BUSINESS LAW TODAY

Are Your Clients Ready for the Impact of Driverless Cars?

By Richard C. Balough

When you drive down the highway in the not-too-distant future, you might see a car with no driver in the next lane. Maybe the car has a driver, but she is reading a book. When you pass that long line of semi-trailer trucks, do not be surprised if the only driver is in the lead truck. Even when you use a ride-sharing app, you might be picked up by a car with no driver.

Welcome to the era of autonomous vehicles.

When is it coming? Actually, portions are already here. Some of today's cars have programs to keep you in your lane without using the steering wheel, apply the brakes if you are too close to the car in front of you, and even help you parallel park. Several states already have laws allowing driverless vehicles on the roads under certain conditions.

In January 2016 at the Detroit Auto Show, U.S. Transportation Secretary Anthony Foxx announced a push for new regulations regarding autonomous vehicles. It is part of a White House proposal to invest $4 billion over the next 10 years to accelerate the development of driverless vehicles. The money would fund pilot programs to test connected vehicle systems in designated corridors throughout the country and work with industry to establish a multistate framework for connected autonomous vehicles. "We are on the cusp of a new era in automotive technology with enormous potential to save lives, reduce greenhouse gas emissions, and transform mobility for the American people," Foxx stated. By mid-2016, the National Highway Traffic Safety Administration plans to

- develop guidance on the safe deployment and operation of autonomous vehicles, providing a common understanding of the performance characteristics necessary for fully autonomous vehicles along with appropriate testing and analysis;
- develop a model state policy on automated vehicles that offers a path to consistent national policy;
- encourage manufacturers to submit requests for exemptions to allow deployment of fully autonomous vehicles; and
- ensure that fully autonomous vehicles, including those designed without a human driver in mind, are deployable in large numbers when they are demonstrated to provide an equivalent or higher level of safety than is currently available.

What should a business lawyer advise clients to avoid the legal potholes of autonomous vehicles?

As with many rapidly developing technologies, it is too early to know how the world of autonomous vehicles will fully unfold, so any legal advice should take several scenarios into consideration. It may be that, at some point, human involvement in driving is eliminated—"drivers" become just passengers and do not actively control the vehicle. Individual cars may be replaced by fleets of autonomous vehicles that are dispatched from a central location for users, or vehicles may still require humans as drivers, but the vehicles will communicate with other vehicles and objects to make driving easier and safer. It is probable that, at some point, the roads will have a mixture of driverless and driver vehicles, requiring new rules of the road.

According to the Transportation Research Board of the National Academies, totally autonomous or driverless vehicles are cars, trucks, vans, and buses that "operate without real-time input of a human driver into the steering, acceleration, and braking, and with varying levels of driver monitoring. . . . These systems may operate only in limited environments, such as at low speed in congested traffic or only on highways; in contrast, a fully automated vehicle one day may operate on all roads, from rural unmarked roads to crowded city centers." For example, one of the cars Google is testing does not even have a steering wheel, but only a button to stop the car.

Semi-autonomous vehicles are vehicles that are not totally driverless. Some driving functions are automated, such as lane control, maintaining distance between vehicles, warnings about a vehicle in a car's "blind-spot," or warnings at intersections. Technology now in use allows semi-trailer trucks to run caravans with the driver in only the lead truck.

Although vehicles may be autonomous or semi-autonomous, the computers actually "driving" the vehicles are connected to the outside world. Today 27 million vehicles worldwide are connected to the Internet, and that number is predicted to triple by 2022 to more than 82 million, according to HIS Automotive, a group of automakers that co-operates on research. This is a far cry from the time when a vehicle's computer was connected to systems only within the vehicle. Complex computer software has been used for years to power cars' performance, but those computerized brains were always walled off inside the cars themselves; they were not connected to the wider world.

In the near future, roadways likely will have side-by-side, driver-controlled vehicles, vehicles with automated driver assistance, and fully autonomous vehicles with no drivers. One big challenge is blending them into a world in which humans do not always behave by the book. For example, Google's autonomous vehicle is programmed to follow the letter of the law. As a result, one Google test car could not get through a four-way stop because its sensors kept waiting for human drivers to stop completely.

