TOWARDS TRANSPARENT REAL-TIME PRIVACY RISK ASSESSMENT OF ITS

Gencer Erdogan, Marit K. Natvig, Aida Omerovic, Isabelle C.R. Tardy
4th Intl. Workshop on Risk Assessment and Risk-driven Quality Assurance
Graz, 18.10.2016
Outline

• What are Intelligent Transport Systems (ITS)?
• Privacy risks within ITS
• Needs and challenges within privacy risk assessment of ITS
• Initial approach (example driven)
• Conclusion and future work
What are Intelligent Transport Systems?

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 [1].

Privacy risks within ITS

• Mainly related to monitoring and tracking of persons and vehicles

• Location data
  • Periodic recording may enable tracking of parts of a journey
  • Continuous recording enables real-time tracking

• Other journey data without location data
  • Distance and time of travel → draw travel patterns

• Data about driving behavior
  • Driving patterns (speed, acceleration, braking power, hours driven, etc.)
  • Health related data (e.g., accidents)
  • Data about breaking traffic laws (e.g., speeding ticket, red light ticket)
Privacy risks within (Cooperative) ITS

- Cooperative awareness messages
  - All cars broadcast openly:
  - Car type and model
  - Position
  - Speed
  - Direction
  - Size
  - Acceleration
  - ...

Image source: https://www.car-2-car.org/
Needs and challenges within privacy risk assessment of ITS
Needs and challenges within privacy risk assessment of ITS

• End-users
  • Need to be informed and be aware of exposed privacy risks caused by ITS
  • ITS is highly dynamic and complex → end-users need to be informed in real-time

• Providers
  • Concerned about privacy-compliance risks (Non-compliance to EU Regulation 2016/679, which applies from May 2018 would lead to fines up to 20 million EUR)
  • Need to provide transparent view to risk assessment to end-users (EU Regulation 2016/679)
  • Need to identify privacy risks early in the development phase
  • Need to obtain privacy risk picture of their services in real-time to support maintenance

• Current approaches (PIA methods)
  • Do not facilitate real-time privacy risk assessment
  • Current approaches mainly facilitate privacy risk assessment from provider point of view and do not include assessment from an end-user point of view
Initial approach to assess privacy risks of ITS
Initial approach applied on an example

MaaS: Transport needs offered through
- One interface
- One provider
Initial approach applied on an example

Share Joe's location with the car sharing service to inform potential drivers close by

Record Joe's traveling routes on MaaS (to suggest optimized routes in real-time)

Joe's identity exposed due to aggregated data (door-to-door route, age, location, health)

Privacy of Joe

The MaaS service sends Joe a customized advertisement on a health product from a nearby pharma company

MaaS aggregates data collected by various services and sells these data to a partner

Obtain Joe's exercise habits from an e-health app on Joe's phone to suggest manual or electric bike

Share Joe's age with the train service to suggest a suitable train ticket

Share TC app

Joe searches on door to door journey

Travel companion app

Travel companion suggests:
Initial approach applied on an example

- Share Joe's location with the car sharing service to inform potential drivers close by.
- Record Joe's traveling routes on MaaS (to suggest optimized routes in real-time).
- MaaS aggregates data collected by various services and sells these data to ad-partner.
- Joe's identity exposed due to aggregated data (door-to-door route, age, location, health).
- The MaaS service sends Joe a customized advertisement on a health product from a nearby pharma company.
- RT: How many times is the train service used/day?
- TC app
- RT: How many times is the bike service used/day?
- Obtain Joe's exercise habits from an e-health app on Joe's phone to suggest manual or electric bike.

- EU: Do you prefer to stay anonymous when using TC app?
- Privacy of Joe
- EU: Are you aware that the TC app sends you advertisements based on your location, age, and exercising habits?
- EU: Have you consented to receive advertisements from the TC app?
- RT: How many times does the commercial partner request aggregated end-user data/day?
Initial approach applied on an example

RT: How many times is the car sharing service used per day? 2/day

Record Joe's traveling routes on MaaS (to suggest optimized routes in real-time) [Possible]

D: Does MaaS save all journey history of the end-user? Yes.

RT: How many times is location data, age, and exercise habits shared to MaaS? 1/day, 1/day, 5/day

Share Joe's location with the car sharing service to inform potential drivers close by [Possible]

RT: How many times is the train service used per day? 10/day

Share Joe's age with the train service to suggest a suitable train ticket [Possible]

The MaaS service sends Joe a customized advertisement on a health product from a nearby pharmacy company [Likely]

EU: Do you prefer to stay anonymous when using the TC app? Yes.

Privacy of Joe: High

EU: Are you aware that the TC app sends you advertisements based on your location, age, and exercising habits? Yes.

EU: Have you consented to receive advertisements from the TC app? Yes.

TC app

MaaS aggregates data collected by various services and sells these data to ad-partner [Likely]

RT: How many times does the commercial partner request aggregated end-user data? 50/day

Obtain Joe's exercise habits from an e-health app on Joe's phone to suggest manual or electric bike [Unlikely]

Low
Initial approach applied on an example

End-user

Risk level 9
Risk level 8
Risk level 7
Risk level 6
Risk level 5
Risk level 4
Risk level 3
Risk level 2
Risk level 1

Likelihood
Certain
Very high
Consequence

Privacy risk 1
Privacy risk 2

Developer
Risk manager
Related approach: the EU project WISER

• CyberWISER Light is freely available (self-assessment): [www.cyberwiser.eu](http://www.cyberwiser.eu)
Conclusion and future work

• Observed challenges
  • ITS may cause privacy risks related to monitoring and tracking of persons and vehicles
  • End-users are concerned about privacy-risks and need to be aware of exposed privacy risks in real-time due to the dynamic nature of ITS
  • Providers are concerned about privacy-compliance risks and need to assess privacy risks in real-time and in a transparent manner
  • Current approaches do not facilitate real-time assessment, and do not assess on behalf of end-users

• Our initial approach:
  • Facilitate real-time assessment based on indicators (data collected from ITS services, end-users, and providers)
  • Carry out privacy risk assessment of ITS service on behalf of end-user
  • Support transparency by making users aware of privacy risks they are exposed to
Conclusion and future work

• Future work
  • How do we best translate a set of indicators into a likelihood value?
  • To what extent is it realistically possible to involve end-users?
  • How and what kind of real-time data can we collect without causing privacy risks?
Technology for a better society