Legal Outlook for Autonomous, Automated, and Connected Cars

A Preview of First Generation Autonomous Cars

Federation of Defense & Corporate Counsel Annual Meeting

Fairmont Banff Springs, July 25 to August 1, 2015

Presented by:
Professor Dorothy J. Glancy
Santa Clara University School of Law
Santa Clara, California
Professor Dorothy J. Glancy obtained her undergraduate degree from Wellesley College in 1967, and her law degree from Harvard Law School in 1970. She was also a postgraduate Fellow in Law and the Humanities at Harvard University (1974-1975). She is admitted to the practice of law in California and the District of Columbia and practiced law in Washington, D.C. She is currently Professor of Law at Santa Clara University School of Law.

Professor Glancy specializes in law and technology issues, particularly matters related to transportation and land use, including Intelligent Transportation Systems. She is currently under contract to the Transportation Research Board of the National Academies of Sciences to write a legal research report, "A Look at the Legal Environment for Driverless Vehicles", which will be published later this year.

She has served as a member of the National Academies of Sciences Committee on the Long-Term Stewardship of Driver Safety Data (SHRP 2) and were the principal investigator and director of a multi-year legal research project regarding the impact of intelligent transportation systems (ITS) on privacy. She assisted in the development of the United States Department of Transportation’s Vehicle Infrastructure Integration (VII) program for which she drafted the VII Privacy Policies Framework (2004). She has served as a consultant to the Vehicle Safety Communications Consortium 3 (VIIC) and assisted Cambridge Systematics in preparation of a Rural Interstate Corridor Communications Study Report to Congress for the Federal Highway Administration. In California, she has worked with the San Francisco Bay Area’s regional transportation agency, the Metropolitan Transportation Commission, on the design and operation of traffic surveillance aspects of the FasTrak toll-tag-based traffic information collection system.

Her research has included an international comparative study of “Privacy Protection in Traffic Surveillance Cyberinfrastructures,” comparing United States, United Kingdom and Japanese practices regarding traffic surveillance. She has written extensively about Event Data Recorders that are now standard equipment in all new vehicles in the United States. She has also worked with the American Association of Motor Vehicle Administrators with regard drivers’ and vehicle licenses. Her seminal article, “Privacy in Autonomous Vehicles” reflects some of her work with regard to autonomous cars.
Professor Glancy practiced law in Washington, D.C. and served as counsel to the United States Senate Judiciary Subcommittee on Constitutional Rights. She also served in the Office of General Counsel of the United States Department of Agriculture. A Life Member of the American Law Institute, Professor Glancy was an adviser to the Restatement, Third, of Property: Servitudes. She is a Research Fellow of the Gruter Institute for Law and Behavioral Research and has served as a member of the Council of the American Bar Association Section of Natural Resources, Energy and Environmental Law. She also chaired sections on Environmental Law, Property Law and Privacy Law of the Association of American Law Schools and was a member of the Executive Committee and an advisor to the State Bar of California Environmental Law Section. She is a member of the California Judicial Council's Information Technology Advisory Committee.
Legal Outlook for
Autonomous, Automated, and Connected Cars:
A Preview of First Generation Autonomous Cars

Professor Dorothy J. Glancy
Santa Clara University School of Law

Having dispensed with human drivers, first generation autonomous cars in the United States will share the road with conventional vehicles, operated in whole or in part by human drivers. This transition to autonomous road transportation will encounter a number of legal issues along the way. Some of these legal issues may turn out to be avoidable potholes, some may seem to be roadblocks; others will be just bumps in the road. It is wise to look out for them.

Sometime within the next decade, autonomous cars will join conventional automobiles, operated by human drivers. We do not now know how many people will decide to forego human driving for autonomous cars. Many people will likely stay with conventional cars, which by then will be highly automated, partially autonomous, connected and generally advanced beyond the conventional cars we drive today. Preferences for enhanced safety will compete with preferences for being in control of a powerful machine. Desires for amelioration of traffic delays will contend with desires to personally manage how one gets from here to there. Legal ramifications of autonomous car use will also be important. Exactly how the legal system will change to accommodate autonomous cars remains somewhat uncertain, partly because of confusion about just what an autonomous car is.

Partly automated, semi-autonomous, and connected vehicles with human drivers will have been on the road for some time before autonomous cars without human drivers join them. It is nearly certain that the first generation autonomous cars available to consumers will look similar to conventional vehicles on the road at the time. Regulatory frameworks requiring safety features, such as bumpers, and fuel economy would apply to autonomous and conventional vehicles alike. Of course, some internal components of first generation of autonomous vehicles will be different and some of the external sensors may be visible. It is unclear whether there will still be some form of dashboards, steering wheels, accelerator and brake pedals. Autonomous car engines and drive trains will likely be similar to those of conventional cars, unless federal regulations require a particular engine type for all autonomous cars. One feature now present in all conventional cars may be entirely absent from some first generation of autonomous cars – that is the presence of a human being.

The first generation of fully autonomous passenger vehicles to reach consumer markets in the United States will be transitional. They will share many
passive safety features with conventional cars because most of the other vehicles they encounter will be conventional vehicles. Decades from now, far more advanced autonomous vehicles could be configured very differently from any car we know now. Before then, society and the legal system will need to transition autonomous vehicles into the flow of traffic. That first generation of autonomous cars is the focus of this discussion.

I. TERMINOLOGY

A tangle of terminology confronts legal policymaking about autonomous cars. There is not even basic agreement about what to call autonomous cars. “Cars” seems to work in talking about passenger automobiles used for personal transportation. But there is no consensus about whether to refer to cars that operate without human drivers as autonomous cars or as driverless cars or as self-driving cars. At the moment, autonomous seems the most useful moniker because it encompasses both driverless and self-driving. Unfortunately, over the past few years “autonomous” has begun to be used, perhaps because of its high-technology cachet, to refer to varied applications of automated vehicle systems - from electronic stability control to automatic lane keeping and braking systems. Common parlance sometimes uses “autonomous” to refer to part-time operation of vehicles by intelligent systems that control some or all vehicle operations for part of a journey or in a specific roadway environment. Examples of useful, but not fully autonomous vehicle technologies include General Motors’ “Super Cruise” and Tesla’s promised “Autopilot.” Both of these brand-associated features are variously described as autonomous, semi-autonomous, and partly autonomous. And yet, a human driver remains legally required to be present and capable of taking operational control of these vehicles at all times. Highly automated vehicle functions and limited self-driving capabilities are valuable and useful developments. Nevertheless, they do not make cars having such automated features fully autonomous, in the sense of dispensing entirely with a human driver.

