Westlaw Journal
AUTOMOTIVE
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 36, ISSUE 11 / NOVEMBER 29, 2016

EXPERT ANALYSIS

Q&A: Privacy, Cybersecurity, Connected Cars and Driverless Vehicles

By Aaron Jacoby, Esq., and James Westerlind, Esq.
Arent Fox LLP

Cybersecurity and privacy are primary concerns in American life, from hacks of the internet through robot devices to vehicle communication and connectivity.

According to a survey conducted by Munich Re, the world's second-largest reinsurer, 55 percent of corporate risk managers who were surveyed identified cybersecurity as their chief concern about driverless vehicles.

Certainly, the general public will share that concern as connected cars and self-driving vehicles become more common. The cybersecurity threat includes the potential hacking of an automated car's data systems and the failure of smart-road infrastructure.

And while driverless vehicles on public roads are unlikely to become a "mainstream reality" for years to come, the potential dangers of the technology are present today.

Driverless cars are already on the road in small numbers. In August Uber began a driverless car pilot test in Pittsburgh, where it fielded a fleet of Volvo luxury SUVs equipped with self-driving capability offering free rides around the city (albeit with a human technician in the driver's seat ready to take control if anything bad happens).

In 2015 the dangers of hacking were revealed in a controlled setting. During a demonstration with a Jeep Cherokee that was being operated by a writer for Wired magazine, researchers/hackers Charlie Miller and Chris Valasek showed the security vulnerabilities in the mobile Wi-Fi system of certain Fiat Chrysler vehicles.

Using a laptop, they were able take control of key vehicle systems in the Jeep. They were able to change the radio volume, adjust the air conditioning, operate the windshield wipers and, most concerning, take control of the vehicle's transmission, bringing the Jeep to a stop on the highway.

This caused Fiat Chrysler to recall 1.4 million vehicles to install software to protect against such hacks.

Safety is also an issue with driverless technology.

On May 7 a Tesla Model S automated vehicle struck a tractor-trailer crossing a highway in Florida, killing the person inside the automated vehicle. This incident followed several crashes involving Tesla vehicles using its Autopilot feature.

Theft is another concern. This past summer, Houston police charged two men with stealing more than 100 cars by using a laptop to signal the cars to open their doors and start their engines remotely.

Since passengers in self-driving vehicles will not have to concentrate on driving, they will likely spend much of their time using the vehicle's wireless internet connection to engage in tasks such as shopping, banking and working, or otherwise transferring potentially sensitive data through the vehicle's potentially hackable system.

In addition, the data being collected and transferred by the vehicle over its Wi-Fi connection may include medical and health information of passengers. For instance, some automakers have been testing sensors that monitor drivers' vital signs and physical reactions to warn about drowsiness, low blood sugar and other possible dangers.

Further, autonomous vehicles will use vehicle-to-vehicle, or V2V, and vehicle-to-infrastructure, or V2I, technology to maximize their potential.

For example, if one car is in an accident or breaks down, it will utilize V2V communications to alert those vehicles behind it on the road of the problem so that they can react sooner and more efficiently. The U.S. Department of Transportation estimated that implementing V2V technology across the nation could save between 780 and 1,080 lives and prevent 400,000 to 600,000 collisions each year.

But if hackers or terrorists were able to take control of this technology, they could create chaos, including by potentially turning driverless vehicles into weapons.

So the dangers and concerns that could arise (and indeed have arisen) from internet-connected cars and driverless vehicles include bodily injury/death, theft, and compliance with data security and data breach notification requirements under state and federal laws — to name just a few.

If hackers or terrorists were able to take control of vehicle-to-vehicle technology, they could create chaos, including by potentially turning driverless vehicles into weapons.

What impact will the U.S. Department of Transportation's new federal policy have on automated vehicles?

In September the DOT issued its federal automated vehicles policy, which it characterized as agency guidance rather than as rules in an effort to speed the delivery of an initial regulatory framework and best practices to guide manufacturers in the safe design, development, testing and deployment of highly automated vehicles, or HAVs.

