Issue 3 | 2019

EDPS

TechDispatch

# Connected Cars

The modern car is a computer on four wheels. Today's cars are constantly processing and transmitting data about themselves, their surroundings and the people in it – in most of the cases even without the knowledge of the driver.

This data is used in navigation, to manage car systems like the engine or to deliver communication and infotainment services to passengers. Figure 1 gives an overview.

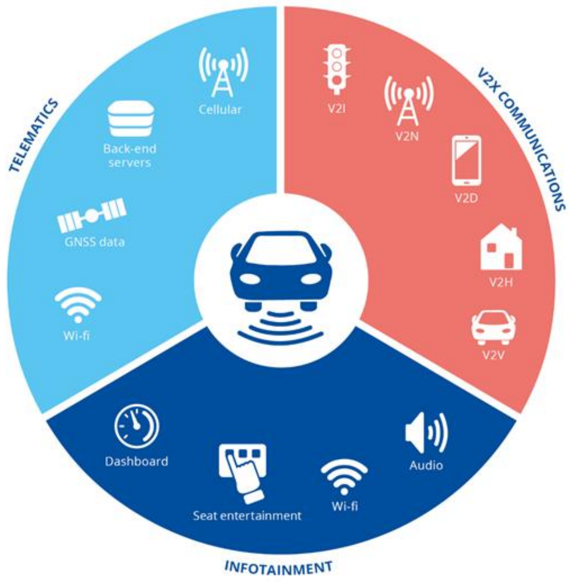

Figure 1: Information Systems in a Connected Car. Source: ENISA (2019)

Increasingly today, the data generated by the car is shared over the internet with other vehicles, traffic infrastructure and private and public entities. These so-called *connected cars* belong to the evolving *Internet of Things* (IoT) - with manifold related risks attached (see TechDispatch #2: Smart Meters in Smart Homes). The growing amount of personal data generated by *connected cars* raises the interest of insurers, automakers, law enforcement authorities and other third parties.

## I. What are connected cars?

A variety of technologies fall under the term *connected cars*. Nowadays, many cars use sensors to measure data concerning driving behaviour (e.g. accelerometer, Global Navigation Satellite System or cameras) and the functioning of its systems, such as engine, air conditioning or air bags. The sensors can be built-in (i.e. offered by the connected car internal system) or brought-in (i.e. connected through an external device, such as a smartphone).

Furthermore, cars are increasingly equipped with functions providing information and entertainment (so-called *infotainment systems*) to the driver and passengers, such as hands free phone calls, WLAN hot spots, music, video, social media, mobile office or *smart home* services.

This data used to be processed and stored locally in the car. The growth of vehicle networking capabilities now allow cars to interact between themselves as well as with any other entity (V2X), such as traffic infrastructure (e.g. traffic lights), the vehicle manufacturer, other third-party service providers and other devices (e.g. smartphones), hence the name *connected cars*. Some examples of connected car applications allow for remote control and diagnostics, mandatory notification of emergency services in case of an accident or assistance in finding available parking spaces.

In the near future, European *connected cars* could become a part of the Cooperative Intelligent Transport Systems (C-ITS), which will allow road users and traffic managers to share information and coordinate their actions.

Although co-related, *connected cars* should not be confused with *autonomous vehicles*. Autonomous vehicles are those in which at least some aspects of safety-critical control functions occur *without direct driver input*. While some systems can provide both functionalities, they can also exist separately.

These technologies can increase road safety, provide a more convenient journey and in some eyes are essential for other emerging technologies such as autonomous vehicles. However, they are also gathering large amounts of personal data about drivers, passengers and other road users. Hence, a broad range of privacy and data protection questions arise.

## II. What are the data protection issues?

According to some estimates, *connected cars* produce up to 25 gigabytes of data every hour, most of which is data about individuals, such as the driver of the vehicle or its passengers. Not only do they gather information on car systems and driving behaviour, but may also process biometric, health, location and communication (metadata and content) data as well infotainment systems data.

