Towards Transparent Real-Time Privacy Risk Assessment of Intelligent Transport Systems

Gencer Erdogan, Aida Omerovic, Marit K. Natvig, and Isabelle C.R. Tardy

SINTEF Digital, Norway
{gencer.erdogan,aida.omerovic,marit.k.natvig,isabelle.tardy}@sintef.no

Abstract. There are many privacy concerns within Intelligent Transport Systems (ITS). On the one hand, end-users are concerned about their privacy risk exposure, while on the other hand, ITS providers need to claim privacy awareness and document compliance with regulations or otherwise 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. The main challenges are related to real-time assessment of privacy risks to (1) inform end-users about exposed privacy risks, and (2) help providers asses privacy-compliance risks. We propose a method to privacy risk assessment addressing these challenges. The method is exemplified on an ITS-example. The initial results indicate feasibility of the method and propose directions for future work.

Keywords: privacy risk assessment, intelligent transport systems, real-time risk assessment

1 Introduction

Intelligent Transport Systems (ITS) are 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 [2].

There are many privacy risks within ITS solutions due to the wide-spread data recording, exchange of data between systems, and monitoring/tracking of persons and vehicles [7, 11]. 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. Moreover, service providers in general have to fulfill strict privacy requirements defined by the recent EU Regulation 2016/679 [3], which also requires the citizen's right to a transparent view into the processing of personal data as well as *related privacy risks* (Article 12). Non-compliance with

The final publication is available at Springer via `https://doi.org/10.1007/978-3-319-57858-3_2`

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 [3]. In light of these privacy concerns, there is a need for additional measures to ensure sufficient and adequate safeguards to the user's privacy [11]. One measure is to use methods specifically developed to assess privacy risk of ITS, which 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 specifically to assess privacy risks of ITS, and the complex and dynamic nature of ITS introduces challenges that need to be properly addressed when assessing privacy risks [1]. In this short paper, we first outline needs and challenges within privacy risk assessment of ITS (Sect. 2). Based on this, we describe our initial method in the context of an example (Sect. 3). Finally, we discuss to what extent our current method is feasible with respect to the needs and challenges, before we conclude (Sect. 4).

2 Needs and Challenges

In order to identify needs and challenges within privacy risk assessment of ITS, we conducted an empirical study in terms of identifying state of the art, carrying out a case study on ITS, and carrying out interviews and a workshop together with experts in the field. The empirical study is documented in a publicly available technical report [1]. In this section, we summarize those findings.

In general, end-users make use of ITS services to get assistance in traffic, as well as to plan and carry out journeys. ITS providers, on the other hand, collect data from end-users through ITS services, which monitor and track end-users, to manage the traffic with the main goal to provide better and more useful services. However, very often data is collected, processed, and stored in a manner completely oblivious to the end-user and not in accordance with laws and regulations [8]. Thus, within ITS, end-users are exposed to privacy risks, while ITS providers are exposed to privacy-compliance risks.

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

ITS providers need to obtain a privacy risk picture of their services in real-time, and to properly assess compliance with respect to privacy laws and regulations – in particular compliance with the recent EU Regulation 2016/679 [3].

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 [13]. 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 [9, 4]. 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 computerized methods for real-time privacy assessment of ITS services to:

- Inform end-users about exposed privacy risks caused by ITS services.
- Help ITS providers assess privacy-compliance risks of their services.

3 Initial Method: Example-Driven Feasibility Study

3.1 Method

The main target group of our method is risk managers of ITS providers. Risk assessment is carried out by risk managers to identify, estimate, and evaluate privacy risks end-users may be exposed to. However, end-users and developers are also target groups of the method in the sense that they contribute to the risk assessment by answering a set of questions, and benefit from the assessment results. Risk managers are interested in discovering privacy-compliance risks. End-users are interested in exposed privacy risks caused by ITS services. Developers are interested in privacy risks caused by design decisions.

