Privacy in intelligent transport systems

Senior adviser Trond Foss

SINTEF Safety and mobility

NTNU March 2018

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."

What is privacy?

Privacy is about the right to a private life and the right to decide on personal information.

All people have an inviolable self-worth. As an individual, you are entitled to a private sphere that you control, where you can act freely without coercion or interference from the state or other people.

Source: Data Inspectorate

The European Convention on Human Rights § 8 – 1: Right to respect for private and family life

Everyone has the right to respect for his private and family life, his home and his correspondence

SINTEF

- in other words

You decide!

Photo: Data Inspectorate

SINTEF

Personal data

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Source: GDPR, § Article 4 Definitions

SINTEF

Norwegian transport industry norms for privacy

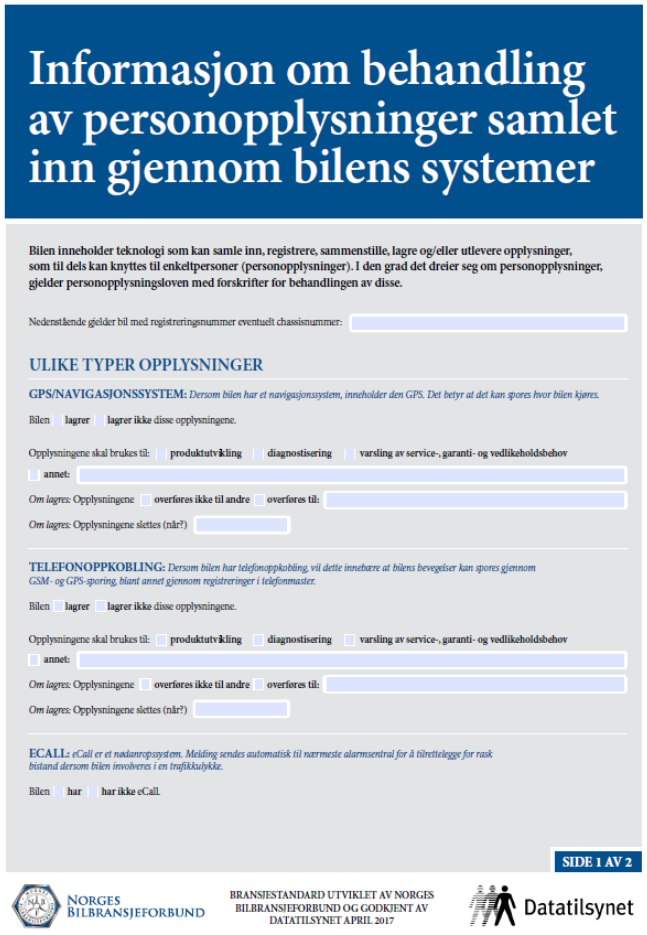
Public transport privacy norm for e-ticketing supports anonymous travels by public transport where the anonymous customer has the same benefits as registered customers.

Norwegian car dealer norms for privacy

Car dealer privacy norm for new cars supports buyer and car producer awareness and consent about data collection and management of data collected by new cars.

SINTEF

Form for data collection from new cars



Informasjon om behandling av personopplysninger samlet inn gjennom bilens systemer

Bilen inneholder teknologi som kan samle inn, registrere, sammenstille, lagre og/eller utlevere opplysninger, som til dels kan knyttes til enkeltpersoner (personopplysninger). I den grad det dreier seg om personopplysninger, gjelder personopplysningsloven med forskrifter for behandlingen av disse.

Nedenstående gjelder bil med registreringsnummer eventuelt chassisnummer:

ULIKE TYPER OPPLYSNINGER

GPS/NAVIGASJONSSYSTEM: *Dersom bilen har et navigasjonssystem, inneholder den GPS. Det betyr at det kan spores hvor bilen kjøres.*

Bilen ☐ **lagrer** ☐ **lagrer ikke** disse opplysningene.

Opplysningene skal brukes til: ☐ **produktutvikling** ☐ **diagnostisering** ☐ **varsling av service-, garanti- og vedlikeholdsbehov**
☐ **annet:**

Om lagres: Opplysningene ☐ **overføres ikke til andre** ☐ **overføres til:**

Om lagres: Opplysningene slettes (når?)

TELEFONOPPKOBLING: *Dersom bilen har telefonoppkobling, vil dette innebære at bilens bevegelser kan spores gjennom GSM- og GPS-sporing, blant annet gjennom registreringer i telefonmaster.*

Bilen ☐ **lagrer** ☐ **lagrer ikke** disse opplysningene.

Opplysningene skal brukes til: ☐ **produktutvikling** ☐ **diagnostisering** ☐ **varsling av service-, garanti- og vedlikeholdsbehov**
☐ **annet:**

Om lagres: Opplysningene ☐ **overføres ikke til andre** ☐ **overføres til:**

Om lagres: Opplysningene slettes (når?)

