Privacy in intelligent transport systems

Trond Foss

NTNU March 2017

Article 1 in The European Charter of Fundamental Rights (2009)

"The dignity of man is untouchable. It is to respect and to protect"

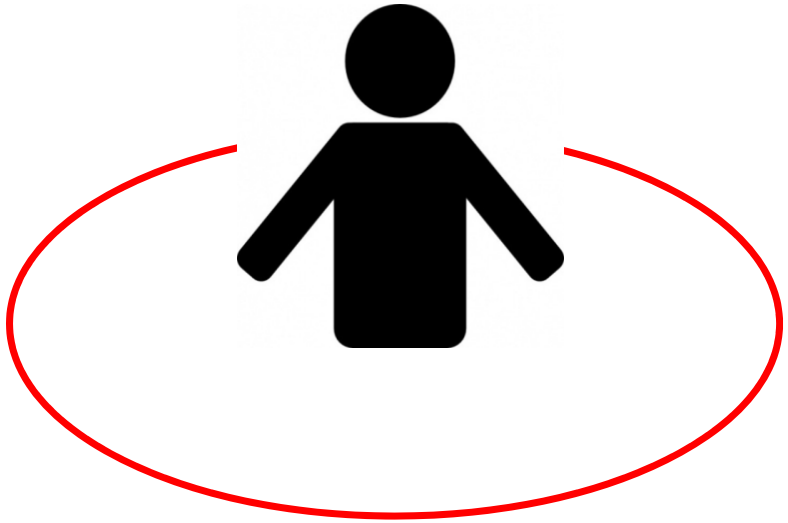
"Den menneskelige verdighet er ukrenkelig. Den skal respekteres og beskyttes."

The right to privacy

The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, thoughts, feelings, secrets and identity.

The right to privacy enables us to choose which parts in this domain can be accessed by others, and control the extent, manner and timing of the use of those parts we choose to disclose.

Yael Onn, et. al., *Privacy in the Digital Environment*



Personal data

Any information and assessments that may be linked to a natural Person

Norwegian Personal Data Act
(Personopplysningsloven § 2 Definisjoner)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

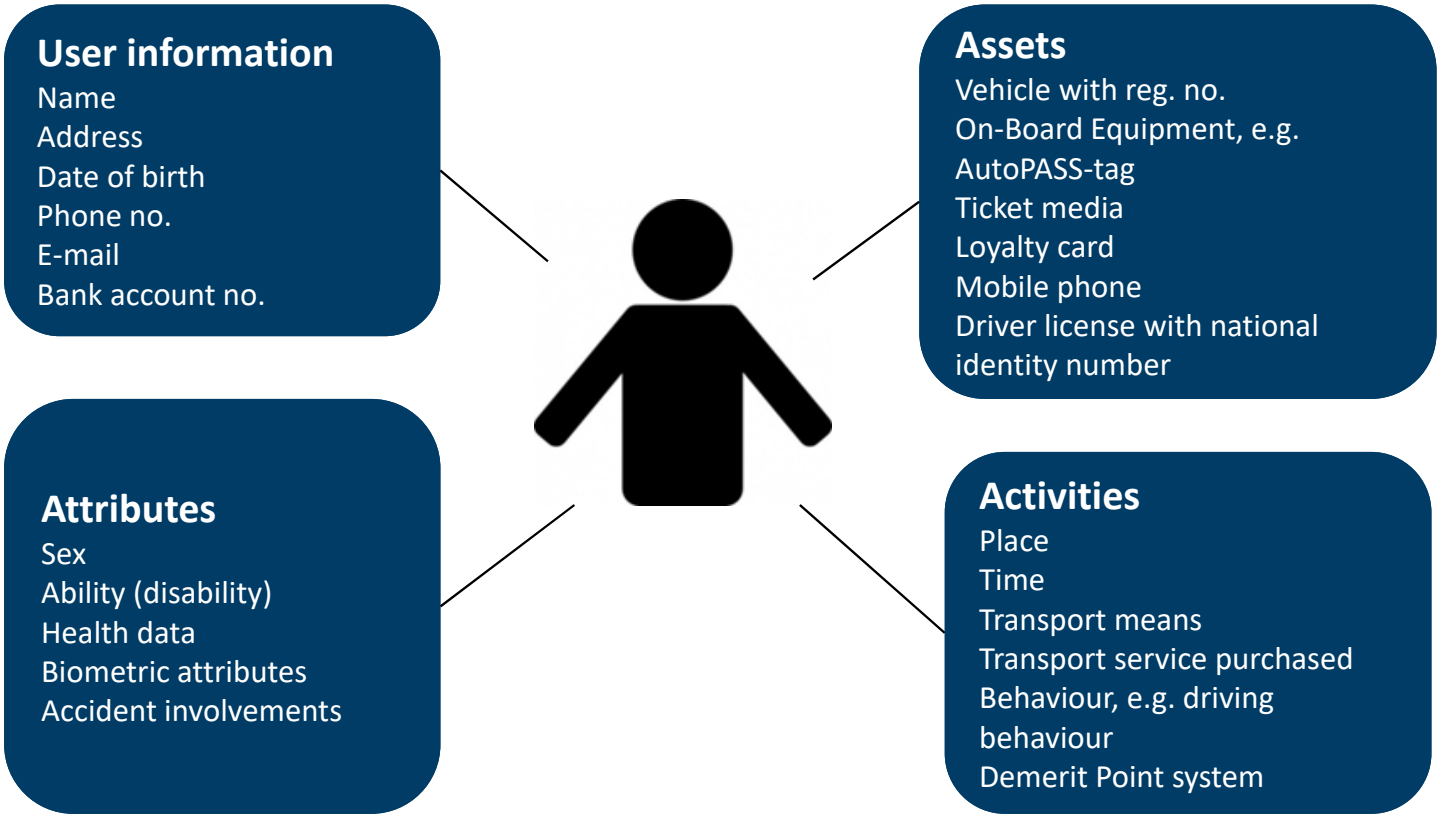
Personal data: Any information relating to an identified or identifiable natural person