For many advanced automotive systems developers, “autonomous” has become sufficiently ambiguous that standard-setting and regulatory bodies avoid using it in favor of “automated.” In fact, there are two separate versions of vehicle automation levels. For both of them, the fully autonomous cars that are the focus of this discussion are at the highest level of full automation - meaning that the vehicle is in complete control of all driving functions at all times. In January 2014, SAE International published a “Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems” as SAE Standard J3016. In 2013, the National Highway Traffic Safety Administration
(NHTSA) had suggested slightly different vehicle automation levels in the agency’s 2013 “Preliminary Statement of Policy Concerning Automated Vehicles.” The two competing sets of categories, or levels, are:

<table>
<thead>
<tr>
<th>SAE Automation Levels</th>
<th>NHTSA Automation Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - No Automation</td>
<td>Level 0 – No Automation</td>
</tr>
<tr>
<td>1 - Driver Assistance</td>
<td>Level 1 – Function-specific Automation.</td>
</tr>
<tr>
<td>2 - Partial Automation</td>
<td>Level 2 - Combined Function Automation</td>
</tr>
<tr>
<td>3 - Conditional Automation</td>
<td>Level 3 - Limited Self-Driving Automation</td>
</tr>
<tr>
<td>4 - High Automation</td>
<td>Level 4 - Full Self-Driving Automation</td>
</tr>
<tr>
<td>5 - Full Automation</td>
<td></td>
</tr>
</tbody>
</table>

Existing vehicle automation under the SAE categories is within levels 2-3, with the top level 5 far into the future. Under NHTSA categories, currently available technologies are at level 2, and are moving into level 3, but are not yet close to the top level 4 of fully autonomous operation. The NHTSA levels tend to be used by federal and state regulators. Vehicle manufacturers tend to refer to the SAE categories, which are similar to vehicle automation categories used in Europe.

One interesting feature of these two sets of categories is the possibility they suggest that partly automated vehicles, or limited autonomous driving may be sufficient for many vehicle purchasers for quite some time. There may turn out to be what might be called a consumer market “stickiness” at levels of automation less than fully autonomous driving, at which consumers are comfortable with considerable driver assistance, but still want to be drivers in control of their own cars. Car buyers, whose adolescence was typically crowned by acquiring a driver’s license, may not be as eager to leave car operation to the car. As a result, it may be many years before first generation fully autonomous cars significantly penetrate actual consumer markets. Todd Litman, “Autonomous Vehicle Implementation Predictions: Implications for Transport Planning” (Jan. 29, 2015) projects:

![Table 6: Autonomous Vehicle Implementation Projections](image)

It also seems possible that some of the “stickiness” in market demand for autonomous cars will reflect legal uncertainties and risks. With a human driver in the control/responsibility loop, most existing legal rules would continue to apply.
Legal consequences of having no human driver in control, or potential control, of a passenger car will be pervasive. In some areas of law, such as vehicle regulation and insurance, entirely new specialized legal regimes will be necessary before first generation autonomous cars can legally operate on public roads. In other areas of law, the legal system will gradually adapt to partially automated or part-time self-driving vehicles. That gradual phasing-in will help to pave the way for some of the more fundamental legal changes needed before the first generation autonomous cars will be permitted to operate on United States roadways.

II. POTENTIAL USES

Slightly different legal rules and policies will respond to different ways in which first generation autonomous vehicles are used. Many experts predict that only high-end vehicle purchasers will initially be offered autonomous cars, which are initially likely to be expensive and few in number. According to Morgan Stanley analyst Ravi Shankar, at today’s prices, full autonomous capability is estimated to add about $10,000 to the cost of a car.” (Morgan Stanley Blue Paper: “Autonomous Cars: The Future Is Now, “Jan. 23, 2015). Still, there appears to be a wide range of potential uses for first generation autonomous cars, including

- Individually-owned personal/family cars;
- On-demand personal-mobility-service cars;
- Rental cars for short term mobility and transport needs;
- Commercial local delivery services;
- Paratransit autonomous cars (disabled services).
- Fleets owned by corporations or other entities for corporate use.

Factors that are likely to encourage market interest in purchasing and using autonomous cars will include safety, convenience, and efficiencies such as multi-tasking. Repeated journeys along the same roads; availability of real-time mapping of roadways and traffic conditions; congenital slow-moving traffic and traffic congestion are all likely to stimulate market interest in the first autonomous cars, as will preferences for personal mobility without a human driver. Suburban and urban settings are likely to be more favorable environments for autonomous cars than rural and remote areas, where accurate and timely roadway mapping/sensing and other infrastructure may be scarce and uneconomic. Among the factors likely to discourage interest in first generation autonomous cars are cost, queasiness about loss of control; roadway risks involving both the infrastructure and non-vehicle road users (pedestrians, bicycles, etc.); and safety risks from other non-autonomous vehicles. It is unclear whether autonomous cars will be preferred for long or short journeys. However, to the extent that
autonomous cars are confined by reliance on continuously updated mapping of local roads, they may be confined to local areas. At least initially, a wider regional and national range of operation for autonomous cars may be unavailable until additional mapping data becomes available.

In order to minimize legal risks that may result from personal injuries, property damage and other adverse interactions, the earliest use of first generation autonomous cars may be in controlled environments, and possibly segregated roadways, where unpredictable events such as unexpected pedestrians, road closures, unanticipated road construction or repairs are infrequent and known in advance. For example, Google, Inc.’s two-person low speed autonomous cars will apparently be designed for such protected applications.

At the end of 2014, Google announced that its prototype autonomous car was production-ready. Google, Inc. is building a fleet of small, low-speed vehicles that the company intends to license in California, once the California Department of Motor Vehicles has adopted operational regulations. Google, Inc. managers note that the corporation does not plan to go into the business of autonomous car manufacturing. Rather, at least initially, the corporation plans to have autonomous cars built for use primarily by employees on and around the corporation’s campus. For regulatory purposes, the cars will be categorized as low-speed vehicles (LSVs) limited to top speeds between 20 and 25 miles per hour. NHTSA regulates these LSVs under a special regulatory category for low speed vehicles, such as golf carts under Motor Vehicle Safety Standard No. 500, which authorizes smaller, lighter vehicles.

Whether such an application characterized by limited, protected, and well-mapped routes is likely to be extrapolated to broader consumer uses remains to be seen. If consumer models of autonomous cars are limited to the LSV regulatory category encompassing small, light, low speed vehicles, the potential consumer market may be limited to retirement and other planned communities that emphasize alternatives to conventional automobiles. On the other hand, in some large cities, such as New York, the maximum speed limit is already 25 miles per hour. In such congested areas, small, low-speed, few-passenger autonomous cars could be useful for local trips.

When consumers are asked about the application of autonomous cars most people want to be available first, consumers often choose on-demand personal mobility services. The name for Google’s autonomous vehicle project - “chauffeur” - reflects this attraction. On-demand autonomous car services would provide convenience and privacy in transporting people to and from local destinations. Existing ride-share applications popularized by Uber, Lyft, Sidecar, and similar ventures in urban areas are a frequently mentioned business model for using autonomous cars. Transportation by a vehicle without a driver may appear potentially more reliable and private than current ride-sharing options that come
with human drivers. Variations on use of autonomous cars for ridesharing could include cooperatives that provide fleets of autonomous cars owned in common and available for use by members of an autonomous car cooperative. First generation autonomous cars could well become the primary mode of on-demand personal service that an individual can summon when needed. Such a transformation would reflect fundamental changes in expectations about personal mobility away from purchase of something that one owns, maintains, and drives. Some studies of millennials appear to indicate a shift toward such a preference for personal transportation as a service as opposed to ownership of a means of transport.

