Driverless Cars:
Avoiding the Legal Potholes

Richard C. Balough

Balough Law Offices, LLC

1 N. LaSalle St., Suite 2020
Chicago, IL 60602
312.499.0000
rbalough@balough.com

Richard C. Balough is a founding member of Balough Law Offices, LLC, in Chicago, Illinois, which focuses on technology and cyberspace law. He co-chairs the American Bar Association's Mobile and Connected Devices subcommittee of the Cyberspace Law Committee. He served as chair of the Chicago Bar Association's Internet Law Committee and as a board member of the Intellectual Property Law Association of Chicago. He has contributed numerous articles and chapters for legal publications on copyrights, technology, and privacy issues. In addition to his J.D. degree, Mr. Balough has masters of law in Intellectual Property and in Information Technology and Privacy Law.

Driverless Cars:
Avoiding the Legal Potholes

Table of Contents

Driverless Cars:
Avoiding the Legal Potholes

I. Evolution of Autonomous Cars

Today's and tomorrow's cars are not your father's cars any more than today's stealth planes are the Wright brothers' airplanes.

Yes, today's and tomorrow's cars will still have four wheels, but they may not have a steering wheel (or even a driver). The old "shade-tree mechanic" is now a hardware and software technician. Forget about making repairs by yourself. And if there is an accident, in addition to battling a PI attorney, you may also face an IP attorney.

A bit of car evolution is in order. From the beginning, cars were self-contained machines. While they had electrical parts, and eventually some computing ability, these early systems were not connected to the outside world. This situation is sometimes referred to as air gapped, which was the practice for many industries. Dealers would manually access the car's computer systems via a government-mandated OMB II port. Once connected to the port, all operating systems become vulnerable because there was no thought about outside intervention and thus no need to protect the systems from the outside world. There were no software or hardware firewalls because no one considered the implications of being connected to the outside world or the Internet.

As cars became more complex with entertainment systems, GPS, tire pressure gauges, and other conveniences, they became computers on wheels. With Bluetooth and Wi-Fi, cars no longer are isolated vehicles but rather are routinely connected to the Internet. As cars become semi-autonomous—think lane change warnings, auto pilot, collision avoidance—the systems gather data from outside sources such as the Internet to take action.

II. Elimination of Human Involvement

At some point, human involvement in driving may be eliminated—"drivers" become just passengers and do not actively control the vehicle. Individual cars may be replaced by fleets of autonomous vehicles 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.

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 version of the Google car does not have a steering wheel but only a button to stop the car. Uber is operating driverless cars in some locations although there is a standby operator in the front seat.

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 only driver being in the lead truck—controlling all of the trucks with the assistance of onboard computers.

While vehicles may be autonomous or semi-autonomous, the computers actually "driving" the vehicles are connected to the outside world. As early as 2017, at least 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 who cooperate on research. This is a far cry from the time when a vehicle's computer was connected only to systems within the vehicle. Complex computer software has been used for years to power cars' performance, but those computerized brains are no longer walled off inside the cars themselves; they are now 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 where 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 has a 32-acre testing ground at Ann Arbor 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 enacted legislation regarding self-driving cars.

But autonomous vehicles are not stand-alone systems. Driverless cars communicate with each other using vehicle-to-vehicle ("VTV") technology. This communication allows vehicles to send each other data such as location, speed, and direction of travel using dedicated short range communications ("DSRC") with the data being updated and broadcast up to 10 times per second. Other data that may be exchanged include lateral acceleration, longitudinal acceleration, throttle position, brake status, steering angle, headline status, and the number of occupants in the vehicle. Traffic lights, in-ground sensors, and digital maps also will communicate with the cars. All of this data would be used to identify risks and provide warnings to vehicles.

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

- Reducing the number and severity of crashes caused by drivers or by other conditions such as weather, pedestrians, and road conditions,
- Reducing aggressive driving,
- Expanding the ability of the disabled and older users to drive, and
- Increasing 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. But drivers need not wait, because some autonomous technologies are available today. Tesla owners now can 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 has a self-driving feature, SuperCruise control, for highways. Jaguar Land Rover developed 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.

While there is no precise roadmap for the legal issues surrounding autonomous or connected cars, issues that are likely to arise include the following.

