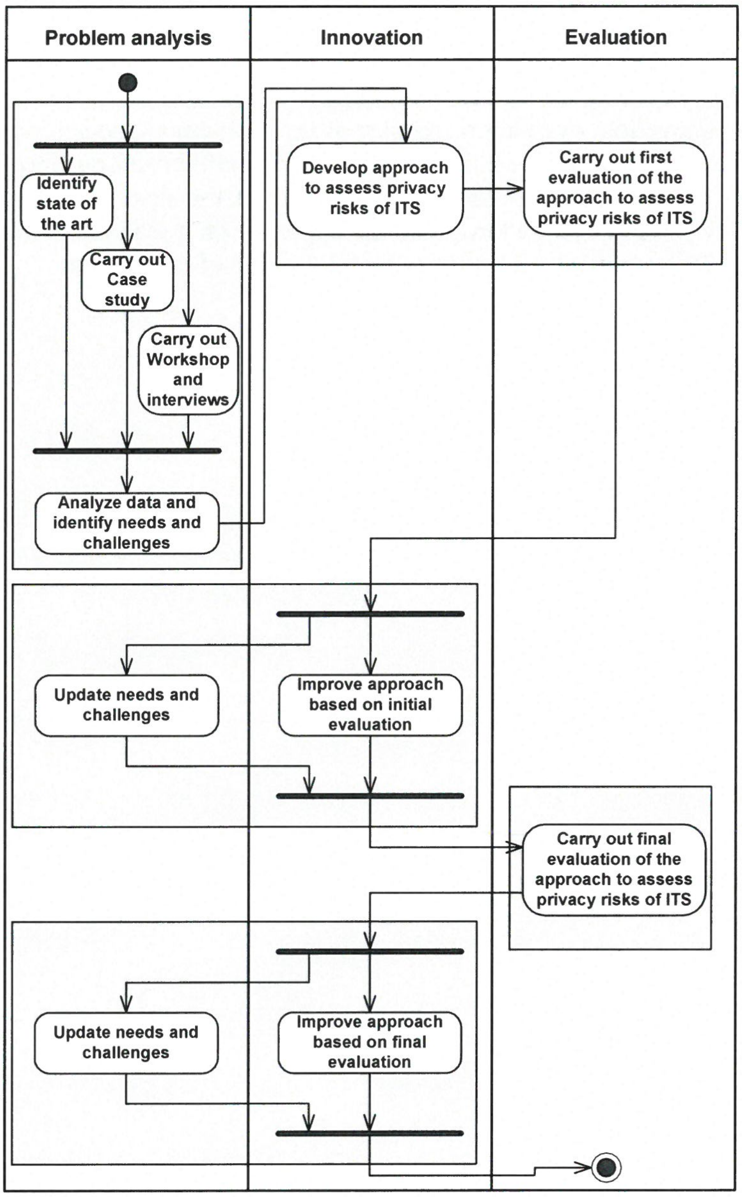
Problem analysis
Innovation
Evaluation
Identify state of the art
Carry out Case study
Carry out Workshop and interviews
Analyze data and identify needs and challenges
Develop approach to assess privacy risks of ITS
Carry out first evaluation of the approach to assess privacy risks of ITS
Update needs and challenges
Improve approach based on initial evaluation
Carry out final evaluation of the approach to assess privacy risks of ITS
Update needs and challenges
Improve approach based on final evaluation

Figure 10: How we plan to carry out the technology research method.

5 Conclusion

In this document, we have highlighted the needs and challenges for tool-based methods to assess privacy risks of smart-city solutions, and in particular for Intelligent Transport Systems. Broadly speaking, the main challenges are related to real-time assessment of privacy risks to (1) inform end-users about exposed privacy risks, and (2) help ITS providers asses privacy-compliance risks, as well as to identify privacy risks at a design and implementation level. The PrivacyAssessment@SmartCity project aims to develop a practically useful tool-based method by addressing the following main research questions:

- RQ1: How can we identify and manage privacy risks in smart city solutions? What privacy-relevant requirements should be posed to the smart city solutions, providers and customers?
- RQ2: How can privacy-awareness of smart city solutions be evaluated and validated in real-time? What kind of methods and decision support is needed for this?
- RQ3: How can we develop and offer useful and pragmatic principles/guidance for privacy management of the smart city solutions?