Our method follows a model-based indicator-driven risk assessment approach. We use the term model in the meaning of graphical/diagrammatic model that captures the privacy risk picture and that supports the calculation of risk-levels based on likelihood and consequence. To this end, we use the CORAS [6] risk modeling language to create privacy risk models. The risk estimation in our method is based on real-time data captured by ITS services, such as the number of times specific parking lots are used, whether electric charging services are in use, the number of times an end-user uses a travel-planning app, etc., as well as information collected from end-users and developers. We collectively refer to such information as indicators and differentiate between three kinds of indicators: real-time ITS indicators (RT), end-user indicators (EU), and developer indicators (D). End-user and developer indicators are obtained through questionnaires answered by end-users and developers, respectively. This information is obtained periodically or on a one-time basis. As illustrated in Fig. 1, the method consists of four steps.

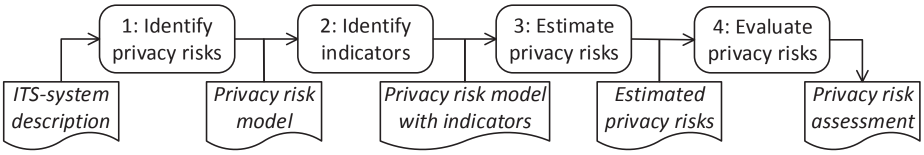

1: Identify privacy risks
2: Identify indicators
3: Estimate privacy risks
4: Evaluate privacy risks
ITS-system description
Privacy risk model
Privacy risk model with indicators
Estimated privacy risks
Privacy risk assessment

Fig. 1. Method for privacy risk assessment of ITS.

In Step 1, we identify privacy risks by analyzing the target ITS system based on its description with respect to certain privacy assets (e.g. identity of end-users), and develop a model that captures the identified privacy risks. As part of this step we also identify a likelihood scale in terms of frequency intervals, a consequence scale describing the impact by which the privacy of end-user is harmed, and a risk evaluation matrix based on the likelihood and consequence scales (see Fig. 4). We define the likelihood scale as {Rare, Unlikely, Possible, Likely, Certain} and associate each value to a corresponding frequency interval. For example, the likelihood Possible may be defined as frequency interval *[10,50⟩:1w*, which means "from and including 10 to less than 50 times per week." We define the consequence scale as {Insignificant, Minor, Moderate, Major, Catastrophic} and describe each consequence value. The output of this step is a privacy risk model expressed in CORAS [6].

In Step 2, we identify indicators relevant to the risk model. All indicators are defined as questions about a particular fragment of the risk model, and attached to the relevant fragment. The questions are formulated in such a way that the answers are used to support risk estimation (see Fig. 3 for examples). Indicators are categorized either as EU, D, or RT. The output of this step is the same privacy risk model as in Step 1, but now updated with indicators.

In Step 3, we first answer the questions posed by the indicators, and then we use the answers as a basis to estimate the likelihood as well as the consequence of identified privacy risks. The output of this step is the same privacy risk model as in Step 2, but now updated with risk estimates.

In Step 4, we evaluate the identified privacy risks by mapping the risks to the predefined risk matrix with respect to their likelihood and consequence estimates. As illustrated in Fig. 4, risks are grouped in five levels horizontally on the matrix where *Very low* is the lowest risk level and *Very high* is the highest risk level. The risk level is identified by mapping the underlying color to the column on the left-hand side of the matrix. The output of this step is the risk assessment in terms of the matrix including identified risks and their risk level. This output is used by the risk manager to evaluate compliance with privacy-related laws and regulations, provide developers with details about privacy risks at design level (captured by risk models), and inform end-users about exposed privacy risks.

3.2 Applying the Method on an ITS Example Case

Our view of ITS is in line with the envisaged transition from the multitude of different transport services to the interconnected Mobility as a Service (MaaS) where "a customer's major transportation needs are met over one interface and are offered by a service provider" [5, 10]. Figure 2a illustrates an example of an ITS system (a simplified version of the example in [1]), while Fig. 2b illustrates a use-case we consider in this example.

Assume an end-user has installed an app named Travel Companion App on the smartphone which enables the user to plan and book multimodal journeys. The user searches on a door-to-door journey using this app. The app sends this request to the MaaS, which in turn requests information from various transport