There are many kinds of arguably autonomous car technologies that are not considered autonomous cars for the purposes of this discussion. Car platoons and remote-controlled cars nevertheless deserve mention. Vehicle platooning has been a feature of advanced transportation discussions for a long time. Early applications of this technology have been developed as truck platoon systems such as that provided by Peloton Technology in the United States. In Europe, the European Commission established the SARTRE Project (Safe Road Trains for the Environment). Successfully developed SARTRE vehicle platoons operated on normal public highways and demonstrated significant environmental, safety and comfort benefits, mostly with regard to long-haul trucking. Such a follow-the-lead–truck strategy does not involve vehicles that are, strictly speaking, entirely driverless. In truck platoons, a driver operates the lead truck; in the following trucks, drivers do not exercise active control while they are in the platoon. In the United States, legal impediments to lawful operation of truck platoons include state laws that specifically ban “truck convoys”. Other state statutes set specific minimum spaces between vehicles under “following too close” prohibitions.

Applications of platoon designs to “car-trains” rely on wireless communications connecting one platooned vehicle with the next, and the rest of the chain. These vehicles need human drivers to hook-up-with, to enter, and eventually to leave the platoon, but are not under active driver control during the part of the journey as part of the platoon, or car-train. For the purposes of this discussion, platooning is an example of a highly promising connected vehicle technology that provides a degree of human driver passivity. But a vehicle in a platoon is not fully autonomous, in the sense that the vehicle operates itself at all times, to the point that a human driver is superfluous.

Cars can also be remotely controlled by external operators, so that human drivers need not be present in the car. However, they are not autonomous in the sense of controlling their own operations. Control by external operators simply moves the car’s “driver” from being a human inside the vehicle to outside the car. Remotely controlled vehicles are often associated with familiar childhood toys. In the real world, they are used in mining and military operations, often in the
form of very large-scale trucks, digging equipment and UGVs (unmanned ground vehicles). Moreover, remote control of trains has been a controversial feature of rail transport for a long time, partly because of job displacement of human train operators. This discussion of first generation autonomous cars instead focuses on cars that comprehensively control all of their own operations.

Part-time or partially autonomous operation without the need for constant, active control by a driver and without wireless communications linking them with other vehicles is already available. There are a variety of automated vehicle systems, such as adaptive cruise control with automatic lane keeping, that operate semi-autonomously in particular driving environments. Although these and other forms of assisted driving have proved to be generally lawful in most of the United States, state laws still require that a licensed driver be in a position to take over driving control at all times in emergencies. Automated driver-assistance systems are limited to particular driving operations (e.g., steering or braking) or specific environments (e.g., limited access highways or slow traffic). All of these assisted driving technologies require a human driver to operate the vehicle in transitions between different types of roadway settings – from highway to arterial to residential roadways.

When autonomous cars can perform all vehicle operation functions as well as or better than human drivers, the first generation autonomous cars will take to the roads. At that point, laws that require vehicle control by human drivers will have to change. Such a change to fully autonomous cars will require both technical advances as well as revised legal requirements that permit complete control over all driving functions all of the time by the autonomous car itself.

III. AUTONOMOUS CAR TECHNOLOGIES

Legal policy regarding autonomous cars requires a basic understanding of the technologies that will enable autonomous cars to operate on public roads without operational control by human drivers. Five functional groups of technologies combine to operate an autonomous car. Each of these groups of vehicle technologies interacts with the legal system in different ways. The integrated application of all of these technologies combines to make a car autonomous.

A. Human-vehicle interface.

The points at which a human user interacts with an autonomous car will be crucial in determining legal responsibility. These interaction points are often called HMI (human-machine-interface). It is likely that first generation autonomous cars will involve an HMI that provides only the choice between using
the autonomous car or not. The relatively simple interface may take the form of a
finger-print, a fob, a push-button or other on-off control. Under existing law in
some states, the human person who turns on an autonomous vehicle is the
“operator” of that autonomous vehicle.

More advanced interactions between humans and autonomous cars than a
simple binary (off-on) choice could also be available. For example, in addition to
switching on, or activating, an autonomous vehicle, the human may be able to
fine-tune in advance how the autonomous vehicle is expected to operate. Initially,
the choices are likely to be simple. For example, hypothetically, there could be
“operational options” for “aggressive driving,” “slow driving,” “scenic routes,”
or “arrival at <specified time>.” These options technically refer to specific ways
in which an autonomous car could be programmed to operate. Eventually,
idiosyncratic styles of autonomous vehicle operation could be programmed into
an array of user choices that would cause an autonomous car to operate in various
ways that uniquely respond to individual user preferences. With increased
human choices, will come responsibility, including legal responsibility. It seems
likely that, at least initially, the first generation of autonomous cars will be
programmed by the manufacturer in standard ways. That manufacturer
programming would lead to product liability if the programming malfunctions.

B. Internal Vehicle Operation Sensors
   Sensors that detect and process the operation of various parts within a
vehicle, such as the brakes, engine, transmission, steering, and the like are already
embedded in all modern vehicles. Under ISO 11898 standards, thousands of
sensor microprocessors communicate over the CAN bus for vehicle coordination,
diagnostic and other purposes. The capacities and configurations of these sensors
are generally proprietary information closely held by vehicle manufacturers.

   Since these sensors reflect the internal mechanical operations of a vehicle
and its parts, internal sensor data and functionality can result in significant legal
consequences in terms of identifying locations and causes of vehicle
malfunctions. Most information from and about sensors is closely guarded
proprietary information, protected as trade secrets. NHTSA regulates internal
sensors that are part of highway safety systems under existing Motor Vehicle
Safety Standards performance criteria, for example with regard to braking
operation.

C. External Roadway Environment Data, Including Location
   Because autonomous cars require exact location awareness for safe
operation, autonomous cars use precise mapping and other roadway awareness
technologies. Global Positioning Satellite (GPS) systems that provide real-time
location information are a nearly universal feature of experimental autonomous
cars. However, because the resolution of ordinary GPS signals is only accurate to a level of 3.5 meters, augmentation (such as through differential GPS) is often used to locate an autonomous vehicle requires more precisely - within a few centimeters. In addition to GPS, dynamic digital 3D mapping keeps track of precise information about previously mapped roads and collects data for input to improve the accuracy of digital maps. Most experimental autonomous cars rely both on digital maps and GPS signals for roadway data.