An identifiable person is one who can be identified, directly or indirectly, ……

Many ITS applications collect personal data

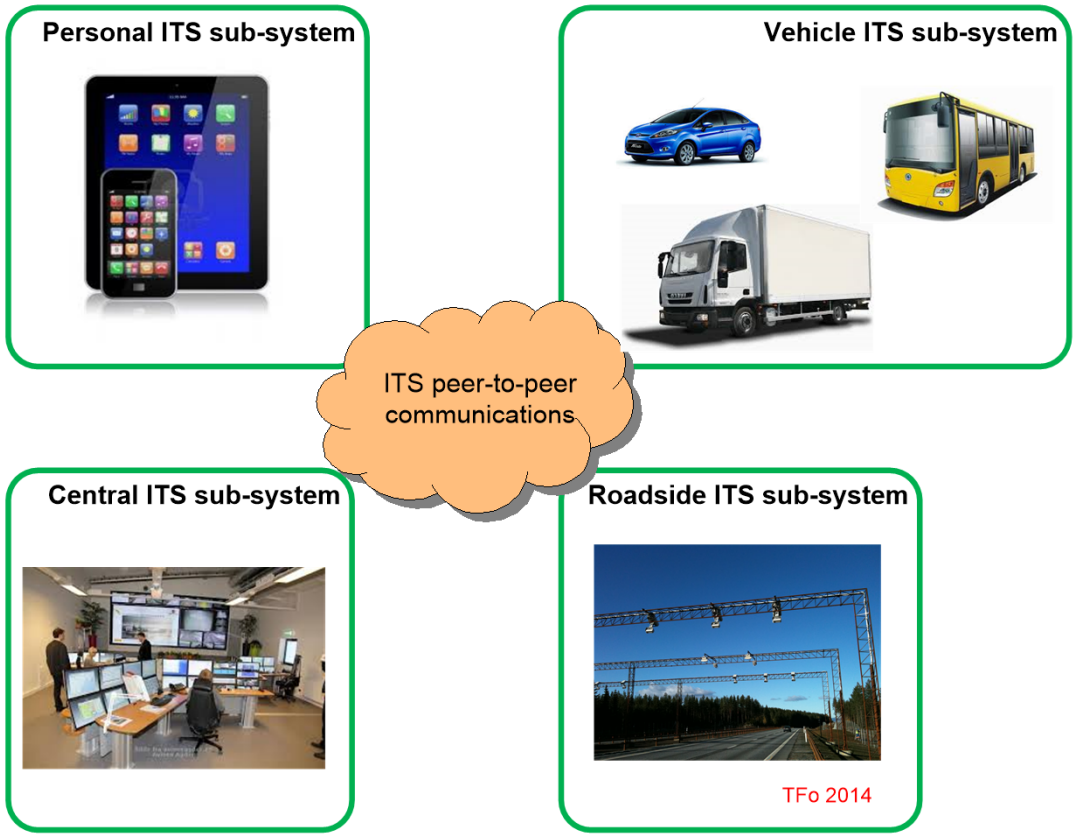
SINTEF

Data related to an ITS service User



SINTEF

Where do we find the personal data?



