Autonomous Vehicles Offer a Ride into the Internet of Things

Presented at National Institute on the Internet of Things
Washington. D.C.
March 30-31, 2016

Richard C. Balough
BALOUGH LAW OFFICES, LLC
1 N. LaSalle St., Suite 2020
Chicago, IL 60602
312.499.000
www.balough.com

Autonomous Vehicles Offer a Ride into the Internet of Things

Presented at National Institute on the Internet of Things
Washington. D.C.
March 30-31, 2016

By Richard C. Balough[1]

If you drove a car to the office, took a cab, rode with Uber, or used public transportation, your trip was assisted by the internet of things.

Today's cars are part of the internet of things—computers on wheels connected to the internet. As the movement to autonomous vehicles continues, cars will be even more dependent on the internet.

Two car companies recently announced funding for research regarding how autonomous vehicle technology can be applied to the internet of things and artificial intelligence. Toyota Motor Corporation is providing funding to Stanford University and the Massachusetts Institute of Technology.[2] In a similar fashion, Tesla through its CEO, Elon Musk, also is contributing to the research project, named Open AI.[3] The long range goal of Open AI is to create an artificial general intelligence machine capable of performing any intellectual task that a human being can perform. "Artificial intelligence is one of the great opportunities for improving the world today. The specific applications range from self-driving cars, to medical diagnosis and precision personalized medicine, to many other areas of data, analysis, decisioning across industries," explained Reid Hoffman, one of the Open AI investors.[4]

While autonomous vehicles are but one aspect of the internet of things, an analysis of how they use the internet now and in the future can help lawyers understand some of the legal issues as the internet of things becomes dominant. Therefore, this paper focuses on autonomous vehicles as a proxy to explore some of these issues.

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.[5] 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

[1] Richard C. Balough is a founding member of Balough Law Offices, LLC, a Chicago-based law firm that focuses on cyberspace and intellectual property law. Mr. Balough is co-chair of the Mobile and Connected Devices Subcommittee of the Cyberspace Law Committee of the Business Law Section. He has written articles and participated on several panels about cyberspace law, including on autonomous vehicles. The firm's website is www.balough.com.

[2] Jonathan Vanian, "Toyota buckles down on artificial intelligence for safer driving," FORTUNE, Sep. 4, 2015, available at http://fortune.com/2015/09/04/toyota-artificial-intelligence-car-research.

[3] John Markoff, "Investors Start Center for A.I. Research," NEW YORK TIMES, Dec. 12, 2015.

[4] *Id*.

[5] Aaron M Kessler, "The Web-Connected Car Is Cool, Until Hackers Cut Your Brakes," NEW YORK TIMES, July 24, 2015.

brains were always walled off inside the cars themselves; they were not connected to the wider world.[6]

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 said. The National Highway Traffic Safety Administration plans in by mid-2016 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.
- 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 now available.[7]

Autonomous Vehicle Benefits

Currently under development are two types of vehicles: totally autonomous vehicles and semi-autonomous vehicles.

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 in conditions ranging from limited roadway environments ultimately to all roads. . . 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.” [8] While the vehicles themselves may be autonomous, the computers actually “driving” the vehicles are connected to the internet or communicate via Wi-Fi with other vehicles as well as other data sources required for safe operation.

[6] *Id*.

[7] https://www.transportation.gov/briefing-room/secretary-foxx-unveils-president-obama%E2%80%99s-fy17-budget-proposal-nearly-4-billion.

[8] Denardo, Zmud, Shaldover, Smith, and Lappin, Transportation Research Board of the National Academies, “Automated Vehicle Technology, Ten Research Areas to Follow,” TR NEWS, available at http://onlinepubs.trb.org/onlinepubs/trnews/trnews292.pdf.

Semi-autonomous vehicles are vehicles that are not totally driverless but allow for both vehicle-to-vehicle and vehicle-to-fixed object communications. This technology enables vehicles to avoid accidents at intersections or to follow other vehicles on highways with appropriate spacing. Some truckers are experimenting with caravans where only the lead truck has a driver.

