# Connected Cars, Autonomous Vehicles and Legal Potholes

by Haroun Khwaja - h.khwaja@tamimi.com - Dubai International Financial Centre

October 2018

As connected cars become the norm and the mainstream rollout of autonomous vehicles gains traction, new legal issues and risks are emerging. This is largely due to the fact that connected cars and autonomous vehicles do not neatly fit into current vehicle related laws across the region. In fact, most jurisdictions globally, do not have a comprehensive regulatory regime to govern the production and use of autonomous vehicles. Existing laws were formulated in an era when connected cars and automated vehicles were only found in science fiction novels. Today, autonomous vehicles are the new reality, and innovative nations are responding by fostering investment in: technology, innovation and physical infrastructure; encouraging consumer adoption; and putting in place appropriate laws and policy. The UAE leads the GCC region and is ranked 8th globally in KPMG's Autonomous Vehicles Readiness Index.

In a previous article (Avoiding Legal Liability Obstacles on the Road to Autonomous Driving – Law Update, October 2017) we gave an overview of the different levels of autonomy, and discussed challenges facing regulators tasked with allocating responsibility and liability (as between automotive manufacturers and users) arising from traffic accidents. This article continues with that theme and highlights additional legal issues associated with connected cars and autonomous vehicles. We will explore questions around the apportionment of liability between vehicle manufacturers and their technology partner vendors; as well as security and privacy risks; and cross border issues where automated vehicles travel from one country to another.

There is a distinction between connected cars and autonomous vehicles. A connected car is driven by a person, but contains features and functionality that enables its systems to share data and interact with other devices and systems (such as smart phones and car dealers' service and maintenance booking systems). An autonomous vehicle contains similar connective features and functionality, but is driven by its own internal computer, with little or no human intervention. Some issues identified in this article apply equally to connected cars and autonomous vehicles, whilst others are specific to autonomous vehicles.

**Liability**

It is common for automotive manufacturers to team up with technology service providers in producing both connected cars and autonomous vehicles. Regulators will have to decide whether the automotive manufacturer will be responsible for design defects and manufacturing defects in the autonomous vehicle as a whole or, whether responsibility for design and manufacturing defects in the technology component will rest with the technology provider. The delineation of liability will be more complicated where a number of parties (e.g. automotive manufacturer, hardware vendor, software licensor and mobile network operator) are involved in the creation of the technology and/or provision of the various components and services required for operation of the vehicle. A further challenge in apportioning liability arises where the damage arises due to a defect or failure in more than one component simultaneously.

Similarly, regulators will need to decide whether insurers can exclude liability in certain circumstances; for instance, is there a case for the insurer of the automated vehicle to exclude liability where the customer makes unauthorised changes to the automated vehicle's software or the customer does not itself install or allow the technology providers to install software updates?

**Data Sharing and Privacy**

Automated or semi automated vehicle control systems as well as security, information and entertainment systems, record a wealth of information including how fast people drive, where they go, details of their telephone conversations (such as time and number called), emails, text messages, contact lists, climate and seat settings and music logs. This data is typically available to the customer via an online account and associated mobile applications. However, this data may also be collected, transmitted, utilised, and even sold, by manufacturers, technology partners and smart city administrators, without the customer's knowledge or consent. The only recourse of customers who object to such use and monetisation of their data is to disable various features, resulting in a loss of other functionality such as navigation systems.

Regulators will need to enact laws and impose standards in order to protect consumers' data and their privacy. Principles such as 'data minimisation' and 'privacy by design', which are found in the data protection laws of other jurisdictions, would be well worth adopting. 'Data minimisation' requires that data storage and processing should be kept to a minimum, and for no longer than necessary. 'Privacy by design' requires companies to think ahead about the possible purposes for use of data in the future so that the necessary data protection measures are implemented from the outset.

Also, strategic decisions will need to be made as to whether data is to be held and processed locally, or in data centres, or cloud infrastructure outside the region. In any case, a cross border data sharing framework may facilitate sharing of data between group companies and partners.

Industry stakeholders must also address privacy issues by implementing the necessary functionality and technology to guard against privacy risk. Recently in Europe, a car manufacturer was found to be providing, inadvertently, the prior owners of connected vehicles with continued access to the data and controls of those vehicles. To guard against similar data breaches, a fail-safe method of disconnecting access to the data and controls of a vehicle is required so that previous owners cannot continue to have access to the new owners' data as well as the vehicle controls. Equally, measures are required to ensure a new owner of a used connected car cannot access personal data belonging to the previous owner. Although some connected cars contain an option to 'clear personal data', the clearing of data is patchy. A comprehensive 'data reset' function (much the same as those found on smartphones) is warranted.

The formulation and enforcement by industry of adequate data use and privacy policies and procedures provide a second layer of protection against privacy risk. The policies will need to align with relevant laws and provide guidance as to whether customers are to be informed about how their data will be used, whether customers' informed consent is required for use of their personal data, and whether personal data can be used for purposes other than that to which the customers have consented.

**Security and Hacking**

Automated control, information, entertainment and navigation systems and smart connectivity

features (such as Bluetooth and Wi-Fi) are soft targets for hackers wanting to sell information to competitors, and compromising vehicle control in order to obtain ransoms. Whilst cars without sophisticated connectivity and automated systems can also be hacked and controlled by a third party, connected cars and automated vehicles are far more vulnerable because they don't require any physical interaction whatsoever.

This risk was highlighted in the United States, where two cyber security experts took over control of a vehicle from 10 miles away through its connectivity unit, which commands a number of the car's features including, its automated driver assist technology. After having demonstrated the various weaknesses in the car's cyber security, the experts brought the car to a complete stop on a highway. The incident led to the recall of approximately 1.5 million cars amongst fears for the safety of passengers if hackers sought to exploit such vulnerabilities.

Technology outsourcing and cloud computing exacerbate this risk as they hinder a company's ability to manage its own security and quickly detect and remediate data security incidents. Also, the technology outsourcing and/or cloud services provider may be subject to less stringent data protection laws if the cloud infrastructure is located abroad.

To address these issues, regulators must work with industry to develop, implement and enforce cyber security standards to prevent hacking of connected, and autonomous vehicle systems as well as the associated supporting infrastructure. Dubai has made good progress on this front, with the Dubai Electronic Security Centre releasing its own set of security standards for autonomous vehicles covering communication, software, hardware and supply chain security. The standards will apply to all Dubai government entities that wish to deploy their own autonomous vehicles.

**Cross Border Issues**

There is significant movement of vehicle traffic across GCC borders. To ensure car owners can use their cars outside their home country, the implementation of interoperable / standardised technologies, consistent infrastructure standards and harmonious laws will be paramount. This will improve customer acceptance as well as reduce costs and complexity for the industry.

Al Tamimi & Company's TMT team regularly advises on technology related matters, including telematics, cyber security and data protection. For further information please contact Haroun Khwaja (h.khwaja@tamimi.com) or Andrew Fawcett (a.fawcett@tamimi.com).