

## **9:30-10:00 Business Panel: Smart cars of Sweden. Cross Industry case on data usage and ownership.**

A joint cross industry case on Sweden's automotive data management and ownership in the past few years. Let's take a closer look at how various types of data generated and utilized by drivers, vehicles, third party systems, authorities and infrastructures have been managed so far?



**Staffan Wallin, Ericsson Sales Director Automotive - Business Line Industry and Society at Ericsson**

The connected Eco system

Connectivity brings changes to the business landscape in most industries today, in an ever increasing velocity. Connecting a product changes the boundaries of product reach. Digital services related to the product will complement the traditional product offer.

Connecting the product opens up for collaboration with other stakeholders in a connected eco-system. We at Ericsson believe that new innovative use-cases, leveraging information provided by connected products, will change the way business is made. Therefore we want to position us as enablers for industries to establish a connected eco-system, thus allowing collaboration between stakeholders, within existing business and cross boundaries connecting to other business areas.

Security and data integrity is paramount for all parties involved in the 3-party relationship between OEMs, Service Providers and Consumers. In the end, the vehicle data shared is owned by the consumer. We provide a solution that allows several layers of consent, where the OEM control what service providers they want to allow access to data from their cloud environment and that these providers live up to their standards and where user consent is secured before any private data is shared.

The already established automotive services market is dominated by services and solutions developed by OEMs or Tier-1 automotive suppliers. Today it is challenging for an unknown service providers to gain access and reach into the OEM eco-system, which is natural as an OEM will focus on already established brands. At the same time we see a trend in small startup companies being established and bringing new innovative services to the marketplace.



**Per Holm-Ovren, Biliva VP Purchasing, Business Development and Business control**

Happy to discuss broadly on strategy, digitalization, business models, customer needs and trends, retailing in the future, transportation needs etc. (equally happy to prepare 3-5 slides on this)

Strategy – What possibilities opens up with available RMI?

Customer needs and trends – Do the customers even care about these new services?

Digitalization and future retail – Which new potential business models will be valid given what we know today - Who is likely to win?

Trust issues – What does it imply in terms of trust to share RMI?

Operational issues - What needs to happen behind the scenes in the workshop?

Not comfortable on: legal issues regarding personal data.



**Fredrik Callenryd, Scania Connected Vehicles Strategist**

No statements shared

## 10:00-10:30 Legal Panel:



**Mattias Sandström Data Inspektionen, Legal Advisor**

Initially we'll bring up the fact that the nature of the car is changing. The currently available technology allows for extensive collection and use of personal data. What used to be a means of transportation may nowadays actually be eavesdropping on you. Is the car still your friend?

We will continue with a brief introduction to the legal framework (mentioning that the GDPR is based upon the Charter of Fundamental Rights of the European Union and the fact that the GDPR is mandatory statutory law).

Thereafter our statement will focus on, and in brief explain, four topics that are of particular interest to the car industry, namely: purpose limitation, data minimization, data protection by design and by default; and finally, conditions for consent.

With these topics as a backdrop, we will describe potential privacy issues concerning connected vehicles. We have decided to give attention to following issues:

- Lack of awareness (car manufacturers may not be aware that their systems process personal data and that these data are subject to the regulatory framework on privacy – for instance the ever occurring discussion about ownership of car data)
- Lack of transparency (car owners and car users may not be adequately informed about the processing of personal data)
- Extensive surveillance of surroundings (the cameras and sensors in cars may not only be used for surveillance of drivers and passengers, but also for surveillance of a large area surrounding the vehicle)

- The amount of personal data collected and processed may be excessive in relation to the defined purpose of processing (essentially it's data hoarding that may violate the requirement that personal data shall be limited to what is necessary in relation to the purposes for which they are processed) - Standard settings in vehicles may not be privacy-friendly.



**Kristina Andersson, Regeringskansliet Project Leader, Utredningen självkörande fordon**

Huvudproblemet utifrån information är –

1. Behöver vi egen lagstiftning för fordon eller klarar vi oss med EU:s dataskyddsförordning (som kommer att gälla som svensk lag)?
2. Om ja, hur få en sådan lagstiftning förenlig med EU:s dataskyddsförordning?

Vad ser vi för problem i utredningen? Fordon kommer att generera stora mängder data. En del data kommer inte att vara personlig, en del data kommer att vara personlig. Antagligen kommer den mesta data från fordon gå att koppla till en person dvs. träffas av EU:s dataskyddsförordning.

Fordon kommer att behöva dela med sig av information t.ex. kartdata, väderdata. När fordonen delar med sig av informationen behöver informationen inte längre vara personlig. Problemet här är att den är personlig vid insamlandet. Hur hantera detta?

Men det kommer även att finnas behov av att hantera personlig information under en lång tid (jämför svart låda). Vi ser ett behov av information utifrån två situationer:

1. Var det självkörande läget aktiverat och fungerar systemet som det skulle
2. Särskilda händelser typ olycka

Problemet här är att avgränsa vilken information som ska samlas in och hur länge. Kommer att krävas någon form av sortering.