It is probable in the near future that roadways will have side-by-side vehicles some with drivers remaining in total control, some with automated driver assistance, and some fully autonomous vehicles with no drivers. One of the biggest challenges is blending them into a world in which humans do not 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.[9]

To conduct testing, the State of Virginia has designated 70 miles of roads in Northern Virginia for autonomous cars. The University of Michigan has a 32-acre testing ground at Ann Arbor specifically designed for researching self-driving cars, which includes 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.[10]

It's estimated that, by 2035, 75 percent of vehicles sold worldwide will have some degree of autonomous capability.[11] But drivers need not wait because some autonomous technologies are available today. For example, Tesla owners can wirelessly download a new autopilot feature as a software update. The 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."[12] Tesla officials nevertheless urge drivers to keep at least one hand on the wheel at all times.

Audi says 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.[13]

Vulnerabilities

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. As noted earlier, while computers in cars are not new, the fact that they are connected to the world is new. Hackers have attacked this new functionality and demonstrated that it is possible to take over today's cars because most

[9] "Matt Richtel and Conor Dougherty, Driverless Car's Nemesis? Drivers" NEW YORK TIMES, Sep. 2, 2015.

[10] Dino Grandoni, "Wooing Driverless Cars with Open Roads and Fake Towns," NEW YORK TIMES, Aug. 10, 2015.

[11] Navigant Consulting, "Three-Quarters of Vehicles Sold in 2035 Are Expected to Have Autonomous Capability," Nov. 6, 2014, available at https://www.navigantresearch.com/newsroom/three-quarters-of-vehicles-sold-in-2035-are-expected-to-have-autonomous-capability.

[12] Kessler.

[13] Dino Grandoni, "Selling the Self-Driving Car, at 120 M.P.H.," NEW YORK TIMES, July 17, 2015.

vehicles do not even have basic firewalls to keep out intruders. As a result, 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.[14] There are even lists of the most hackable cars on the road, led by the 2014 Jeep Cherokee, which was hacked via Chrysler-Fiat's UConnect system and later recalled because of its vulnerability.[15]

As a result of the publicity surrounding the Cherokee hacking, legislation was introduced to establish cybersecurity standards for motor vehicles to prevent hacking.[16] 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."[17]

Copyright

The millions of lines of software code that control autonomous or semi-autonomous vehicles may be protected by copyright. Similar to the licensing of other software, new cars come with end-user license agreements (EULAs) to protect the code from copying. While courts have not yet addressed vehicle-specific EULAs, courts generally enforce shrink wrap agreements and EULAs.

The vehicle's code also is 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. When parties sought to include vehicle software as an exemption to the DMCA's anti-circumvention provision, automakers objected claiming that permitting access "to automotive software is likely to have uniquely long-lasting and far-reaching, harmful effects."[18]

In October, the U.S, Copyright Office Library of Congress, granted two exemptions for when circumvention would be fair use.[19]

The first exemption allows an "authorized owner" to diagnose, repair, or "lawfully" modify the code as long as such modification does not violate other statutes. This exemption retains 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 or 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." This

[14] Lucus Mearian, "Firewalls can't protect today's connected cars," COMPUTERWORLD, July 24, 2015.
[15] "The Most Hackable Cars on the Road," available at www.ptclwg.com/resources/Hackable-Cars_8-19.png.
[16] The Security and Privacy in Your Car Act of 2015 or SPY Car Act of 2015.
[17] Kessler.
[18] Comments of Association of Global Automakers, Inc. Regarding Exemption for Proposed Class 22 from Liability Under 17 U.S.C. 1201, Docket No. 201407 filed with the Library of Congress.
[19] http://copyright.gov/1201/2015/fedreg-publicinspectionFR.pdf.

exemption was unsuccessfully opposed by car manufactures who claimed that the security research could be used by “bad actors” to hack into cars.

The Copyright Office has delayed the implementation of the exemptions for 12 months to allow the Environmental Protection Agency and the Department of Transportation to issue rules regarding what software modifications would be prohibited, such as disabling pollution control software.[20]

Data Protection and Privacy

The increased connectivity needed to direct autonomous vehicles means that unprecedented amounts of data will be generated, requiring new methods to collect, transmit, sort, store, share, segregate, analyze, and apply the data to manage and operate these systems.[21] Because autonomous vehicles cars are connected to the internet and Wi-Fi, they are vulnerable to hacking. As one cybersecurity consultant said, “Almost all OEMs 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.”[22]

Several issues regarding the data generated and collected need to be addressed. 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? Driving habits could be used to determine premium rates for not only 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 the specified purposes.
- Security. Consumers should know what physical, technical, and procedural measures will be taken to protect their data.[23]

[20] *Id.*

[21] ITS 2015-2019 Strategic Plan, U.S. Department of Transportation at 21, available at www.its.dot.gov.