Experimental autonomous cars also use a wide range of innovative sensors that collect data about what is happening in the roadway environment through which an autonomous vehicle is moving. This external sensor data is typically used for navigation. It is also collected to improve the accuracy and timeliness of digital maps. Indeed, self-driving car developers, such as Google, have invented and experimented with many different types of sensors. Typically, a robust “picture” of the immediate and farther away roadway environment uses multiple sources of data about the roadway. Several forms of radar, lidar, infrared, sonar, and optics are deployed in experimental versions of autonomous cars. In first generation autonomous cars, multiple sensors will provide redundant sources of roadway data. Because adverse weather conditions interfere with sensors that rely on line-of-sight, even redundant arrays of multiple sensors may fail to provide adequate roadway environment input for operation of autonomous cars under especially bad weather conditions, such as snow, sleet, and heavy rain. Although development of roadway sensors has been actively encouraged by USDOT, so far roadway sensors are not substantively regulated by NHTSA or any other agency.

Because of sensor limitations, it is likely that some type of wireless signals will be needed to supply real-time roadway situation information to first generation autonomous cars. These wireless technologies are not literally sensors; but they provide vital data inputs about a vehicle’s driving environment. The exact nature of the wireless systems that will provide external data input for autonomous cars is uncertain at this time. DSRC communications of vehicle operation is currently affected by controversies over the US Department of Transportation’s Connected Vehicle program, as described in section IV, below. The Federal Communications Commission (FCC) regulates communications aspects of these transmissions of external data either as mobile wireless systems or as DSRC vehicle communications over the dedicated 5.9 GHz spectrum. Both SAE, International and IEEE provide standards for some of these communications.

D. Automated Controls

In an autonomous vehicle, control over vehicle operation is automated through networks of actuator microprocessors triggered by the vehicle’s artificial intelligence, discussed below. So far, automated controls appear to have been
remarkably reliable in accomplishing designated vehicle operations, for example in anti-lock brakes and electronic stability control, both of which are required under NHTSA Motor Vehicle Safety Standards. Some of the more recently developed automated car controls appear to be more dependable than others. For example, lane-keeping controls appear to have proved less reliable than electronic stability control. Legal and regulatory approvals are likely to be crucial for public confidence in automated controls embedded in increasingly automated cars.

Automated cars and some of their automated safety controls are regulated under NHTSA Motor Vehicle Safety Standards. These federal motor vehicle safety standards provide “minimum safety performance requirements” but do not prescribe particular automated technologies. Aside from these performance standards, legal regulation of automated cars and their automated controls is rare. Some of the existing automated car controls that provide driver assistance include: adjustable speed limiters; adaptive cruise control; lane-keeping systems; blind spot warnings and cross-traffic alerts; automatic parking assistance; rear view cameras; curve control warnings; active stopping in slow traffic; traffic sign recognition; hill start assistance; and automatic headlight adjustment for corners, curves and oncoming traffic. As helpful as these automated car technologies are, they assist, rather than replace human drivers.

E. Artificial Intelligence

An autonomous vehicle will rely on a highly sophisticated central processing unit to integrate and analyze internal vehicle operational data and roadway sensor information and then to determine which automated controls to activate and activate them. This heuristic artificial intelligence with advanced machine-learning is designed to replace the decisionmaking and reflexes of a human driver.

An autonomous car’s artificial intelligence is self-learning as it integrates internal vehicle operational data with external roadway environment inputs described in B and C, above. That analytic function occurs prior to actuating automated vehicle controls, described in D, above. Simultaneously, the intelligent system learns from and provides feedback data into vehicle operation at the same time it actuates vehicle controls. So far, sufficient computational power to instantaneously manage autonomous vehicle data integration, analysis, and activation appears to be available. Capacities for vehicle system data fusion and control architecture are not, however, unlimited. A first generation autonomous car’s artificial intelligence, tasked with taking over management functions otherwise performed by a human driver, will need to be at least as accurate and reliable as human intelligence. Assurance that autonomous cars can achieve that level of performance has proved difficult for state regulators in California, which has delayed adoption of operational regulations that would permit autonomous
cars, without human drivers, to be licensed for regular use on California roads. Although there are SAE, International and IEEE standards for some aspects of these analytic systems, legislation or regulation setting or requiring an overall standard as a matter of law has not yet been adopted.

F Manufacturing Processes

Existing automobile companies may manufacture all autonomous vehicles, their parts and systems. However, the most likely manufacturing process will rely on component manufacturers to make specific parts or technologies (such as sensors or artificial intelligence) that autonomous car manufacturers will integrate into autonomous cars. For products liability purposes, such a manufacturing process tends to extend the supply chain and to distribute liability risks across a broad range of potential defendants.

Specialized companies, such as Bosch and Continental, are already developing autonomous and automated vehicle modules. Technology companies, such as Google, are capable of developing sophisticated components or modules that could permit conventional vehicles to be manufactured as autonomous cars. Although aftermarket transformations of conventional cars into autonomous cars may be possible someday, the first generation autonomous cars will almost certainly be manufactured with embedded autonomous operational controls as original equipment.

IV. CONNECTED VEHICLES

“Connected vehicle” technologies (as such technologies are categorized by USDOT) may or may not be essential parts of first generation autonomous cars. As a result, first generation autonomous cars may or may not be “connected vehicles.” It is nearly certain, however, that there will be large numbers of connected cars long before there are any autonomous cars in regular commercial use. Certain types of connected vehicle technologies are already built into late-model conventional cars. Whether operation of first generation autonomous cars will rely on these vehicle connections or other more specialized “connected vehicle” technologies remains unresolved. Indeed, some experimental autonomous cars are deliberately designed not to connect with any external source of information for their operation. For example, the Google Car does not rely on externally communicated information for the car’s operation, aside from GPS that provides basic location data. In a 2012 article about “Privacy in Autonomous Vehicles,” I described Google-type autonomous cars as “self-contained,” as distinguished from “interconnected” autonomous cars.

The USDOT Connected Vehicle Program, there is an additional distinction between (1) Connected Vehicle Safety Systems in which vehicles
share vehicle operation data with other vehicles, and (2) Connected Vehicle Mobility Applications, which provide information and entertainment rather than data input for vehicle operation. Both systems are, given vehicle movement, wireless. The main difference between USDOT’s two categories of connected vehicles is that they use different types of wireless communications. Connected Vehicle Safety Systems rely on specialized Dedicated Short Range Communications (DSRC) transceivers to send and receive vehicle data over ad hoc vehicle networks. On the other hand, Connected Vehicle Mobility Applications generally use commercial cellular wireless networks (currently 4G and LTE; but by the time first generation autonomous cars are introduced, probably some form of 5G) to send and receive a wide range of data, from the status of vehicle operation to navigation assistance and infotainment. This category also includes satellite communications, such as Serius XM Satellite Radio, that transmit digital signals into moving vehicles, under circumstances where slow transmission speed and high latency do not interfere with the transmission.

To add to potential confusion about connected vehicles, NHTSA sometimes uses “Connected Vehicle” to refer only to vehicles with DSRC connections (Connected Vehicle Safety Applications in the taxonomy used elsewhere in USDOT). Such a distinction can be important because there are legal differences among various ways of connecting vehicles. DSRC vehicle communications have both technical and legal characteristics that are very different from the technical and legal characteristics of other modes of wireless communications that provide convenience, information, and entertainment to people in moving vehicles.

