Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Autonomous Vehicles And European Data Protection: Part 1

By **Oliver Yaros and Ryota Nishikawa**

Oliver Yaros

Ryota Nishikawa

Law360, New York (July 21, 2017, 12:19 PM EDT) -- The emergence of connected and autonomous vehicles (CAVs) will lead to numerous industry participants collecting, analyzing and exploiting immense amounts of data from those vehicles for many different purposes.

Original equipment manufacturers (OEMs) may use data transmitted by CAVs, such as vehicle speed, battery life, engine injection behavior and fuel pump performance, to develop more efficient, safer and more advanced vehicles. Insurers could capitalize on car data by offering usage-based insurance contracts based on the analysis of data indicative of driving behavior.

Roadside assistance providers could collect and process distress calls in real time from vehicle sensors and automated alerts, optimize the dispatch of rescue vehicles and analyze accident and breakdown data to provide valuable information to car OEMs and road infrastructure operators. Retailers and service centers could use car data analytics and in-vehicle technology for in-car monetization opportunities, such as advertising shops and restaurants that may be of interest en route.

CAVs will also be able to communicate with other CAVs and on-road infrastructure to make lane changing and junction crossing easier and safer. But before industry participants can truly benefit from the wealth of business opportunities that CAV-generated data presents, key legal issues will have to be addressed. In Europe, there are several challenges, which are discussed here.

Ownership of the Data

Given the many possible opportunities that arise from CAVs, a key question is which individual or industry participant owns the data that is being recorded and transmitted by different systems within the vehicle. Naturally, manufacturers and OEMs will be keen to assert that they are the rightful owners of the data because of the role that their IT infrastructure (whether it forms part of equipment installed onto the CAV or otherwise) plays in the collection and transmission of the data and, as a result, that they have the right to restrict how others can use the data.

In Europe, the European Automobile Manufacturers Association (ACEA) recently published a position paper that discusses a desire to charge for access to the data generated by vehicles.[1] However, the answer to who owns the data is not clear-cut. To explore this point, an analogy can be drawn between event data recorders (EDR) and telematics data transmitted from CAVs.

EDRs are akin to the "black boxes" found on airplanes and record information about vehicle functions around the time of a crash. In Europe, a report for the European Commission in 2014 concluded that the most likely owner of the data is the vehicle owner.[2]

CAVs record similar types of data as EDRs, such as speed, acceleration and braking, but CAVs record a greater number of categories of data than EDRs. Furthermore, the EDR data is relooped so that only the minutes just before an incident are retained, as opposed to CAV data, which is continuously recorded and stored.

CAVs will likely store data for a much longer time period than EDRs. Given that the type, quantity and retention period of the data may differ significantly with EDRs, ambiguities remain over who owns the data.

In some jurisdictions, it may be the car owner; in others, it may be the car manufacturer. In addition, it is likely that OEMs of different devices in a vehicle will lay claim to the data emanating from their particular devices. These different stakeholders in the vehicle will need to come to an agreement to establish who exactly owns the data, to whom it should be licensed and how that data can be used by successive vehicle owners, their passengers and third parties that they interact with (such as insurance companies, car dealerships etc.).

In fact, it has been reported in the Financial Times that a consortium consisting of insurers, technology companies and others in the transport industry have, in a recent report, asked the U.K. government to clarify who has ownership of and access to this data.[3]

Dealing with Personal Data

Regardless of who owns the data, to the extent it consists of personal data, manufacturers must notify and obtain the consent of the owner and other drivers of a vehicle — or rely on a statutory justification — before sharing "personal data" with third parties (such as insurance companies) to use that data in compliance with EU data protection laws. The European Data Protection Directive 95/46/EC defines "personal data" as any information relating to an identified or identifiable natural person ("data subject").[4]

The General Data Protection Regulation 2016/679 (GDPR), which will replace Directive 95/46/EC in May 2018, has a very similar definition of "personal data." Personal details such as a driver's name, address and contact details (whether those have been directly inputted into a digital interface or infotainment system by the user or collected or inferred by the car manufacturer or systems provider) will be personal data, and European data privacy laws will apply to the use of that data.

In the European Union, location data collected by smartphones is generally considered to be personal data because individuals can be directly or indirectly identified through their patterns of movement,[5] and so geolocation data collected by CAVs is likely to be considered personal data where this data alone or in conjunction with other information identifies an individual driver, passenger or user of a CAV through their patterns of movement.

The GDPR has confirmed this position by expressly stating that an individual can be identified directly or indirectly by reference to "location data."[6] Even technical telematics data produced by sensors in the vehicle, such as about speed, acceleration and use of brakes, could constitute personal data.

The unique identification number given to vehicles can be linked with the individuals who have registered as owners of those vehicles. The technical data generated by vehicles and associated with the unique vehicle identifier could, therefore, be linked to individual drivers and relay information about their driving habits, for example.

In Germany, the data protection authorities and the German Association of the Automotive Industry have already stated this to be the case.[7] As a result, connected car data will in most cases be deemed personal data, unless data processing has been designed to avoid data becoming personally identifiable (e.g., where sensors and other data-generating items have been designed to only generate anonymous data and aggregate it when recorded on an industry participant's system).

In the second part of this article, we will consider the three legal bases for the use of such personal data under European data protection law, as well as other data protection requirements, and the best approach to addressing these challenges.

Oliver Yaros is a partner in the intellectual property and IT group of the London office of Mayer Brown LLP.

[1] https://www.acea.be/uploads/publications/ACEA_Strategy_Paper_on_Connectivity.pdf.

[2] https://ec.europa.eu/transport/sites/transport/files/docs/study_edr_2014.pdf.

[3] https://www.ft.com/content/0ebdd2aa-5dc5-11e7-9bc8-8055f264aa8b.

[4] Article 2(a) of Directive 95/46/EC.

[5] Article 29 Data Protection Working Party — Opinion 13/2011 on Geolocation services on smart mobile devices.

[6] Article 4(1) GDPR.

[7] http://germanitlaw.com/smart-cars-industry-and-germanauthorities-agree-on-certain-aspects-of-data-protection/.