ECALL: *eCall er et nødanropssystem. Melding sendes automatisk til nærmeste alarmsentral for å tilrettelegge for rask bistand dersom bilen involveres i en trafikkulykke.*

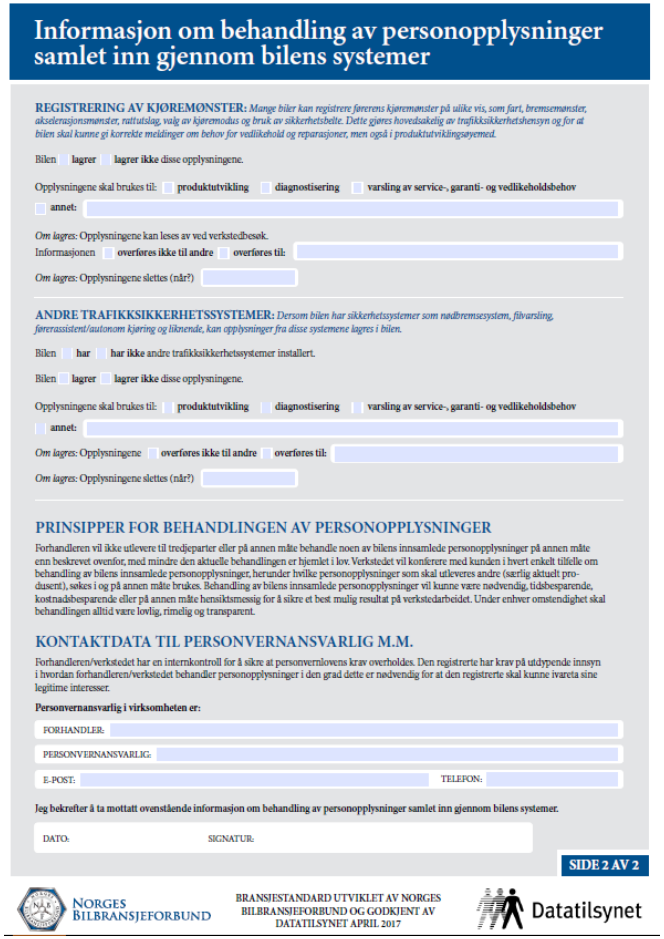
Bilen ☐ **har** ☐ **har ikke** eCall.

SIDE 1 AV 2

NORGES BILBRANSJEFORBUND

BRANSJESTANDARD UTVIKLET AV NORGES BILBRANSJEFORBUND OG GODKJENT AV DATATILSYNET APRIL 2017

Datatilsynet



Informasjon om behandling av personopplysninger samlet inn gjennom bilens systemer

REGISTRERING AV KJØREMØNSTER: *Mange biler kan registrere førerens kjøremønster på ulike vis, som fart, bremsemønster, akselerasjonsmønster, rattutslag, valg av kjøremodus og bruk av sikkerhetsbelte. Dette gjøres hovedsakelig av trafikksikkerhetshensyn og for at bilen skal kunne gi korrekte meldinger om behov for vedlikehold og reparasjoner, men også i produktutviklingsøyemed.*

Bilen ☐ **lagrer** ☐ **lagrer ikke** disse opplysningene.

Opplysningene skal brukes til: ☐ **produktutvikling** ☐ **diagnostisering** ☐ **varsling av service-, garanti- og vedlikeholdsbehov**
☐ **annet:**

Om lagres: Opplysningene kan leses av ved verkstedbesøk.
Informasjonen ☐ **overføres ikke til andre** ☐ **overføres til:**

Om lagres: Opplysningene slettes (når?)

ANDRE TRAFIKKSIKKERHETSSYSTEMER: *Dersom bilen har sikkerhetssystemer som nødbremsesystem, filvarsling, førerassistent/autonom kjøring og liknende, kan opplysninger fra disse systemene lagres i bilen.*

Bilen ☐ **har** ☐ **har ikke** andre trafikksikkerhetssystemer installert.

Bilen ☐ **lagrer** ☐ **lagrer ikke** disse opplysningene.

Opplysningene skal brukes til: ☐ **produktutvikling** ☐ **diagnostisering** ☐ **varsling av service-, garanti- og vedlikeholdsbehov**
☐ **annet:**

Om lagres: Opplysningene ☐ **overføres ikke til andre** ☐ **overføres til:**

Om lagres: Opplysningene slettes (når?)

PRINSIPPER FOR BEHANDLINGEN AV PERSONOPPLYSNINGER

Forhandleren vil ikke utlevere til tredjeparter eller på annen måte behandle noen av bilens innsamlede personopplysninger på annen måte enn beskrevet ovenfor, med mindre den aktuelle behandlingen er hjemlet i lov. Verkstedet vil konferere med kunden i hvert enkelt tilfelle om behandling av bilens innsamlede personopplysninger, herunder hvilke personopplysninger som skal utleveres andre (særlig aktuelt pro-dusent), søkes i og på annen måte brukes. Behandling av bilens innsamlede personopplysninger vil kunne være nødvendig, tidsbesparende, kostnadsbesparende eller på annen måte hensiktsmessig for å sikre et best mulig resultat på verkstedarbeidet. Under enhver omstendighet skal behandlingen alltid være lovlig, rimelig og transparent.

KONTAKTDATA TIL PERSONVERNANSVARLIG M.M.

Forhandleren/verkstedet har en internkontroll for å sikre at personvernlovens krav overholdes. Den registrerte har krav på utdypende innsyn i hvordan forhandleren/verkstedet behandler personopplysninger i den grad dette er nødvendig for at den registrerte skal kunne ivareta sine legitime interesser.

