

Innovation & Security
for Connected Cars

INNOVATIONEN
INSTITUT

White Paper

Dr. Axel Glanz, Markus Lang,
Doanh Ngyuen, Damien Schmidt

Supported by
BMW Group, ESG,
HUF & Vodafone Group



Management summary

The Connected Car represents a major challenge and opportunity for current and future stakeholders in the automotive industry. In 2014, 10 million new cars, globally, were equipped with embedded connectivity functions. As presented in Chapter 1, the demand for connected cars is increasing due to legal factors as well as customer benefits, leading to an overall increase of connected cars sold. Exhibit 1 shows that the GSM Association and the Innovationen Institut estimate that by 2020, the annual number of connected cars sold with embedded systems will increase to nearly 50 million globally. Four out of five new delivered cars will be equipped with networking functions in 2020. With Apple and Google recently committing to this market through CarPlay (Apple) and the Open Automotive Alliance (Google), their impact will be substantial as well.

In this survey, over 300 experts (executives and decision makers from the automotive, computer and telecommunication industry) were asked about the related topics of connectivity, data management, security and legal issues.

- The annual global revenue with connected cars services will increase to approximately 160 billion euro annually (exhibit 2).
- Connected cars will exponentially increase the volume of collected data resulting in challenges related to data management, data-security and data-privacy.
- Key topics are the data transfer, management and privacy/security. People value their privacy and security and will hesitate to share data if the value benefits do not exceed privacy and security concerns.

Annual sales of connected cars with embedded systems

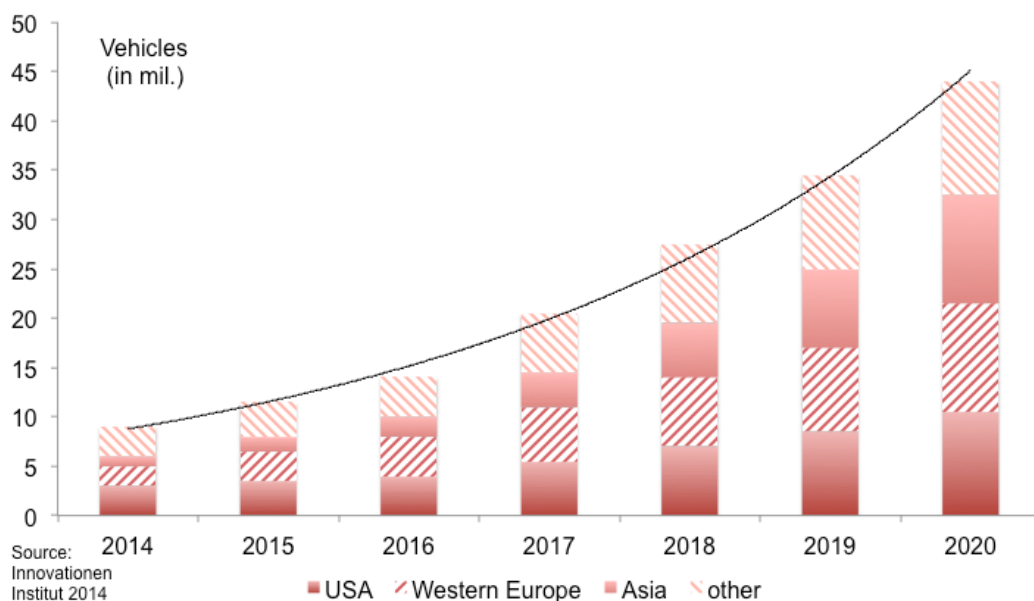


Exhibit 1

- De-facto standardization with Android, iOS and Windows embedded is helpful for manufacturers, suppliers and telecommunication firms to enhance and channel their competences and business practices. But in the theory of network externalities this leads to oligopolistic market structures.
- As stated in exhibition 12, many security risks and vulnerabilities exist. To overcome these barriers to adoptions, a shared responsibility of user (firewalls, virus scans, software updates) and manufacturer (secured protocols, authorization) will be necessary, which in turn may cause restricted consumer acceptance.
- Clarifications in the legal framework are necessary in order to address data ownership and liability. For consumers in particular, the knowledge of who uses the data for which services or business models has to be improved upon. Consumers need to be given the choice, whether to accept or deny connected services in each case.
- The IT and Communication sector can benefit from the data that will amount alongside the increased number of connected cars.
- New and improved business models across countries will be necessary for companies to accelerate the consumer adoption and generate profits.



"Human error is involved in 95% of all traffic accidents on Europe's roads, in which more than 30 000 people are killed and 1.5 million injured every year".



"Electronic-Safety, especially "smart" technologies based on the powers of computers and telcos, can make a major difference to these figures." (European Commission 2020 Initiative)



Report Contents



Introduction (2)

1. Demand for connected cars (3)

Functions of networked cars and their benefits



2. Data management (6)

Data ownership and automation preferences



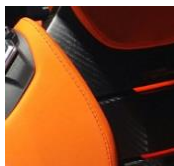
3. Apple/Google/MS' market commitment (9)

Recent market activities of Apple/Google/Microsoft



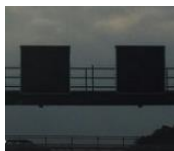
4. Security (11)

Possible security risks and vulnerabilities



5. Concepts to improve security (13)

Possible prevention and location of endangered equipment



6. Assessment for political regulations (16)

Requests for legal framework



7. Perspectives and market opportunities

2020 (18)

Who will benefit from connected cars?

8. Conclusion (22)

Introduction

In the automotive industry, the “connected car” is a topic with increasing relevance. Whilst being a potentially significant market opportunity, it appears to be a threat for some established market players, caused by the participation of new players/competitors. Google recently announced the formation of a strategic alliance (OAA) focusing on the connected car. Apple has also entered the market with its CarPlay. Microsoft’s first steps in the automotive sector were made much earlier with the introduction of Windows Embedded Automotive. Apples iOS and Googles Android are established standards for mobile operating systems and may also be implemented into the automotive sector.

We have distinguished six product packages related to connected cars: Mobility management, vehicle management, entertainment, driver assistance system, passenger comfort and security.

As shown in Exhibit 2, it is expected that on average, driver assistance systems will be the best selling product package with almost 50% of the volume of sales, followed by security with 33%. Security includes danger alerts for the driver as well as internal response to dangerous situations by the car itself. Examples include: anti-collision devices, emergency call functions and security software services.

Experts presume that by 2020 a large part of the volume of sales will be driven by security features.

The numbers for security services revenues range from 33 billion euro (Booz & Company) to 50 billion euro (Innovationen Institut). Management Engineers expect the largest volume of sales in the security category, with nearly 60 billion euro.

Global annual volume of sales of security services and other functions in connected cars

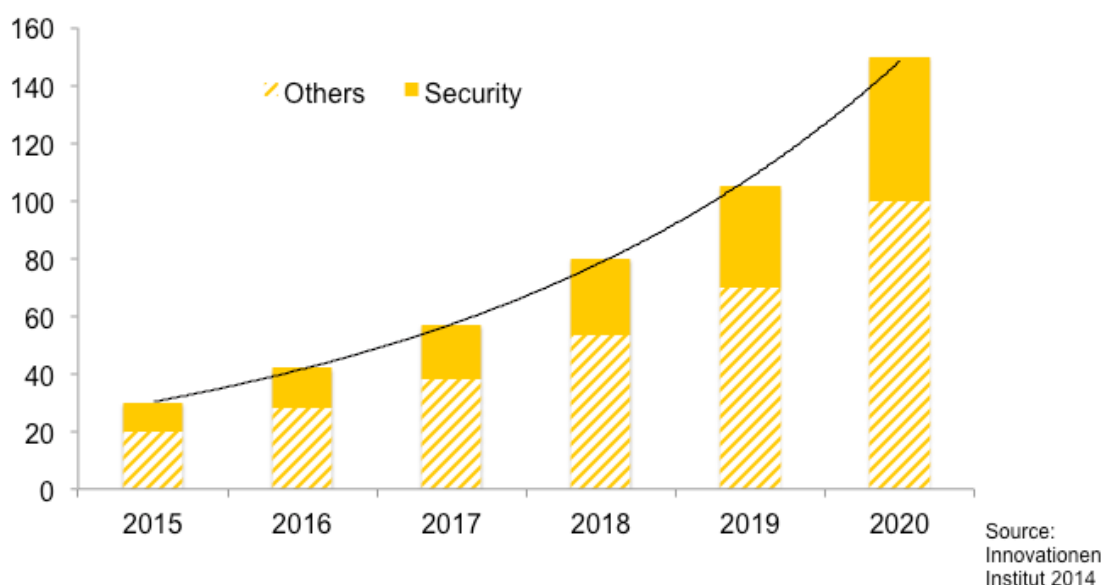


Exhibit 2

1. Demand for connected cars

Demand creating functions of connected cars



With the introduction of the networked car, driver assistance functions can be improved and new comfort generating solutions can be offered to the customer.

