

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"

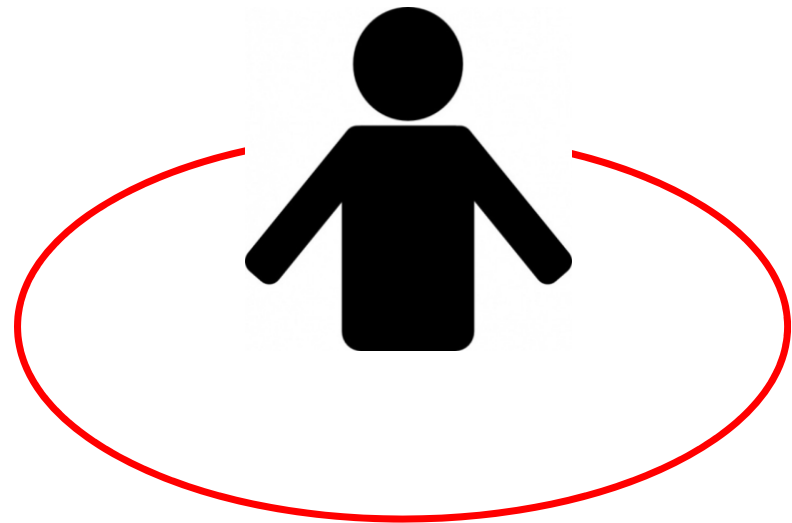
"Den menneskelige verdighet er ukrenkelig. Den skal respekteres og beskyttes."

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



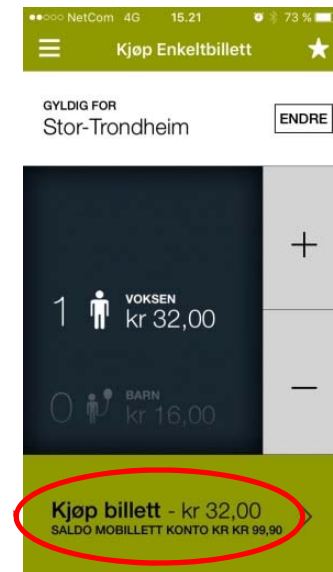
*Norwegian Personal Data Act
(Personopplysningsloven § 2 Definisjoner)*

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

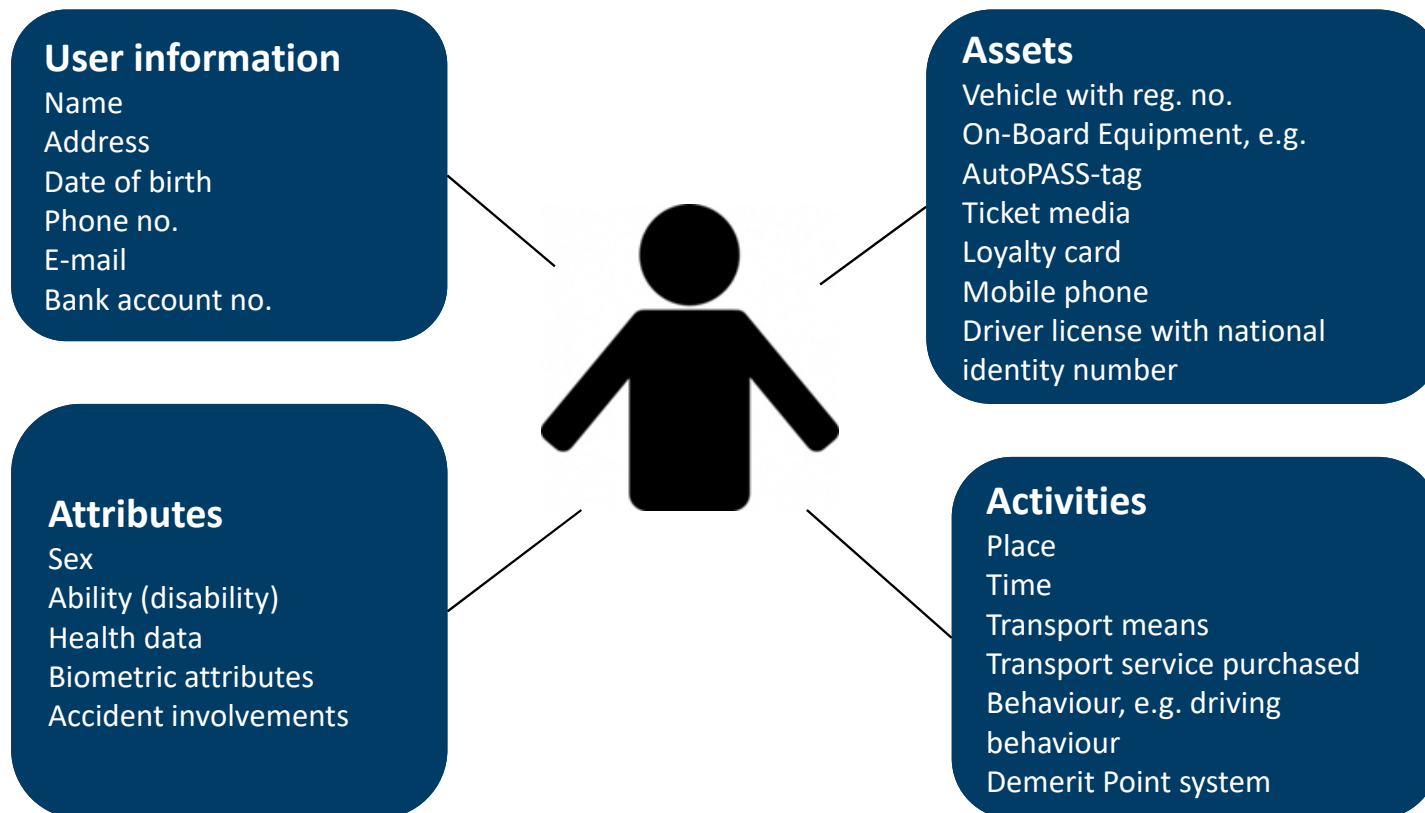
Personal data: Any information relating to an identified or identifiable natural person