Personvernansvarlig i virksomheten er:

FORHANDLER:

PERSONVERNANSVARLIG:

E-POST: TELEFON:

Jeg bekrefter å ta mottatt ovenstående informasjon om behandling av personopplysninger samlet inn gjennom bilens systemer.

DATO: SIGNATUR:

SIDE 2 AV 2

NORGES BILBRANSJEFORBUND

BRANSJESTANDARD UTVIKLET AV NORGES BILBRANSJEFORBUND OG GODKJENT AV DATATILSYNET APRIL 2017

Datatilsynet

SINTEF

New Norwegian law on personal data

- The new law shall implement the EU General Data Protection Regulation (GDPR)
- Based on the GDPR that comes into force May 2018
- Easier for both individuals, enterprises and organisations to act in accordance with privacy laws and regulations
- Takes into account the technological evolution

Foto: GÉANT Community Blog

SINTEF

Many ITS applications collect personal data

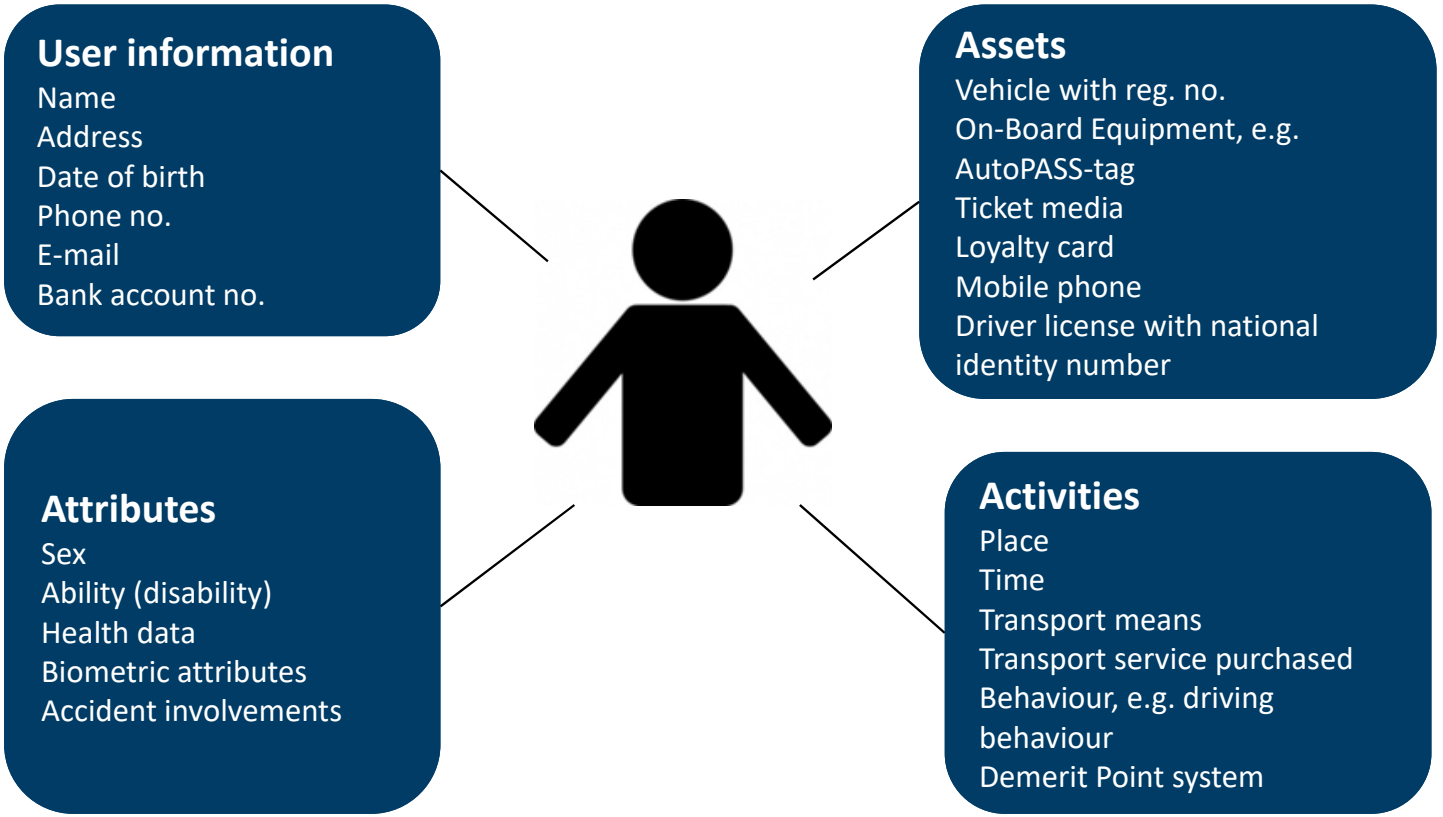
SINTEF

However, the bad guy is really the car

Foto: B Secure

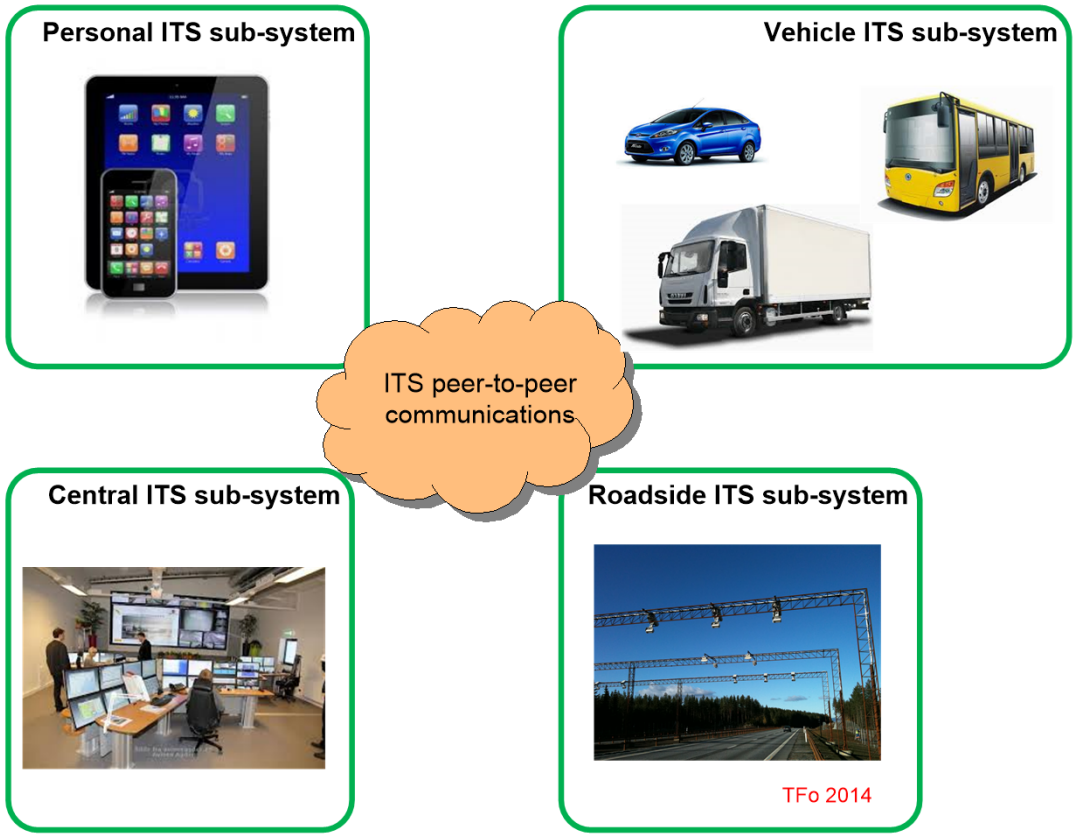
SINTEF

Data related to an ITS service User



SINTEF

Where do we find the personal data?



SINTEF

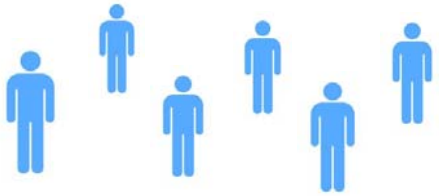
Three major challenges in ITS services?

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



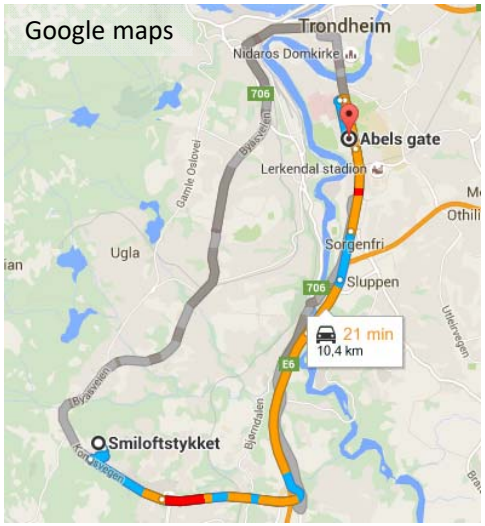
SINTEF

Examples on privacy threats

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

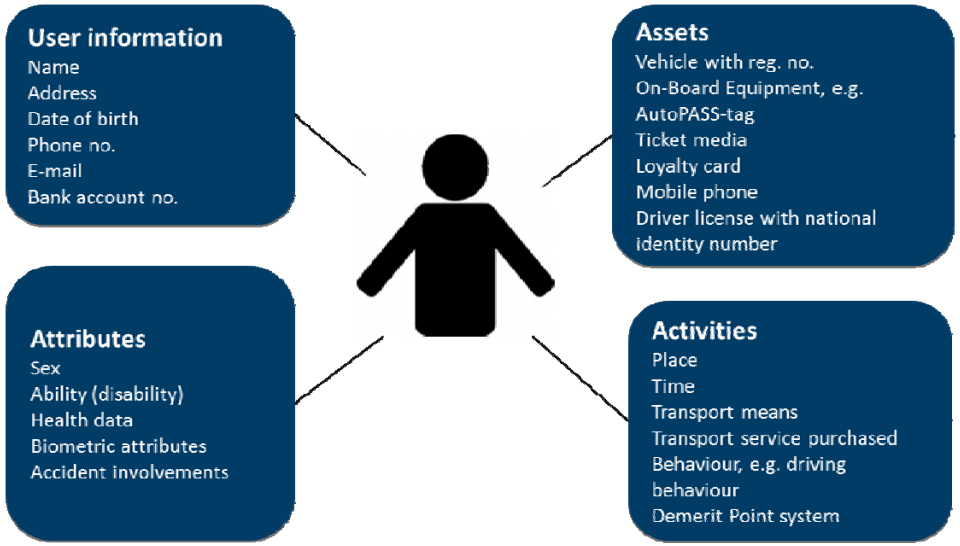
- **The ITS service User is there now**
  Registration of the presence of a person