SINTEF

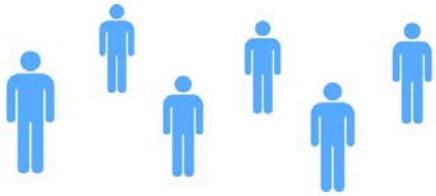
Three major challenges in ITS services?

1. Privacy

2. Security in ICT systems supporting the ITS services

www.techzim.co.zw

3. Authorities, operators and users awareness in relation to security including privacy



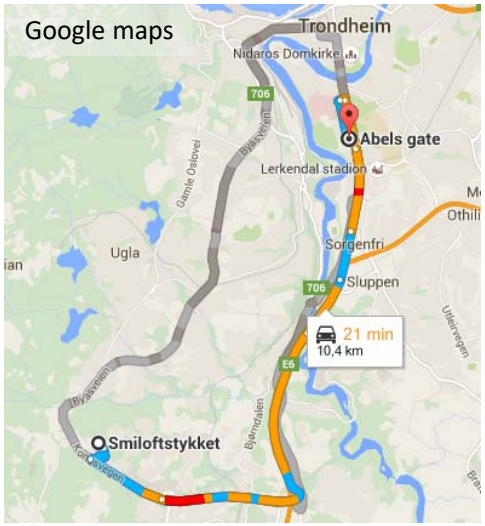
SINTEF

Examples on privacy threats

- **The ITS service User was there**
  Electronic tracking of transport users (construction of travel patterns)

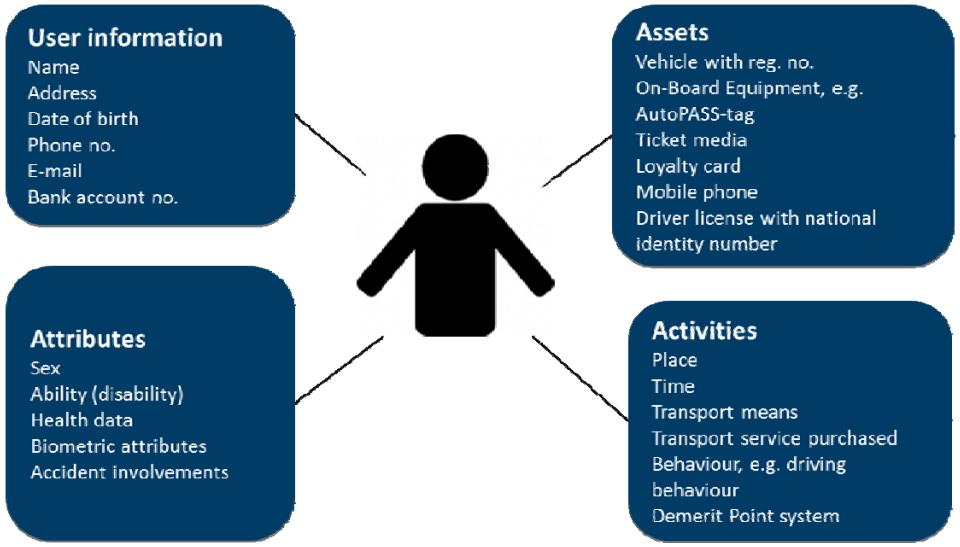
- **The ITS service User is there now**
  Registration of the presence of a person

- **Person profiling**
  Coupling of information from ITS with information in other systems



