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 2

By **Oliver Yaros and Ryota Nishikawa**

Oliver Yaros

Ryota Nishikawa

Law360, New York (July 24, 2017, 12:10 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. 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.

The first part of this article considered who should be legally considered the owner of data generated by CAVs, and how personal data associated with CAVs should be dealt with. In this installment, we consider the legal basis for the use of personal data from CAVs, other applicable data protection requirements, and the best approach to addressing these challenges.

Legal Grounds for Using Personal Data from CAVs

In practice, there are three legal bases for the use of such personal data under European data protection law.

Consent is one legal basis that could be relied on in the context of processing personal data emanating from CAVs, whether by the manufacturers, social or data platforms or third-party developers. However, written consent from the owner of the vehicle at the outset (i.e., when the vehicle is purchased or hired) may not be sufficient.

One issue is that the driver's consent must be fully informed, which can be difficult to demonstrate as time passes, and that the driver must be capable of withdrawing his or her consent at any time, which can be difficult to accommodate in the design of an IT system.

Another issue is that, if the purchase of the CAV or the performance of the CAV is conditional on consent to the processing of the personal data, the consent may not be deemed to be freely given. Owners should not have degraded access to the capabilities of their vehicles if they decide not to consent to processing of personal data.

Finally, obtaining consent from future users who the vehicle may be shared with or sold to will be

difficult. In essence, consent will only work as a legal basis if the data subject is fully and clearly informed and has full control over the processing of his or her personal data.

A suitable level of control could be achieved by adopting a “data protection by design” approach as required by the GDPR.[1] This approach consists of ensuring that privacy protections are built into the design and development of new products and services, as opposed to being implemented later on as part of a legal review process.

For example, obtaining consent as a legal ground for processing personal data could be demonstrated if the data subject is able to, via an interactive dashboard, turn on or off or customize the CAV's ability to collect and transmit different types of personal data, thereby giving the data subject more control over the processing of his or her personal data.

Also, a mode that distinguishes between different individuals using the same car could allow different drivers, passengers and owners of the same car to control their own separate privacy preferences. Manufacturers should also consider a “privacy by default” approach by, for example, having sensors that collect personal data switched off by default. This would help to ensure that data subjects' personal data are not processed automatically without their consent.

Personal data can also be legally processed where it is necessary for the purposes of a contract to which the data subject is party. However, the scope of this legal ground is limited by the criterion of “necessity”, which requires a direct and objective link between the processing itself and the purposes of the contractual performance expected from the data subject.

A manufacturer could also legally process personal data from the CAV if it is necessary for the purposes of the legitimate interests pursued by the manufacturer or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

The Article 29 Working Party has stated that, in the context of internetconnected devices, such as CAVs and the internet of things (IoT) more broadly, the processing of an individual's personal data is likely to affect significantly his or her fundamental rights to privacy and to the protection of personal data in situations where, without the IoT, data could not have been interconnected or only with great difficulty.[2]

Therefore, in light of the potential seriousness of that interference, it is clear that such processing may not be justified by merely the economic interest that a stakeholder in a CAV has in that processing. On the other hand, where the inability to process personal data will undermine CAV safety features, it has been argued that protecting third parties' rights to life under the European Convention on Human Rights may override the data privacy rights of the CAV owner.

For example, if an owner denies consent or opts out of transmissions of location data from the CAV, this may hinder the autonomous vehicle's ability to connect with surrounding cars and other elements of the environment and to navigate the roads safely. It is also possible that insurance companies and the police could use the legitimate interest ground to access personal data from CAVs after an accident to ascertain what has happened and who (or what) was at fault.[3]

Other Data Protection Requirements

European data protection law imposes purpose limitation and data minimization requirements that may restrict the manner in which “big data” is typically collected and used. Specifically, under Directive 95/46/EC and the GDPR, the use of personal data for different purposes than the purpose for which it was originally collected is prohibited.[4] The processing of personal data is also required to be kept to a minimum,[5] and it should not be held for longer than necessary.[6]

Again, manufacturers and other stakeholders will need to ensure that the “Privacy by Design” requirement is followed and think carefully in advance about the potential opportunities to use data collected by cars for new purposes so that data protection safeguards can be incorporated from the beginning. Furthermore, many stakeholders may only need to have anonymized, aggregated data and will have no need to receive the raw data collected by the CAVs.

The Article 29 Working Party recommends that such stakeholders delete the raw data as soon as they have extracted the data required for their data processing.[7]

Data subjects also have the right to access any personal data that has been collected concerning them[8] and to exercise that right easily and at reasonable intervals.[9] The GDPR also provides data subjects with the right to transmit the data they have provided to another service provider (the right to data portability).[10]

To protect these rights, data subjects should be provided with remote access to a secure system that would provide the data subject with direct access to his or her personal data.[11] The ACEA and the European Association of Automotive Suppliers (CLEPA) have proposed a system whereby vehicle-generated data will be relayed to a back-end server maintained by the manufacturer. The data could then be directly transferred from the manufacturer's secure back-end interface to third parties for the provision of services.[12]

Presumably, data subjects would need to be provided direct access to the back-end server to satisfy their data access and data portability rights. In addition, such data should be machine-readable and in an interoperable format.[13]

Data subjects will clearly hold a more immediate interest in the interpreted data (e.g., driving habits) than in the raw data that may not make sense to them (e.g., movement data of the vehicle). However, such data can prove useful for the data subjects to understand what the manufacturer can infer from it about them.

Also, obtaining this raw data would give them a capacity to transfer their data and switch vehicles more easily. Finally, although manufacturers may refuse a portability or access request if it would adversely affect intellectual property rights or trade secrets,[14] data protection authorities still expect that some steps should be taken to provide the personal data in a form that does not release information covered by trade secrets or intellectual property rights.[15]

How to Address the Challenges

To tackle the various ownership and privacy issues arising from data generated by CAVs, the various stakeholders seeking to access and use CAV data will have to enter into carefully structured agreements that clearly identify each party's respective obligations with respect to the ownership of data collected, the use and protection of personal data and the apportionment of risk, particularly in the case of a loss or misuse of data.

This is particularly important given that European data protection authorities may impose fines of up to four percent of the annual global turnover of an industry participant that is responsible for breaches of, for example, the principles governing data processing and data subjects' rights under the GDPR.

A “privacy by design” and “privacy by default” approach should be taken by stakeholders to ensure that data protection is put at the heart of the CAV design. For example, many of the legal risks identified above could be reduced if data can be used on an anonymized and aggregated basis.

In any case, prior to carrying out “big data” analyses that might involve the profiling of individuals who use CAVs, the relevant stakeholders should carry out a privacy impact assessment to identify any data protection risks and how those risks should be mitigated.

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

[1] Article 25 GDPR.

[2] Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.

[3] House of Lords Science and Technology Select Committee — “Connected and Autonomous Vehicles: The future?”

[4] Article 5(1)(b) GDPR.

[5] Article 5(1)(c) GDPR.

[6] Article 5(1)(e) GDPR.

[7] Article 29 Working Party Opinion 08/2014 on the Recent Developments on the Internet of Things.

[8] Article 15 GDPR.

[9] Recital 63 GDPR.

[10] Article 20 GDPR.

[11] Recital 63 GDPR.

[12] https://www.smmt.co.uk/wp-content/uploads/sites/2/SMMTCAV-position-paper-final.pdf.

[13] Recital 68 GDPR.

[14] Article 20(4) GDPR.

[15] Article 29 Working Party Guidelines on the right to data portability.