- **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)

AutoPASS-tag and ANPR

SINTEF

Electronic ticketing

Contactless smartcard as ticket media

Photo: Grid Transportdesign

Mobile phone as ticket media

Photo: Google Play

Mobile phone as ID (Be In – Be Out)

Photo: Wikimedia Common

Photo: techradar.com

NB! We have an industry norm in Norway!

Access control based on ANPR

Photo: NetConnect

SINTEF

Parking payment and parking surveys based on OBE or ANPR

Photo: linkedin.com

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

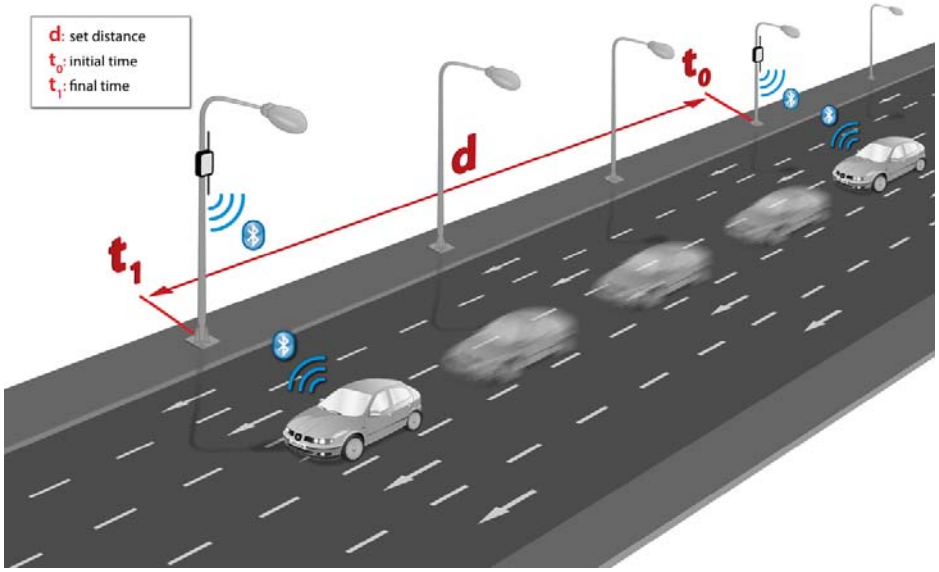


Photo: IcyApril

Photo: pixapay.com

SINTEF

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

Foto: NRK/NRK

Control of :

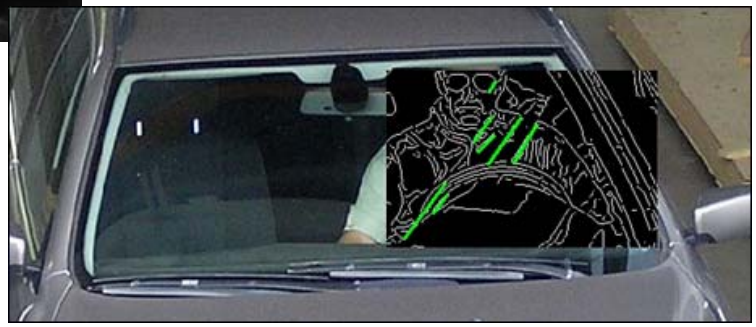
- Annual vehicle fee
- Insurance
- EU vehicle control