SINTEF

Some examples on where and when personal data may be collected

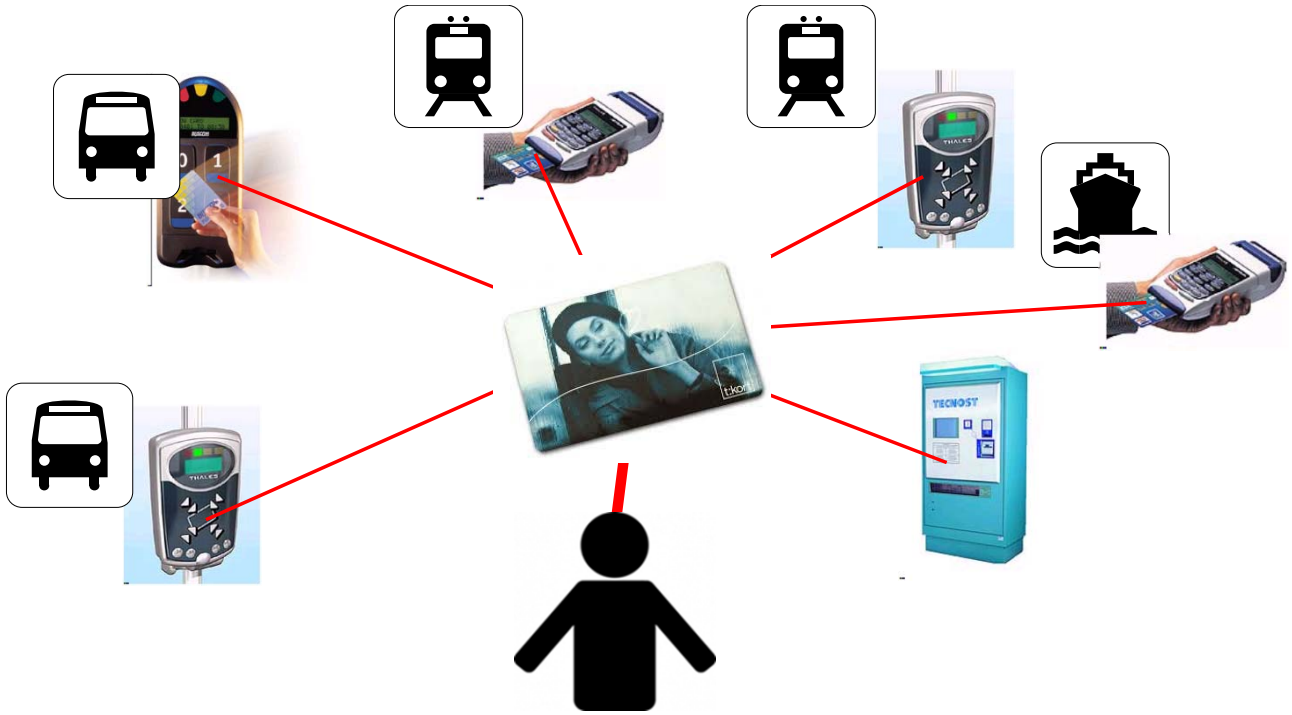


SINTEF

Electronic fee collection by means of an OBE and Automatic Number Plate Recognition (ANPR)

SINTEF

Electronic ticketing



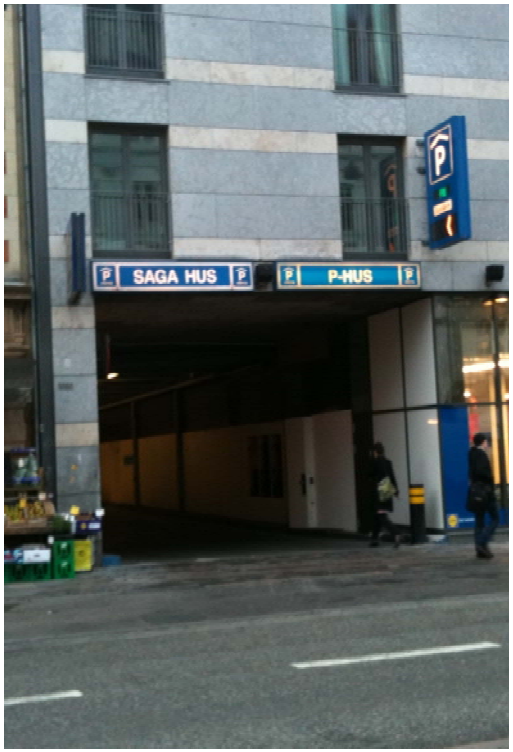
NB! We have an industry norm in Norway!

Access control based on ANPR

Foto: http://www.anpr-tutorial.com/

Parking payment and parking surveys based on OBE or ANPR

Foto: Parking Trend International – June 2008



SINTEF

Traffic data collection based on OBE, ANPR and mobile phones ID

Foto: Parking Trend International – June 2008

Examples

- Individual speed
- Origin – Destination matrixes

SINTEF

Enforcement of Payment of fees, taxes and insurance based on ANPR

Foto: NRK/NRK

Control of :

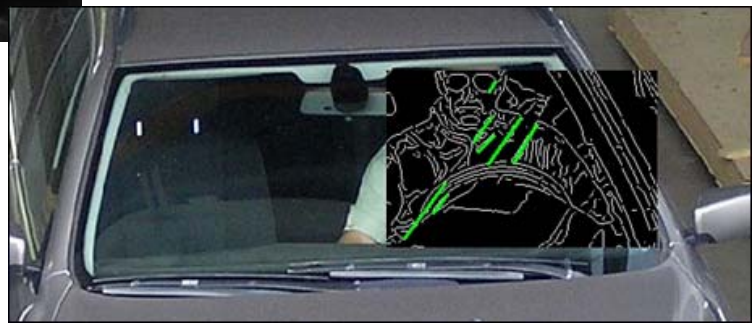
- Annual vehicle fee
- Insurance
- EU vehicle control

Mobile unit for collection of traffic data (ASSET – EU prosjekt)