In other contexts, vehicle connectivity has expanded to include a wide assortment of ambiguous terminology. In the United States, “telematics” and sometimes “automotive telematics” refer generically to various forms of wireless communications to and from vehicles – connected vehicles. Yet, the consulting firm, Gartner, considers only communications from vehicles to be telematics: Telematics refers to the use of wireless devices and “black box” technologies to transmit data in real time back to an organization. Typically, it’s used in the context of automobiles, whereby installed or after-factory boxes collect and transmit data on vehicle use, maintenance requirements or automotive servicing.

“Mobile telematics” sometimes refers connections between an automobile’s computer systems to wireless communications networks that send vehicle data to others, such as manufacturers or insurers. On balance, connected vehicle technologies do not become easier to understand by often-obscure references to “telematics.”
Under whatever name, or misnomer, any of these vehicle communications technologies could find their way into first generation autonomous cars. On the other hand, first generation autonomous cars may not have any of them.

A. Connected Vehicle DSRC Safety Systems

For more than a decade it was assumed in the United States and elsewhere in the world, that “connected vehicles” would rely on DSRC transmissions for exchanges of vehicle safety information from one vehicle to another vehicle (V2V) or between a vehicle and the roadside infrastructure (V2I). At the beginning of this technology’s development just after the turn of the 21st century, the USDOT research program was called VII (Vehicle Infrastructure Integration). The initial concept was that human drivers would make better, safer driving choices based on more immediate information about what other nearby vehicles were doing, even when those nearby vehicles were not yet visible. In 2014, the National Highway Safety Administration announced that agency’s intention to require these DSRC “Connected Vehicle” transceivers as mandatory safety equipment in all new vehicles in the United States, under proposed Motor Vehicle Safety Standard 500. This to-be-proposed mandatory connected vehicle safety requirement was not intended specifically, much less only, for autonomous cars. Nevertheless, the potential usefulness of DSRC safety data in autonomous car operation was obvious. However, several recent events (some of them law-related) have raised uncertainties about the potential near-term availability of Connected Vehicle DSRC-based vehicle data transmissions (also known as V2V) for use in first generation autonomous cars.

First, the Federal Communications Commission (FCC) is under Congressional pressure to re-allocate parts of the now-dedicated 5.9 GHz DSRC spectrum to other types of wireless users. In 1999 the FCC reserved 75 megahertz of spectrum at 5.850–5.925 GHz (usually referred to as the 5.9 GHz spectrum) solely for vehicle safety and mobility communications over DSRC. Other, non-vehicle uses of this spectrum could cause interference that would degrade the usefulness of DSRC real-time vehicle communications to the point that these long-planned V2V Connected Vehicle communications may become insufficiently reliable for use by autonomous cars, particularly in congested urban areas.

Second, when the National Transportation Safety Administration (NHTSA) announced the agency’s intention to require Connected Vehicle DSRC transceivers in all passenger vehicles and light trucks, substantial objections were raised about the continuing absence of measures to protect privacy and security, and to prevent the use of V2V for surveillance. Some of these privacy, security and surveillance concerns are based on the fact that vehicle operational data (the Basic Safety Message or BSM) are unencrypted as they are transmitted from car to car.
Third, there have been recent policy objections to NHTSA’s announced proposal of agency regulations to require a DSRC transceiver to be embedded in every new passenger vehicle and light truck. There is no Congressional statute that expressly authorizes, much less directs, such a requirement. The likely need for legislative authorization further increases the possibility that NHTSA’s DSRC Connected Vehicle requirement may be delayed or even blocked. If V2V DSRC data from nearby vehicles is not available, first generation autonomous cars may either have to rely on alternative external data sources, such as mobile wireless, or not function as “connected vehicles” at all.

Fourth, some transportation technology experts are beginning to view DSRC as 1990s technology that needs reassessment in light of newer and better communications technology. Unfortunately, existing alternative communications technologies tend not to be as suitable for transmitting real-time safety-related vehicle data with the necessary speed and low latency. So far, alternative communication technologies do not perform well enough, particularly with regard to latency. Nevertheless, there is growing interest in improvements in mobile wireless technologies (such as 4G LTE, or perhaps 5G) as alternative ways to transmit specialized vehicle data. If such improved communications technologies become available by the time first generation autonomous cars are available, first generation autonomous vehicles may rely on them, instead of currently planned Connected Vehicle transmissions over DSRC.

B. Connected Vehicle Mobile Wireless Applications

Connected Vehicle Mobility Applications are very different from the circumscribed, standardized, and about-to-be-required Connected Vehicle Safety Systems based on DSRC discussed in the previous section. Connected Vehicle Mobility Applications embrace a much wider variety of technologies and applications than DSRC safety systems. The technologies that USDOT categorizes as “Connected Vehicle Mobility Applications” provide information to enhance vehicle mobility and convenience. They include existing commercial services that provide navigation and parking advice, automatic accident reporting, weather, and traffic reports. Some of the wireless services simply provide audio-video entertainment and information. Additional mobility applications become available virtually every day.

This second USDOT “connected vehicle” category actually shares with Connected Vehicle Safety Applications only communications connectivity with vehicles. Calling both of these sets of technologies “connected vehicles” tends to confuse important policy decisions. For example, the cybersecurity vulnerabilities posed by DSRC Connected Vehicles are markedly different from those posed by mobility applications communicating over wireless Internet connections.
One way to wirelessly connect a vehicle is to carry a device that connects to the Internet into the vehicle. Connected Vehicles seamlessly integrate wireless communications directly into vehicles. Most of these mobility applications embed one of two primary smartphone connection platforms offered by Apple and Google. These embedded communications systems enable smartphone functions to appear on a vehicle’s dashboard display screen and smartphone control by using the vehicle’s controls, including voice controls. Apple’s interface, called CarPlay, was launched in March 2014. Google’s similar interface, called Android Auto, launched in June 2014.

In addition to these integrated wireless internet and phone interfaces, vehicle manufacturers have often embedded closed-network wireless communications capacities that automatically communicate data from vehicles, vehicle parts and operations back to the vehicle’s manufacturer. Some of these systems may also provide infotainment services. Automotive operating systems commonly used to run this type of embedded vehicle connectivity include: Microsoft Embedded Automotive, open-source MeeGo, and QNX Car from Research in Motion. Android Auto and Apple’s CarPlay, noted above, are recent additions with broader functionality. Advanced embedded communication systems for vehicles are designed to provide cross-platform mobile access to phone, Internet sites, infotainment, and email, as well as integration between a vehicle’s automotive systems and its manufacturer.

Currently available mobility applications generally use cellular and PCS wireless communications provided by a wide range of wireless carriers to communicate between the vehicle and the outside world. 4G-LTE has recently increased the speed of these vehicle communications. Many vehicles are also equipped with receivers for satellite radio transmissions of infotainment programming. For short-distances within a vehicle, Bluetooth is frequently used for communications among devices.