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

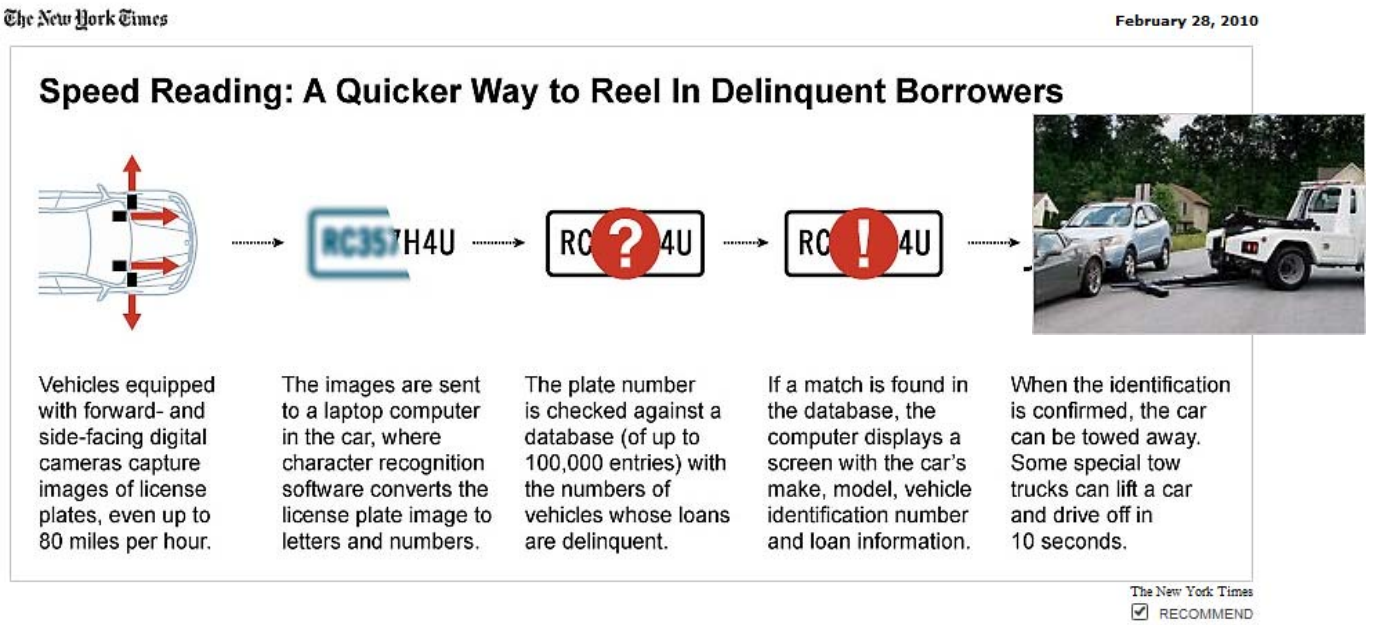
Personal advertising based on ANPR

Foto: www.safespeed.org.uk/

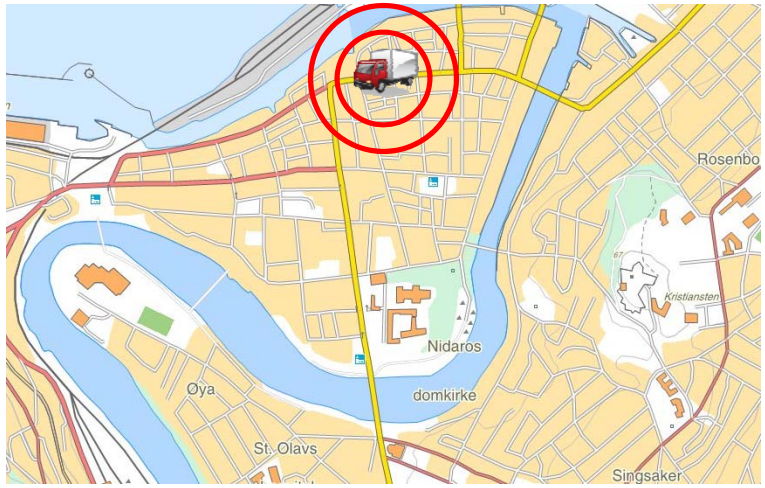
- A hidden camera reads the number plate and access the UK vehicle register to find the car make and model
- The driver is informed about which oil type to use for his vehicle referring to the license plate number of the vehicle

