



The modern car as a possible spy

Digital threats in smart vehicles

Modern vehicles are getting smarter and smarter. More digital systems which collect data and connect to the internet are introduced into vehicles. While this does have practical advantages, these systems collect a lot of information on the passengers, the vehicle itself, and objects and persons in the immediate surroundings. Different parties, including state actors, could gain access to this data. In this publication the AIVD calls for awareness of the risks of espionage posed by modern vehicles. The AIVD also indicates via which systems these risks can manifest and how you can mitigate these.

Who can benefit from this advice?

Each passenger of a modern vehicle may be subject to information gathering through various systems, but there are persons whose conversations, activities, or travel movements could be monitored with special interest. Think, for example, of dignitaries, key figures in the corporate world or the government, and other persons who have access to sensitive information. The advice below is aimed at this group, with the purpose of helping them deal with the posed risks of espionage. The advice also provides instruments to people outside this group on how to deal with broad data collection by modern vehicles and how they can turn off their 'autopilot'. Not every element of the advice will apply to each situation, so it is important to assess the risks in each situation and take appropriate measures.

Espionage risks in and via the vehicle

Modern vehicles collect many different types of information. The user of a vehicle often has no control over which data is saved or communicated by the vehicle, because this happens automatically and without being noticed. This is the case for both internal systems and external (camera) systems. The manufacturers of these vehicles often have access to this data. In addition, car dealers, leasing and maintenance companies, app developers, manufacturers of car parts, and cloud services could also obtain access to (some of) this data. This may entail risks.

In addition to these companies, malicious parties are interested in and can highly likely also gain access to this data. This data flow is an interesting source of information for state actors. Some state actors can request this data from companies or carry out hacking operations themselves to access the data or the relevant systems. For 'normal' cybercriminals and hackers this data can also be interesting to obtain, for example to hold the data hostage or sell it.

**"Be conscious of the espionage risks
posed by modern vehicles"**

Systems which pose a risk



Microphones

Many vehicles are equipped with multiple microphones. It is possible through technical means to remotely enable microphones, which allows malicious actors to listen to conversations held in vehicles.

Advice: Do not have confidential conversations inside or close to the vehicle.



Cameras

Modern vehicles are often equipped with internal and external cameras. It is technically possible to remotely enable these cameras. Malicious actors can use these to make recordings inside and around the vehicle.