Foto: ASSET

ASSET mobile unit is equipped with 3D-camera, infrared camera and ordinary camera for collection of data from individual vehicles:

- Number plate data
- Time and place for road use
- Type of vehicle
- Vehicle dimensions
- Speed
- Headway
- Picture of vehicle front including number plate
- Usage of safety belt



SINTEF

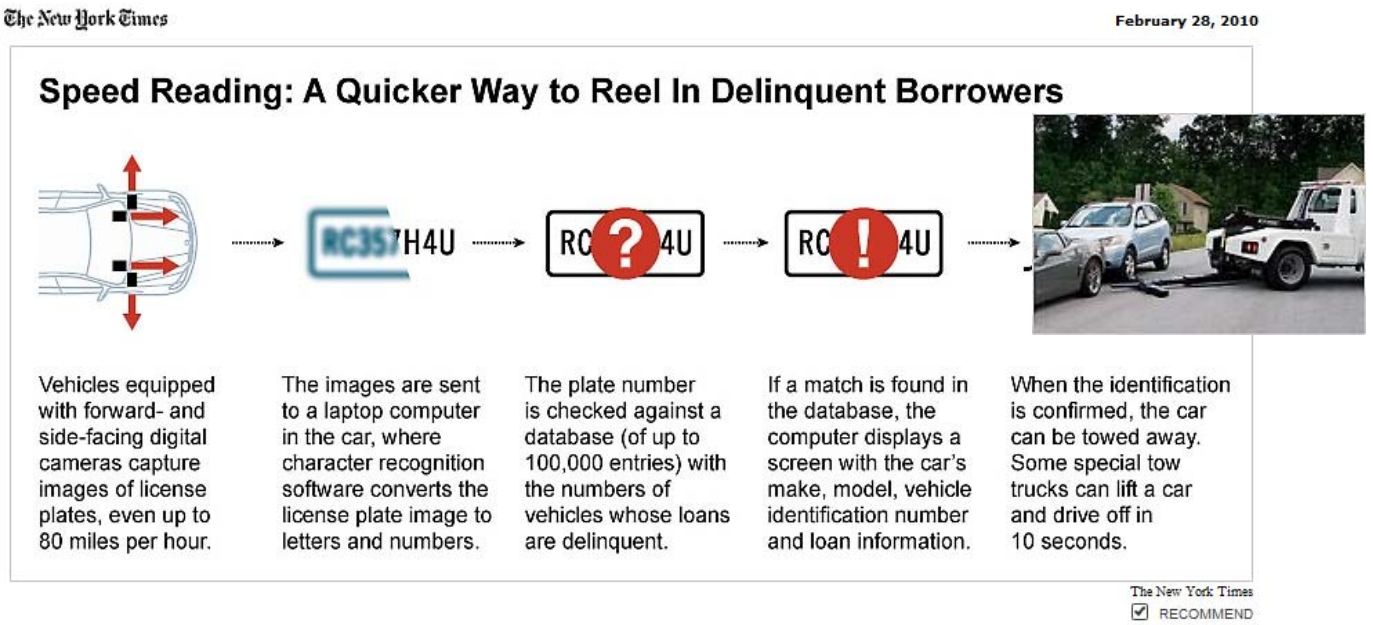
Personal advertising based on ANPR

Foto: www.safespeed.org.uk/

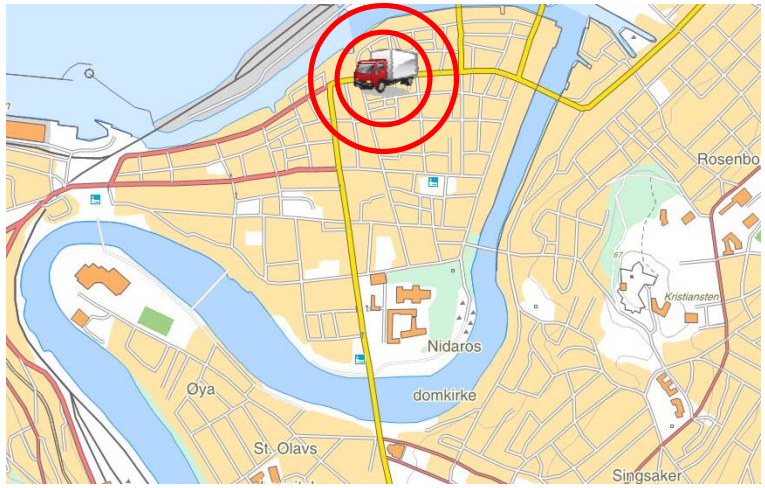
- A hidden camera reads the number plate and access the UK vehicle register to find the car make and model
- The driver is informed about which oil type to use for his vehicle referring to the license plate number of the vehicle