The US Department of Transportation does not generally regulate these mobile wireless Connected Vehicle applications, except insofar as they may pose safety hazards in the form of driver distractions that will not be relevant in the context of autonomous cars without human drivers that might be distracted. NHTSA has published voluntary guidelines that restrict visual and tactile access to many types of in-vehicle devices and displays that could be included in Connected Vehicle Mobility Applications. These 2013 guidelines only affect the driver-facing interface of Connected Vehicle Mobility Applications. Nevertheless, NHTSA has warned that NHTSA may initiate enforcement if in-vehicle electronic devices contain safety-related defects or cause driver distraction. So far, NHTSA has brought no formal enforcement actions against connected vehicle mobility applications in conventional cars that do have potentially distractible human drivers.
The content provided by Connected Vehicle Mobility Applications is highly varied. Subject matter ranges from satellite navigation assistance and mapping to video and audio entertainment, as well as Internet communications. These mobile applications are particularly useful in targeted advertising that can focus on the vehicle’s occupants, based on the type of vehicle, its location, previous content, and what is known about the occupants.

In March 2014, the Federal Highway Administration published a Federal Register Notice requesting information about Connected Vehicle Mobility Applications “that leverage the full potential of trusted communications among connected vehicles, travelers, and infrastructure to better inform travelers, enhance current operational practices, and transform surface transportation systems management.” This research program seeks “applications that synergistically capture and utilize new forms of connected vehicle and mobile device data to improve multimodal surface transportation system performance and enable enhanced performance-based systems management.”

As of 2015, USDOT launched a research program to encourage “Dynamic Mobility Applications.” This USDOT program seeks to “combine connected vehicle and mobile device technologies in innovative and cost-effective ways to improve traveler mobility and system productivity, while reducing environmental impacts and enhancing safety.” The Dynamic Mobility Applications program envisions competitive commercial development with the federal government playing “an appropriate and influential role as a technology steward for the continually evolving integrated transportation [information] system.”

Among the most serious challenges faced by Connected Vehicle Mobility Applications are heightened cybersecurity needs. In the context of mobility applications, security threats can be difficult to guard against because there are so many data inputs and types of communications carried by Connected Vehicle Mobility Applications. In such a setting, identifying, isolating, and preventing security threats from hackers, malware and other cybersecurity threats is especially difficult.

The Internet of Things increasingly includes vehicles using wireless Internet connections. Accessible over Internet connections, sensor-rich systems within vehicles—including tires, fuel injection, brakes, steering, and transmission—are already becoming attractive hacker targets. According to a recent report from Vision Zero,

A new car may have more than 145 actuators and 75 sensors, which produce more than 25GB of data per hour. The data is analyzed by more than 70 onboard computers to ensure safe and comfortable travel.

Connected Vehicle Mobility Systems also provide feedback data to the manufacturer of the vehicle. The Vision Zero report warns,
Many modern cars have infotainment systems, engine management units, onboard diagnostic units, radios operating at different frequencies, GPS receivers, transponders, Bluetooth devices, and cell phone chips. Malware in any subsystem could compromise the safety of not only the people in the car, but also those around them.

Research is underway with regard to potential security threats to this type of connected vehicle. However, investigation and development of security solutions for Connected Vehicle Mobility Applications have only just begun.

The FCC licenses both telecommunications devices and wireless telecommunications carriers that transmit communications to and from vehicles through Connected Vehicle Mobility Applications. Although there have been suggestions that the FCC adopt specific licensing regulations with regard to providers of these services (which the FCC refers to as telematics) so far, the FCC has asserted jurisdiction only over communications devices and wireless service providers. The FCC does not yet specifically regulate particular mobility applications or platforms. Because location information is required for wireless communications under the FCC’s E911 regulations adopted in 2010, most Connected Vehicle Mobility Applications include GPS location information. These regulations (Phase II of the Commission’s E911 rules) now require wireless service providers to provide precise location information (the latitude and longitude of the caller) to Public Safety Answering Points. FCC-required location information must be accurate within fifty to three hundred meters, depending upon the type of location technology used.

Although Connected Vehicle Mobility Applications have been available much longer than DSRC V2V Connected Vehicle Safety Systems, both types of vehicle connectivity are in the process of rapid change. Specific ways in which they will ultimately develop will depend in part on the legal and policy environment these technologies encounter. By the time first generation autonomous cars become commercially available, some of the potential technical and policy uncertainties will have been resolved.

Whether autonomous vehicles will be “Connected Vehicles” may require the answers to further questions about which type of Connected Vehicle – V2V Safety or Wireless Mobility – is at issue. Some type of wireless mobility connected vehicle technology is almost certain to be available in first generation autonomous vehicles, if only for entertainment purposes. Connected Vehicle Safety Systems, primarily DSRC, that involve more specialized technology may or may not be used in first generation autonomous vehicles. Current doubts and disputes about requiring Connected Vehicle V2V Safety technologies may not have been resolved by then. It is also possible that, perhaps for security reasons,
first generation autonomous cars will not be interconnected through either type of Connected Vehicle technology, but rather will be self-contained, as the Google car is now.

V. LEGAL ENVIRONMENT FOR FIRST GENERATION AUTONOMOUS CARS

First generation fully autonomous cars will face a legal environment not designed for them. Laws that apply to conventional vehicles will be applied to first generation autonomous cars, unless exceptions are carved out for autonomous cars. Most current laws do not discriminate in favor of or against autonomous cars. Although, automated and assistive driving features such as cruise control are generally legal in the United States, some aspects of current laws will have to change before first generation autonomous cars can lawfully dispense with human drivers. For example, speed limits of sixty miles per hour will in the near future continue to apply to both conventional and autonomous cars. However, insurance laws based on the characteristics and driving experience of human drivers will need to change, particularly in states that require automobile insurance.

A. Federal and State Jurisdiction
Legislative and regulatory jurisdiction over automobiles is currently divided between the federal government, the states, and local municipalities. Absent radical changes in federal law that would preempt state laws applying to autonomous cars, state law systems will continue to govern autonomous cars. The multiple layers of federal, state and local laws that will confront first generation autonomous cars include

- federal legislation and administrative regulation with regard to such matters as highway construction, vehicle safety and fuel efficiency standards;
- state common law with regard to property, tort and contract matters;
- state legislation and administrative regulations regarding such matters as minimum vehicle standards, insurance, roadway usage, traffic laws, as well as other issue including privacy, security and environmental regulation; and
- local ordinances regarding traffic, pedestrian and bicycle safety and parking.

Each of these sources of legal rules and requirements will operate simultaneously and somewhat independently, although federal law can preempt state and local
laws and state law can preempt local law. Relationships between federal state and local transportation regulators are typically cooperative.