Connected cars features like “Traffic Optimization” “eCalls” “City safety” and “Car to infrastructure” will significantly increase the security. Two key components of security driven shifts in the demand can be identified.

First of all, some features will be mandatory by law, causing a high demand for connected cars. By 2018 all new models of European cars and light duty vehicles will have to be equipped with the eCall system, which will automatically call emergency services in case of a serious accident. On 13.06.2013, the European Commission announced that eCall could speed up emergency response times by 50 percent in the countryside

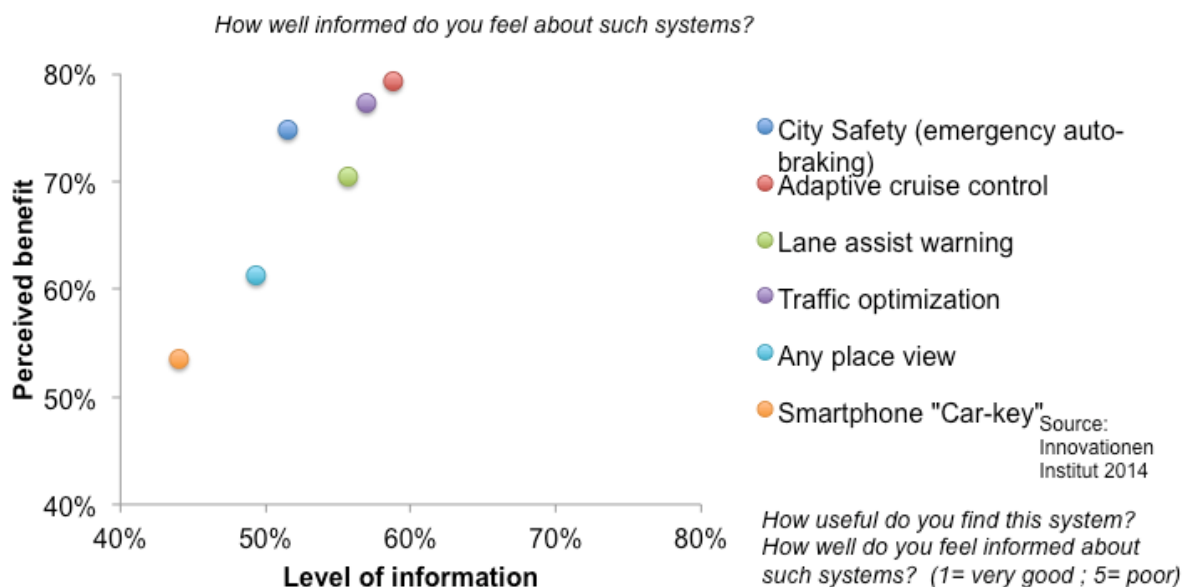
and 40 percent in urban areas to save an estimated 2500 lives a year. (European Commission 2020 Initiative)

Additionally, as shown in Exhibit 3, perceived benefits created by the new security functions of connected cars can be increased by appropriate communication systems. This will further expand the demand for connected cars.

Other features of connected cars result in an increase of the customer’s comfort, rather than his security. Features including “Any Place View”, for the remote control of vehicles and Smartphone “Car-key” for car access can increase the perceived benefits by increasing the customers’ driving comfort.

Exhibit 3 shows that the higher the level of information – the better the received benefit seems to be. “Adaptive cruise control”, “Traffic optimization”, City safety” and “Lane assist” are especially useful.

Functions of networked vehicles and driver assistance functions



Concepts for different target groups

Current vehicles already carry special instrumentations and data loggers, which collect data from different sensors, e.g. emission control or electronic management. The user still drives to a dealer's service bay to capture this data for off line analysis.

The automation of the data transfer "over the air" is very comfortable for user/driver and for professional support as well. Drivers benefit by paying less attention to safety assistant systems while the fleet operators can evaluate a logbook or check the need for maintenance more easily. However, unlimited data transfer is of more importance to some users.

Other users care more about unlimited data transfer. To further develop the market for connected cars, it is important to differentiate between different target groups. For the diffusion of new technologies, at least two target groups should be separated:

1. "Innovators" are the first who adopt new technologies. In this report, 45 percent of the attendees belong to this target group. The group of "Innovators" is typically much smaller, but in this case, only experts participated.

2. The "Majority" is the second target group. This group covers the remaining 55 percent of the contributors.

Acceptance of automated data transmission

In your opinion, do you think this data should be transferred automatically?

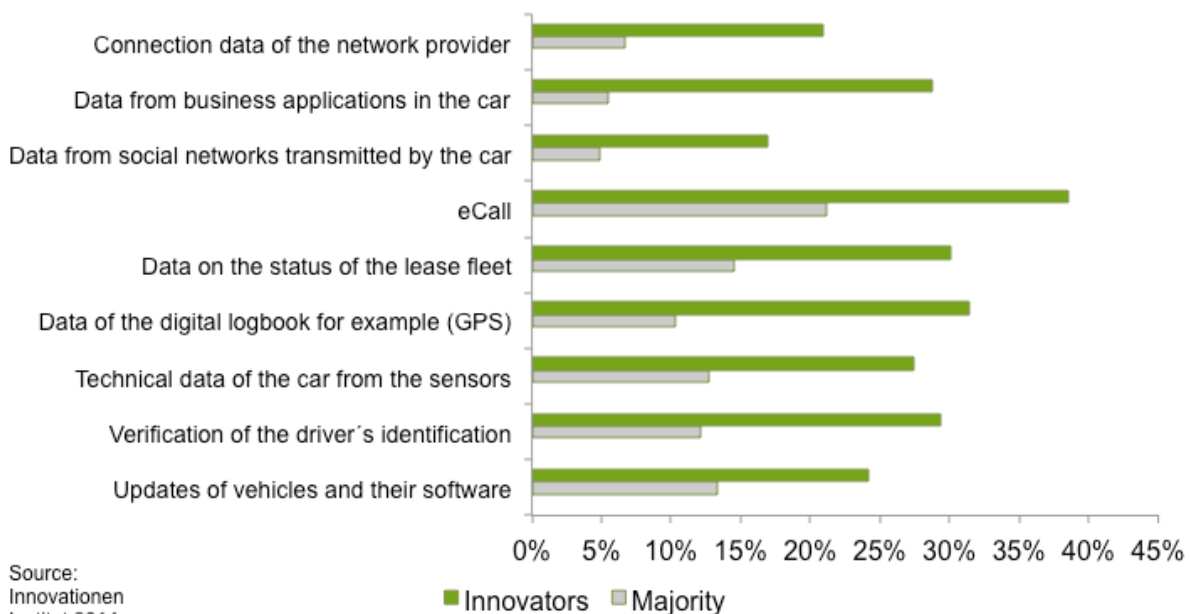


Exhibit 4

The strongest acceptance for totally automated data transfer comes from the group of “Innovators”.


They accept automated data transfer from 40 percent for “eCall” to 20 percent for “Data from social networks”.


The picture completely changes when the “Majority” expresses their level of acceptance of automated data transfer of connected cars.


Some drivers want to either give explicit permission, or not use an automated service at all.


Only 10 percent agree to the automated transfer of “connection”, “business” and “social network” data collected by the connected cars.


Based on the level of openness and trust displayed by the first group of adaptors of connected cars, the current concept of connected cars seems appropriate. The “Majority” will follow within the next years, but will require more control over data transmission functions and services. This should be an important part of further concepts for connected vehicles.

 The higher the level of information – the better the received benefit of connected vehicles seems to be.

 The automation of the data transfer “over the air” is very comfortable for user/driver and also for professional support.

 To further develop the market for connected cars, it is important to differentiate between the different target groups.

 The strongest acceptance for totally automated data transfer comes from the group of “Innovators”.

 The “Majority” of customers will follow within the next years, but will require more personal control over data transmission functions and services.

2. Data management



In 2014, data management is already a major topic in the connected cars market.

In a current publication, BMW unveiled 60.000 diagnosis sessions per day worldwide.

In February 2014, Audi reported that since the launch in April 2011, Audi connect customers used more than 75 terabyte of data.

Therefore, the question of which market participant has the capability to handle large amounts of data and is trustful enough to possess the data should be raised.

Additionally, there will be new partners staking out a claim. For instance, insurance companies are interested in information on driver behaviour as well as crash data.

All partners must find an optimal balance between customers' sensitivity needs and economic benefits.

On the one hand, it is seemingly impossible to find solutions to single-handedly manage these complex systems. On the other hand, an increase in the number of partners involved may lead to more weak spots.