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

Many ITS applications collect personal data



Data related to an ITS service User



Where do we find the personal data?

Personal ITS sub-system



Vehicle ITS sub-system



ITS peer-to-peer communications

Central ITS sub-system



Roadside ITS sub-system



TFo 2014

Three major challenges in ITS services?

1. *Privacy*

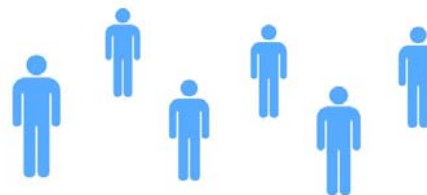


2. *Security in ICT systems supporting the ITS services*



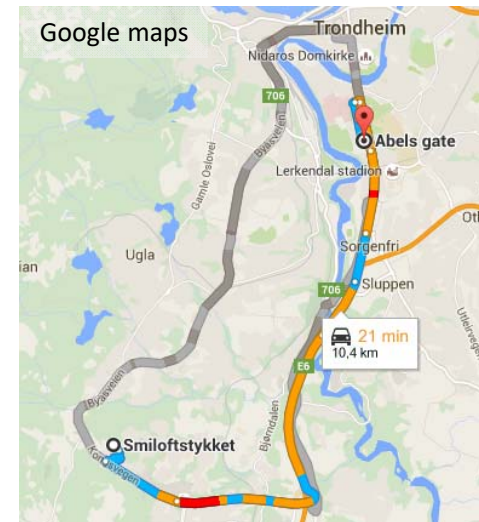
www.techzim.co.zw

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

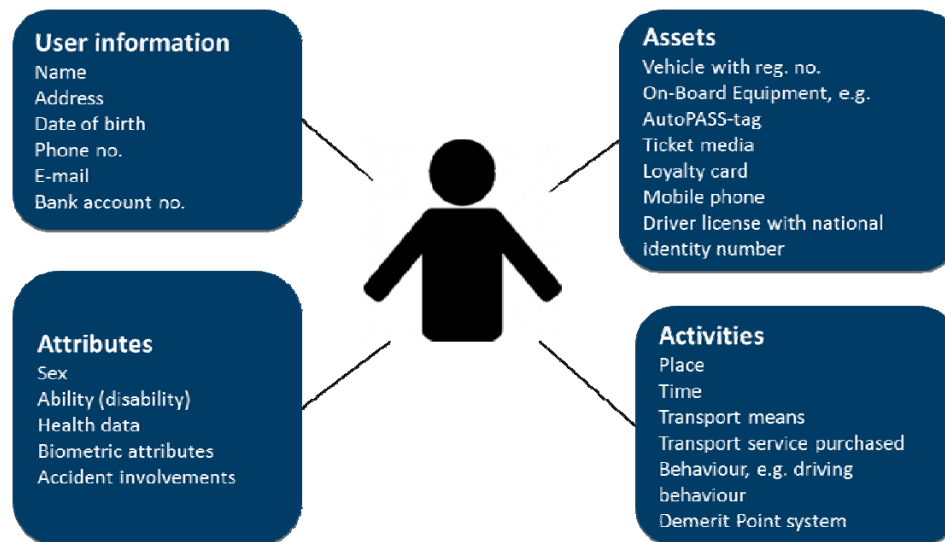


Examples on privacy threats

- **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



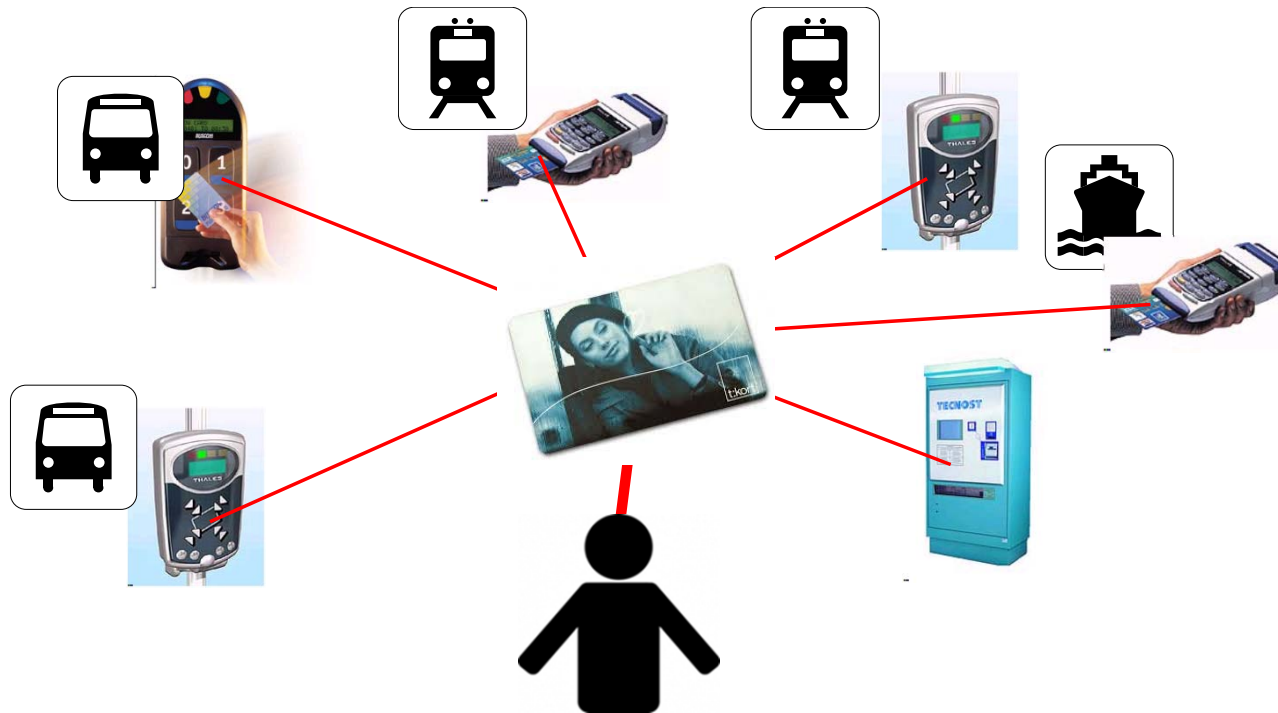
Some examples on where and when personal data may be collected



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



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

The screenshot shows a web application titled "Parking Revenue Verification" by Alpha Vision Design. It displays two camera feeds: "Entry Point: ersin" and "Exit Point: ersout". Both feeds show a car with license plate "00-MH-6086". Below the feeds is a "Real Time Revenue Checker" section with a "Total Revenue Collected Today (Euro): 248.00". A table shows revenue and vehicle counts for the last 6 days. A "Last Vehicle" section displays the license plate "00MH6086", entry and exit times, occupancy time, and revenue.