To conduct testing of driverless vehicles, the State of Virginia has designated several roads in the northern part of the state for autonomous cars. The University of Michigan at Ann Arbor has a 32-acre testing ground specifically designed for researching self-driving cars, including a mock suburb with asphalt and gravel roads lined by brick and glass building facades. Florida Polytechnic University is setting up a fake town for testing autonomous vehicles. Florida, Michigan, California, and Nevada have legislation regarding self-driving cars.

Autonomous vehicles offer several potential benefits. The U.S. Department of Transportation includes as benefits

- a reduction in the number and severity of crashes caused by drivers or by other conditions, such as weather, pedestrians, and road conditions;
- a reduction in aggressive driving;
- an expansion of the ability of the disabled and older users to drive; and
- an increase in the efficiency and effectiveness of existing transportation systems.

Navigant Consulting estimates that by 2035, 75 percent of vehicles sold worldwide will have some degree of autonomous capability. Drivers need not wait, however, because some autonomous technologies are available today. Tesla owners can now wirelessly download a new autopilot feature as a software update. The *New York Times* reports the Tesla autopilot "allows hands-free, pedal-free driving on the highway under certain conditions. The car will even change lanes autonomously at the driver's request (by hitting the turn signal) and uses sensors to scan the road in all directions and adjust the throttle, steering and brakes." Tesla officials nevertheless urge drivers to keep at least one hand on the wheel at all times.

Audi has announced that within the next three years it will sell a luxury sedan that can control itself in a traffic jam. Cadillac is planning to introduce a self-driving feature, SuperCruise control, for highways in a coming model. Jaguar Land Rover is developing a smartphone app that controls a Range Rover from outside, taking control of its steering, accelerator, and brakes to allow off-road drivers to navigate steep embankments or city drivers to park the vehicle in tight spaces.

Today's and tomorrow's cars are computers that happen to move physically on the roadway. As with any computer, they are subject to malware and hacking. Hackers have demonstrated that it is possible to take over today's cars because most vehicles do not have even basic firewalls to keep intruders out. The result is that, once the control area network of a vehicle is accessed, all systems in the car can be controlled, including the brakes, transmission, acceleration, and other vital components. There are even lists identifying the most hackable cars on the road. For example, PT&C Forensic Consulting Services published its most hackable car list, which is topped by the 2014 Jeep Cherokee hacked via Chrysler-Fiat's UConnect system and later recalled because of the car's vulnerability.

As a result of the publicity surrounding the Cherokee hacking, legislation was introduced to establish cybersecurity standards for motor vehicles. As one of the sponsors, Sen. Richard Blumenthal said, "It's as basic as selling a car without door locks. No automaker would think of doing that, and they shouldn't sell cars connected to the Internet without minimal protections against hackers."

Business lawyers should be aware that there are no precise roadmaps for the legal issues surrounding autonomous or connected cars. However, they should plan to address the following issues likely to arise.

Copyright

Copyrights protect the millions of lines of software code that control autonomous or semi-autonomous vehicles. Similar to the licensing of other software, new cars come with end-user license agreements (EULAs) to protect the code from unauthorized copying. Although courts have not addressed vehicle-specific EULAs, courts generally enforce shrink-wrap agreements and EULAs when consumers have notice.

The vehicle's code also is generally protected by devices to prevent access, which means the anticircumvention provisions of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(1), apply. However, in late October 2015, the U.S. Copyright Office Library of Congress, over the objections of car manufacturers, granted two exemptions where circumvention would be fair use.

The first exemption allows an "authorized owner" to diagnose, repair, or "lawfully" modify the code so long as it does not violate other statutes. This exemption retains the ability of car owners to work on their own vehicles so long as they do not make modifications that would disable or downgrade pollution control systems in violation of the Environmental Protection Act. However, the exemption does not apply to computer programs chiefly designed to operate a vehicle's entertainment and telematics systems.

The second exemption permits security research "for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability, when such activity is carried out in a controlled environment designed to avoid any harm to individuals or the public." The exemption was opposed by car manufactures, claiming that the security research could be used by "bad actors" to hack into cars.