We carry out the research by making use of the technology research method, which consists of three iterative steps: problem analysis, innovation, evaluation. As part of the problem analysis (documented by this report) we identified state of the art, analyzed a realistic case on ITS, and carried out interviews and a workshop together with experts in the field, as described in Section 2. In the next step we will develop an initial approach to assess privacy risks of ITS and evaluate the approach on a realistic ITS case. Then based on the evaluation, we will update the approach and carry out a final round of evaluation.

6 References

[1] P. Cincilla, A. Kaiser, B. Lonc, H. Labiod, R. Blancher, C. Jouvray, R. Denis, and A. Boulanger. Security of C-ITS messages: A practical solution - the ISE project demonstrator. In Proc. 7th International Conference on New Technologies, Mobility and Security (NTMS'15), pages 1-2. IEEE Computer Society, 2015.

[2] European Commission. Roadmap on Highly Automated vehicles, 2016. GEAR 2030 Discussion Paper.

[3] European Commission, Mobility and Transport. C-ITS Platform Final Report (http://ec.europa.eu/transport/themes/its/c-its_en.htm), 2016.

[4] European Parliament, Council of the European Union. Directive 2010/40/EU - Framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport, 2010.

[5] European Parliament, Council of the European Union. Regulation (EU) 2016/679 - Protection of natural persons with regard to the processing of personal data and on the free movement of such data, 2016.

[6] J. Friginal, J. Guiochet, and M.-O. Killijian. Towards a Privacy Risk Assessment Methodology for Location-Based Systems. In Proc. 10th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MOBIQUITOUS'14), pages 748-753. Springer, 2014.

[7] S. Hietanen. Mobility as a Service - the new transport model? Eurotransport Magazine, 12(2):2-4, 2014.

[8] International Organization for Standardization. ISO 22307:2008(E), Financial services - Privacy impact assessment, 2008.

[9] International Organization for Standardization. ISO/IEC 27005:2011(E), Information technology - Security techniques - Information security risk management, 2011.

[10] International Organization for Standardization. ISO/IEC 29100:2011(E), Information technology - Security techniques - Privacy framework, 2011.

[11] C. Jouvray, G. Pellischek, and M. Tiguercha. Impact of a smart grid to the electric vehicle ecosystem from a privacy and security perspective. In Proc. 27th International Electric Vehicle Symposium & Exhibition (EVS'13), pages 1-10. IEEE Computer Society, 2013.

[12] P. Jureczek and A. Kozierkiewicz-Hetmańska. A Privacy-Preserving Framework for Mining Continuous Sequences in Trajectory Systems. In Proc. 1st European Network Intelligence Conference (ENIC'14), pages 52-58. IEEE Computer Society, 2014.

[13] B. Kitchenham and S. Charters. Guidelines for performing systematic literature reviews in software engineering. EBSE Technical Report EBSE-2007-01 v2.3, Software Engineering Group, School of Computer Science and Mathematics, Keele University and Department of Computer Science, University of Durham, 2007.

[14] F. Knirsch, D. Engel, C. Neureiter, M. Frincu, and V. Prasanna. Model-driven Privacy Assessment in the Smart Grid. In Proc. 1st International Conference on Information Systems Security and Privacy (ICISSP'15), pages 173-181. SCITEPRESS, 2015.

[15] A. Mylonas, M. Theoharidou, and D. Gritzalis. Assessing Privacy Risks in Android: A User-Centric Approach. In Proc. 1st International Workshop on Risk Assessment and Risk-driven Testing (RISK'13), pages 21-37. Springer, 2014.

[16] National Institute of Standards and Technology. NIST SP 800-30, Guide for Conducting Risk Assessment, 2012.

[17] M. K. Natvig, H. Westerheim, T. K. Moseng, and A. Vennesland. ARKTRANS - The multimodal ITS framework architecture. Technical Report SINTEF A12001, SINTEF Information and Communication Technology, 2009.

[18] L. Øvstedal, L.-E. Lervåg, and T. Foss. Personvern og trafikk: Personvernet i intelligente transportsystemer (ITS). Technical Report SINTEF A10670, SINTEF Technology and Society, 2010.

[19] V. Psaraki, I. Pagoni, and A. Schafer. Techno-economic assessment of the potential of intelligent transport systems to reduce CO2 emissions. IET Intelligent Transport Systems, 6(4):355-363, 2012.