By Hour		Last 6 days	
04-Nov-07 REV: 259	V/C: 128	01-Nov-07 REV: 333	V/C: 138
03-Nov-07 REV: 418	V/C: 170	31-Oct-07 REV: 238	V/C: 107
02-Nov-07 REV: 421	V/C: 177	30-Oct-07 REV: 249	V/C: 108

Last Vehicle:	
License	00MH6086
Entry Time	05_Nov_07 15:29:54
Exit Time	05_Nov_07 16:53:43
Occupancy Time	83 min, 49 sec
Revenue	Euro €2.40

Foto: Parking Trend International – June 2008



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



Foto: Parking Trend International – June 2008

Examples

- Individual speed
- Origin – Destination matrixes

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



Personal advertising based on ANPR

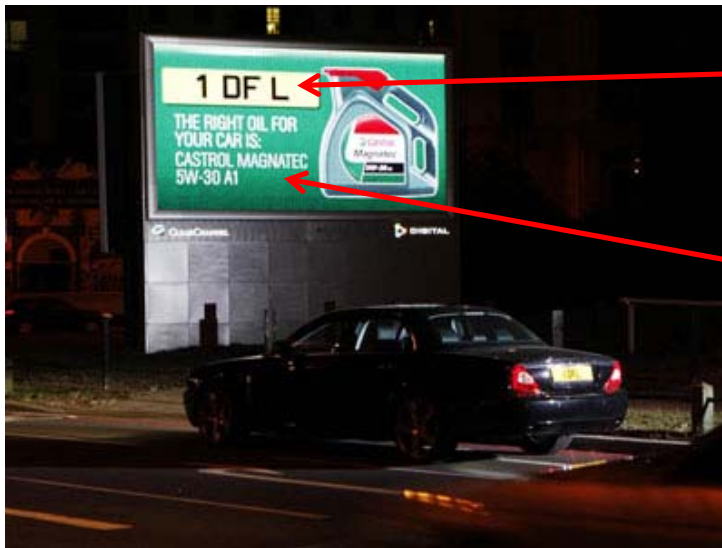


Foto: www.safespeed.org.uk/

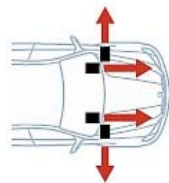
- A hidden camera reads the number plate and access the UK vehicle register to find the car make and model
- The driver is informed about which oil type to use for his vehicle referring to the license plate number of the vehicle

Enforcement of non-performing loans based on ANPR

The New York Times

February 28, 2010

Speed Reading: A Quicker Way to Reel In Delinquent Borrowers



Vehicles equipped with forward- and side-facing digital cameras capture images of license plates, even up to 80 miles per hour.



The images are sent to a laptop computer in the car, where character recognition software converts the license plate image to letters and numbers.



The plate number is checked against a database (of up to 100,000 entries) with the numbers of vehicles whose loans are delinquent.