Data ownership for connected cars

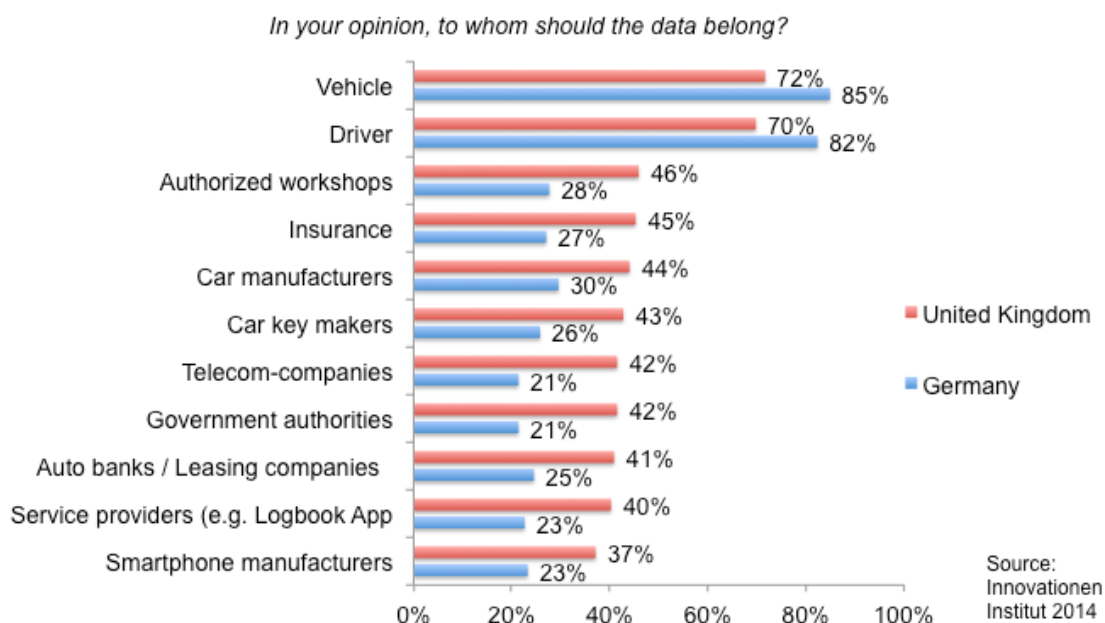


Exhibit 5

Data ownership

A dataset with specifically measured figures across the vehicle life cycle is very useful. Manufacturers and suppliers are able to improve their products by assessing the data while IT/telecommunication firms are able to evaluate customer behaviour.

Regardless of the experts' origin, it is stated that the data should belong to the vehicle owner or the driver himself with an average of 71 percent in the UK (Germany: 83 percent). Concluding, clarifications are nec-

essary in the legal framework to address data ownership. It is especially important that knowledge of who uses the data for which services or business models is improved as a means of giving consumers the choice of whether to accept or deny connected services in each case.

Other options for data ownership are less desirable: Car manufacturers, authorized workshops and insurance providers have limited trust from the public relating to data handling and ownership. In Germany 27 to 30 percent could accept data ownership by such parties and in the UK, there was support from 44 to 46 percent of the respondents.

Competences to manage large data volumes

Certainly, the amount of data will increase with the possibility to transfer vehicle's data over the air.

It is necessary to distinguish between two sorts of data. One should be considered as critical, e.g. data from the motor control unit, emission control or coordination. Different kinds of data occur from entertainment systems, which consist of app usage or multimedia consumption behaviour.

“Innovators” estimate the IT service providers' capability to manage large amounts of data best with 60 percent (Majority 37 percent, but still the best). The reason, on one hand, could be the physical capability, for example, servers, and on the other hand, the fast adaptability.

The competence of IT service providers to manage large data volumes are followed by car manufactures with 53 percent. It is interesting to note that the group of “Innovators” still evaluate Apple, Google and Microsoft with 46 percent behind the “traditional” IT service providers and OEM’s for connected cars.

Competence to manage large data volumes for connected cars

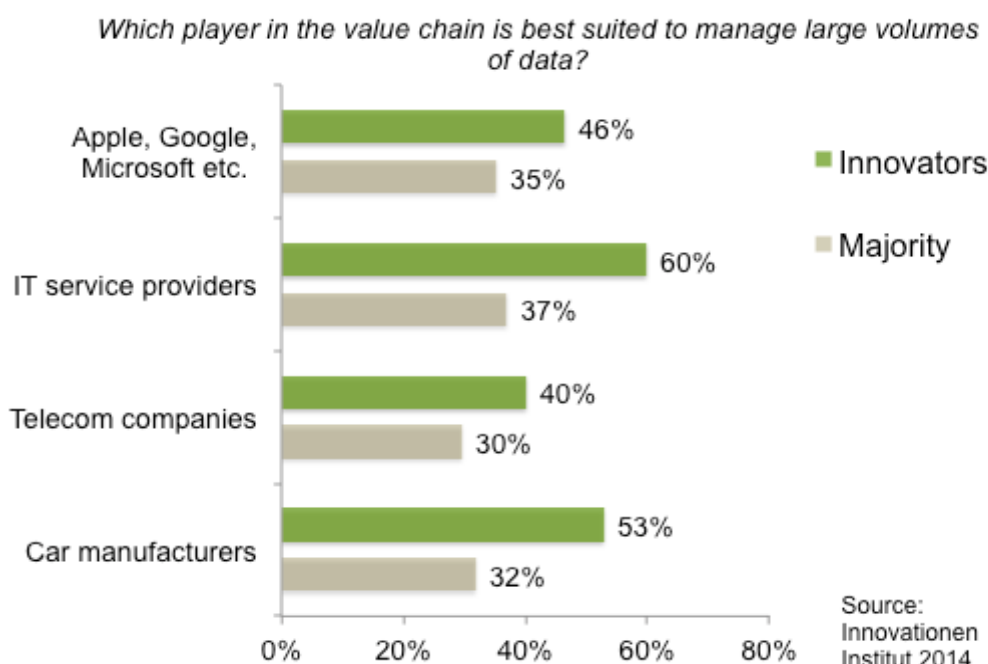



Exhibit 6


Economic and technical issues with data ownership


In Exhibition 7, almost two thirds of the executives miss a common business model for the breakthrough – having the possibility to turn on and off connected services seems to be the more desirable option.


Approximately one half of the executives would be open to replacing the car key with a smartphone, which in turn, would enhance the demand for individual car functions.

Individual speed limits, engine power and interior features will improve insurance options and comfort.

 It is critical for the diffusion of connected vehicles in Europe to have a common, well-functioning business model across Europe.

 Giving customers the option to turn on and off any connected services at any given time could accelerate the diffusion.

 Apple, Google and Microsoft seem to still be behind in competences to manage large data volumes of connected cars.

 Almost every second expert states a replacement of the keys by the smartphone is desirable.

Economic and technical issues with data ownership for connected cars

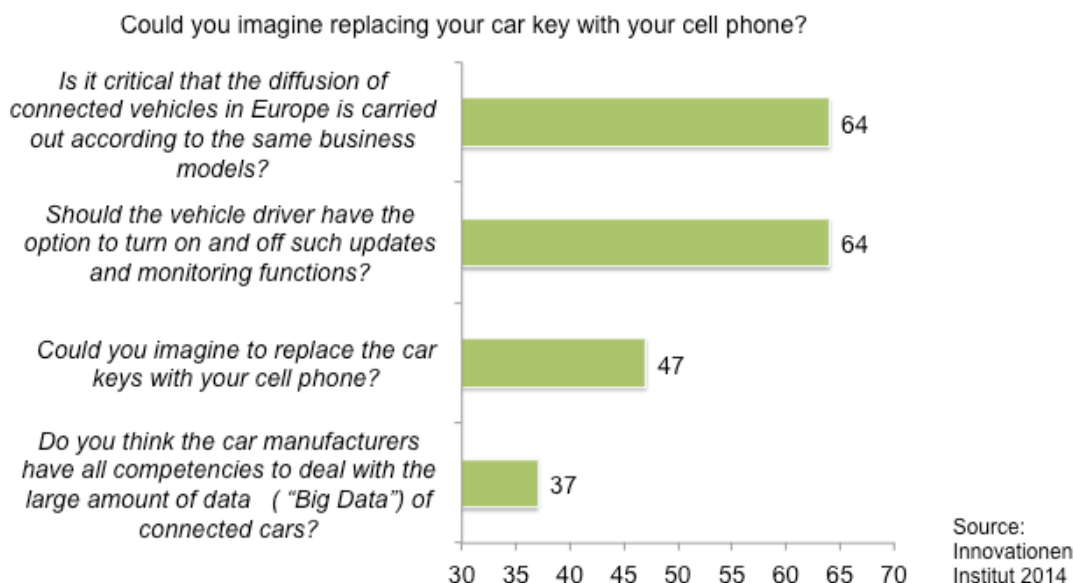


Exhibit 7

3. Apple/Google/Microsoft's market commitment



Microsoft has been involved in the connected car software for nearly 10 years, providing embedded software systems.