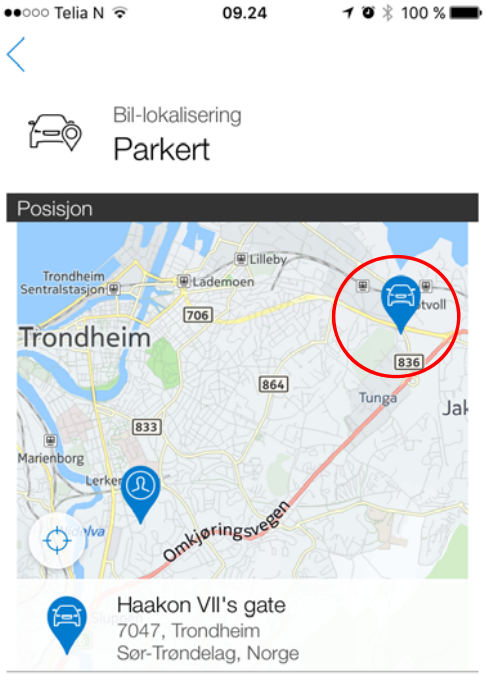
SINTEF

Enforcement of non-performing loans based on ANPR



Fleet management with vehicle tracking, real time applications, stolen vehicles and smart apps (e.g. Volvo OnCall)





Volvo OnCall

SINTEF

Jamming of GPS – privacy or crime?

Mange peker på at stadig flere selskaper med en bilflåte, og ikke bare lastebileiere, bruker GPS-styring. Da er det ikke underlig at arbeidstakere vil hindre å bli overvåket, skriver en leser. Foto: Erlend Tangerås Lyger

GPS-JAMMERE

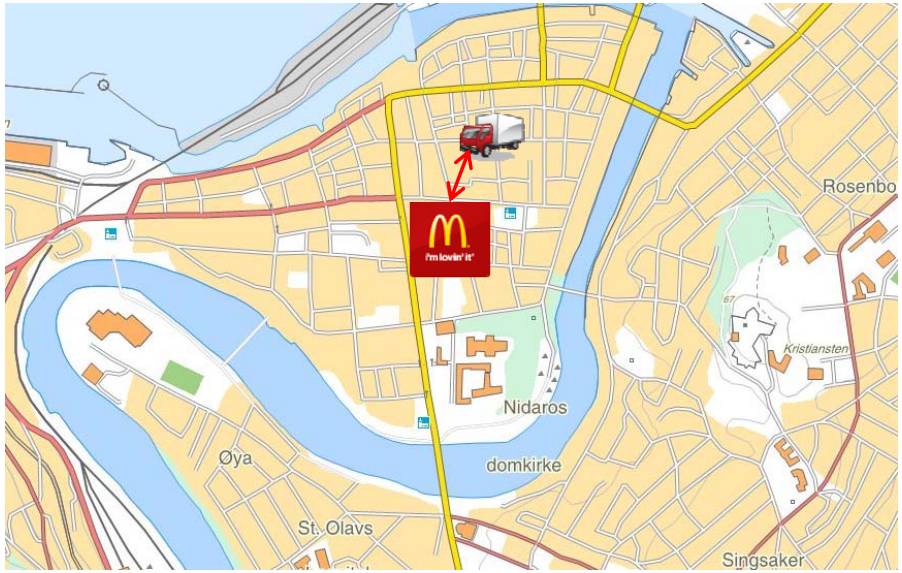
Tyver, taxi-sjåfører og radiosendere

Mange mulige svar på hva som jammer GPS-ene våre.