Data Protection and Privacy

Controlling autonomous vehicles generates unprecedented amounts of data as to their operation and location. This data must be collected, transmitted via the Internet or Wi-Fi, stored, and analyzed, creating opportunities for hacking. As one cybersecurity consultant explained to *ZDNet*, almost all car manufacturers "have a history of developing closed in-vehicle systems that would only interact through wires within their environment. This physical access restriction may have justified proprietary and security measures that are inefficient for protecting vehicles in this rapidly evolving cybersecurity landscape. Attackers will search for vulnerabilities in the complex vehicle ecosystem—not just the vehicle itself."

The data will contain personal information, such as where the vehicle was driven and how fast it was driven. Is the data owned by the vehicle owner or by the car company? What can be done with the data? For example, driving habits could be used to determine insurance rates not only for auto insurance but also life insurance. The Department of Transportation has identified several privacy considerations:

- **Transparency.** Consumers should know what data is collected and how the data will be used.
- **Participation.** Consumers should have a reasonable opportunity to make information decisions about the collection, use, and disclosure of their data and personally identifiable information and have the opportunity to correct, amend, or delete it.
- **Use Limitation.** Consumers should have assurance that their data will not be used for purposes incompatible with clearly specified purposes.
- **Security.** Consumers should know what physical, technical, and procedural measures will be taken to protect their data.

Liability and Insurance

The issues relating to hacking into autonomous vehicles are not limited to protecting copyrighted code. There is also a liability issue. In the case of the Jeep Cherokee, computer scientists took over control of the vehicle's various systems, enabling them to stop, speed up, and even steer. If the hacker were malicious, drivers, passengers, and third parties could be seriously injured or even killed by such actions. Terrorists in remote control of vehicles could inflict damage and widespread fear. Who is liable for a hack? The car manufacturer or the software coder? To protect vehicles, will it be necessary to run antivirus software every time the vehicle is started? Guarding against hacking and viruses will be a full-time job for automakers, which may have a duty to warn when hacks occur just as today's consumers must be told when their personally identifiable information is compromised.

Although it may be generally acceptable that computers sometimes crash because of faulty code or other design problems, it may not be acceptable when a driverless vehicle's computer crashes, causing physical injuries or death. What legal standard will apply? If the computer flaws are foreseeable, will strict liability apply? Is there a duty to warn drivers of potential software flaws and to push out software updates?

Additional liability questions arise when a car is in a self-driving mode. If there is an accident, who is liable? Is the driver negligent for not taking control of the car prior to the accident? Is the software designer liable because the program did not avoid the accident?

Autonomous cars may require rethinking of insurance. Today's drivers are insured. Insurance companies offer discounts for drivers who are willing to install devices that monitor their driving habits. How is this data used? With whom is this information shared? Is there proper disclosure of how the data is used or shared? If there is no driver, however, who or what would be insured? Could the fact that there is no driver affect the insurance industry? One potential benefit of driverless cars is that there will be no driver-caused accidents. Although fewer accidents may mean the insurance companies pay out less in the short term, insurance companies may have to reduce premiums in the long term.

Conclusion

Autonomous vehicles will require business attorneys to reinterpret existing law and to monitor legislative changes as the technology drives changes on the highway. Attorneys cannot simply fasten their seat belts and go along for the ride.

Richard C. Balough is co-chair of the American Bar Association's Mobile and Connected Devices Subcommittee of the Cyberspace Law Committee. He previously co-authored the November 2013 Business Law Today article, "Cyberterrorism on Wheels: Are Today's Cars Vulnerable to Attack?" He is a founding member of Balough Law Offices, LLC, a Chicago-based law firm that represents businesses in protecting intellectual property assets.

ADDITIONAL RESOURCES

For other materials related to this topic, please refer to the following.

Business Law Section Program Library

Autonomous Vehicles: Steering Your Client around the Legal Potholes (PDF) (Audio)

Presented by: Cyberspace Law, Business and Corporate Litigation, Corporate Counsel, Intellectual Property

Location: 2015 Annual Meeting

* * *

Business Law Today

Cyberterrorism on Wheels: Are Today's Cars Vulnerable to Attack?

By Cheryl Dancey Balough and Richard C. Balough

Vol. 23, No 3. November 2013