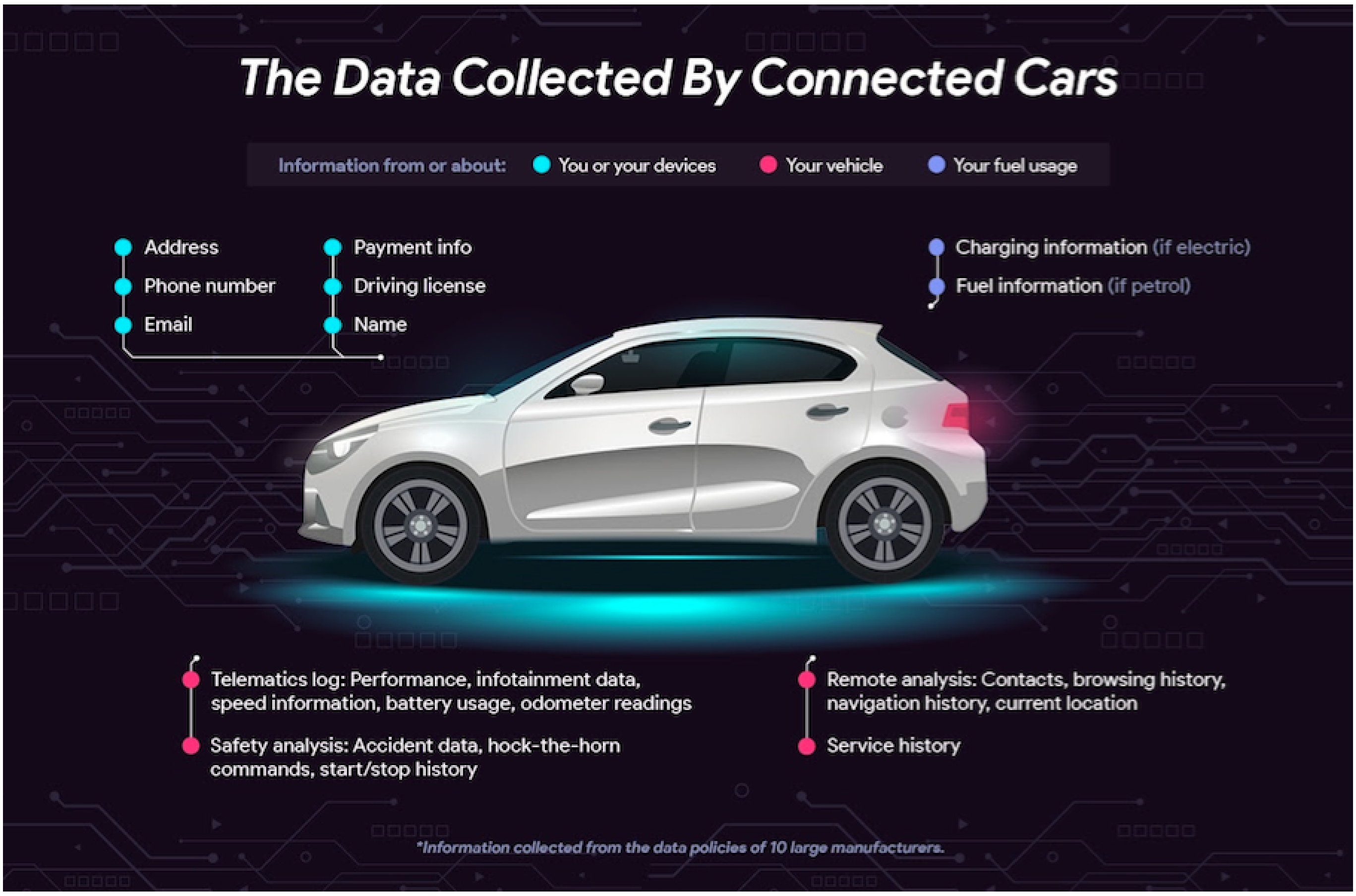
WHEELS-ALIVE! www.wheels-alive.co.uk

Caution – Your 'Connected' car may be giving away private information about you!