Teknisk Ukeblad 12. mars 2014

SINTEF

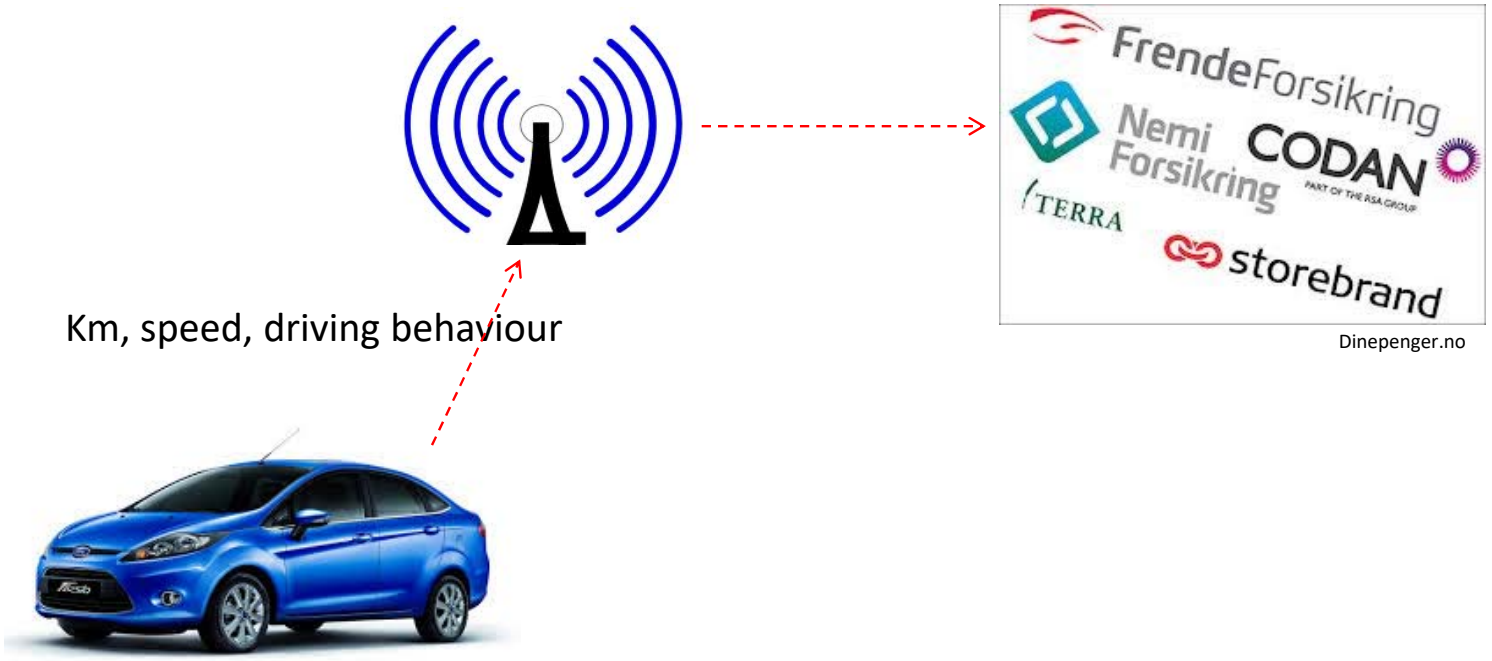
Location based services



- Information about
  - Services
  - Points of Interest
  - Public transport
- Driver assistance systems, e.g. route guidance

SINTEF

Pay as you drive



Dinepenger.no

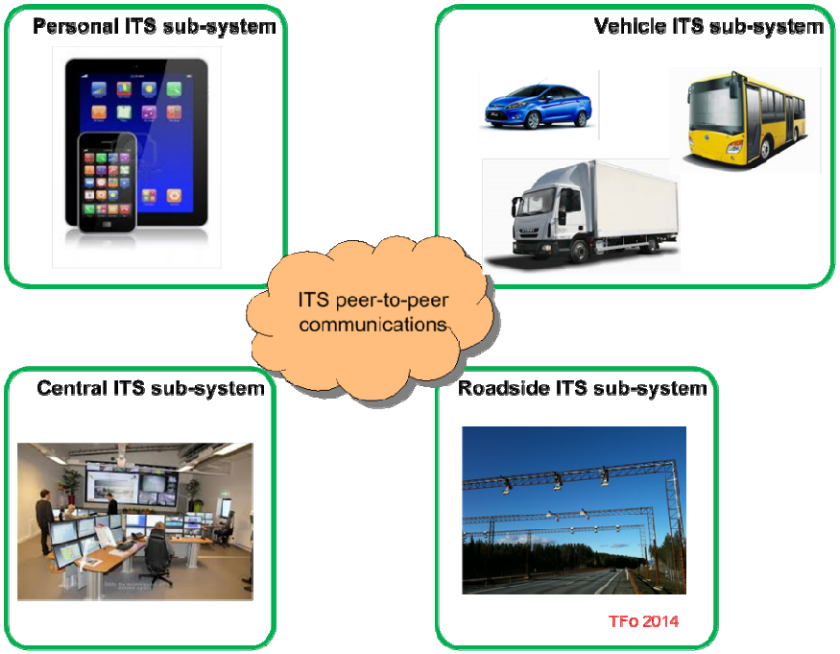
SINTEF

Security in ITS sub-systems

Potential attackers:

- Hackers
- Activists
- Terrorists
- Criminal organisations
- ITS service Users
- Operators
- Authorities
- Foreign powers