Now, Apple and Google are entering the market more intensively. Apple's CarPlay was launched in March 2014 and was originally supported by Ferrari, Mercedes Benz and Volvo.

BMW, Ford, General Motors, Honda, Hyundai, Jaguar, Land Rover, Kia, Nissan, Subaru, Suzuki and Toyota will also support CarPlay.

Google, with its newly formed Open Automotive Alliance (OAA) has recruited Audi, General Motors, Honda, Hyundai and NVIDIA to the alliance.

Microsoft has already gathered competences by providing embedded systems, for example, Windows 7 based embedded systems

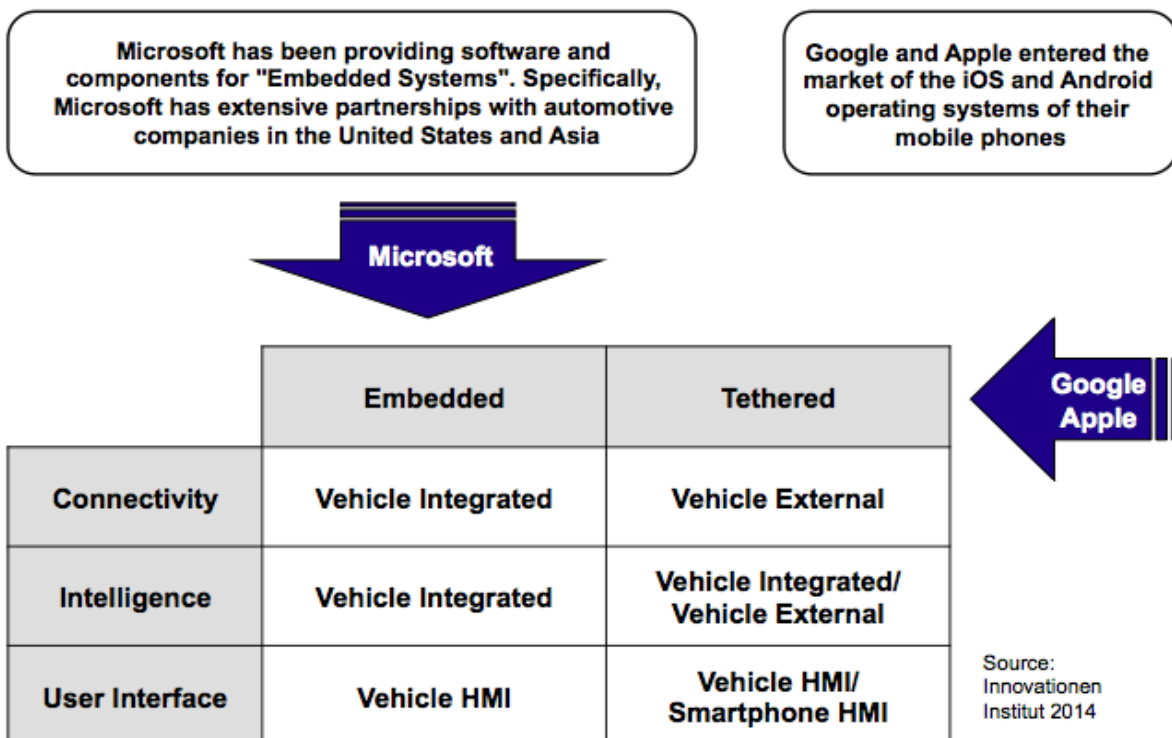
in electric cars (i.e. Nissan Leaf). Other strategic partners of Microsoft are Toyota, Kia and Ford.

Google and Apple are primarily targeting tethered/smartphone integration solutions. Given the fact that Microsoft, Apple and Google have an existing customer base, they can easily acquire competences and therefore can be seen as potential enablers for further innovations.

Since Microsoft, Apple and Google have a great potential in catalysing innovations and developments, they create a technological push, which results in lower prices and additional demand.

Especially Google and Apple have a massive customer base with smartphones. In addition, they have implemented de facto standards with their Android and iOS and offer millions of more or less useful apps for cars.

Connectivity and market entry of a new "player"



Furthermore, Google and Apple developed efficient data-mining competences over time as well as competences in turning the collected data into sources of profit.

The collection of users' data by Google and Apple may be of great interest for third parties who could analyse and use this information to create profitable business models. For example, Google could create a portfolio of the safest drivers and offer them a cheap, premium customized insurance.

Another type of risk that is inevitably compounded with the collection and transmission of data are privacy and security risks.

This gives the OEMs the chance to use their excellent trustworthiness acquired over the past decades. However, the more networked vehicles develop to autonomous driving, the more these cars need to interact with external data about traffic, geographic and other information that are managed by other participants – and in this case, interact with engine control or breaks of the motorcar. The question of how deeply iOS, Android and Windows will be embedded into the core systems of the vehicles remains.



The commitments of Google, Apple and Microsoft will catalyse innovation with their agile product development and by creating new standards.



Security and privacy concerns by the potential customers could arise from Google's and Apple's involvement.



Car manufacturers could lose upcoming potential business models to Apple and Google.



The strength of the car manufacturer is that potential customers will prefer to give data to them due to the trustworthiness associated with their brand images.

4. Security



The fact that the connected car is a complex system containing software, hardware, and communication capabilities, exposes it to many threats. For instance, the software may be compromised by hacker attacks or the wireless communication may be the target of interceptions. In addition to the single component's weak point, many leaks can exist between the interfaces of the different elements.

Possible security risks

It is interesting to compare non-automotive and automotive executives. In tendency, they assess the risk lower. The potential risk of “copying other vehicles software or installing third party devices” is of less importance to participants of the automotive industry.

However, both groups agree that a “Compromised ECU (Engine Control Unit)” is the most vulnerable interface with nearly a half of all interviewees agreeing.

Approximately one third of all attendees expect “Tire-pressure monitoring systems (TMPS), and “Media player attacks” to be a possible risk for networked vehicles.

Vulnerabilities and their impacts

Embedded computers, software and transfer modules must have a seamless and secure interaction.

The participants have ranked the vulnerabilities and mapped them, distinguished by “Innovators and “Risk-averse group”. The “Risk-averse group” are the participants with the most security concerns.

Possible security risks of networked vehicles

In your opinion, which interface represents a relevant threat to the security of connected cars?

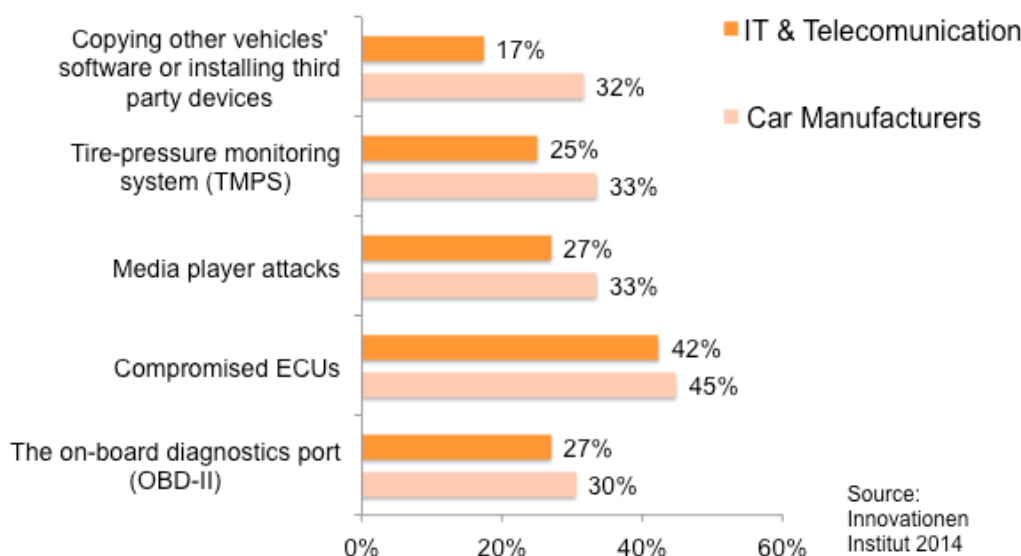


Exhibit 9

They assess the access by unauthorized persons to application data as the highest risk. The innovators only placed it in fourth place.

All the other options are ranked similar between the groups:

The greatest fear for all is the “Causing of breakdowns through remote access by unauthorized persons”, Manipulation of the diagnostic software” and “Updates of the vehicle software with manipulated content”.

“Reading along SMSs or other messages by unauthorized persons, which are destined for other recipients” is the lowest concern.

