

Calling at all stations?

Exploring privacy-friendly e-ticketing using smartphones

Martin Pekárek, MSc



Background

- Focus of my PhD research
  - Privacy, e-ticketing, location based-services
- *Which parameters are required for the design of a privacy-friendly smartphone based e-ticketing system for public transport?*
- Start with a tangible situation and investigate its **location** privacy consequences
  - Limited number of actors
  - No payments
  - Simple objective
    - price calculation based on location info (distance and routing)

TILBURG UNIVERSITY

TILT
Tilburg Institute
for Law, Technology,
and Society

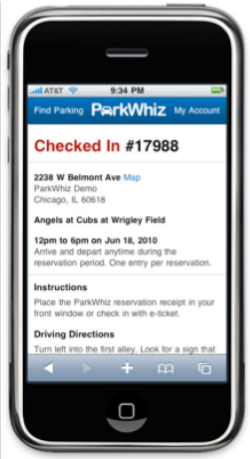
Exhibit 1: the smartphone

A smartphone containing the following 3 elements:

1. GPS receiver
2. NFC capability, supporting
   - smart card emulation
   - read/write mode of RFID tags
3. Data connectivity using GSM or UMTS networks







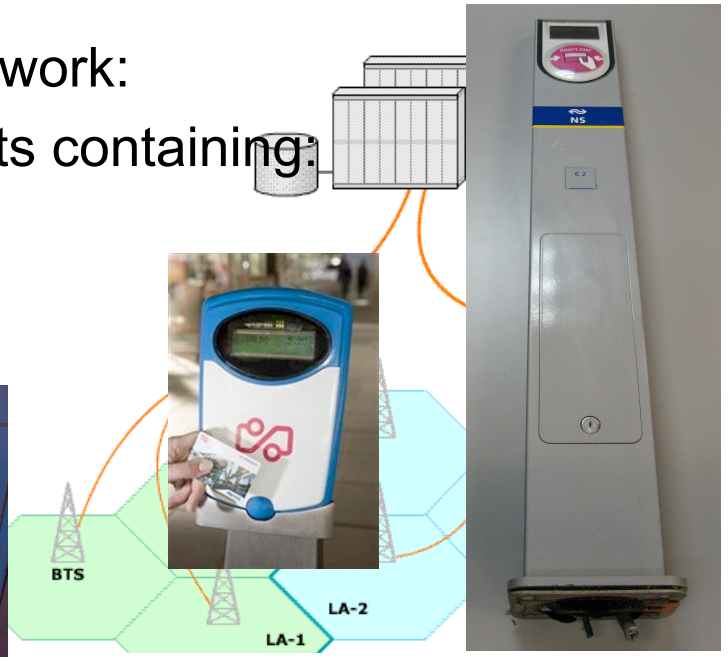
TILBURG UNIVERSITY

TILT
Tilburg Institute
for Law, Technology,
and Society

Exhibit 2: the network

- The telecommunications network (GSM, UMTS)
  - supporting data communication with subscribers
  - support of location-based services (LBS)
    - simple cell-based positioning
- The check-in check-out network:
  - consisting of checkpoints containing:
    - an NFC reader
    - an RFID tag







Two key parameters

- ***Positioning locus***
  - Network
    - e.g. cell-based positioning
  - Device
    - e.g. GPS positioning

- ***Pricing locus***
  - Network
    - Central unit performing price calculations
  - Device
    - Pricing rules and algorithms are stored on the device



Two key parameters (alternative)

- ***Positioning locus***
  - Network
    - e.g. network of card readers
  - Device
    - e.g. reading the RFID tag on the checkpoint

- ***Pricing locus***
  - Network
    - Central unit performing price calculations
  - Device
    - Pricing rules and algorithms are stored on the device



Four possible configurations

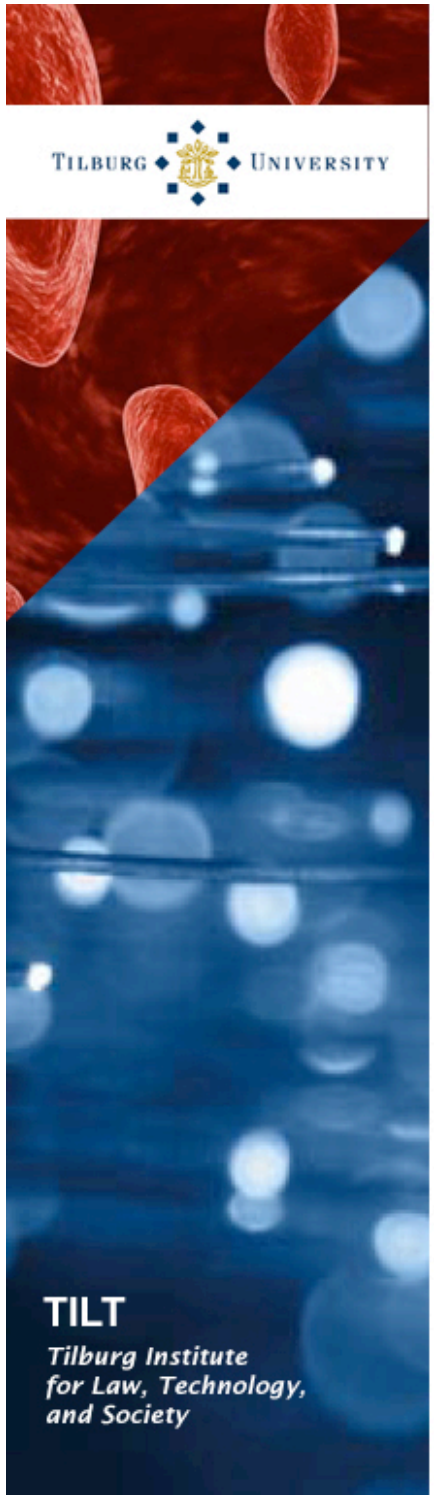
	Positioning locus	Pricing locus
Configuration 1	Network	Network
Configuration 2	Network	Device
Configuration 3	Device	Network
Configuration 4	Device	Device