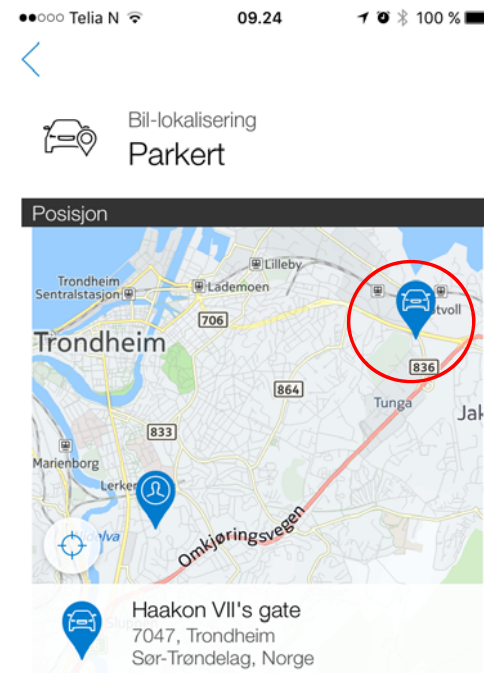
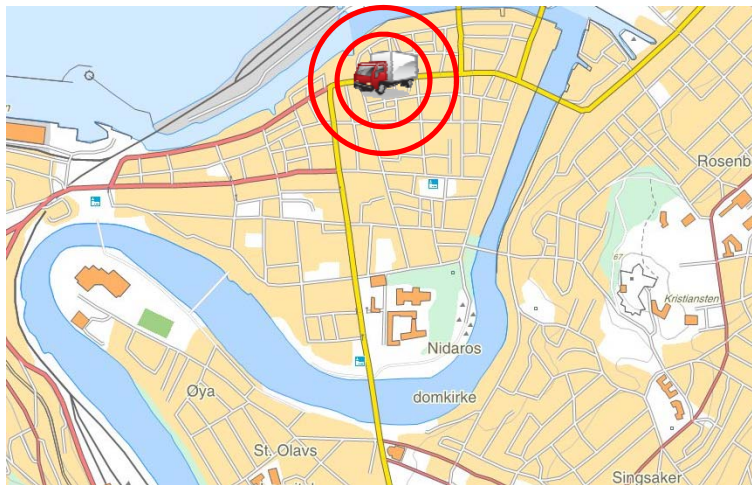
If a match is found in the database, the computer displays a screen with the car's make, model, vehicle identification number and loan information.



When the identification is confirmed, the car can be towed away. Some special tow trucks can lift a car and drive off in 10 seconds.