Attacks against sub-systems and interfaces



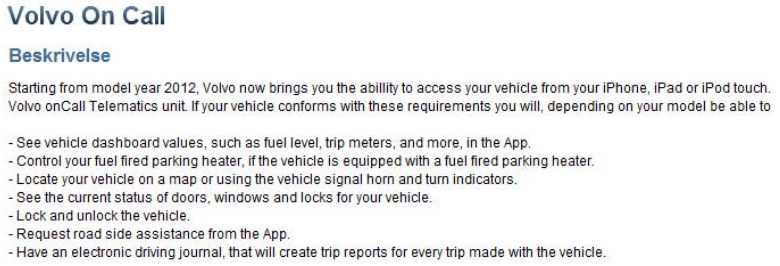
SINTEF

How to get access to the vehicles internal ICT system?

www.canbushack.com

www.hackaday.com

www.caranddriver.com



iTune Appstore

SINTEF

digi.no

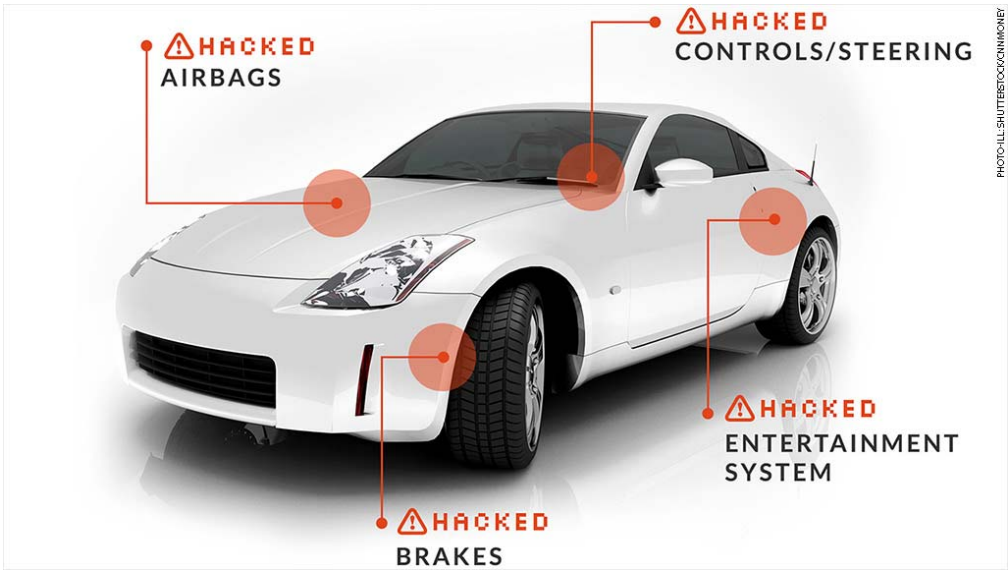
Informasjonssystemet til Nissan LEAF mangler enhver form for tilgangskontroll. Foto: Nissan

ELBIL MED NULL DATASIKKERHET

Nissan Leaf lar seg kontrollere fra internett. Uten passord

Nordmann avslørte skremmende mangel på sikkerhet. – Ren og skjær galskap.

Av Harald Eromboch - Marius Jørgenrud



SINTEF

What is the awareness of authorities, operators and users?

Literature review shows that :

- The awareness of safety and security in intelligent transport systems is limited and there is a gap that should be closed
- The awareness on privacy is better which probably is caused both by laws and regulations and more attention regarding privacy in other sectors, e.g. the health sector.

SINTEF

Could privacy be ensured in intelligent transport systems?

'The simplest is often the best'

Avoid as far as possible collecting and/or using data that could be linked to a person

In worst case, - encrypt or make the data anonymous

Privacy by design shall be the default methodology

Specification and development of ITS applications should take place in close cooperation with the Data Inspectorate

SINTEF

Three very important principles

CIA

KIT

- **C**onfidentiality – data shall be protected against non-authorised access (**K**onfidensiell)
- **I**ntegrity – data shall not be changed between authorised sender and authorised receiver of the data (**I**ntegritet)
- **A**vailability – data shall be available when the ITS application requires the data (**T**ilgjengelighet)

Other principles

- **User consent of the use of personal data**
- **Deletion of data as soon as they have served their purpose**
- Transparency for the Transport user
- Transport user involvement
- Easy accessible and understandable description of the purpose of the data management
- Minimisation of the data collection
- Limited use of the collected data
- Personal data shall be correct, relevant, timely and complete
- The data shall be protected against loss and non-authorised access, deletion and changes
- Revisions shall be carried through
- Training of personal handling the data

SINTEF

Could privacy be ensured in intelligent transport systems?

The answer is Yes, if ……

Thank you for your attention!

trond.foss@sintef.no

SINTEF