The DOT policy specifically addresses vehicle cybersecurity, and it instructs manufacturers to follow a robust product development process based on a systems-engineering approach to minimize risks to safety, including cybersecurity threats and vulnerabilities.

In particular, the policy recommends that manufacturers consider and incorporate guidance, best practices and design principles published by National Institute for Standards and Technology, the National Highway Traffic Safety Administration, SAE International, the Alliance of Automobile Manufacturers, the Association of Global Automakers, and the Automotive Information Sharing and Analysis Center.

Cybersecurity considerations should be fully documented, and all actions, changes, design choices, analyses, testing and data should be traceable. Manufacturers within the industry should share information so that cybervulnerabilities are not unnecessarily repeated in the industry.

In addition, the DOT policy includes a model state policy, which was created in collaboration with the American Association of Motor Vehicle Administrators, or AAMVA.

The model state policy was designed to enable manufacturers to focus on developing a single HAV fleet rather than 50 different versions to meet individual state requirements. Under the policy, states would retain their traditional responsibilities for vehicle licensing and registration, traffic laws and enforcement, and motor vehicle insurance and liability regimes.

The DOT strongly encourages states to allow the DOT alone to regulate the performance of HAV technology and vehicles. It also says that if a state does decide to regulate in this area, it should consult with NHTSA and base its efforts on the vehicle performance guidance provided in the DOT policy.

The model state policy has been issued for public comment.

It recognizes that states are responsible for determining liability rules for HAVs and how liability should be allocated among HAV owners, operators, passengers, manufacturers and others when a crash occurs. In addition, states are to determine who among these people and entities should bear the burden of insurance for the foreseeable risks.

What are some of the liability issues?

As noted above, under the model state policy created by the DOT in collaboration with AAMVA, the determination of who should bear liability for losses arising from automated vehicles, and who should purchase insurance to cover that liability, is a state issue.

It is likely that losses arising from driverless vehicles will shift from the consumer/driver/owner to the manufacturer.

This is because accidents involving fully automated vehicles will likely be the result of a defect in the design or manufacturing process for the vehicle rather than the operation of the vehicle by its owner/occupant. It will be difficult to blame the owner of a driverless vehicle for an accident caused by his car if he did not, and could not by the vehicle's design, influence the operation of the vehicle on the road.

So it is likely that product liability lawsuits against manufacturers for accidents involving their fully automated vehicles will increase, while claims against the owners/non-drivers (indeed, mere passengers) of those vehicles will decrease.

And if the tort liability shifts from the driver to the manufacturer, it is also likely that the burden of purchasing liability insurance should shift from the consumer/owner to the product manufacturer.

The U.S. Department of Transportation's strongly encourages states to allow the DOT alone to regulate the performance of driverless vehicles.

But while the consumer may experience a reduction in auto liability premiums, it is likely that costs associated with the shift in liability from vehicle owners to vehicle manufacturers (such as increased premiums for product liability insurance or reserves for self-insured insurance programs maintained by manufacturers) will be passed back to the consumers in the form of increased product price.

The pricing of insurance and shifting of costs will likely be another issue to be addressed by the states, including their insurance departments and legislatures.

If the 'system is the driver,' how does this affect contributory negligence?

We assume for purposes of this question that the plaintiff would be the owner of the driverless vehicle who was injured when a vehicle's automated system malfunctioned, and that the defendant would be the driverless vehicle's manufacturer. In such a product liability lawsuit, depending on which state's law applied, the manufacturer may attempt to assert a defense based on the alleged contributory or comparative negligence of the owner/consumer.

Only a few states follow the pure contributory negligence rule.

Under this rule, if the plaintiff was liable for his injuries in whole or in any part, then he cannot recover from the defendant. Most states have abandoned the pure contributory negligence rule and have instead adopted a form of comparative negligence.

In comparative negligence jurisdictions, if a defendant proves that the plaintiff was partially liable for his injuries, then the defendant's liability for the plaintiff's injuries will be reduced but may not be completely eliminated. In a pure comparative negligence state, a plaintiff's damages are totaled and then reduced to reflect his contribution to the injury.