Published: September 7, 2021

Author:

Online version: https://www.wheels-alive.co.uk/caution-your-connected-car-may-be-giving-away-private-information-about-you/


The Data Collected By Connected Cars
Information from or about:
● You or your devices
● Your vehicle
● Your fuel usage
Address
Phone number
Email
Payment info
Driving license
Name
Charging information (if electric)
Fuel information (if petrol)
Telematics log: Performance, infotainment data, speed information, battery usage, odometer readings
Safety analysis: Accident data, hock-the-horn commands, start/stop history
Remote analysis: Contacts, browsing history, navigation history, current location
Service history
*Information collected from the data policies of 10 large manufacturers.

Many people do not realise how much information their 'connected' car can give away to others; Vanarama has carried out a study into this and how to protect yourself…

Vanarama has conducted a study into the important question of privacy and data safety within connected cars, comparing the information that is collected from 10 of the biggest car companies, and who can gain access to it.

Cars today are closer to smartphones than ever before, for example with the new Tesla chip able to perform 72 trillion operations per second. Like smartphones, will cars start to gain a bad reputation for sharing user's data without their knowledge or have poor security mechanisms?

Full details of the Vanarama study are included here: What your car knows…

Aspects to consider include:

What Information is Collected?

Information collected about you from your car or synced mobile devices includes:

Name, Address, Phone Number, Email, Payment Information, Driving Licence

Vanarama also tells us:

If your connected car comes complete with its own application, then any information that you submit will be automatically connected to your car and will help to build a profile of you, especially when this is matched with data from the infotainment system within the car.

Personal information such as your name and address (findable from your saved location on your sat nav) will all be accessible, around with your phone number and email. Your payment information will also be stored with the car manufacturer you pay for any additional content like apps on your phone or infotainment unit.

Who Can Access The Data?

There are four parties that are able to access your data, both legally and illegally including:

Car Manufacturers: The most obvious party that can access your data is the manufacturer of your car. Due to the data being hosted on their servers, they have direct access.

Third Parties: There are two types of third parties that car companies will share your information with. Firstly, third parties that you decide to authorise, whether it be on a mobile application or on the car's infotainment unit. Make sure to check the permissions before accepting them all! Also, car manufacturers are required to share your information with third parties by law, such as the police if you are involved in an accident.

Hackers: If you have a connected car, your data may be stored in the cloud. Although it's extremely unlikely, hackers may have the ability to access your information remotely.

Next Owner: If your information is stored locally on the internal computer of the car and you forget to erase it before handing it back to the leasing company or selling it, the new owner or driver of the car my gain access to your private information.

How Can I Protect My Data in a Connected Car?

Like all connected devices, modern cars store lots of personal information that you might prefer not to share, or if you're happy to share – it's always best to keep it as secure as possible.

Lauren Smith, a Senior Policy Counsel at the Future of Privacy Forum (FPF) and a leader FPF Connected Cars Working Group said on data privacy within cars:

"It's time for people to treat their cars like a computer or a smartphone. They do not specify data sharing and use practices, and they offer limited individualized controls to consumers. In the end, consumers had trouble understanding how they can limit the data that is being shared."

To make sure you get the most out of your car's systems but are still on the safe side when it comes to data security, here are Vanarama's tips for keeping your personal information safe:

1. When selling or returning your car, make sure you've removed your personal data: When it's time to part ways with your car, ensure that your entire address or phone book is erased from the internal computer, along with any accounts that may be logged in. This will make sure that no one ends up having access to your private numbers or passwords.

2. Disconnect from the cloud: Disconnecting from the cloud will ensure that all your information is at least stored locally – all in one place on a physical device. This won't be possible for services that require location connection e.g. safety features, but you should thoroughly check to see what you do and don't need to be always connected.

3. Update your software regularly: It's important that you update the car's software regularly to give you the best protection and to make sure you have access to the latest features and functionality.

4. Read the small print: If your car comes complete with its own mobile application, make sure to read and understand the permissions to see what's essential and what isn't before you decide to click 'accept all'. This is also good practice with your car's infotainment system.

5. Perform a factory reset: If you want to be sure that there is no personal data left on your car's internal computer, the best way to do this is to perform a factory reset. However, with this option there is no going back. Once the reset is complete you won't be able to recover any data you may have lost.

Read more about this topic on Vanarama's blog post here: What your car knows…