ISSUE 4 | FEBRUARY 27, 2024

INTERNATIONAL DEVELOPMENTS

"Cyberattack-Secured" Autonomous Vehicles to Hit the Market in Europe this Year

The European self-driving car company Vedecom Tech and Israel's Karamba Security announced in June 2017 that they are partnering to develop a fully autonomous car. According to the announcement, the completely autonomous vehicles will be launched for commercial use in late 2017 and 2018 by municipalities in France, Germany, Italy, Portugal and the Netherlands. David Barzilai, Karamba's executive chairman, informed Reuters that the first vehicles will be "short-haul" cars available for tourists in Versailles and will drive on about four miles of specially assigned lanes.

Vedecom Tech will equip the new vehicles with Karamba Security's Carwall and Autonomous Security software, which will help protect the cars' electronic control units against the risk of hacking. Karamba's systems will protect the car from possible cyberattacks on external communications between vehicles and surrounding infrastructure as well as the car's internal electronics. In their announcement, the companies said, "This marks the industry's first production of cyberattack-secured, commercially-available automobiles."

Vedecom Tech is a commercial subsidiary of Vedecom Public Foundation, an organization dedicated to developing autonomous transportation with several companies in the European automotive industry, including Renault, Peugeot and Valeo. Karamba Security is an Israeli company that provides cybersecurity for connected and autonomous vehicles.

At the forefront of defending automotive companies, Shook understands our clients' products, their businesses and the industry as a whole, as well as the legal and regulatory landscape, including emerging technology and liability theories.

For additional information about Shook's capabilities, please contact

Doug Robinson
949.475.1500
dwrobinson@shb.com

Amir Nassihi
415.544.1900
anassihi@shb.com

New technologies often present liability risks, and autonomous vehicles are no exception. The perceived responsibility for road traffic incidents would shift from drivers to the manufacturer of the vehicle. While adding software providing security from cyberattacks is an important safety feature, companies still risk liability if the software should fail to prevent an attack. The European Product Liability Directive 85/374 EEC (implemented in the U.K. by the Consumer Protection Act 1987) imposes strict liability for defective products if the claimant proves a defect (i.e., the claimant does not need to prove fault). The manufacturer will be liable if the defect causes damage. A court will consider a product to be defective if its safety "is not such as persons are generally entitled to expect." In addition to undertaking rigorous testing to ensure that the software is unlikely to fail, manufacturers using such technology should ensure that warnings and disclaimers are adequate and that consumer expectation levels are set appropriately in marketing campaigns.

Alison Newstead
+44 (0)20 7332 4500
anewstead@shb.com

LEGISLATION, REGULATIONS & STANDARDS

House Subcommittee Approves Deployment of Self-Driving Vehicles

A U.S. House of Representatives subcommittee recently approved a proposal allowing automakers to deploy up to 100,000 self-driving vehicles without satisfying current auto safety standards. The bill, H.R. 3388, will proceed to the House Energy and Commerce Committee. The proposed legislation would require automakers to submit safety assessment reports to regulators but would not require pre-market approval of advanced vehicle technologies. To be exempt from meeting safety standards, automakers would have to show that their self-driving vehicles function as intended and contain fail-safe features. If passed, this legislation would be a significant step towards creating a federal standard for self-driving vehicles and would preempt current state laws trying to impose barriers to deployment. While states would continue to regulate registration, licensing, liability, insurance and safety inspections, they would not be able to set self-driving car performance standards.

Regulating Drones: A State Issue?

In May 2017, the District of Columbia Circuit Court struck down the Federal Aviation Administration's (FAA) December 2015 rule requiring recreational drone registration. In the absence of clear federal regulations, state legislatures are taking it upon

themselves to regulate drone use in their skies to protect its citizens from accidents and address privacy concerns.

Before 2017, at least 40 states enacted laws addressing unmanned aircraft systems, commonly called unmanned aerial vehicles or drones, and three other states adopted resolutions. In this year's legislative session, at least 38 states are considering legislation relating to unmanned aircraft systems. These laws and regulations range from defining "drone" to determining how they can be used by state agencies and the general public.

Many have criticized local law enforcement for its implementation of drones. The public outcry was so strong in response to Seattle's announcement on the use of drones in its force that the entire program was grounded prior to implementation. Los Angeles faces similar public outrage following its announcement of a one-year pilot program to incorporate drones into the city's police force. Two seven-foot drones, which have been grounded since 2014 due to public criticism, would be used to gather critical information without placing officers at risk during dangerous situations such as hostage standoffs, bomb scares or shootings with a gunman still at large. It will be months before the police department can fulfill the necessary requirements of holding public hearings, obtaining Police Commission approval of its guidelines and receiving certification from FAA to train officers to use the drones in order to implement its pilot program.

In an effort to limit the scope of FAA's preemption of drone regulations and protect states' rights to implement drone laws and regulations, Sen. Dianne Feinstein (D-Calif.) teamed up with Sen. Mike Lee (R-Utah), Sen. Tom Cotton (R-Ark.) and Sen. Richard Blumenthal (D-Conn.) to introduce the Drone Federalism Act of 2017. The act would give states the power to regulate the time, place and manner of drone use in their airspace and permit states to implement "prohibitions that protect public safety, personal privacy rights, or that manage land use to restrict noise pollution."

Additionally, the act attempts to clarify the issue of airspace over private property, which is defined by the act as the airspace within 200 feet of the ground or a structure, including "any area where operation of the aircraft system could interfere with the enjoyment of use of property."

The National Council of State Legislatures applauds the act for "protect[ing] the FAA's authority to ensure safety of the airspace, while also maintaining state and local authority to protect public safety and security, personal privacy, property rights and manage land use regarding the operation of drones." However, critics argue that the act may burden the drone industry with a

patchwork of 50 separate sets of regulations. Opponents further criticize the act's definition of airspace, noting that obtaining permission from property owners to fly drones within 200 feet of their property will greatly hinder both recreational and commercial drone use.

The act has twice been referred to the Committee on Commerce, Science, and Transportation.