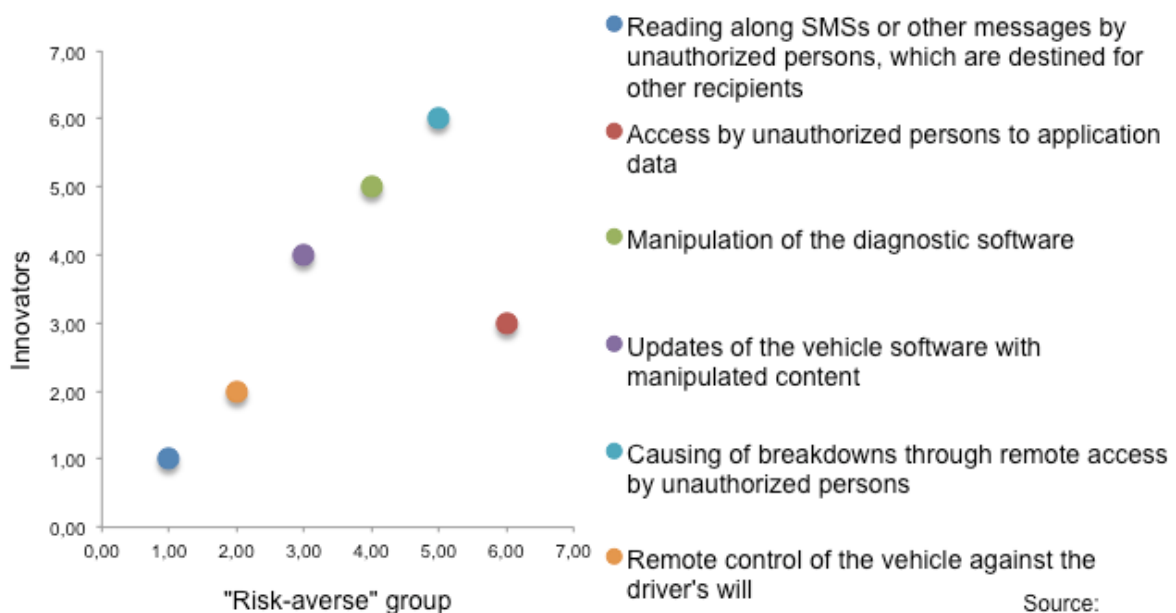
Only a few fear “Remote control of the vehicle against the drivers will” although this is an often mentioned scenario against connected vehicles.



The highest ranked vulnerability and their impact is the causing of breakdowns through remote access by unauthorized persons.

Vulnerabilities and their impact

After we presented you the vulnerabilities, we would like to know which arising dangers do you rank as the highest?



Source:
Innovationen
Institut 2014

Exhibit 10

5. Concepts to improve security



Nowadays it is common practice for the dealers to update the vehicle's software with a physical plug-in connection from time to time. The update is carried out in dealer workshops or transferred from the computer to vehicles using a storage device. The possibility to perform updates and diagnostics over the air will improve service levels but entail security threats. There are systems, e.g. the electronic immobilizer, which were designed with security in mind, but others were designed as standalone systems. Hence, it is vital to improve the security to create more trust in such systems.

Security software

The car security architecture must be considered more with connectivity and security risks in mind. This is where M2M technology and Mobile Network Operators can be of significant value.

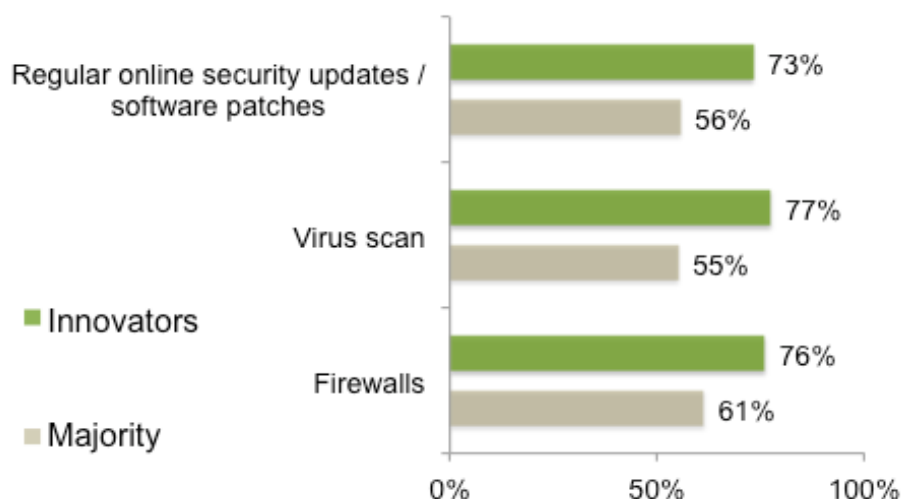
Connectivity can be limited to trusted parties, the vehicle can be made invisible to distrusted parties, and each vehicle has a SIM and is therefore identified with a customer. Wifi and other technologies are far more limited in the security features they support.

In this context, there are two approaches conceivable, one from the user side and one from the technological side. Partly, the user is aware of several security solutions from everyday personal computer or smartphone use. Both “Innovators” and the “Majority” welcome the installation of virus scanners, firewalls and regular security updates in the vehicle.

Innovators assess “Software patches”, Virus scan” and “Firewalls” as significantly more important than the “Majority” believes it to be. They seem to be better informed about security aspects of connected cars and possibly about the power of these instruments.

Security software for connected Cars

How important do you consider the following policies and measures to be in order to improve security?



Source:
Innovationen
Institut 2014

This should be regarded as a big opportunity for proactive marketing, removing concerns, and building trust in the new car generation.

Security needs to be “baked” into the product. Few consumers will be happy to continuously deal with security issues. They simply want a product that works.

A positive aspect is that vehicle updates, which were formerly perceived as maintenance or repairs, are accepted in networked cars.

However, if updates occur too frequently it will certainly cause resistance. It is known from computer and phone updates that updates do not always work as expected.

Much more work has to be done in the field.

Preferred location for the collection and processing of data

The most secure solution for the location of the collection and processing data is in the backend with the car manufacturer.

Taking this information into consideration, it is surprising that most of the attendees would prefer the intelligence to be in the car. Exhibit 12

Additionally, a significant part of 25 percent of the “Innovators” would give preference to the smartphone as the ideal storage place. In the theory of technical diffusion the majority tends to follow the “Innovators” with useful innovations.

If this is the case, in the future, a growing number of the majority will prefer their smartphone as the place where such intelligence and data should be located.

This would imply that the control over the car functions, intelligence and services will be more under the control of the smartphone industry (with dominant players like Apple and Google) rather than the automotive industry.

Preferred location of the intelligence of connected cars

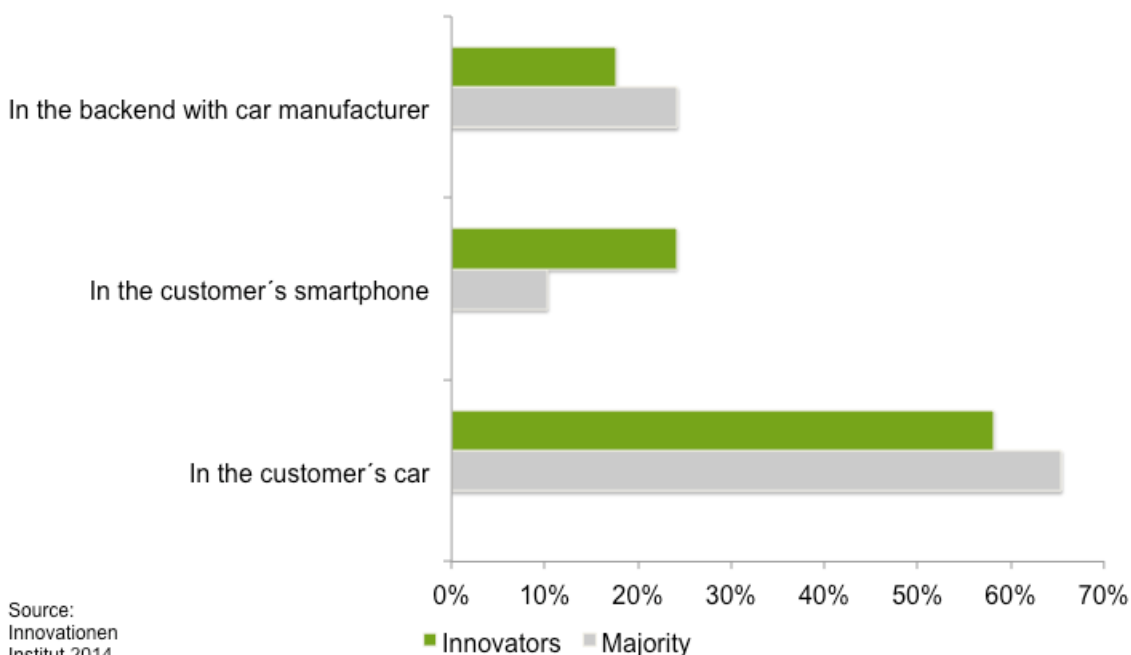


Exhibit 12

With this scenario in mind, it is very important to evaluate the different app concepts of the manufactures.