In the existing layered legal environment, federal regulation normally sets baseline vehicle safety standards that are usually incorporated into state laws and regulations. For example, if USDOT were to adopt regulations that establish Motor Vehicle Safety Standards that apply only to autonomous cars, or were to regulate autonomous cars (or all autonomous vehicles) as a separate vehicle category, these federal safety standards would apply nationwide and override conflicting state or local regulation. State laws and regulations would apply these standards in state requirements regarding vehicle licensing and operation on state roadways. Once state law permits autonomous cars to operate on state roadways, local ordinances would regulate local aspects of autonomous car usage, typically parking, local speed limits, and the like.

It is possible that earlier accommodation of autonomous cars may require complete replacement of this layered legal structure with uniform national standards and requirements applicable to autonomous cars. Perhaps because such preemption would raise fundamental political and constitutional questions about federalism and states’ rights, no such legislative proposals have been introduced. It will be interesting to see whether the importance of getting the first generation of fully autonomous cars on United States roads quickly will lead to a more assertive federal presence and broad preemption of state laws. In a forthcoming article in Volume 16 of the MINNESOTA JOURNAL OF LAW, SCIENCE & TECHNOLOGY (2015), I explore what a national regulatory system for autonomous cars might look like.

1. Present Federal-State-Local Autonomous Car Legal Regimes

At present, the federal government has not enacted specific national laws to govern autonomous cars or other types of autonomous vehicles. Under federal law, the National Highway and Traffic Safety Administration (NHTSA), part of the United States Department of Transportation (USDOT), has broad authority to regulate the safety of “motor vehicles.” “Motor vehicles” are defined by statute as vehicles “that are driven or drawn by mechanical power and manufactured primarily for use on public streets, roads, and highways.” 49 U.S.C. 30102(a)(6). NHTSA regulates by establishing safety performance standards for motor vehicles and motor vehicle equipment under Federal Motor Vehicle Safety Standards (FMVSS). 49 U.S.C. 30111. As a result, first generation autonomous cars will have to meet Motor Vehicle Safety Standards in effect at the time these cars are built or imported. Unless existing FMVSS are changed, first generation autonomous cars will have to comply with passenger vehicle FMVSS standards that require a wide range of safety features from headlights to bumpers.
Compliance with these national standards partly explain why first generation autonomous cars will look like other cars available at the time.

So far, NHTSA has not promulgated regulations or safety standards that specifically address autonomous vehicles. Just as NHTSA created a special LSV regulatory category for low-speed vehicles, NHTSA could create a separate regulatory category for autonomous cars. However, so far, NHTSA has evidenced no intention to regulate autonomous cars or autonomous vehicles separately from conventional cars. To the contrary, in NHTSA’s 2013 “Preliminary Statement of Policy Concerning Automated Vehicles,” the agency concluded that

We believe there are a number of technological issues as well as human performance issues that must be addressed before self-driving vehicles can be made widely available. Self-driving vehicle technology is not yet at the stage of sophistication or demonstrated safety capability that it should be authorized for use by members of the public for general driving purposes.

The agency also noted that “NHTSA does not recommend that states authorize the operation of self-driving vehicles for purposes other than testing at this time.”

By 2015, four states and the District of Columbia had enacted legislation authorizing testing of autonomous vehicles. Nevada law permits both testing and operation of autonomous vehicles on Nevada roads. In California, 2012 legislation directed the state’s Department of Motor Vehicles (DMV) to adopt regulations for both testing and operation of autonomous vehicles in California. The California DMV has adopted regulations that permit testing of autonomous vehicles in California. However, because of uncertainties about just how safe first generation autonomous cars should be required to be in California, the DMV has been unable to promulgate regulations permitting regular public use of autonomous vehicles on California roads, despite missing a January 1, 2015 statutory deadline. State legislation authorizing autonomous vehicles to operate on state roads remains pending in a number of states; but such legislation has been introduced and failed to pass in a far greater number of states than the number of states that have enacted autonomous vehicle authorizing legislation.

So far, municipal ordinances have not yet focused on autonomous cars for special local regulation. As a result, existing local ordinances regarding parking, speed limits, yielding to pedestrians and bicycles will apply to first generation autonomous cars. Experience with regulation of electric vehicles at the local level suggests that once state laws approve operation of first generation autonomous cars on public roads, local municipal regulation will almost certainly follow.
General State Roadway Laws and Regulations

First generation autonomous cars will have to comply with then-applicable state roadway laws and regulations before they will be allowed to operate in the United States. Each state owns and controls the highways and roadways within that state, including interstate highways. That makes the states’ interests in regulating the use of state property particularly strong. In addition, first generation autonomous cars will only be a very small proportion of vehicles on state roads. All of the rest of the roadway users – conventional cars, trucks, busses, motorcycles, etc. - will continue to subject to existing roadway rules. To have a completely different set of roadway laws and regulations just for autonomous cars could result in confusion and the kind of unpredictability that leads to vehicle crashes. As a result, most state roadway laws and regulations will apply to first generation autonomous vehicles, just as they apply to other types of road users. For example, first generation of autonomous cars will likely have to obey existing traffic laws, speed limits, stop signs, roadway maintenance directions, road closures, and the like, just as conventional vehicles will be required to comply with such laws and regulations.

After the first generation, when autonomous cars become more numerous and their specialized safety capacities are demonstrated, continued application of some state regulations to autonomous cars may seem to make little sense. Modified regulations for autonomous cars may then be adopted. However, state laws and regulations that apply to conventional vehicles will continue in force, as long as there are conventional vehicles that need to be regulated. Ultimately, vehicle regulations that apply only to autonomous cars are likely to evolve. In the farther more distant future, state laws may phase out road use by conventional vehicles and require all cars on public roads to be autonomous, just as automobiles took over roadways from horse-drawn wagons. Such an eventuality may occur in the far distant future.

Adopted under state authority, local vehicle laws and ordinances typically regulate vehicle usage, particularly with regard to local roadway safety, pedestrian safety, and parking. Initially, these existing local ordinances will also apply to autonomous cars. Normally protective of pedestrians and bicycles against any form of motorized vehicle, local ordinances will almost certainly include protections for these vulnerable road-users against autonomous cars. The most interesting local-law adaptations to autonomous cars are likely to be with regard to parking. Because autonomous cars will be capable of more precise and compressed parking, parking facilities for them can be more compact and dense, as well as located in remote facilities, away from congested urban areas. Moreover, scenarios for use of autonomous vehicles in fleets providing personal-mobility-as-a-service would reduce requirements for on-street parking in commercial areas. Distinctive autonomous car parking patterns (potentially
relegated to remote facilities) should eventually bring substantial changes in local parking regulations. In the more distant future, there may be even no need for on-site garage space for residential buildings, because an autonomous car can be summoned when needed from off-site parking facilities.