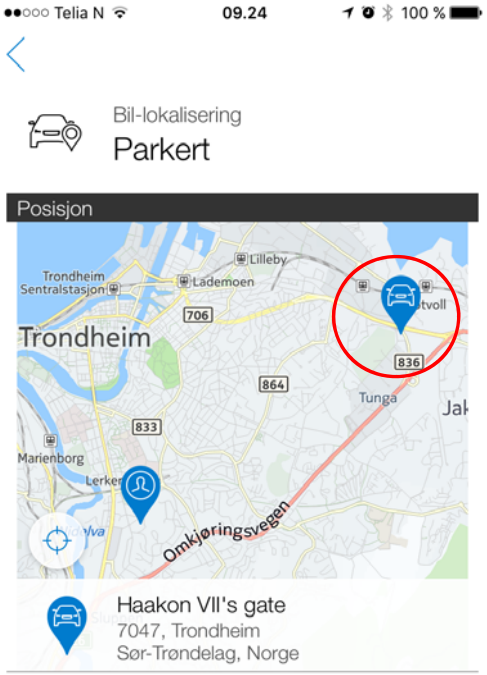
SINTEF

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

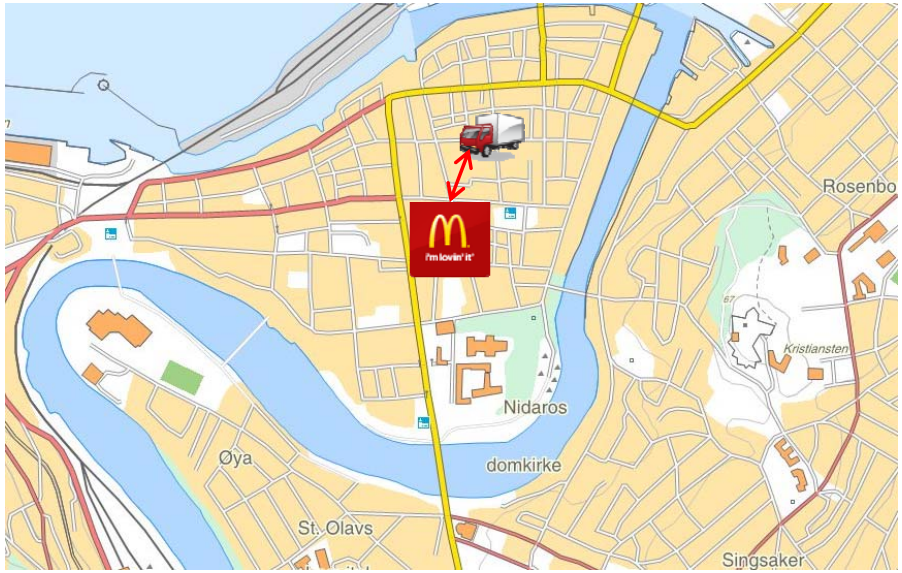
Tyver, taxi-sjåfører og radiosendere

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

Teknisk Ukeblad 12. mars 2014

SINTEF

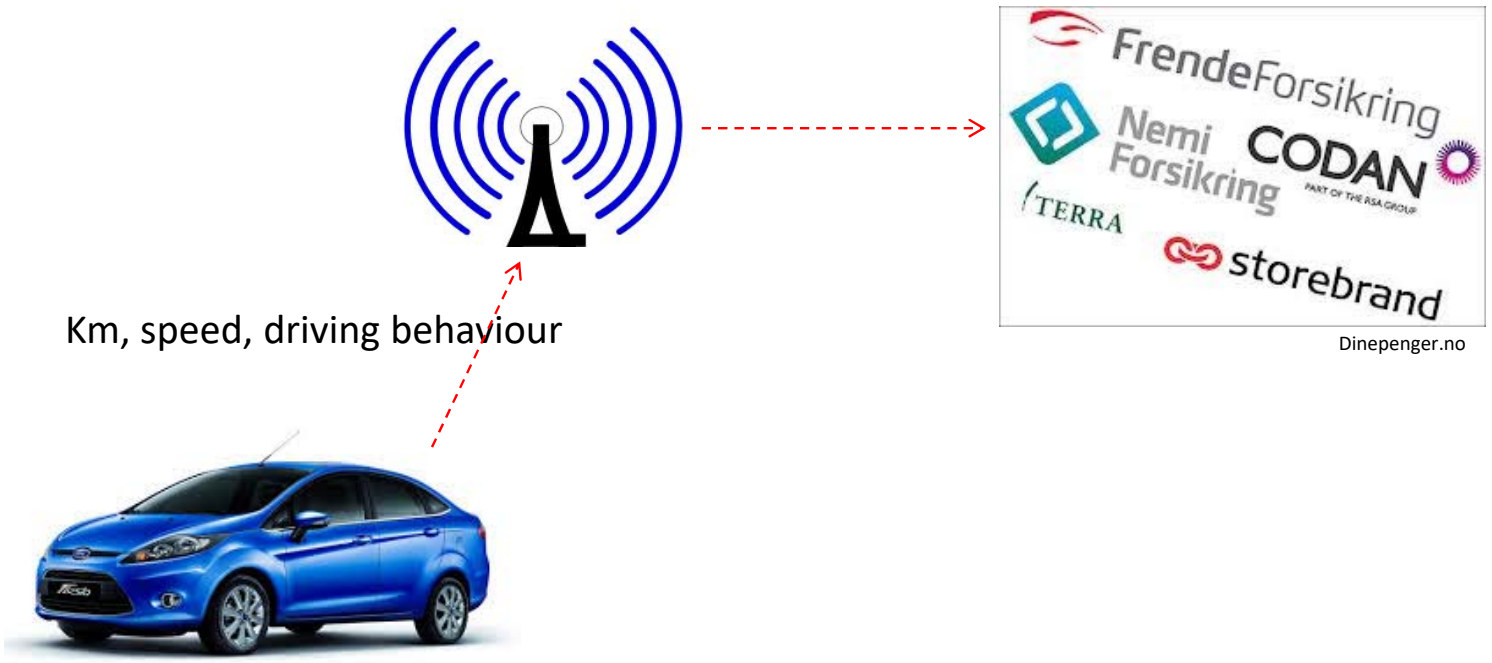
Location based services



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

SINTEF

Pay as you drive



Dinepenger.no

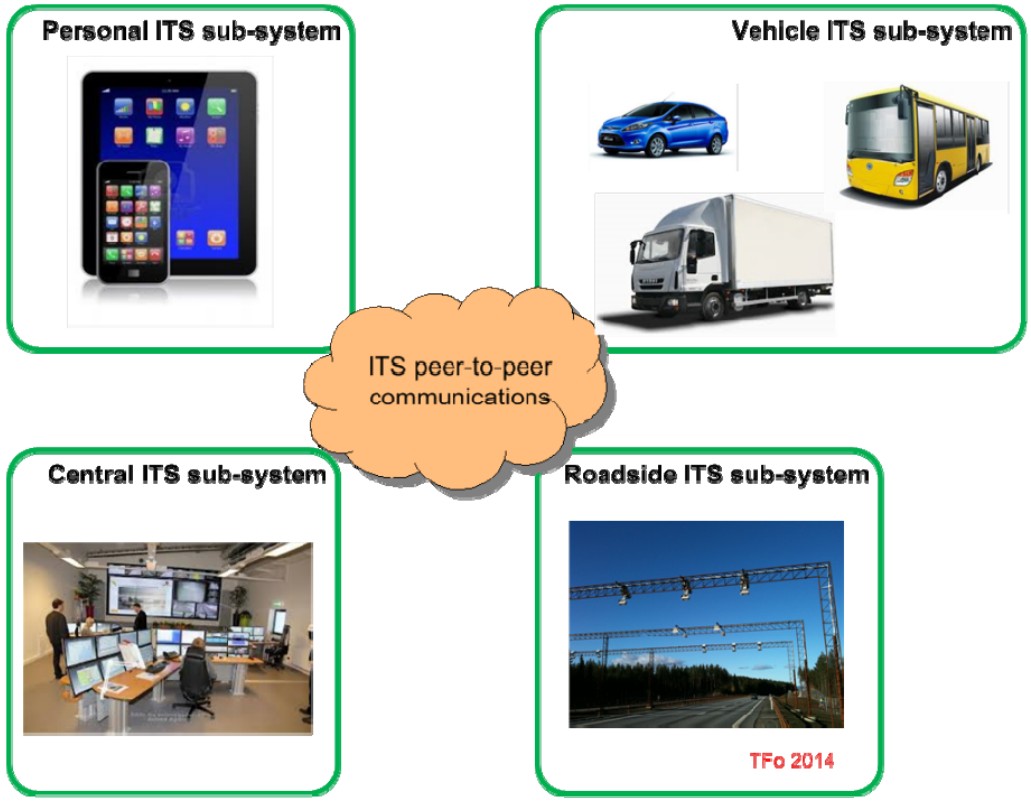
SINTEF

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



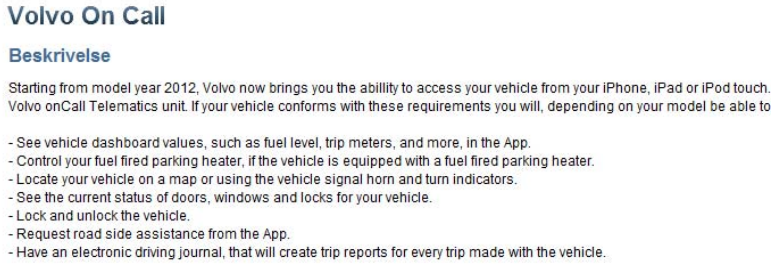
SINTEF

How to get access to the vehicles internal ICT system?

www.canbushack.com

www.hackaday.com

www.caranddriver.com