The New York Times
 RECOMMEND

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



Volvo OnCall

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

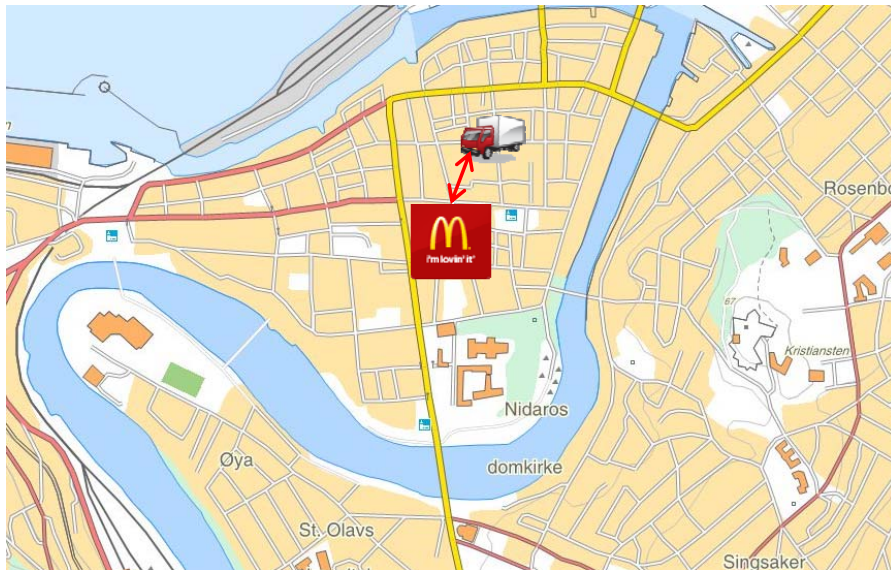
GPS-JAMMERE

Tyver, taxi-sjåførere og radiosendere

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

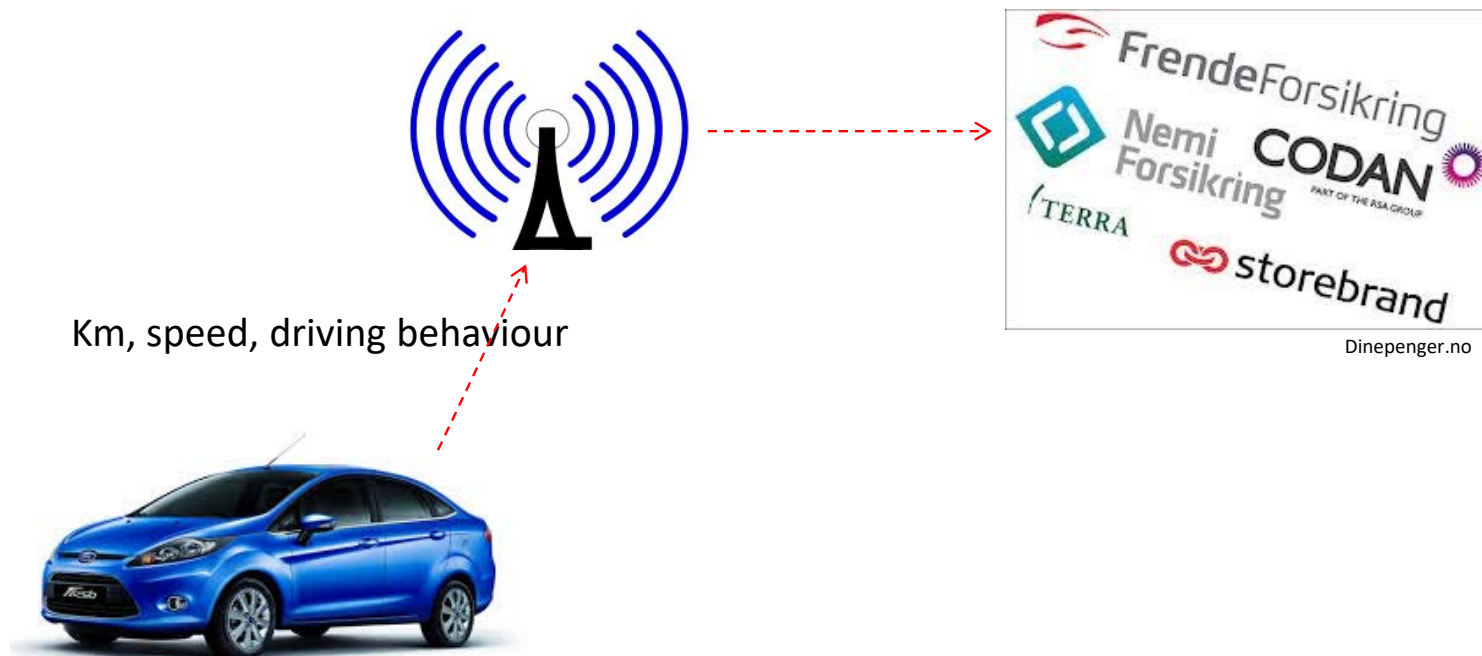
Teknisk Ukeblad 12. mars 2014

Location based services



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

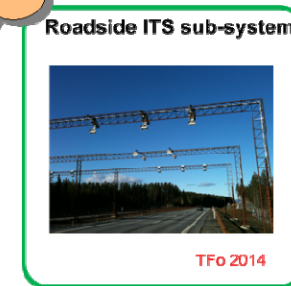
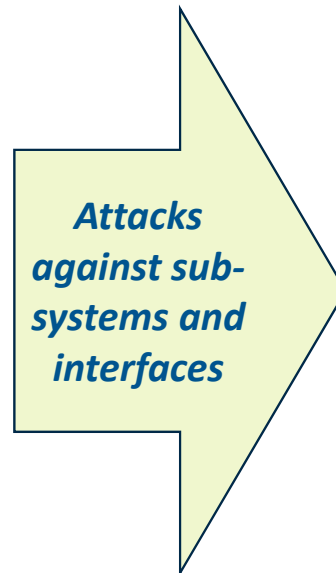
Pay as you drive



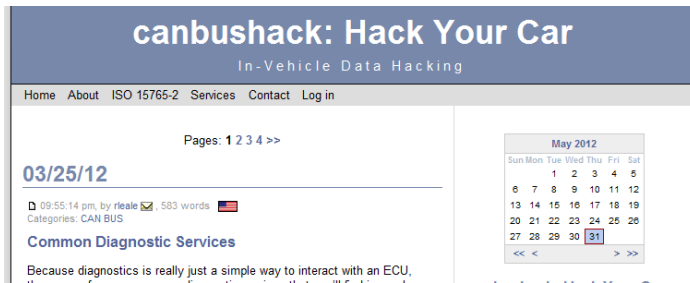
Security in ITS sub-systems

Potential attackers:

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



How to get access to the vehicles internal ICT system?



www.canbushack.com



www.hackaday.com



www.caranddriver.com



Kategori: Verktøy

Volvo On Call

Beskrivelse

Starting from model year 2012, Volvo now brings you the ability to access your vehicle from your iPhone, iPad or iPod touch. Volvo onCall Telematics unit. If your vehicle conforms with these requirements you will, depending on your model be able to