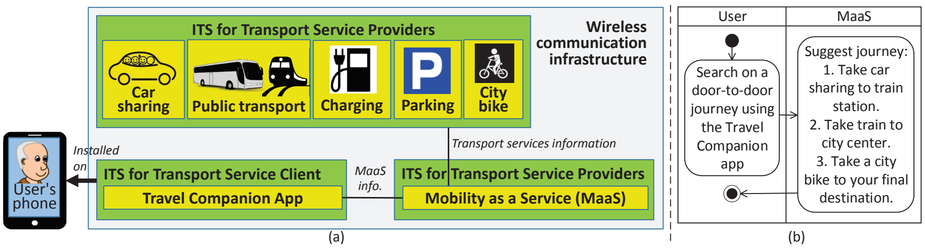

ITS for Transport Service Providers
Car sharing
Public transport
Charging
Parking
City bike
Wireless communication infrastructure
Transport services information
Installed on
User's phone
ITS for Transport Service Client
Travel Companion App
MaaS info.
ITS for Transport Service Providers
Mobility as a Service (MaaS)
(a)
User
MaaS
Search on a door-to-door journey using the Travel Companion app
Suggest journey: 1. Take car sharing to train station. 2. Take train to city center. 3. Take a city bike to your final destination.
(b)

Fig. 2. (a) Simplified example of an ITS system. (b) A use-case in the ITS system.

service providers, such as car sharing, public transport etc., in order to construct possible journey routes. Assume now that the MaaS suggests the following journey: (1) take car sharing to the train station, (2) take the train to the city center, (3) take a city bike and bike to your final destination.

Step 1. Let us say we are interested in identifying privacy risks with respect to the asset *identity of end-user* (A1). Figure 3 shows a risk model capturing one possible privacy risk UI1 that may compromise the identity of the end-user. This may be caused by a set of threat scenarios (TS1, TS2, TS3, and TS4) initiated by the Travel Companion App (T1). The threat scenarios TS1, TS2, and TS3 are scenarios in which the Travel Companion App shares with the MaaS the end-user's location, age, and exercise habits, respectively. These data may be aggregated by the MaaS and shared with advertisement partners (TS4), which in turn causes the risk UI1. In this example, we define the following likelihood scale {Rare=$[0,5\rangle{:}1w$, Unlikely=$[5,10\rangle{:}1w$, Possible=$[10,20\rangle{:}1w$, Likely=$[20,70\rangle{:}1w$, Certain=$[70,\infty\rangle{:}1w$}. For the purpose of the example we only define consequence Major as "personally identifiable information exposed."

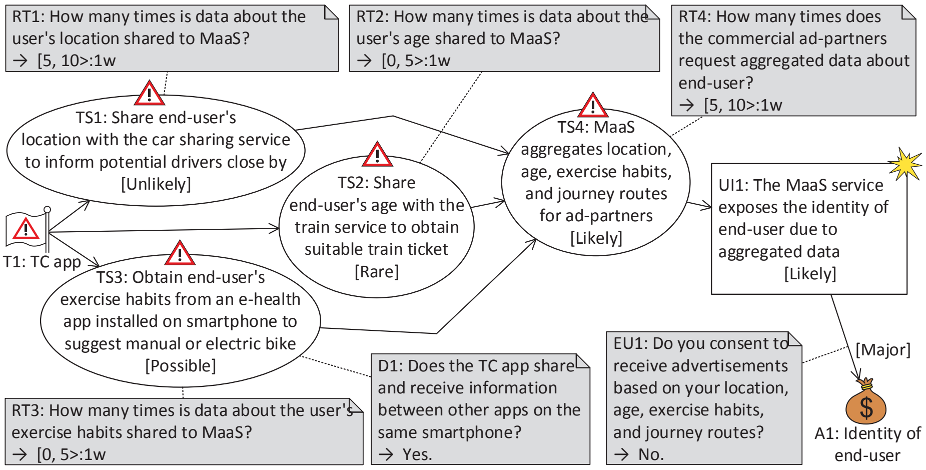
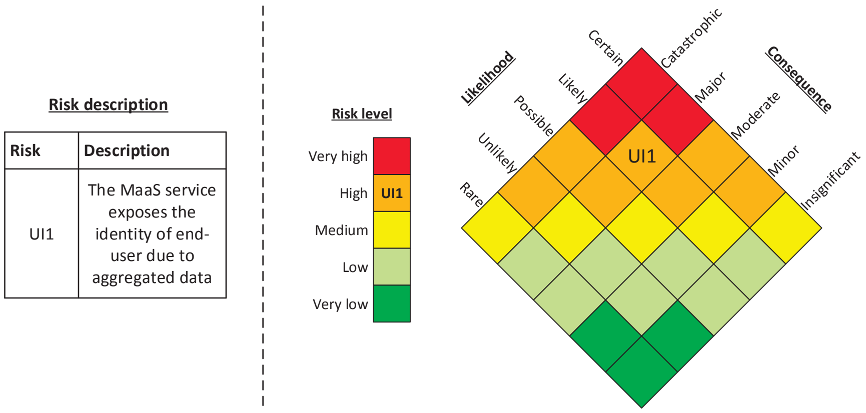