Many of these data are linked either directly or indirectly to an individual and are thus personal data in accordance with European Union data protection legislation. This includes any vehicle data as long as it can be associated with a natural person, notably via the car serial number or the licence plate number. This means several data protection challenges for the use of *connected cars*. Depending on the specific personal data processing operations, data controllers likely have to conduct a Data Protection Impact Assessment (DPIA) as shown in (Article 29 Working Party 2017) and (EDPS 2019).

### II.1. Lack of Transparency

Connected cars allow complex personal data processing with different purposes, possibly involving automakers, insurers, law enforcement authorities and other third parties. Informing car users in *a concise, transparent, intelligible and easily accessible form* of which personal data is processed by who, for how long, and for which purposes can prove to be challenging for data controllers. Therefore, it is important to accurately identify data controllers, data processors and recipients for each relevant processing operation.

The necessary information also needs to be presented in a concise, transparent, intelligible and easily accessible form. One car maker now shows a 15 pages long privacy policy on a 20 cm/ 8′ screen. As a consequence, user interface design as well as privacy policy formatting will be especially important if information regarding personal data processing is provided to car users using the (still reduced sized) screens available in a connected car.

Transparency to the data subjects is a data protection requirement on its own, but it is also a prerequisite for obtaining a valid consent from users. Without transparent information, consent is not deemed to be valid.

### II.2. Excessive data collection

The increasing amount of sensors used in *connected cars* raises the risk of excessive data collection beyond the needs for the provided services. For example, a car insurer offering a *pay by miles* product that collects a broad range of behaviour data for a vast number of secondary purposes.

Excessive data collection is particularly common in applications powered by machine learning, which use large datasets, often collected over a long period of time, to build their predictive models. Thus, companies might be inclined to collect more data than necessary for the services. This issue emphasises the importance of adopting practices such as *data protection by design* and *by default*, to enforce the data minimisation principle as required by the General Data Protection Regulation (GDPR).

### II.3. Data Retention

Data generated by connected cars and exchanged with other vehicles or IT systems (e.g. traffic infrastructure) could be retained by any of them. Personal data should not be stored for longer than necessary for their declared purposes. However, in a complex personal data processing scenario such as connected cars, the risk of an excessive storage of personal data is high. *Connected cars* have triggered incidents related to the exchange of drivers. Users of car-sharing and can rental services have been able to track and exert some control over these vehicles, even after the service termination. Also, previous car owners were still able to access the car system through their phones, and in some cases even control car functions remotely.

The lack of a data retention policy or its implementation could result in an indefinite storage of personal data, which is not in line with the storage limitation principle. Furthermore, the longer data is retained, the more it is prone to unauthorised disclosure or reuse.

### II.4. Lack of control

*Connected cars* may lack sufficient functionalities or options for individuals to exercise control over their personal data. Communications in the vehicle can be triggered automatically as well as by default without the individual being aware of it, and the countless data flows can make it extremely difficult for data subjects to control their personal data. To avoid this, *connected cars* should offer both drivers and passengers controls enabling the update and deletion of the data collected about them.

Furthermore, when the personal data processing is based on consent, users should have means to withdraw it. When consent is the legal basis, the principle of data protection by default dictates that services processing personal data should be originally inactive, giving data subjects the autonomy to turn them on.

### II.5. Lack of purpose limitation

The privacy policies governing personal data processing on *connected car* related services sometimes bundle loosely defined and/or non-compatible purposes (e.g. providing requested services, credit and behaviour scoring and operating and expanding business activities).

For example, data originally collected for maintenance purposes could be used by insurance companies to enrich driver profiles, custom pricing, and offer driving behaviour-based insurance policies or investigate liability in car accidents. Road safety authorities could use such data to enforce traffic regulations, such as monitoring speed limits.

### II.6. Collection or inference of sensitive information

Each piece of data about a person's car use, like driving routes and travel destinations, in-car communications or infotainment services, can reveal sensitive information on a person's life. People's driving routine and places of interest may permit not only their identification, but also conclusions on sensitive information, such as religious and political associations, sexual orientation, and relationships. Therefore, the collected data is useful for profiling and monitoring of individuals, especially when associated with existing databases of personal data (private or governmental).