[20] D. Ren, S. Du, and H. Zhu. A Novel Attack Tree Based Risk Assessment Approach for Location Privacy Preservation in the VANETs. In Proc. IEEE International Conference on Communications (ICC'11), pages 1-5. IEEE Computer Society, 2011.

[21] M. Sato, M. Izumi, H. Sunahara, K. Uehara, and J. Murai. Threat Analysis and Protection Methods of Personal Information in Vehicle Probing System. In Proc. 3rd International Conference on Wireless and Mobile Communications (ICWMC'07), pages 58-63. IEEE Computer Society, 2007.

[22] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor. A Design Space for Effective Privacy Notices. In Proc. 11th Symposium on Usable Privacy and Security (SOUPS'15), pages 1-17. USENIX Association, 2015.

[23] A. Spickermann, V. Grienitz, and H. A. von der Gracht. Heading towards a multimodal city of the future?: Multi-stakeholder scenarios for urban mobility. Technological Forecasting and Social Change, 89:201-221, 2014.

[24] D. Tancock, S. Pearson, and A. Charlesworth. A Privacy Impact Assessment Tool for Cloud Computing, pages 73-123. Springer, 2013.

[25] M. Theoharidou, N. Papanikolaou, S. Pearson, and D. Gritzalis. Privacy Risk, Security, Accountability in the Cloud. In Proc. 5th International Conference on Cloud Computing Technology and Science, pages 177-184. IEEE Computer Society, 2013.

[26] N. Vandezande and K. Janssen. The ITS Directive: More than a timeframe with privacy concerns and a means for access to public data for digital road maps? Computer Law & Security Review, 28(4):416-428, 2012.

[27] D. Wright. The state of the art in privacy impact assessment. Computer Law & Security Review, 28(1):54-61, 2012.

[28] D. Wright and P. de Hert. Privacy Impact Assessment. Springer, 2012.

[29] I. Solheim and K. Stølen. Technology research explained. Technical Report A313, SINTEF Information and Communication Technology, 2007.

[30] R. Davison, M.G. Martinsons, and N. Kock. Principles of canonical action research. Information Systems Journal, 14(1):65-86, 2004.

[31] J.E. McGrath. Groups: interaction and performance. Prentice-Hall, 1984.

[32] R.J. Wieringa. Design Science Methodology for Information Systems and Software Engineering. Springer, 2014.

[33] M.V. Zelkowitz and D.R. Wallace. Experimental Models for Validating Technology. Computer, 31(5):23-31, 1998.

[34] P. Runeson, M. H ost, A. Rainer, and B. Regnell. Case Study Research in Software Engineering: Guidelines and Examples. John Wiley & Sons, 2012.

[35] R.K. Yin. Case Study Research: Design and Methods (5th edition). SAGE Publications, 2013.

[36] http://www.aftenposten.no/norge/Ekspertene-om-mobildataene-61155b.html 2015.

[37] Atle Årnes. Beacons en ny utfordring for personvernet. https://www.personvernbloggen.no/2015/07/22/beacons-en-ny-utfordring-for-personvernet/ 2015.

[38] "Bluetooth Core Version 4.0 specification", June 2010. [Online]. Available: https://www.bluetooth.org/Technical/Specifications/adopted.htm

[39] "Bluetooth Core Version 4.1 specification", December 2013. [Online] Available: https://www.bluetooth.org/Technical/Specifications/adopted.htm.

[40] On the Potential of Bluetooth Low Energy Technology for Vehicular Applications. Jiun-Ren Lin, Timothy Talty, and Ozan K. Tonguz, IEEE Communications Magazine, 2015.

[41] Jihun Seo, Keuchul Cho, Wooseong Cho, Gisu Park, Kijun Han, A discovery scheme based on carrier sensing in self-organizing Bluetooth Low Energy networks, Journal of Network and Computer Applications 65 (2016) 72–83.

[42] http://release1.its-standards.eu/ , Accessed 21.10.2016.

[43] http://dl.acm.org/ , Accessed 21.10.2016

[44] https://scholar.google.no/ , Accessed 21.10.2016

[45] http://www.kismetwireless.net/ , Accessed 21.10.2016

[46] http://www.argenox.com/bluetooth-low-energy-ble-v4-0-development/library/a-ble-advertising-primer , Accessed 29.11.2016.

SINTEF

Technology for a better society

www.sintef.no