RT1: How many times is data about the user's location shared to MaaS? → [5, 10>:1w
RT2: How many times is data about the user's age shared to MaaS? → [0, 5>:1w
RT4: How many times does the commercial ad-partners request aggregated data about end-user? → [5, 10>:1w
TS1: Share end-user's location with the car sharing service to inform potential drivers close by [Unlikely]
TS2: Share end-user's age with the train service to obtain suitable train ticket [Rare]
TS4: MaaS aggregates location, age, exercise habits, and journey routes for ad-partners [Likely]
UI1: The MaaS service exposes the identity of end-user due to aggregated data [Likely]
T1: TC app
TS3: Obtain end-user's exercise habits from an e-health app installed on smartphone to suggest manual or electric bike [Possible]
[Major]
RT3: How many times is data about the user's exercise habits shared to MaaS? → [0, 5>:1w
D1: Does the TC app share and receive information between other apps on the same smartphone? → Yes.
EU1: Do you consent to receive advertisements based on your location, age, exercise habits, and journey routes? → No.
A1: Identity of end-user

Fig. 3. Privacy risk model for the example use-case in Fig. 2b.

Step 2. Figure 3 shows six indicators (gray note-icons) identified for the risk model. Indicators RT1, RT2, RT3, and RT4 are identified for threat scenarios TS1, TS2, TS3, and TS4, respectively. RT1, RT2, and RT3 are based on the rationale that when the Travel Companion App is used, then certain information about the end-user required by the service is transmitted to the MaaS. Moreover, the MaaS aggregates this information to help advertisement partners construct customized advertisements for each end-user. Thus, the rationale for indicator RT4. In addition to RT3, we have identified indicator D1 for threat scenario TS3. Indicator D1 is included to help assess a more correct frequency for TS3 because it is a question directed to developers. Indicator EU1 is attached to the relation going from UI1 to the asset *identity of end-user*. Based on the answer provided by the end-user for EU1 we may assess the consequence of UI1. This is because some end-users may be willing to provide their identity in order to receive customized advertisements. In that case the consequence of UI1 is reduced.

Step 3. As illustrated in Fig. 3, indicator RT1 returns estimate *[5,10⟩:1w*, which means that threat scenario TS1 occurs with likelihood *Unlikely* according to the predefined likelihood scale. Similarly, we see that the likelihood of TS2 is *Rare* based on indicator RT2. TS3, however, is estimated to likelihood *Possible*. This is because the answer to indicator D1 is *Yes*, and based on this we choose to increase the likelihood from *Rare* (in the case where only RT3 is considered for TS3) to likelihood *Possible*. Assuming TS1, TS2, and TS3 are separate, we find out the likelihood of TS4 by adding the likelihoods of TS1, TS2, and TS3 [6], which gives *[15,35⟩:1w*. We also need to add the frequency provided by RT4. This results in frequency *[20,45⟩:1w*, which means that TS4 occurs with likelihood *Likely*. Thus, UI1 has likelihood *Likely*. The answer to indicator EU1 is *No*. Based on this, we choose to estimate the consequence of UI1 as *Major*.

Step 4. Based on Step 3, we see that the privacy-risk UI1 occurs with likelihood *Likely*, and has a *Major* consequence on asset *identity of end-user*. We map this to the risk matrix and see that UI1 has risk level *High* (see Fig. 4).



Risk description

Risk	Description
UI1	The MaaS service exposes the identity of end-user due to aggregated data

Risk level

Very high	🟥
High	UI1
Medium	🟨
Low	🟩
Very low	🟩

Fig. 4. Privacy risk evaluation matrix.

4 Discussion and Conclusion

In this section, we first discuss to what extent our method is feasible w.r.t. the needs and challenges pointed out in Sect. 2, before we conclude.