In a modified comparative negligence state (which a majority of states follow), a plaintiff's damages are totaled and reduced to reflect his contribution to the injury. If the plaintiff is found to have been a threshold percentage at fault for the injury (49 percent or less in some states, and less than 51 percent in other states), then the plaintiff cannot recover against the defendant.

Applying the principles of contributory or comparative fault to a lawsuit by an injured owner/consumer against a manufacturer of a driverless car, the issue would likely largely depend on what degree of control the injured owner/consumer had over the operation of the vehicle at the time of the accident.

In addition, if the owner/consumer failed to properly maintain the driverless vehicle, and that failure proximately caused the accident, then the defense may be available to the manufacturer.

It is likely that losses arising from driverless vehicles will shift from the consumer/driver/owner to the manufacturer.

The Tesla fatal injury this past May, discussed above, is an example. Tesla issued a press release June 30, titled "A Tragic Loss," which stated, in part:

> It is important to note that Tesla disables Autopilot by default and *requires explicit acknowledgement that the system is new technology and still in a public beta phase* before it can be enabled. When drivers activate Autopilot, the acknowledgment box explains, among other things, that Autopilot "*is an assist feature that requires you to keep your hands on the steering wheel at all times,*" and that "*you need to maintain control and responsibility for your vehicle*" while using it. Additionally, every time that Autopilot is engaged, the car reminds the driver to "*Always keep your hands on the wheel. Be prepared to take over at any time.*" The system also makes frequent checks to ensure that the driver's hands remain on the wheel and provides visual and audible alerts if hands-on is not detected. It then gradually slows down the car until hands-on is detected again [emphasis added].

Thus, it appears that Tesla may attempt to assert that the person who was killed in the May accident was liable for the crash in whole or in part, if the facts show that he took his hands off the steering wheel during the incident.

The more automated a vehicle is, the less likely it is that the contributory or comparative-fault defense will be available to the manufacturer.

Google's driverless prototype used on private roads, for instance, does not have a steering wheel; it is completely driverless and cannot be controlled by an occupant. So if the Google-type vehicle is eventually permitted to be sold to a consumer, the defense of contributory or comparative fault may be limited to failure to properly maintain the vehicle.

CALIFORNIA ISSUES

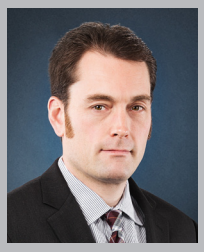
California seems to be at the forefront when it comes to privacy regulations. How does the state's action regarding driverless cars sync with federal legislation/regulation? Hacking is a real concern as well. How are automakers going to prevent it?

On Sept. 20, the California Department of Motor Vehicles issued a statement on the DOT policy discussed above, stating that the state welcomes NHTSA's release of the DOT policy and that the DMV worked closely with AAMVA on the model state policy within the DOT policy.

The California DMV stated that it supports NHTSA's goal of creating a consistent approach and national framework for the testing and deployment of autonomous vehicles. The DMV intends to revise its regulations based on the DOT policy after considering public comments to its draft revised regulations.

While California has been at the forefront with respect to privacy regulations and automated vehicles, it appears that its regulators want to work with federal regulators on the subject to design uniform regulations that will promote the use of automated vehicles while protecting its citizens.

To prevent their automated vehicles from being hacked, manufacturers should comply with the vehicle performance guidance for automated vehicles in the DOT policy. As noted above, that guidance recommends that manufacturers follow the guidance and protocols promulgated by various other federal agencies and industry groups with respect to cybersecurity



Aaron Jacoby (L) is the managing partner of **Arent Fox LLP** in Los Angeles and chair of the firm's automotive industry practice group. Jacoby and the practice group have been recognized by Chambers USA as a leader in the category Transportation: Road (Carriage/Commercial). Jacoby focuses his practice on class actions and consumer litigation, federal and state regulatory matters, business transactions, and government investigations in the automotive industry. **James Westerlind** (R) is counsel in Arent Fox's automotive industry litigation and cybersecurity and data protection practice groups. He represents auto dealers in franchise disputes with auto manufacturers in various federal and state actions and administrative proceedings.