**10:30 - 11:00 COFFEE BREAK**

**11:00 - 11:30 Privacy Radar: The new General Data Protection Regulation and the wireless car – theory meets practice.**



Agnes Hammarstrand, Delphi IT Lawyer

Is it possible to build in privacy to prepare for compliance with the new General Data Protection? When is consent needed and how to obtain it?  
How to comply with information requirements and other privacy requirements in practice?

**11:30 - 12:00 Breaking the eternal clash of "LegalsVS Techs" through Privacy by Design**



Maria Alm Springworks Legal Director

Former Google lawyer and legal director of connected car company Springworks gives practical examples on how lawyers can implement agile principles of PBD into their ways of efficient collaboration with technology and business objectives. To simply launch better products faster.

**12:00 - 12:30 SCANIA & ACEA: Interpreting GDPR principles for the automotive industry.**



Fredrik Callenry Scania Connected Vehicles Strategist

Get yourself prepared and take a look at the ground principles jointly developed by Scania and ACEA around the GDPR. Fredrik will let us know what they mean in practice.

**12:30 - 13:30 Lunch & Networking Zones**

**13:30 - 14:00 How to put the consumer in the driving seat for control of car data.**



Karin Rehbinder Telia Company Senior Product Manager



Maria Alm Springworks Legal Director

1. How do we verify that users are in control of their data although sharing it with various partners?
2. How can privacy by design principles be implemented at different stages of integration into shared infrastructure?

3. How do we implement privacy as a business strategy?

**14:00 - 14:30 Urban Mobility: Experimenting with autonomous public transportation**



Johannes Koponen Foresight Strategist

Connected and sustainable mobility pilots in Nordic public transportation. Where will it take the commuters as well as the entire public transport infrastructure?

Exciting projects of **Kutsuplus** and **SOHJOA** shook up and were the first ride-hailing services arrived – that completely changed expectations and perception of the way we use this kind of service.

Let's talk about the vision and the reality of Hyper connected Society. False premises in how autonomous public transportation scales up. Regulatory recommendations to secure the future of connected public transport.

**14:30 - 15:00 The future of mobility from an auto importer and dealer's perspective.**



Adam Erritzøe, Innovation Manager Semler Gruppen

Transforming passengers' experience. In 2017 self-driving Ollis will hit the roads of Scandinavia.

Semler is preparing collaborating with Local Motors to start operating fleets of autonomous vehicles Olli in the Nordics. Currently representing LM in 8 countries Semler is planning to start piloting Ollis in H2 2017, transforming the market and society to become more autonomous, more shared and more sustainable

**15:00 - 15:30 Networking & Energizer**

**15:30 - 16:00 Cyber Vulnerabilities & Risk Study: NISSAN HACK**



Scott Helme Feisty Duck Researcher

Whether it's a car manufacturer or a toy manufacturer, security has to be built into the design and should never be an afterthought.

Nissan vulnerability stood out because the hack was so easy to execute allowing any smartphone to remotely control any of the 200,000 impacted Nissan cars – no matter where they were located.

In fact, Troy Hunt made a video of himself in Australia hacking a friend's car based in the UK to prove the point.

The owner of the car and the security researcher Scott Helme is going to present the vulnerability that allowed anyone with the right Nissan Leaf and eNV200 vehicle identification number (VIN) to remotely access the car's climate controls, battery status, and GPS logs that included the dates, times, and distances the car had traveled. Most drivers expect a level of privacy when it comes to GPS tracking data, that includes time and distance traveled. But beyond the clear privacy violation, the Nissan vulnerability posed that there are ways the hack could cause real damage to Nissan car owners.

**16:00 - 16:30 Security as the key to unleashing the real power of the connected and autonomous vehicle.**



**Martin Hunt, BT Global Services Automotive Industry Practice Lead**

We have the opportunity to get security right now for connected cars, to be ready for the autonomous cars of the future. And with autonomous cars, connected cars, pedestrians and cyclists sharing the same roads, wouldn't you want to trust the security?

While user education is one part of the solution, a full and comprehensive assessment of fleet technical risks is essential to shape appropriate mitigation strategies. To address security and privacy issues, auto manufacturers and their expanding partner and supplier ecosystems will need to become more secure, vigilant, and resilient.

In this panel talk we are going to discuss the main cyber related pain-points and the framework of solutions available now.

**16:30-17:00 Telecoms or Manufacturers: Who owns the road of digitization?**



Karin Rehbinder, Telia Company, Senior Product Manager  
Senior Product Planner



Jörgen Wahlund, Volvo Group Trucks Technology



Martin Hunt, BT Global Services Automotive Industry Practice Lead  
Vehicles Strategist



Fredrik Callenryd, ScaniaConnected

Promotion of the wider deployment of connected and automated driving requires tight cooperation of manufacturers and operators. Let see who owns the knowledge and operations within the key fields:

How to create an open eco-system of partners that can benefit from car generated data and in the same time letting the consumer being in control who sees their car data. Instant security for connected cars and the upcoming autonomous cars of the future. Collaboration of carriers and manufacturers. What's done so far.