THE
NATIONAL LAW REVIEW

UK Government Issues Cybersecurity Guidance for Connected and Automated Vehicles

Wednesday, September 13, 2017

McDermott Will & Emery

Article By
Michael G. Morgan
McDermott Will & EmeryOf Digital Interest

Communications, Media & Internet
Utilities & Transport
Global
United Kingdom

On 6 August 2017, the UK government released ‘The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles’, guidance aimed at ensuring minimum cybersecurity protections for consumers in the manufacture and operation of connected and automated vehicles.

Connected and automated vehicles fall into the category of so-called ‘smart cars’. Connected vehicles have gained, and will continue to gain, adoption in the market and, indeed, are expected to make up more than half of new vehicles by 2020. Such cars have the ability through the use of various technologies to communicate with the driver, other cars, application providers, traffic infrastructure and the Cloud. Automated vehicles, also known as autonomous vehicles, include self-driving features that allow the vehicle to control key functions–like observing the vehicle’s environment, steering, acceleration, parking, and lane changes–that traditionally have been performed by a human driver. Consumers in certain markets have been able to purchase vehicles with certain autonomous driving features for the past few years, and vehicle manufacturers have announced plans to enable vehicles to be fully self-driving under certain conditions, in the near future.

The principles set forth in the UK government’s guidance are part of a wider push by the government to establish the UK as a player in the development of smart cars. Earlier this year, the government announced its plans for the Automated and Electric Vehicles Bill, which will aim to establish the UK as a global leader and ensure that “the next wave of self-driving technology is invented, designed and operated safely in the UK” and it has further pledged £200 million to this cause.

The guidance has been produced in response to the large (and growing) risk of cybersecurity attacks presented by connected and autonomous vehicle technology. Increased connectivity and autonomy necessarily rely heavily on continuous streams of data. As Grayson Brulte, one of the leading authorities on autonomous vehicles, recently commented, “the scientific breakthroughs in artificial intelligence, LiDAR and edge computing combined with high-definition 3D mapping have made it possible for fully autonomous vehicles to operate in unpredictable environments such as cities.”

All of these scientific breakthroughs involve the collection and processing of massive volumes of data, which creates potential vulnerabilities from a cybersecurity perspective. With respect to autonomous vehicles, there are significant threshold questions that remain unanswered and that will significantly affect the cybersecurity risks of such vehicles. For example, it is unclear to what extent autonomous vehicles will interact with the transportation infrastructure and other vehicles or whether such vehicles will be designed to rely as heavily as possible on data that is generated by the vehicle itself. Similarly, it is unclear whether and under what conditions human intervention will be permitted, or whether it will be determined that the human risks of fallibility, distraction, and occasional malicious intent offset the potential safety benefit of human involvement. The autonomous vehicle industry has not reached consensus on these issues.

Nevertheless, it is apparent that providers will need to focus on developing robust programs for attempting to maintain the security of connected and autonomous vehicles. They also will need to pay close attention to the storage, processing and transfer of personal data in light of increased regulation and scrutiny under EU and international data protection and privacy regimes. As examples, providers will need to carefully consider disclosure obligations to relevant authorities as well as consents from consumers.

The principles set forth in the UK guidance are targeted towards the prevention of hacking and data theft by ensuring that cybersecurity becomes a key consideration for everyone in the automotive manufacturing supply chain. The guidelines consist of the following eight principles:

- **Principle 1**: Organisational security is owned, governed and promoted at board level–this is aimed at promoting a 'culture of security' within an organisation
- **Principle 2**: Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain
- **Principle 3**: Organisations need to provide product aftercare and incident response to ensure systems are secure over their lifetime
- **Principle 4**: All organisations, including sub-contractors, suppliers and potential third parties, must work together to enhance the security of the system
- **Principle 5**: Systems are designed using a defence-in-depth approach–security measures should be designed to address failures and breaches through defence-in-depth and segmented techniques
- **Principle 6**: The security of all software is managed throughout its lifetime
- **Principle 7**: The storage and transmission of data is secure and can be controlled
- **Principle 8**: The system is designed to be resilient to attacks and respond appropriately when its defences or sensors fail

These principles are articulated at a high level and are fairly self-evident to those with experience in the cybersecurity industry. Also, as of yet, these principles are not binding and do not impose concrete obligations on manufacturers of connected and automated vehicles. This cautious approach may reflect an appreciation that this emerging technology does not lend itself to detailed rules that might, in hindsight, turn out to be misguided. It may also reflect a recognition that development of autonomous vehicle technology is occurring on a global scale, and thus stringent regulation risks the loss of development projects to less regulated jurisdictions.

This article was written by Antonina Nijran, Dennis Brunner and Ashley Winton.

© 2019 McDermott Will & Emery

Source URL: https://www.natlawreview.com/article/uk-government-issues-cybersecurity-guidance-connected-and-automated-vehicles