BMW's Connected Drive, on the other hand, has more partner integration options. Apps are extended with optimization for in-

Preferred App concepts in connected vehicles

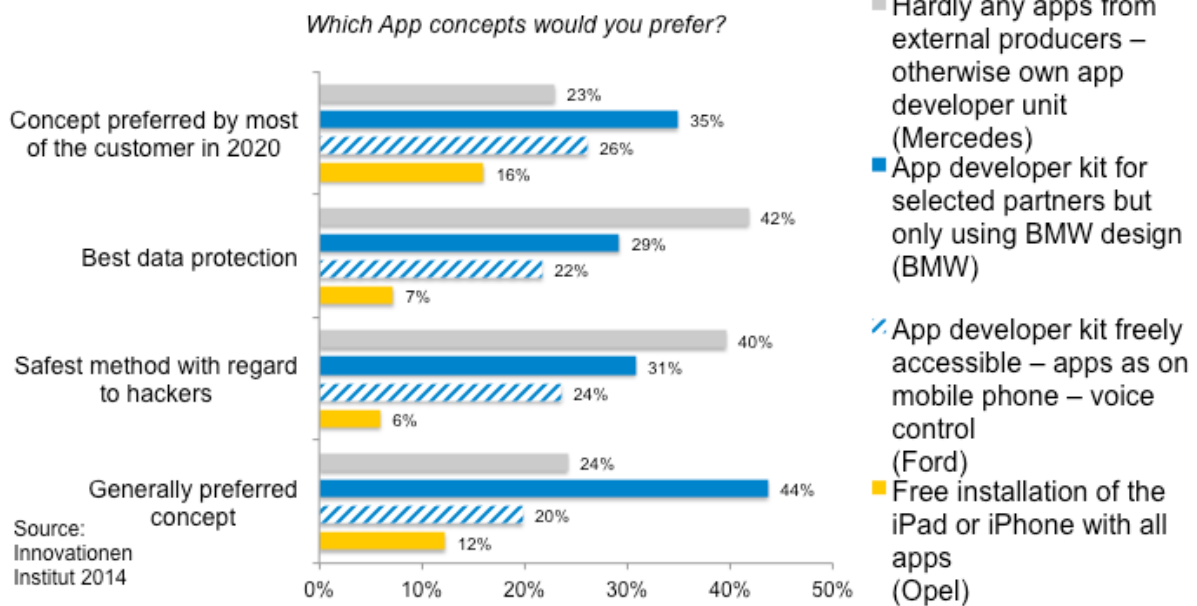


Exhibit 13

App concepts in vehicles

The OEMs compete for customers with different app concepts.

Mercedes follows a very close approach. In the “command online“-system, there are hardly any apps from external producers, instead, mainly from their own Daimler app developer unit. This may be the reason why most of the participants favor this system as the “Best data protection” and “Safest method with regard to hackers” with 40 percent.

vehicle use and BMW vehicle HMI. The BMW concept is generally the most preferred concept with 44 percent and seems as though it will be the best concept in 2020.

The more open Ford and Opel free installation concepts lie behind the others, but may be adopted easier in the future with lower costs.

6. Assessment of political regulations

Obligations to ensure a safe handling of user data



Since political regulations have national requirements, we have to distinguish and compare opinions from the UK and Germany. It is interesting to compare obligations to ensure legal practices and requirements for the safe/ethical/responsible handling and processing of personal data.

The opinion about official indication of remote-controlled supervision and closure is quite similar in Germany and the UK. This also applies to security software with virus scanners.

Respondents from the UK see the need for a security assessment by a third independent party more than German respondents with 66 percent vs. 60 percent.

In Germany, participants prefer an “Official indication of remote-controlled supervision and closure” (58 percent to 69 percent).

In General, there is a strong demand for obligations to ensure a safe dealing with user data in connected cars. Nearly 70 percent of the participants wish for “Verification of security of additional software and mobile service technologies” and “Security software with virus scanner”.

Obligations to ensure a safe dealing with user data in connected cars

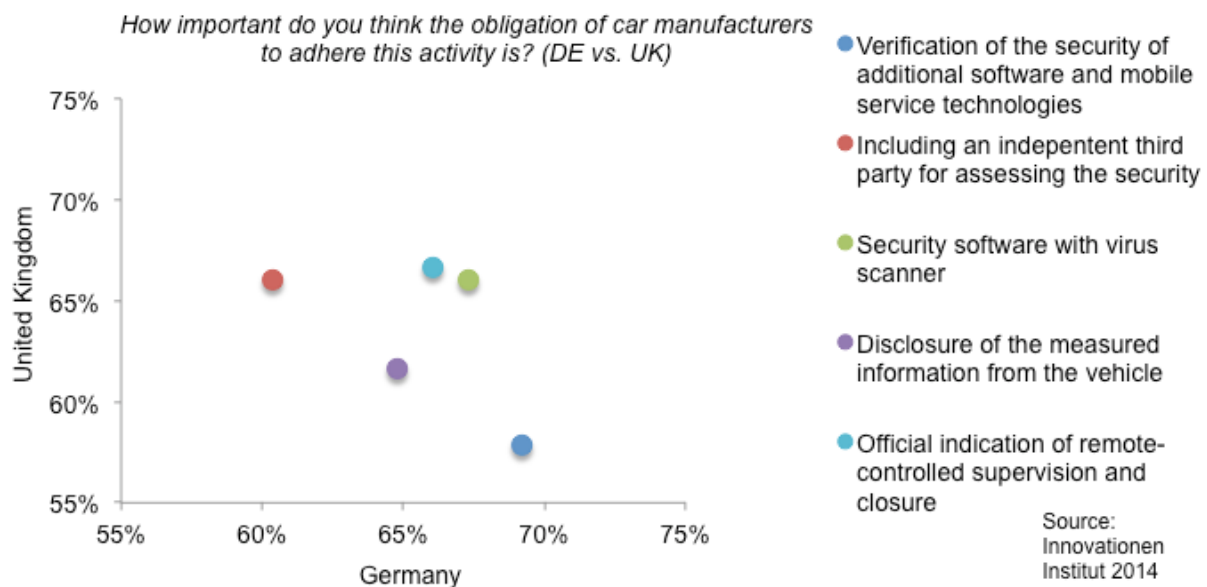


Exhibit 14

Legal framework and the need for clarification

Less than a third of the people are of the opinion that current laws adequately address the new privacy and security threats. The existing legal framework is not sufficient. Additionally, the international nature of communications technology requires a greater harmonization of legal frameworks globally.

Almost 6 of 10 participants think that connected cars will be purchased and maintained differently in the next 5 years. This implies a more flexible maintenance process that is based more on the actual technical situation of the car than on certain intervals after an approximated 30.000 miles or 3 years.

Nearly 60 percent of the executives wish for a legal framework for user's data, since the market does not regulate itself. Little more than a half of the participants voted that a mobile phone based eCall is sufficient in order to fulfill its purpose of quickly calling ambulance vehicles to decrease fatal casualties and injuries in accidents. The same amount of persons believe that the obligatory initiation of the so-called eCall (automatic distress call in case of an emergency) will accelerate the adoption and market penetration of connected cars in Europe.

Neutral authorities like VDA (Verband der Deutschen Automobilindustrie), in Germany or RAC (Royal Automobile Club) in the UK have to accelerate political activities to establish legal frameworks for connected cars.