III. 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. While courts have not addressed vehicle-specific EULAs, courts generally enforce shrink-wrap agreements and EULAs when consumers have sufficient notice. Even if car buyers receive notice of EULAs, however, they are unlikely to read or understand them.

The vehicle's code also is generally protected by devices to prevent access, which means the anti-circumvention provisions of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. Sec. 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 as long as it does not violate other statutes. This exemption preserves the ability of car owners to work on their own vehicles as 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 manufacturers who claimed that the security research could be used by "bad actors" to hack into cars.

Some of a car's code may be available anyway because some developers use open source code. Open source code does not mean it is free code that a developer can use in any way he or she wants. Instead, open source code is licensed with restrictions as to its use and incorporation into other code. Depending on which open source license accompanies the code, different use restrictions apply. Using open source code may mean changes will need to be open to the public for others to use.

For example, under the GNU Lesser Public License all versions of a program remain as free software for all users to use and modify. Section 3 of the license (Version 3) provides that anyone using a "covered work" cannot forbid someone from accessing the source code when the program is conveyed. A "covered work" is either an unmodified program or a work based on a licensed program. "Convey" means "any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network with no transfer of a copy is not conveying." If the software is incorporated into a program that does not enable "other parties to make or receive copies," then its user does not "convey" the software under the license and would not trigger the requirement to disclose or provide access to the modified software.

Vehicle manufacturers and companies which manufacture vehicle components need to consider carefully how they incorporate open source software to avoid unintentionally waiving any intended copyright protection of their code.

IV. Cybersecurity, Data Protection, and Privacy

Because today's and tomorrow's cars are computers that happen to move physically on the roadway, they are subject to performance failures by inadequate design, malware, or 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 out intruders. 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 led by the 2014 Jeep Cherokee, which was hacked via Chrysler-Fiat's UConnect system and later recalled because of the car's vulnerability.

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."

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, who may have a duty to warn when hacks occur, just as consumers must be told when their personally identifiable information is compromised today.

As a result of the publicity surrounding the hacking of a Jeep Cherokee, legislation was introduced to establish cybersecurity standards for motor vehicles. Sen. Richard Blumenthal, one of the sponsors, 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." The measure failed to pass in the last session of Congress.

The National Highway Traffic Safety Administration ("NHTSA") has proposed rules for determining if cybersecurity vulnerabilities pose an "unreasonable risk to safety," requiring a vehicle recall. The NHTSA noted that vehicle software "presents its own unique safety risks." For example, "[w]here an autonomous vehicle or other emerging automotive technology causes crashes or injuries, or has a manifested safety-related failure or defect, and a manufacturer fails to act, NHTSA will exercise its enforcement authority to the fullest extent." To avoid NHTSA action, "manufacturers of emerging technology and the motor vehicles on which such technology is installed are strongly encouraged to take steps to proactively identify and resolve safety concerns before their products are available for uses on public roadways." The NHTSA would consider the following factors to determine if a vulnerability imposes an unreasonable risk to safety:

- The amount of time elapsed since the vulnerability was discovered (*e.g.*, less than one day, three months, or more than six months);
- The level of expertise needed to exploit the vulnerability (*e.g.*, whether a layman can exploit the vulnerability or whether it takes experts to do so);
- The accessibility of knowledge of the underlying system (*e.g.*, whether how the system works is public knowledge or whether it is sensitive and restricted);
- The necessary window of opportunity to exploit the vulnerability (*e.g.*, an unlimited window or a very narrow window); and

- The level of equipment needed to exploit the vulnerability (*e.g.*, standard or highly specialized).

The NHTSA said it is not necessary that actual hacking has occurred for it to initiate a recall, but a recall may be required if it is foreseeable that hackers will try to exploit the vulnerability. "For instance, if a cybersecurity vulnerability in any of a motor vehicle's entry points (*e.g.*, Wi-Fi, infotainment systems, the OBD-II port, or tire pressure gauges) allows remote access to a motor vehicle's critical safety systems (*i.e.*, systems encompassing critical control functions such as breaking, steering, or acceleration), the NHTSA may consider such a vulnerability to be a safety-related defect compelling a recall."