Inform end-users about exposed privacy risks caused by ITS services. The risk evaluation matrix (Fig. 4) is the final output of our method and is provided to the end-user. The matrix contains the identified privacy risks, their likelihood, their consequence, as well as their risk level. The risk descriptions provide an explanation to the end-user about the exposed privacy risks. The likelihood and consequence scales on the matrix show the end-user the likelihood and consequence for each exposed privacy risk. The risk-level column provides the risk level of each identified risk plotted in the matrix. Based on this information the end-user is informed about exposed privacy risks as well as their risk level in a transparent manner. This is transparent in the sense that the risk assessment is carried out by the ITS service provider and made available to the end-user. We do not describe the risk levels because the risk acceptance criteria may vary among end-users. Finally, the EU indicators not only support the risk assessment, but also inform the end-user about user-specific information taken into account in the risk assessment.

Help ITS providers assess privacy-compliance risks of their services. Our method is mainly developed to carry out risk assessment on behalf of end-users with respect to privacy-related assets important to end-users, such as identity (example in Sect. 3.2). Laws and regulations such as the EU Regulation 2016/679 [3] mainly consist of requirements specifically focused on the privacy of end-users that providers must fulfill. Thus, to this end, our approach is useful for assessing privacy-compliance risks that address requirements focused on the privacy of end-users. Moreover, the usage of indicators in the risk models helps the ITS providers to link risks to privacy-specific laws and regulations in one model.

Real-time privacy risk assessment. Our current (initial) approach is supported by the necessary foundation for tool support and automation. CORAS [6] is supported by formal rules to calculate risks, and we may use existing guidelines [12] to schematically translate CORAS risk models into executable algorithms. Based on input provided by the indicators, the algorithms may assess the privacy risks captured by the risk models. We are confident that this envisioned solution for tool-support is feasible as we have in fact taken part in implementing a similar approach in a framework for real-time cyber-risk assessment developed by the WISER-project [12]. However, although indicator-driven real-time assessment do exist within cybersecurity [12], this is yet an unexplored area within the domain of privacy assessment of ITS [1], and as future work we plan to investigate how real-time information may be obtained from ITS to support privacy risk assessment.

In conclusion, there is need for practically useful support for real-time privacy assessment of ITS services to (1) inform end-users about exposed privacy risks caused by ITS services, and (2) help ITS providers assess privacy-compliance risks of their services. In this short paper, we provide an initial method for a transparent real-time privacy risk assessment of ITS addressing the aforementioned needs. The innovative contribution of the paper is integration of indicators in the privacy assessment. If valid and reliable, the indicators are expected to facilitate the capturing of relevant changes in privacy issues so that end-users and ITS providers can timely be informed. We currently claim that the approach is ITS-specific since we so far have only evaluated it on the ITS domain. Generality of the approach will depend on results of future evaluations on other domains. The evaluation so far indicates that our approach is one step at the right direction. A natural part of further evaluation would be to assess the effectiveness of our approach w.r.t. needs of the stakeholders.

Acknowledgments. This work has been conducted as part of the PrivacyAssessment@SmartCity project funded by SINTEF, as well as the WISER project (653321) funded by the European Commission within the Horizon 2020 research and innovation programme.

References

1. G. Erdogan, A. Omerovic, M.K. Natvig, and I.C.R. Tardy. Needs and challenges concerning privacy risk management within Intelligent Transport Systems. Technical Report A27830, SINTEF, 2016.
2. European Parliament. *Directive 2010/40/EU*, 2010.
3. European Parliament. *Regulation (EU) 2016/679*, 2016.
4. 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.
5. S. Hietanen. MaaS–the new transport model? *Eurotransport Mag.*, 12(2):2–4, 2014.
6. M.S. Lund, B. Solhaug, and K. Stølen. *Model-Driven Risk Analysis: The CORAS Approach.* Springer, 2011.
7. 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.
8. A. Pultier, N. Harrand, and P.B. Brandtzæg. Privacy in Mobile Apps: Measuring Privacy Risks in Mobile Apps. Technical Report A27493, SINTEF, 2016.
9. 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, 2011.
10. 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.
11. 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.
12. WISER. Cyber Risk Modelling Language and Guidelines, Preliminary Version. Technical Report D3.2, WISER, 2016.
13. David Wright and Paul de Hert. *Privacy Impact Assessment.* Springer, 2012.