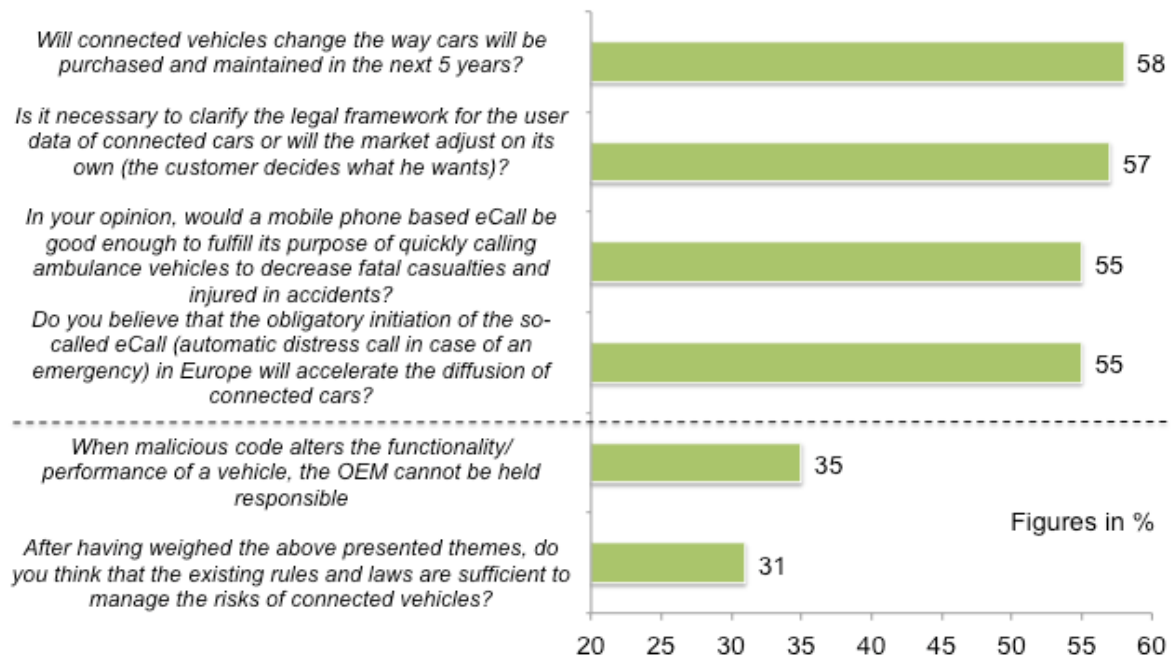


Exhibit 15



7. Perspectives and market opportunities 2020



Biggest obstacles

With the introduction of connected cars, some obstacles occur. Obviously, the largest one still seems to be the lack of competences of some car manufacturers.

The interviewees from information, communication, and telecommunication firms (76 percent) as well as car manufacturers (71 percent) rate it as most important.

Even interviewees in car retail, car maintenance and traffic, realize a lack of their competences (67 percent). Inadequate laws and interests of customers are rated equally, with individual differences.

Inadequate laws are the largest obstacles for IT/telecommunication firms with 71 percent.

It is interesting that information, communication and telecommunication firms rank missing business models highest at 67%.

On the contrary, Vodafone, for example, has announced an additional investment of 7 billion euro in its network infrastructure over and above its regular network investment. Included within this programme is an expansion of the M2M platform to provide enhanced service delivery capabilities across Europe.

Biggest hurdles for the development of telematics services in Europe

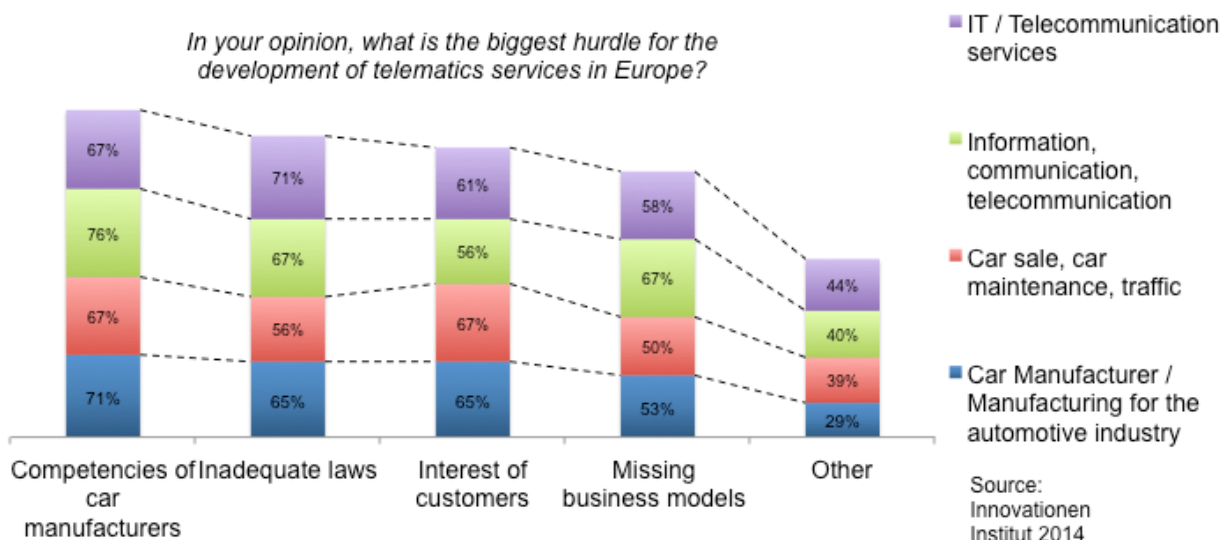


Exhibit 16


Revenue distribution software and hardware


The expected revenue distribution of in-car connectivity software and hardware leads to a surprising result:

The OEM's are anticipated to make the most profit by participants of "IT & Communication" with 33 percent (more than "IT & Communication" itself with 29%)

The opposite position from "Car Manufacturers" experts is that "IT & Telecommunication" will make the most profit in 2020 with 30 percent and only 26 percent for their own share.

However "Tier 1 suppliers" "Lifestyle business" and also "New suppliers" are estimated to make the most profit from nearly 20 percent of the attendees.

 IT & communication businesses and OEMs are expected to benefit most from connected cars.

 However, Tier 1, lifestyle business and new suppliers will play a significant role.

Expected revenue distribution of in-car connectivity software and hardware in 2020

How do you access the revenue distribution of In-Car Connectivity hardware and software in 2020?

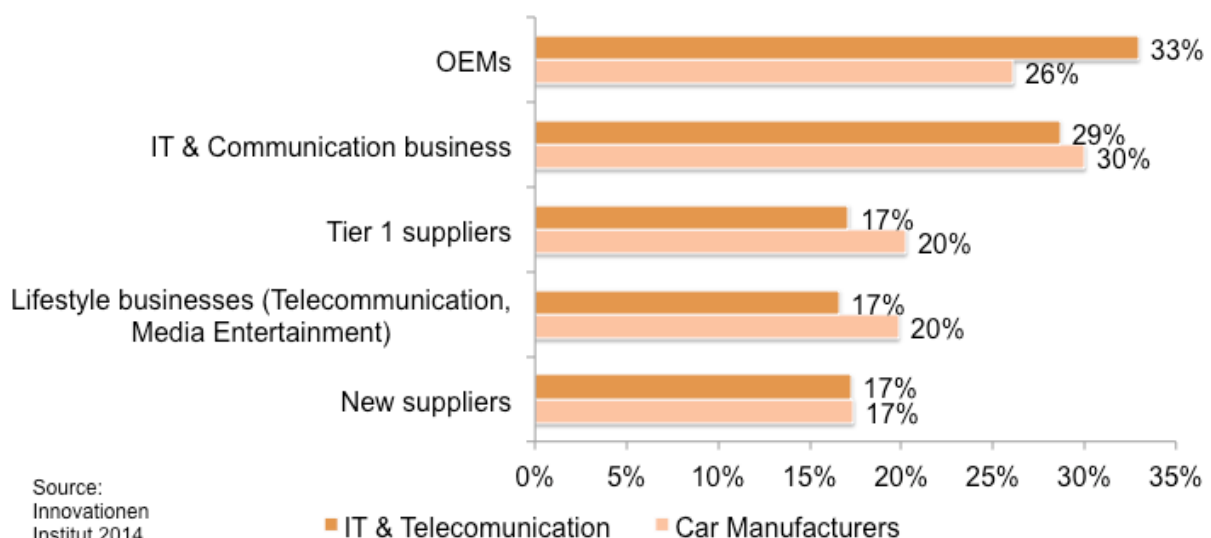


Exhibit 17

Software standards

The anticipated software standard for connected vehicles in 2020 will be Android, closely followed by iOS. Employees from the car industry are even more confident in Android's reign over the market.

This is a very important insight since Linux and the Genivi Alliance are supported by the automotive industry.

At the same time, new alliances from several OEM's are formed with Google, Apple and Microsoft. But with mounting network externalities from mobile phones, apps and connected vehicles with certain standards, the choice for OEM's for alternative systems will decrease.

In the economic theory, this phenomenon is well known as the "bandwagon effect". Once the "bandwagon" starts rolling, one can decide to jump on it or stay alone.

Desired and estimated location of the intelligence

The intelligence placement is of particular importance. The player, who provides the intelligence, will most likely hold a large share of benefits assuming that this requires the most powerful hard- and software.

The question of the desired intelligence has previously been mentioned in this Paper. Even more interesting are the findings in comparison to the estimated distribution in 2020.



Android is expected to be the market leader in the 2020 connected car sector, closely followed by iOS.