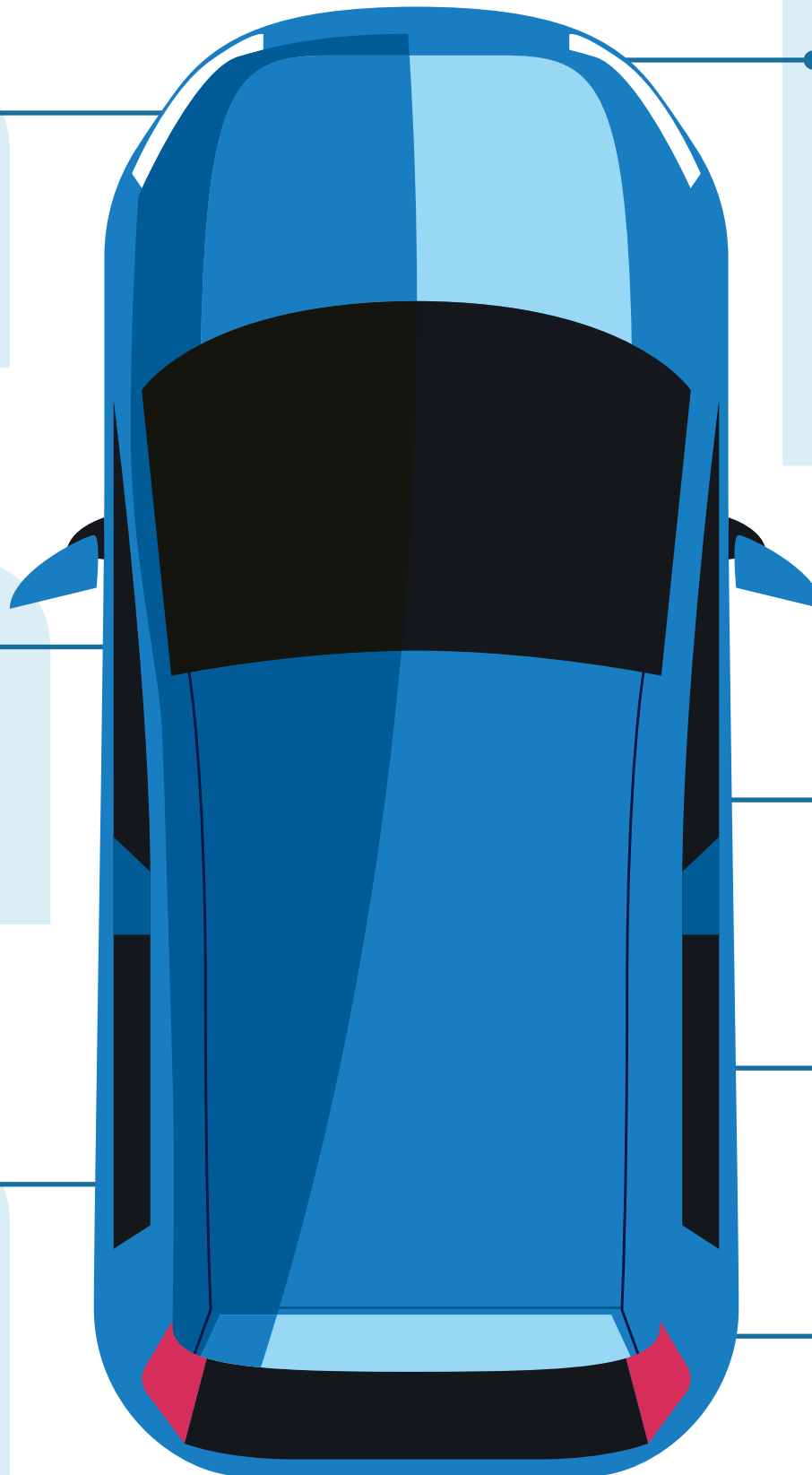
Advice: Be aware of what the camera may be able to record in the vehicle. Do not use a vehicle with an external camera to travel to a sensitive location.



Connection phone and other devices

There are different methods to link a phone or another device with the vehicle, such as Bluetooth, Wi-Fi, a physical USB connection, or a wireless charging station. It is possible through technical means for malicious actors to gain access to internal systems of the vehicle through these connections and to obtain data from the linked devices through the vehicle.

Advice: Avoid (automatically) connecting with Bluetooth or Wi-Fi. Do not use wireless charging. Do not use connect a mobile phone through USB without using a data blocker.



Infotainment systems

The built-in infotainment system is the central point for data gathering and storage in the vehicle. From the infotainment system (some of) the gathered data is made available to the vehicle supplier and other parties. This data gathering is far-reaching. Think, for example, of unique identification numbers of the linked devices, contact details, internet traffic, sent messages, or navigation data. It is possible through technical means to obtain data which is stored in the infotainment system.

Advice: Be careful when entering specific name and address details into the navigation system, such as your home address or the address of a sensitive location. Consider the use of built-in navigation systems in relation to the destination and purpose of the trip.



GPS & Track and trace

Vehicle manufacturers use these systems to follow a vehicle in real time and register travel movements. It is possible through technical means for malicious actors to track the live locations of vehicles.



Telematics module

Modern vehicles use a telematics module. This module has access to the internet to get information on traffic jams, location data, or updates from the manufacturer. This module also shares vehicle data with the manufacturer.



Charging stations

Charging stations for electric vehicles are used to forward data on the connected vehicles



Advice for the above: Risks from these systems cannot be prevented with technology or through behaviour. Consider the risks of using the vehicle in relation to the destination and purpose of the trip.

General Intelligence and Security Service
P.O. Box 20010 | 2500 EA The Hague

Visit our website at:
<https://english.aivd.nl>

September 2026