	Positioning locus	Pricing locus
Configuration 1	Network	Network

- Example
  - Network registers traveller location throughout a trip
  - Collected detailed location information is processed and priced in a central system

- Privacy impact
  - Full transparency of location information at central level



	Positioning locus	Pricing locus
Configuration 2	Network	Device

- Example
  - Network registers traveller location throughout a trip
  - Collected detailed location information is
    - (a) sent to the device
    - (b) processed and priced on the device

- Privacy impact
  - Full transparency of location information at central level
  - However, other factors influencing price (e.g. identity information) may be stored on the device only
    - This information is thus kept from any central system



	Positioning locus	Pricing locus
Configuration 3	Device	Network

- Example
  - Device registers traveller location throughout a trip
  - Detailed location information is sent to a central system
  - Collected location information is processed and priced in a central system

- Privacy impact
  - Less transparency of location information at central level
    - The amount of device-based pre-processing of location information depends on the pricing scheme
  - Alternative ownership of central system is possible
    - Not necessarily the PTO or the MSP



	Positioning locus	Pricing locus
Configuration 4	Device	Device

- Example
  - Device registers traveller location throughout a trip
  - Collected detailed location information is processed and priced on the device

- Privacy impact
  - No location information available at central level
  - Device owner is the only actor with access to location data
    - Encrypted data remains available for auditing purposes



Conclusion

- When considering the **location** privacy of the traveler, it appears that the more activities are located on the device instead of in the network, the more privacy-friendly the configuration is.
- This holds for both positioning and pricing.



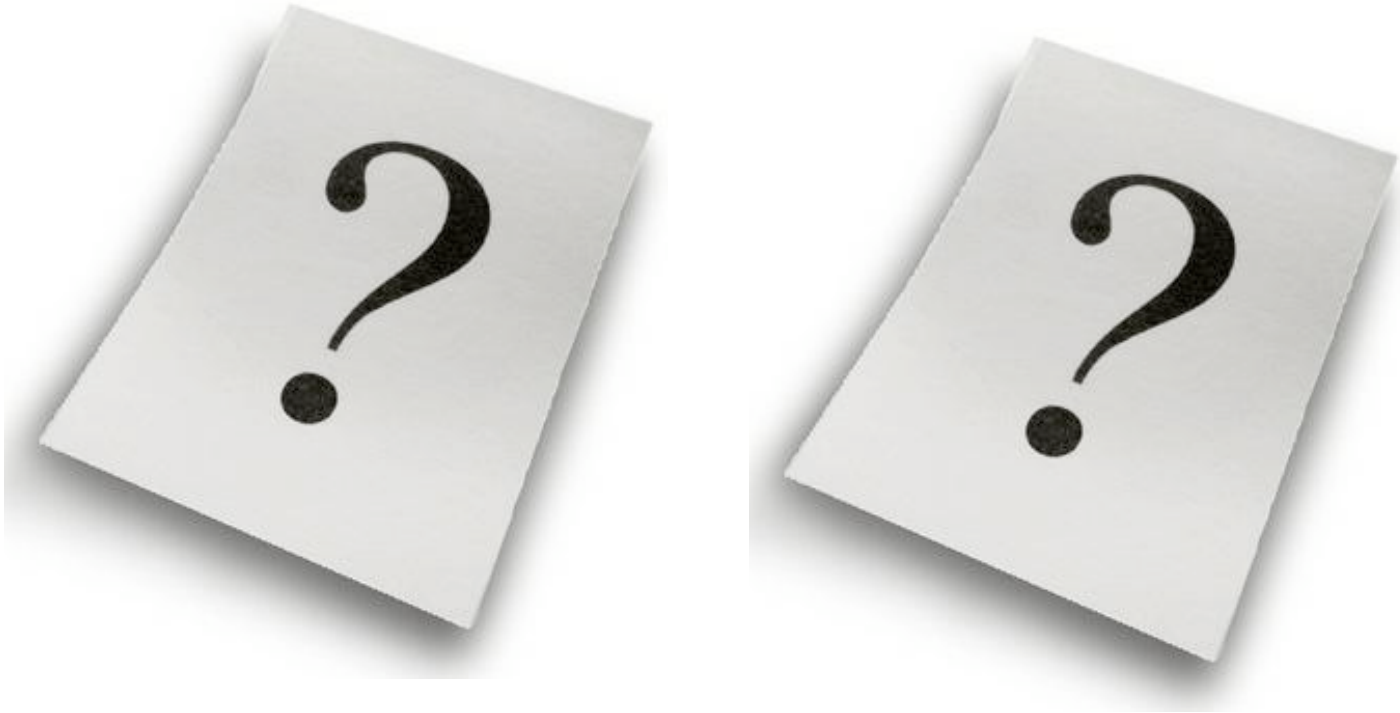
Possible model extensions

- Include personal information
  - Not only location information
- Include other actors
  - E.g. banks, more PTO's, alternative LBS providers
- Include other communication technologies
  - E.g. Bluetooth, Wi-Fi

TILBURG UNIVERSITY

TILT
Tilburg Institute for Law, Technology, and Society

Questions? Comments?



Thanks for your attention!