iTune Appstore

SINTEF

Teknisk Ukeblad 8. mai 2017

Fiat Chrysler måtte tilbakekalle 1,4 millioner biler etter at Charlie Miller og Chris Valasek hacket seg inn i en bil og tok kontroll over både bremser og styring.
(Bilde: JOE RAEDLE/ Scanpix)

HACKING AV BIL

Mannen som hacket en Jeep advarer: – Alle biler lar seg hacke

– Det er vanskelig å hacke en bil. Men det burde være enda vanskeligere, mener Charlie Miller.

digi.no

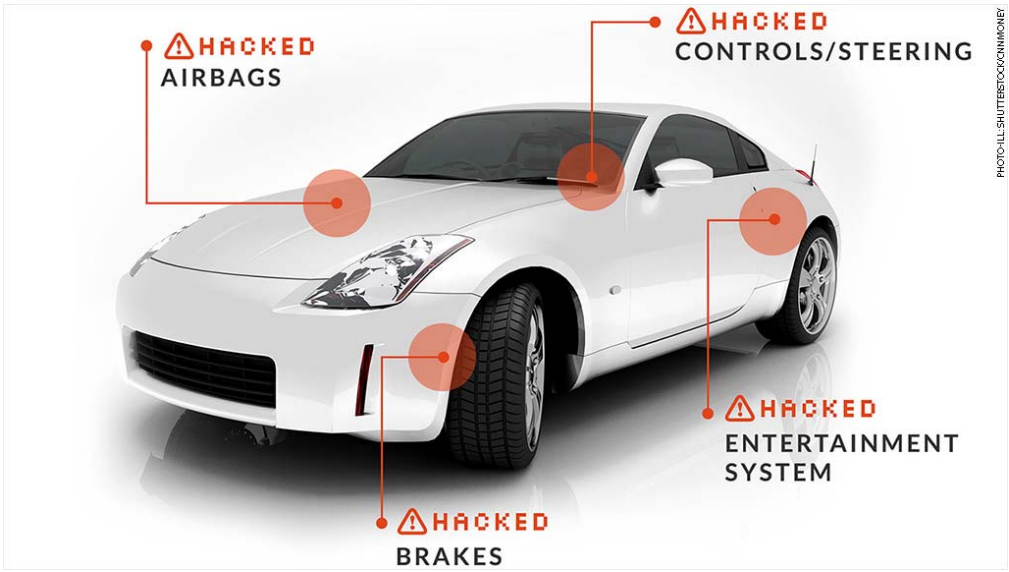
Informasjonssystemet til Nissan LEAF mangler enhver form for tilgangskontroll. Foto: Nissan

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



PHOTO+ILL: SHUTTERSTOCK/CNNMONEY

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