Expected software standards for connected vehicles in 2020

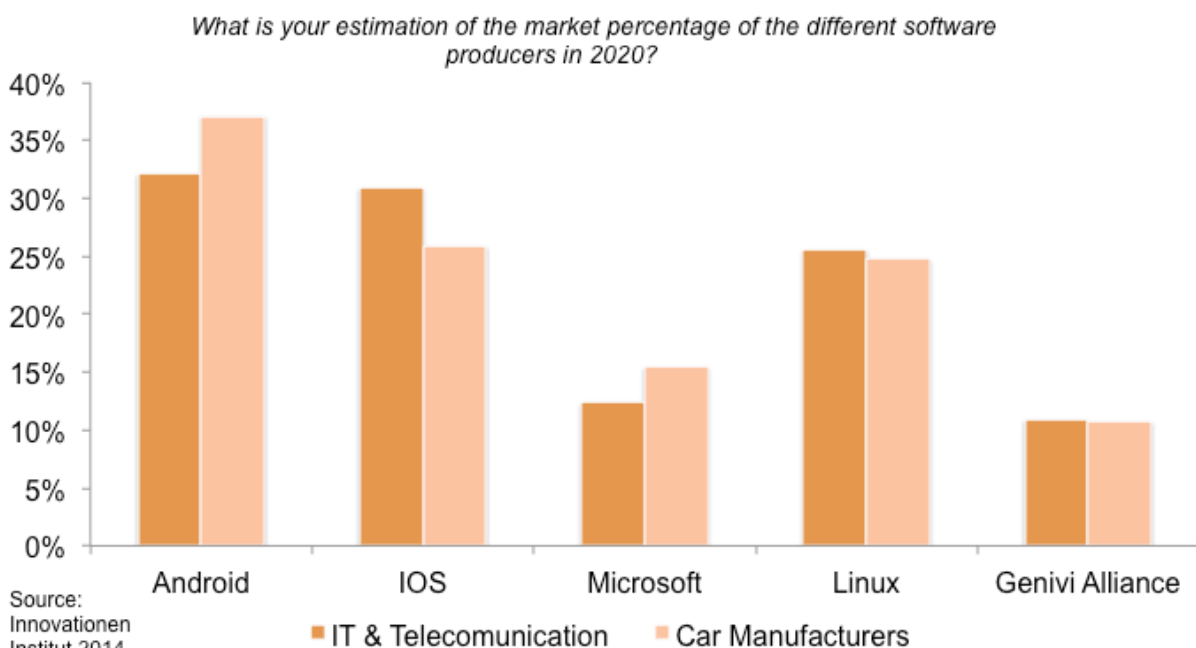


Exhibit 18

The large majority (62 percent) wishes to have the intelligence in the vehicle but only 42 percent expect it to be implemented in the near future.

Further results show that only 17 percent of the respondents want the intelligence to be located in the mobile device but 33 percent of them expect it to be the case in 2020.

This outcome is compatible with chapter 5 where 25 percent of the innovators preferred the mobile device for the location of intelligence and data processing.

The implication is that user habits and market power of the mobile device industry is high and may have a strong impact on the profit distribution in the connected car industry.



Only 17 percent of the experts want the intelligence to be located in the mobile device but 33 percent of them estimate that in 2020, the location of the intelligence will be the mobile device.

Intelligence distribution between connected cars, smartphones and backend's

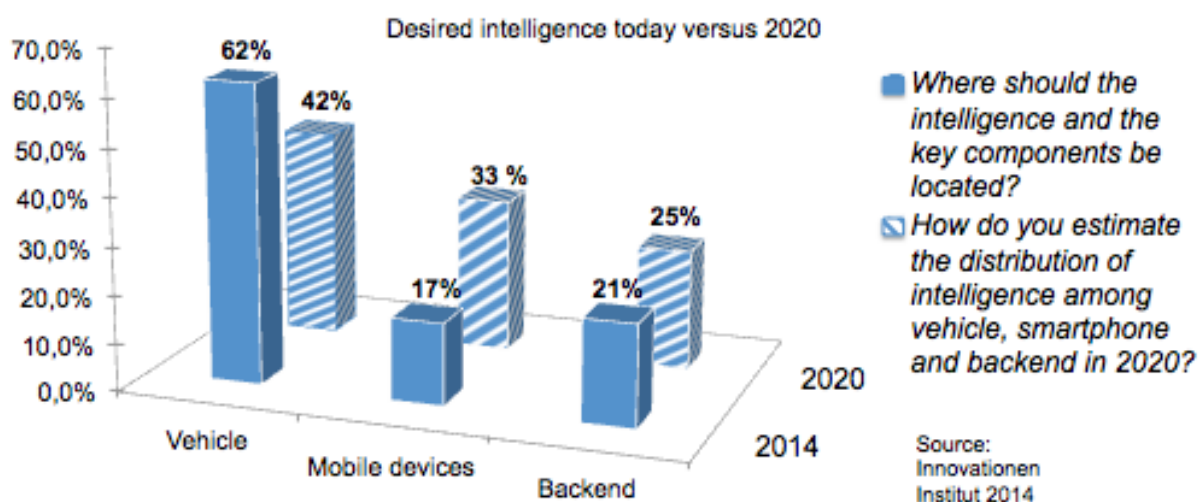


Exhibit 19



8. Conclusion

Annual data traffic volume per car in gigabyte

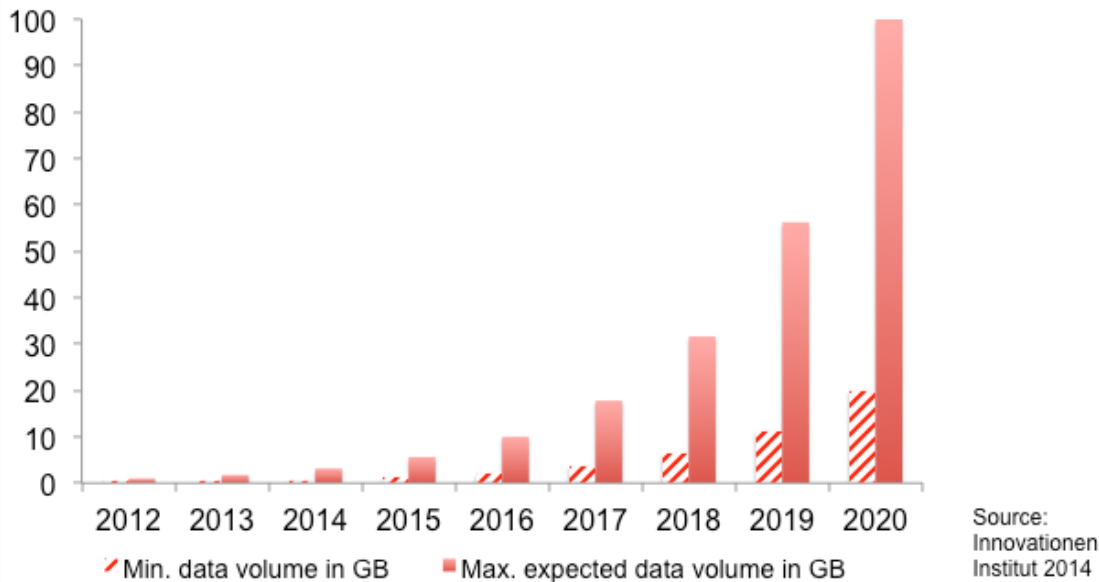


Exhibit 20

Growing supply and data volume

While the maximum data transfer volume per car in 2004 was a mere 10 MB, in 2020 the data transfer volume will exponentially climb to at least 20GB or even expand to 100GB per car. IHS automotive expects a volume of data of 11.1 petabytes of connected cars in 2020 (350 megabyte per second).

With a mounting data volume and much more functions and services, new applications and interaction with the core functions of cars become possible.

For instance, Google presented the Ion system in the Saab PhoeniX concept car in 2011. The system allowed the user to download a wide range of applications and online services from the Saab IQon store. Based on Google's Android operating system, apps can use over 500 sensors in the vehicle.

Now this technology belongs to the Chinese automotive companies that acquired Saab.

Therefore, this scenario might not be the end, but the beginning of a deep integrated Android operating system in connected cars.

Increasing demand for connected cars

The more customers get used to new driving support and comfort functions, the more demand will grow.

The prospering demand will be driven by "Care, "Comfort" and "Control" (3C).

Care: The drivers wish for reliable and secure connected systems that make desirable functions possible. Furthermore, to care about others supported by functions to avoid accidents.

Comfort: To use functions like "Traffic optimization", "Lane assist" or "Individualized car functions via smart phone" for more comfortable driving.

Control: To be informed about data collection, data ownership and usage and to have the possibility to explicitly agree to such functions, especially for the coming majority.

An aerial photograph of Frankfurt, Germany, showing a dense urban landscape. Two prominent skyscrapers, the Commerzbank Tower and the Main Tower, stand out against the city skyline. The Commerzbank Tower is on the left, and the Main Tower is on the right. Both buildings have dark, reflective glass facades. The surrounding city is filled with various residential and commercial buildings, with a mix of architectural styles. The sky is clear, and the overall scene is captured from a high vantage point, looking down on the city.

**Innovation Institut
Schillerstraße 14
60313 Frankfurt
Germany**

**Paris
Maastricht
Miami**

**Tel.: +49 (0) 69-5555 00
Web: Innovationeninstitut.com**