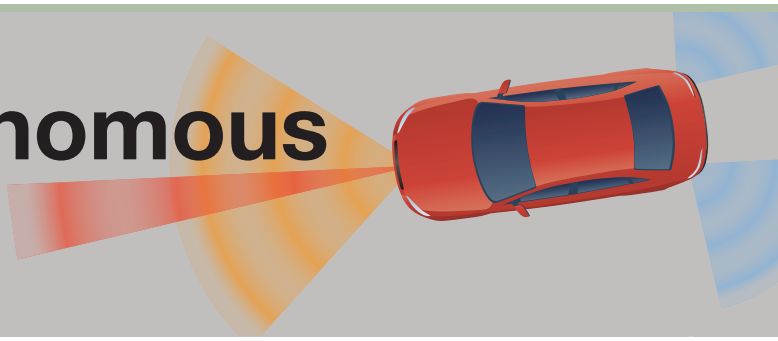
The road to autonomous



Christoph Moeller explores the data issues surrounding future mobility

Automobiles of the future are even more connected and feature a higher degree of automation than today's vehicles. Artificial intelligence (AI) is also finding its way into on-board systems to an ever-increasing extent. These two aspects, especially, create problems that may not be quite apparent at first. The greater use of connectivity and autonomy increases the demand for sensors and software, thus generating more data – which will be at the heart of these reshaped mobility ecosystems.

In this context, and especially bearing in mind that the average connected car will produce an estimated four terabytes of data a day. The issues surrounding data ownership are complex.

Who holds the wheel?

Connected and autonomous vehicles are also changing the way customers interact with the original equipment manufacturers (OEMs). In the past, these manufacturers only had occasional direct contact with their customers, mainly through dealers. In the advent of autonomous or even just connected services, a more direct contractual relationship starts to appear.

Historically, the situation was much easier for OEMs wanting to collect data from connected vehicles. When purchasing a vehicle and signing the contract, in the general terms and conditions the authorisation to collect and "appropriately" use obtained data was included. There was no way to object to the collection and transmission of data, short of not buying the vehicle. Once given, the OEM could either refuse to acknowledge the withdrawal or discontinue a certain service.

The changed dramatically in 2018 with the General Data Protection Regulation (EU) 2016/679. When the GDPR became into force on 25 May 2018 it significantly strengthened the rights on data protections and privacy for all individuals in the EU and EEA, specifically addressing issues surrounding their respective personal data (or personally identifiable information), which enjoy special protection.

The European Union Agency for Network and Information Security (ENISA) in its study *Cyber Security and Resilience of smart cars* made it clear that protecting user data, which is all data relating to an identified or identifiable person, is of particular relevance and should thus be protected accordingly. It was further said that in the case of connected cars, such data may especially include all location-based data.

In 2016, the European Commission in its publication on *EU Strategy on Cooperative Intelligent Transport Systems* pointed out that "the protection of personal data and privacy is a determining factor for the successful deployment of cooperative, connected and automated vehicles. Users must have the assurance that personal data are not a commodity and know they can effectively control how and for what purposes their data are being used." The EC continues that essentially it can be assumed that all data generated by and originating from a vehicle is personal data or personally identifiable information. This statement clearly had the GDPR in mind, and was once again emphasised by the European Commission's communication (2018) 283 on the *EU strategy for mobility of the future*. It was said that while "there is no sector specific approach on the protection of the vehicle against cyberattacks, for data protection on the other hand, the EU rules on the protection of personal data apply to any processing of personal data, including those collected from vehicles".

The protection of individual's data has thus been established as the ultimate goal, clarifying that data ownership effectively lies with the driver and no one else. Contrary to before, a service provider cannot refuse to provide a service anymore simply because the user has not given consent to a particular data use, or has withdrawn it. In a case where consent to a certain data use is demanded, but that specific data use is unrelated to the actual service provided, this is a violation of the GDPR. As a consequence, an OEM or another service provider cannot refuse or stop providing that service, without violating the GDPR as well.

Another step along the road will be the new ePrivacy Regulation (ePR), to replace the ePrivacy Directive of 2002. While the ePR is still in draft, its aim is to consolidate the implementation by member states, and is intended to complement the GDPR. While the ePrivacy Regulation is mainly directed towards electronic communications service providers, the regulation still impacts how data obtained from vehicles is shared with third parties. In case the intended data sharing standards of the European Commission are not met, an OEM may well be prohibited from selling such connected cars to its customers, and as with GDPR, significant penalties could be imposed.

One important area of future connected and autonomous cars is vehicle-to-vehicle (V2V) communication. The aim of V2V communication is to avoid accidents by enabling nearby vehicles to exchange position and speed data while driving. Depending on the implementation, the driver of a vehicle may receive a warning if there is a risk of an accident, or the vehicle itself can take preventive measures such as braking or evading the other vehicle.

This falls under the ePrivacy Regulation definition of 'interpersonal communications services', which enable interpersonal and interactive exchange of information between a limited number of individuals, designated by the sender of the communication. Interactive communication means that the service enables the recipient of the information to respond. Whether this meets the requirements of exemption to the ePrivacy Regulation, such as the exchange of information between machines, is something that needs to be resolved. This can only come after the ePR comes into force.

OEMs and other players must make privacy a key part of their firm's culture and approach this field with a holistic view on data privacy. After all, it is the journey that is the product, not the transported.

Author

Christoph Moeller is a partner at Mewburn Ellis.