Chapter 1

Connected Cars
Impact on Cars and Other Intelligent Transportation Systems

Stephen S. Wu

I. Introduction
The Internet of Things (IoT) connects machines to other machines in a wide variety of fields and industries. In our digital lives, we are connecting devices to our networks at work and at home. In addition to work and home, however, we spend much of our waking time in transit from one place to another, often in our private automobiles. The Internet of Things is extending our digital lives to our cars, trucks, and other road vehicles. With this new integration comes privacy, security, and other legal issues.

A 2015 episode of the CBS television show 60 Minutes vividly illustrates what can happen when we connect cars with information technology networks. In the show, reporter Lesley Stahl sat behind the wheel of a nondescript dark gray sedan while driving through a tree-lined suburban parking lot. She appeared on a 60 Minutes segment that aired on February 8, 2015.¹ In the driver’s seat next to her was Kathleen Fisher, a veteran of the Defense Advanced Research Projects Agency or DARPA for short. As Stahl navigated

¹ A preview of the segment is available on YouTube. 60 Minutes, Preview: DARPA Dan (Feb. 6, 2016), https://www.youtube.com/watch?v=7E1WsdODxu0.
one end of the cleared parking lot, two men stood at the other end—Karl Koscher, a University of Washington Ph.D. student, and Dan Kaufman, who was then director of DARPA’s Information Innovation Office. Koscher used a laptop sitting on black boxes of what appeared to be equipment, while Kaufman provided instructions.

Kaufman told Koscher, “You wanna hit the fluids?” Koscher typed something on the laptop and suddenly the windshield wiper fluid sprayed onto the windshield of Stahl’s car and the wipers started moving back and forth. Stahl said “I did nothing” to turn on the spray. And yet, without Stahl doing anything, Koscher had taken control of the wipers and fluid. In a cut-away scene, Stahl explained that hackers had contacted the car’s emergency communications system, flooded it with sound data, and inserted a piece of code that reprogrammed the car’s software so the researchers could take complete remote control of the car. Further demonstrating this control, Koscher caused the horn to sound, again without Stahl’s knowledge or action.

Fisher then instructed Stahl to drive up to a set of cones in the lot and stop in front of them. As Stahl drove forward, at Kaufman’s direction, Koscher disabled the brakes remotely. A close-up showed Stahl’s black pump shoe pressing down on the brake pedal. Nonetheless, the brakes would not work and Stahl called out “Oh, no. No. No. No. No. No. No!” Notwithstanding Stahl’s vigorous attempt to apply the brakes, the car wouldn’t stop and instead bowled over the cones Stahl was trying to avoid.

This television segment showed the vulnerability of contemporary cars to hacking. Cars are increasingly connected to various kinds of communications systems. While connected cars have the promise of making our lives easier, safer, more comfortable, and more entertaining, connecting information technology to cars also has a dark side. In the future, with even tighter integration of cars with external information technology systems, security risks will only increase. Moreover, security vulnerabilities give rise to legal
Chapter 1 Connected Cars

issues, and data security raises just one set of issues. This chapter covers various issues attorneys are likely to face in coming years and decades with the sale and deployment of connected car technologies and other intelligent transportation systems.

II. Overview

Welcome to the future of intelligent transportation. The era of connected transportation is already underway. Within the next ten years, we will increasingly connect our on-road motor vehicles—cars, trucks, and other vehicles—to networks, both public and private.

Connecting cars, trucks, and other vehicles to the Internet of Things is part of the picture of the future of intelligent transportation systems. In the narrowest sense, the IoT involves connecting electronic devices to the public Internet. Accordingly, vehicles can become part of the IoT if manufacturers and owners connect them to the public Internet. For example, connections may involve pushing new software to vehicles through the Internet or manufacturers collecting data via the public Internet from the vehicles they sell to understand how purchasers use them and the vehicles’ performance. Connectivity may be embedded, requiring the car to have one or more antennas and communications chips, or an operator may be able to connect a device already connected to the Internet, like a smartphone, to the vehicle by tethering.

2. See Jacob Morgan, A Simple Explanation of “The Internet of Things,” FORBES (May 13, 2014, 12:05 AM) (“Simply put, this is the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other).”), https://www.forbes.com/sites/jacomorgan/2014/05/13/simple-explana nation-internet-things-that-anyone-can-understand/#230c65351d09.


4. See id.
Nonetheless, direct and indirect networking and connectivity beyond the public Internet are also possible. Other examples of connectivity include:

- Connecting vehicles by closed information technology networks (e.g., “walled gardens,” so that they are separated from the public Internet).
- Unconnected sensors and systems that collect data aboard the vehicle, which are accessed sometime after data gathering for the purpose of downloading or transferring the data to other systems for analysis.
- Connected sensors aboard the vehicle that communicate only with special purpose communications devices, such as devices to read information from event data recorders (black boxes), which are in turn connected to the public Internet or closed networks.