Data controllers must pay especial attention to the requirements imposed by the GDPR to the processing of the special categories of data, such as the limited available legal grounds. Data controllers need to inform connected car users clearly about the purpose of the processing of location data. Due to the sensitive nature of location data, a thorough application of data protection principles to location data, particularly purpose limitation, data minimization and data storage is necessary.

### II.7. Security and access control

As part of the IoT environment, *connected cars* are equally vulnerable to security risks, such as cyberattacks from non-authorised third parties and data breaches from authorised third parties. A global report has revealed that in 2019 more than 80 cyber-attacks on the smart mobility ecosystem, many of those related with connected cars. An ill-intentioned attacker might not only steal data, but also disable its security features, or even gain control over a car, as shown in the Jeep Cherokee hijack case in 2014 and 2016.

In consequence, negligence in IT security leads directly to risks endangering road safety for drivers, passengers, and pedestrians.

Furthermore, unauthorised access, loss, misuse, modification and disclosure of personal data may happen in many circumstances, especially when the car is part of a car-sharing scheme (such as rental cars and some taxi services), where many different drivers and passengers may have their data collected. If appropriate security measures are not in place, these users may improperly access the personal data of others. Thus, there is a need for coherent guidelines and easy-to-use tools for users of *connected cars* to control personal data.

According to a 2017 report on Access to In-vehicle Data and Resources, there are three technical approaches to access in-vehicle data: (i) on-board application platform; (ii) in-vehicle interface; and (iii) data server platform.

From these, only the first approach avoids data transfers to external servers. Even so, updating and patching the software is fundamental to keep the system secure against known and newly found vulnerabilities, since third parties may still be able to access data through the on-board platform.

## Recommended Reading

39th Intl. Conf. of Data Protection and Privacy Commissioners (2017). *Resolution on Data Protection in Automated and Connected Vehicles*.

Allot (2018). *Connected Cars Attack Vulnerabilities*. Threat Bulletin.

Article 29 Working Party (2017). *Guidelines on Data Protection Impact Assessment (DPIA)*.

*Automation - From Driver Assistance Systems to Automated Driving* (2015). Verband der Automobilindustrie.

Commission Nationale Informatique et Libertés (2017). *Compliance Package - Connected Vehicles and Personal Data*.

*Datenschutzrechtliche Empfehlungen der BfDI zum automatisierten und vernetzten Fahren* (2017).

EDPS (2019). *Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies*.

ENISA (2019). *Good practices for security of Smart Cars*.

European Commission (2016). *A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility*.

Federation Internationale de l'Automobile (2016). *What Europeans Think About Connected Cars*.

FIPA (2015). *The Connected Car: Who is in the Driver's Seat?* Office of the Privacy Commissioner of Canada.

International Working Group on Data Protection in Telecommunications (2018). *Working Paper on Connected Vehicles*.

Privacy International (2017). *Connected Cars: What Happens To Our Data On Rental Cars?*

Terris GPS (n.d.). *GNSS / GPS Differences Explained*.

This publication is a brief report produced by the Information Technology Policy Unit of the European Data Protection Supervisor (EDPS). It aims to provide a factual description of an emerging technology and discuss its possible impacts on privacy and the protection of personal data. The contents of this publication do not imply a policy position of the EDPS.

Issue Author: Simon REBIGER,
Thiago MORAES,
Xabier LAREO LÓPEZ DE VERGARA
Editor: Thomas ZERDICK
Contact: techdispatch@edps.europa.eu

To subscribe or unsubscribe to TechDispatch publications, please send a mail to techdispatch@edps.europa.eu. The data protection notice is online on the EDPS website.

HTML: ISSN 2599-932X
ISBN 978-92-9242-427-5
QT-AD-19-003-EN-Q
data.europa.eu/doi/10.2804/35031
PDF: ISBN 978-92-9242-428-2
QT-AD-19-003-EN-N
data.europa.eu/doi/10.2804/70098