[22] Charlie Osborne “Automakers need to make security ‘part of the conversation,’” Zero Day, July 7, 2015, available at http://www.zdnet.com/article/automakers-need-to-make-security-part-of-the-conversation.

[23] 2015 Federal Highway Administration Vehicle to Infrastructure Deployment Guidance and Products, Sep. 29, 2014, available at http://www.its.dot.gov/meetings/pdf/V2I_DeploymentGuidanceDraftv9.pdf.

Liability and Insurance

The issues relating to hacking into autonomous vehicles are not limited to protecting copyrighted code. Hacking also presents a liability concern. 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 widespread damage and fear.[24] 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? "Automakers will need to be watching this around the clock to spot threats right away. And we could see warnings for drivers as well, when suspected intrusions are detected."[25]

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. 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?

The ability to hack into a vehicle and bring it to a stop can be used for other purposes. For example, law enforcement used a vehicle's OnStar program to disable a stolen car during a high speed chase.[26] In addition, the technology has aided the repossession industry by disabling a car's engine when a car loan is past due.[27]

Autonomous cars may require the rethinking of insurance. Today, drivers are insured. But if there is no driver, who or what would be insured? One potential benefit of driverless cars is that there will be no driver-caused accidents. While fewer accidents mean the insurance companies pay out less in the short term, "it becomes detrimental to the rate insurers will be able to charge," said one securities analyst for the auto insurance industry.[28]

Also to be determined is who to identify as the driver of a driverless car? For example, the self-driving vehicles (SDV) being developed by Google, Inc. lack, among other things, steering wheels, accelerators, and brake pedals because the cars are controlled by a self-driving system (SDS). Google asserts that allowing humans to operate the vehicles' systems could be detrimental to safety because humans could attempt to override the SDS. Google asked the

[24] Cheryl Dancey Balough and Richard C. Balough, "Cyberterrorist On Wheels: Are Today's Cars Vulnerable to Attack?" BUSINESS LAW TODAY, Nov. 2, 2013, http://www.americanbar.org/publications/blt/2013/11/02_balough.html.

[25] Kessler.

[26] "Cops use OnStar to disable suspect's engine and end high-speed chase," SOUTH BEND (IND.) TRIBUNE, Jan. 21, 2016, http://www.southbendtribune.com/news/publicsafety/cops-use-onstar-to-disable-suspect-s-engine-and-end/article_33029180-bfb7-11e5-9667-1f1e3bb2f345.html.

[27] Michael Corkery and Jessica Silver-Greenberg, "Miss a Payment? Good Luck Moving That Car," NEW YORK TIMES, Sep. 24, 2015, http://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car.

[28] Becky Yerak, "Will driverless cars total insurance industry?" CHICAGO TRIBUNE, July 28, 2015.

National Highway Traffic Safety Administration to clarify if its SDV complies with the Federal Motor Vehicle Safety Standards.

“We agree with Google its SDV will not have a ‘driver’ in the traditional sense that vehicles have had drivers during the last more than one hundred years,” Chief Counsel Paul Hemmersbaugh wrote in response to Google’s questions, “If no human occupant of the vehicle can actually drive the vehicle, it is more reasonable to identify the ‘driver’ as whatever (as opposed to whoever) is doing the driving. In this instance, an item of motor vehicle equipment, the SDS, is actually driving the vehicle.”[29]

The current safety standards define a driver as an occupant, who must be seated in the left front of the vehicle. This creates a problem for Google’s SDV, which has no occupant performing any function. For example, the standards require that brakes must be activated via a foot control. The SDV has no brake pedal for a foot to engage. The SDS obviously has no foot. Google argued that it would not be necessary or beneficial for safety for a human occupant to be able to brake the vehicle. The NHTSA responded that, even though the SDS may be programmed to perform braking, it does not overcome the plain language of the rule. As a result, Google’s system “would not comply” with the braking rule as written. The letter cited several other standards that require human intervention, which cannot be met by the SDS.

Conclusion.

Autonomous vehicles will require reinterpretation of existing laws and monitoring of legislative changes. Fasten your seatbelt; it will be an interesting ride.

[29] http://isearch.nhtsa.gov/files/Google%20--%20compiled%20response%20to%2012%20Nov%20%2015%20interp%20request%20--%204%20Feb%2016%20final.htm