Machine-to-machine communications covered by this chapter may include communications that occur over the public Internet, private wired networks, cellular wireless networks, Wi-Fi, radio, or satellite systems.

Regardless of the type of connectivity, we are connecting our vehicles for a number of reasons. Some of the connections will assist in the task of driving, such as providing navigation assistance, warnings, traffic information, and eventually coordinated automated driving systems of all aspects of the dynamic driving task for autonomous driving. We already have systems to connect cars to roadside assistance services to obtain help after an accident or other event. Other connections will facilitate occupant communications, including text, voice, and video communications. Fleet owners are already capable of using communications to track the location of fleet vehicles. Additional applications will focus on entertainment systems, integrating onboard systems with offboard media and preferences. Some cars already serve as Wi-Fi hotspots,
which manufacturers market to families to enable entertainment, social media, and other personal uses. Manufacturers will work together with technology companies to expand these capabilities for personal and business productivity, such as integrating navigation and communication systems with personal calendars. Yet other connections will integrate vehicles with other smart systems, including smart home and smart city systems. In short, our digital lives will extend to our cars and other vehicles, integrating them with numerous information technology systems, and making them, in essence, another mobile computing platform.

While connected transportation systems have the potential to increase road safety, improve traffic, save energy, entertain us, promote efficient fleet operations, and increase our personal and business productivity, advanced systems also pose risks. Recent crashes of partially automated vehicles show risks associated with automation. For instance, on March 18, 2018, an Uber test car driving in autonomous mode, with a safety driver in the vehicle, struck and killed a woman walking a bicycle across a street in Tempe, Arizona. Volvo and Uber worked together on the autonomous driving system controlling the car, although unfortunately, Volvo’s default advanced collision avoidance technology was not enabled in the car. While the Uber vehicle was not centrally controlled, it was a “connected car” in the sense that it communicated with the satellite-based GPS system to monitor its location.

Failures in connected transportation systems will inevitably cause accidents. Moreover, information technology systems in ground vehicles may distract human drivers and cause other accidents. Accidents will, in turn, generate legal issues and litigation. Aside from accidents, various kinds of legal issues involved with connected transportation systems will arise in connection with the manufacture, distribution, sale, and operation of connected transportation systems.

This chapter discusses the legal issues arising for lawyers counseling sellers and operators of connected transportation systems.
Section III provides an overview of technologies for connecting on-road motor vehicles. Section IV covers the regulation and governance of connected transportation and the compliance issues raised by such regulation. It explains the key laws that place requirements on sellers and operators. Section V focuses on liability arising from the sale and operation of connected transportation systems. This section describes the various types of claims that can create liability, possible defenses, and techniques for managing risk. Section VI discusses data protection, including privacy and security risks. Finally, Section VII concentrates on transactional issues relating to connected transportation technology.5

III. Overview of Connected Transportation Technology

“Connected” motor vehicles make use of a number of different IoT and other technologies. The communications technologies that are and will connect motor vehicles in the future include:

- Wired Internet and private network connections to the vehicle
- Wi-Fi connecting the vehicle to the Internet or private networks

5. This chapter covers on-road motor vehicles: cars, trucks, motorcycles, buses, shuttles, and recreational vehicles. The focus of this chapter, “connected transportation systems,” includes the on-road motor vehicles themselves as well as supporting information technology systems to facilitate communications, computing, and intelligence on the vehicle or in supporting communications infrastructure. This chapter does not cover connected bicycles and scooters, although sharing services for bicycles and scooters are becoming increasingly common. Farm equipment and off-road vehicles, such as racing motorcycles, trail bikes, mini bikes, dune buggies, all-terrain vehicles, jeeps, and snowmobiles, are outside the scope of this chapter. This chapter focuses on ground vehicles, rather than airborne or maritime vehicles, which have different regulators and laws than ground vehicles. Nonetheless, some of the general principles in this chapter may be helpful to manage legal issues of vehicles and transportation systems beyond the scope of this chapter.
Cellular communications, including allowing the vehicle to create its own local Wi-Fi hotspot.

- Bluetooth, such as keyless entry systems or allowing consumer mobile devices to connect with the vehicle.
- Dedicated short-range radio communications (DSRC), which facilitates high bandwidth data transmission for safety applications.\(^6\)
- Satellite communications, including receivers on vehicles that can receive data from global positioning system (GPS) satellites.\(^7\)

The main applications for connecting motor vehicles include:

- **Driving automation.** Partially automated and autonomous vehicles will, as a practical matter, need connectivity to receive GPS location data and updated maps. In the future, they will also coordinate with other vehicles and coordinate with traffic management supervision systems to allow traffic to flow more efficiently.
- **Vehicle operation.** Examples include keyless entry systems and smartphone-operated remote unlocking and starting.