The Government Accounting Office ("GAO") in a report to Congress on vehicle cybersecurity noted the NHTSA's expectation that the threat of a vehicle cyberattack will increase "in the coming years as autonomous and connected-vehicle technologies are deployed." The GAO wrote that it "will be important for NHTSAQ to continue to take proactive steps in the interim to ensure that it is meeting the agency's goal of being ahead of vehicle cybersecurity challenges." But the GAO warned "until NHSTA defines and documents the agency's role and responsibilities in the event of a real-world vehicle cyberattack affecting safety-critical systems, it may not be in a position to quickly and effectively respond should a threat materialize."

The data from autonomous vehicles 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 premium rates not only for auto insurance but also life insurance. The Department of Transportation has identified several privacy considerations:

- Transparency. Consumers need to know what data is being collected and how the data will be used.
- Participation. Consumers need to 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.
- The data. If code and software are the heart of intellectual property protection for the Internet of things, then data is the payoff. Data is intellectual property that includes not only the method by which the data is obtained but also what the data discloses, which can be monetized.

But who owns the data? If I drive my car, or in the case of a self-driving car, it drives me, who owns the data generated? The data includes when I drove, where I drove, how fast I was driving, and how aggressive I was in my driving. This is great information for an insurance company to use in setting my premium. It also may be great information for health insurance rates. If I pass by a certain store every day, then would they like to send me a push notification on a sale? These questions also have privacy implications. Proper disclosure of what is being collected and how the information is being used is critical to avoiding legal liability.

The Alliance of Automobile Manufacturers, Inc. has proposed principles for the collection of personally identifiable information ("PII") via connected cars. The principles include seeking affirmative consent for collecting geolocational, biometrics, or driver behavior information.

Once the PII is collected, then the collecting and storing party will become exposed to liability in the event of a data breach, including costly data breach notices, which vary by state and federal regulatory agencies. On top of the notification requirements, there may be mitigation efforts and lawsuits for the privacy breach.

V. Liability and Insurance

While 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. It will be important to have access to software code to determine if an accident was caused by human error, mechanical failure, malware, or defective code. As discussed above, manufacturers may have an obligation to push out software updates, especially if a defect poses an "unreasonable risk to safety." Would a failure to update a software program expose a car manufacturer to liability in the event of an accident? Does this failure rise to negligence or a products liability claim? 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?

In addition, there is the question of whether the software developer has any liability at all if the program "learns" over time utilizing artificial intelligence ("AI"). If the AI program changes the software or logic that results in an accident, is the original programmer liable?

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? In May 2016, a 2015 Tesla collided with a white tractor trailer crossing an uncontrolled intersection in Florida. The car was operating in an "autopilot" mode. Neither the driver nor the car initiated any braking. In January 2017, a National Highway Traffic Administration examination "did not identify any defects in the design or performance of the AEB or Autopilot systems of the subject vehicles nor any incidents in which the systems did not perform as designed." If the systems performed as designed, then was the accident the driver's fault or should the design have included a way to keep the driver engaged to react when the autopilot was operating?

The handoff between driverless and driver modes creates its own problems. In a report, the Insurance Information Institute asked, "What kind of training will people need to safely handle these semi-autonomous vehicles? How well prepared will drivers be to handle emergencies when the technology returns control to the driver? How will beginning drivers gain the necessary experience and how will experienced drivers stay sharp enough when they are only infrequently called upon to react?"

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? But if there is no driver, 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, or at least fewer, driver-caused accidents. While fewer accidents may mean insurance companies will pay out less in the short term, in the long term insurance companies may have to reduce premiums. But some commenters question whether this is true. A recent report in the *New York Times* observed that no one knows for sure how many lives could be saved by driverless cars "because data on the role of human error in crashes is incomplete and misleading. The types of accidents we'll face in this automated future, in which cars are meant to run together in proximity at high speed, may be fewer, but they'll be new, different, unpredictable and, on occasion, larger and more grisly that the ones we know today."

VI. Conclusion

As vehicles move from human driver to semi-autonomous to driverless, there will be a reinterpretation of existing laws, new laws and regulations, and evolving liability issues that will affect manufacturers, suppliers, and insurance companies.