- See vehicle dashboard values, such as fuel level, trip meters, and more, in the App.
- Control your fuel fired parking heater, if the vehicle is equipped with a fuel fired parking heater.
- Locate your vehicle on a map or using the vehicle signal horn and turn indicators.
- See the current status of doors, windows and locks for your vehicle.
- Lock and unlock the vehicle.
- Request road side assistance from the App.
- Have an electronic driving journal, that will create trip reports for every trip made with the vehicle.

iTune Appstore

digi.no

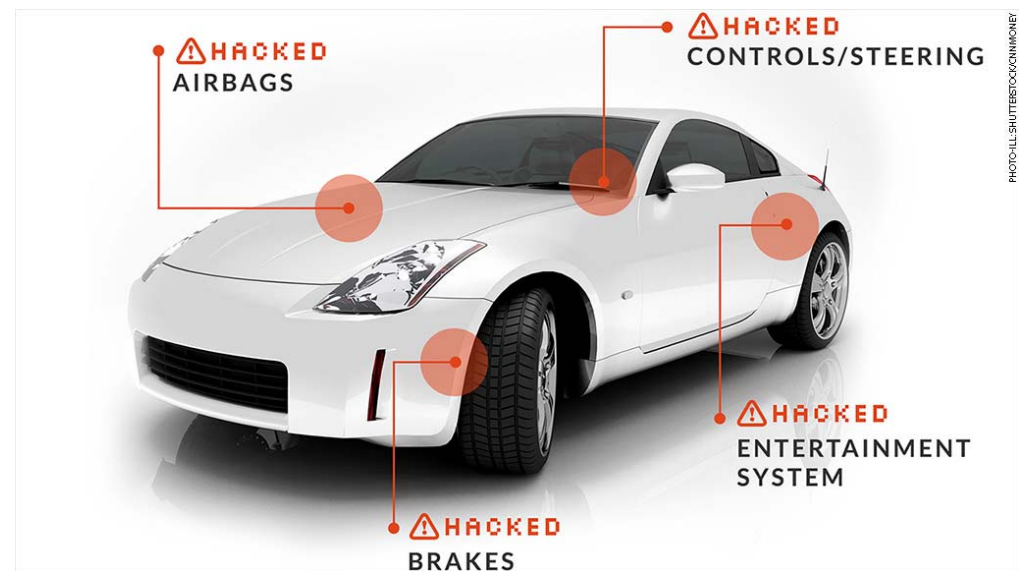


Informasjonssystemet til Nissan LEAF mangler enhver form for tilgangskontroll. Foto: Nissan

ELBIL MED NULL DATASIKKERHET
Nissan Leaf lar seg kontrollere fra internett. Uten passord

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

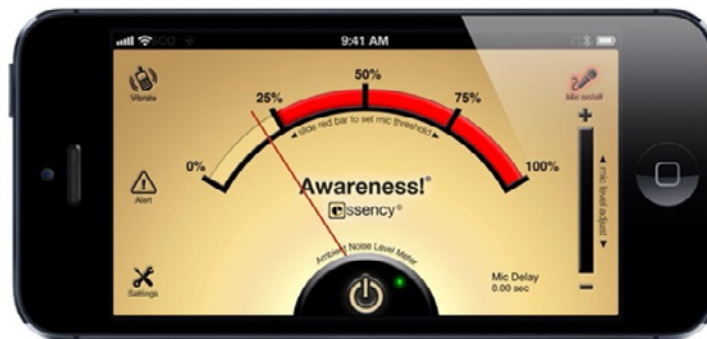
Av Harald Brønnebach - Markus Jørgensen



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.



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

Three very important principles

CIA



- **C**onfidentiality – data shall be protected against non-authorized access (Konfidensiell)
- **I**ntegrity – data shall not be changed between authorized sender and authorized receiver of the data (Integritet)
- **A**vailability – data shall be available when the ITS application requires the data (Tilgjengelighet)

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-authorized access, deletion and changes
- Revisions shall be carried through
- Training of personal handling the data



Could privacy be ensured in intelligent transport systems?

The answer is Yes, if

Thank you for your attention!

trond.foss@sintef.no