---

\(^6\) DSRC can enable vehicle-to-vehicle (V2V) communications, for instance to signal location and speed to alert other vehicles. DSRC can also enable vehicle-to-infrastructure (V2I) to communicate alerts and traffic information to operators. Other communications are possible, such as vehicle-to-pedestrian (V2P) and vehicle-to-network (V2N). Collectively, these forms of communication are referred to as “vehicle-to-everything” (V2X). Siam Ahmed, *Get to Know Connected Vehicle Technology: V2V, V2X, V2I* (Feb. 9, 2018), https://www.geotab.com/blog/connected-vehicle-technology/. Likewise, information from cars can feed back to traffic management supervision systems to adjust traffic light timing and set variable speed limits.

\(^7\) GPS systems allow motor vehicles to locate themselves with a high degree of accuracy. Satellite radio receivers in vehicles can utilize sideband channels to receive data such as firmware updates and more in bulk.
Part I New and Emerging IoT Technologies

- **Operation safety.** Examples include coordination with a central traffic management facility, other vehicles, and pedestrians.
- **Updates and maintenance.** Motor vehicles are already making use of connections to update their software.
- **Entertainment.** Connections allow operators to integrate their sources of entertainment media with the motor vehicle to enjoy during travel and facilitate Internet connections.
- **Personal productivity.** Manufacturers are working on the integration of personal productivity applications (such as calendar apps) with motor vehicle systems.
- **Smart home integration.** Operators will be able to monitor events in their homes and control home automation devices using integration with smart home systems.
- **Smart city integration.** Communications can allow municipal systems to monitor traffic and drivers can use apps to use city services, such as automatic parking payments.

IV. Regulation and Governance of Connected Transportation Systems

A. Backdrop of Regulating and Governing Driving Practices and Motor Vehicle Safety

Regulation of operating motor vehicles in the United States consists of a mixture of state, federal, and international law. The states have vehicle codes that govern the rules of the road and the safe operation of motor vehicles on highways. They have requirements for drivers to act safely, and state vehicle codes prohibit driving unsafe vehicles on state highways. Federal law, principally

---
8. State vehicle codes may contain specific incompatible requirements regarding certain aspects of vehicle operation, such as emissions requirements, use of certain types of lighting and equipment, and traffic laws (e.g., permitting right turns on red lights).
through Federal Motor Vehicle Safety Standards, governs the safety of motor vehicles themselves. The United States is also a signatory to the Geneva Convention on Road Traffic. The Geneva Convention harmonizes traffic laws among the signatory nations and establishes certain minimum standards for operating motor vehicles. Manufacturers need to make sure that any connected vehicle systems they install in their vehicles will comply with these laws.

In addition to applicable law, manufacturers may work among themselves and industry groups to establish technical standards to facilitate safety, interoperation, and efficiency. Technical standards may establish protocols and methods of implementing certain technologies. Organizations such as the International Organization for Standardization (ISO), Institute of Electrical and Electronics Engineers (IEEE), SAE International, and Underwriters Laboratories (UL LLC) establish these standards. Manufacturers may need to adhere to these standards in order to sell their connected car products.

B. Regulating Communications with and among Vehicles

The federal government has established a program overseen by the Federal Communications Commission (FCC) and the Department of Transportation (DOT) to regulate dedicated short-range radio communications (DSRC) used for vehicle-to-vehicle communications and vehicle-to-infrastructure communications. The FCC sets aside and allocates radio frequency spectrum based on


its rulemaking authority under the Communications Act of 1934, as revised under the Telecommunications Act of 1996. The Federal Communications Commission reserved 75 MHz of spectrum around the 5.9 GHz band in 1999 for DSRC communications. Manufacturers seeking to sell connected vehicle systems and infrastructural base station systems will need to comply with FCC rules.

C. Truck Platooning Legislation

Connecting freight trucks with connected systems permits trucks to coordinate the driving function. Platooning allows two or more trucks to form ad hoc groups traveling down a highway in which the acceleration and braking is coordinated. A cloud-hosted network operations center communicates with trucks to coordinate creating or dissolving platoons. Drivers continue to be responsible for the steering function. But the lead truck sets the pace for speed. And if the lead truck driver applies its brakes, the following trucks automatically brake. With this coordination using vehicle-to-vehicle communications, trucks can follow each other much more closely. Closely coordinated travel reduces air resistance and thus saves fuel. It also improves safety.

Currently, 16 states have laws that exempt platooning trucks from laws against following too closely or otherwise allow platooning.11 One other state allows testing and pilots for platooning.12

---