B. Federal Preemption of State Laws

Congress could enact national legislation that regulates autonomous vehicles on a uniform national basis, to the exclusion of state and local laws. Under the Supremacy Clause of the United States Constitution, such federal autonomous vehicle legislation, could preempt varied state laws that would otherwise apply to first generation autonomous cars. If a diversity of state laws regulating autonomous vehicles in different ways appears to stifle the development of autonomous cars, the Congress might seriously consider such a national autonomous vehicle law. However, near-term prospects for comprehensive national autonomous vehicle legislation make such preemption extremely unlikely. Nevertheless, it remains possible for federal law, either by statute or by regulation, to preempt most state laws that would otherwise apply to first generation autonomous cars. As noted earlier, I explore that possibility in an article forthcoming in the *Minnesota Journal of Law, Science & Technology* (2015).

Current preemption law, particularly with regard to ground transportation matters, is somewhat uncertain. Over the past fifteen years, the United States Supreme Court has unevenly decided preemption issues in the context of vehicle regulation. Two United States Supreme Court decisions appear to indicate that, absent an express statutory provision that explicitly preempts state law, federal law might not sufficiently “occupy the field” of autonomous car standards and requirements. *Geier v. American Honda Motor Company*, 529 U.S. 861 (2000), dealt with air bag standards that differed between federal and state law and upheld the application of state standards in the context of determining tort liability. *Williamson v. Mazda Motor of America, Inc.*, 130 S. Ct. 3348 (2011), dealt with state law seat-belt standards that were different from federal standards. State laws establishing liability standards in the context of automobile crash litigation may not be preempted unless the intent to override state law is explicit. Automobile crash litigation is an area of law that has historically been considered especially appropriate for state law to control. Moreover, standards regarding use of a state’s roadways are also traditionally considered particularly appropriate matters for state regulation. Although federal autonomous car legislation, if enacted, could preempt even state common law with regard to tort liability, the legislation would need to be direct and explicit about overriding state law.
C. Areas of Law Affecting and Affected by Autonomous Vehicles

First generation autonomous cars will interact with many existing areas of law. In some areas, current laws will simply apply to contexts involving autonomous cars. In other areas, it may be necessary to adapt existing laws or develop entirely new laws in response to the advent of first generation autonomous cars.

Litigation involving first generation autonomous cars is likely to be somewhat different from other litigation. To the extent that autonomous vehicles are successfully programmed to completely avoid all traffic infractions, car crashes and other harm, there may not be very much litigation involving autonomous cars. To the extent that such litigation does occur, it is likely to be technologically challenging and more than usually expensive. Evidence in autonomous car litigation will involve heuristic algorithms, sensor data, and experts from such fields as automated systems and optics.

1. Civil Liability

The fifty different state-law civil liability systems across the United States complicate evaluation (or even description) of civil liability regarding autonomous cars. Uncertainties about potential civil liability risks of significant damage awards already affect both investment in autonomous vehicle technologies and consumer interest in purchasing first generation autonomous cars. In addition to these expected defendants, there may also be peripheral defendants, such as the entities that own and operate roads and infrastructure.

   a. Manufacturer/Supplier/Seller Products Liability

      Assuming that there continue to be no liability limitations or other safe havens created by legislation, autonomous car manufacturers, parts suppliers, and sellers will encounter civil liability based on tort or warranty. Tort law, primarily in the form of products liability, would apply when an autonomous car leads to personal injury or damage to property other than the autonomous car itself. Warranty law adds a basis for liability when harm associated with an autonomous car involves either the car being less valuable or fit for use than expected or the car causing “economic” losses to its purchaser because it is a defective product.

      Within tort law, manufacturers, distributors, and sellers of autonomous cars will be subject to civil liability based on either negligence or products liability law. Negligence would apply when injuries result from a failure to exercise reasonable care in producing, distributing, or selling an autonomous car. Strict products liability will apply when a defective autonomous car causes harm, regardless of the defendant’s fault.

      A vast majority of states will apply some form of strict products liability, rather than negligence, to products liability claims regarding injuries and damages
caused by a defective autonomous car. Only Delaware, Massachusetts, Michigan, North Carolina, and Virginia do not recognize strict products liability and require proof of negligence in products liability suits. Most states follow the Restatement, Third, of Torts, in recognizing three different types of product defects: “manufacturing” defects, “design” defects and “warning” defects. For the most part, products liability would be normally limited to situations in which a problematic design or warning choice made an autonomous car “not reasonably safe.” Applying products liability to autonomous cars is likely to be complicated by the technologically advanced nature of the product that blends interactive technologies and components from a number of sources into enabling a car to operate autonomously. Moreover, to the extent that autonomous cars will require continuing updates (both programming and mapping) from manufacturers of the vehicles and their components, the products-liability-based warning obligations of autonomous car manufacturers will continue far beyond the point of sale. At the same time, proving product design-defect claims arising out of autonomous cars is likely to encounter novel challenges, such as establishing which particular algorithm or program installed within the vehicle was not reasonably safe. Most products liability cases involving autonomous cars will present important technical challenges in explaining advanced technologies such as sensors, actuators, and artificial intelligence to lay juries.

An additional basis for autonomous car manufacturer and seller liability for defects in autonomous cars that result in losses to purchasers is warranty law. Both express and implied warranties regarding the autonomous car’s fitness or merchantability could result in civil liability based on the Uniform Commercial Code. Under U.C.C. § 2-314, by placing an autonomous car on the market, a manufacturer or seller impliedly certifies that the car is reasonably capable of its intended use as an autonomous car.

Based on federal or state consumer protection statutes, manufacturers or sellers of autonomous cars could also be sued for unfair trade practices in actions that allege fraud or misrepresentation in the sale of defective products. For example, defective autonomous cars or improper marketing and sales tactics, can be actionable under the Magnuson–Moss Warranty Act, 15 U.S.C. §§ 2301–2312 (2012), and state “Lemon Laws.”

b. Civil Liability of Owners and Users

Owners and users of first generation autonomous cars may face negligence liability for injuries associated with their use. In addition to common law negligence that typically complains of harm caused by “human error,” statutory negligence, or “negligence per se,” may be based on a statutes or ordinances that apply to autonomous vehicles. A number of states already have statutes that impose liability on registered owners of run-away vehicles, which are often
described in the statutes as “driverless vehicles.” These “driverless car” statutes impose liability on registered owners as presumed “drivers”. Since there may be no humans at all in autonomous cars used to transport only cargo, either these statutes or some form or vicarious liability may impose damages liability on either the autonomous car’s owner or its operator. Some state autonomous vehicle regulations provide that the “operator” of an autonomous car is the human person who powers up the autonomous car or directs it to go to a particular location. Such a regulatory definition of “operator” does not necessarily create legal responsibility for motor vehicle crashes. When car-crash cases involve autonomous cars, no human driver or potential for “human error” may be present and yet comparative responsibility for avoiding the accident may be at issue. In such cases, legal responsibility could be vicariously imposed on autonomous car owners or operators. It is also noteworthy that employees injured in crashes of first generation autonomous cars used to transport employees around a corporate campus in corporate-owned autonomous car fleets, may also litigate civil liability under workers’ compensation laws.

c. Liability of Peripheral Defendants

Some potential defendants in civil liability suits involving autonomous cars may not expect to be held liable. In civil lawsuits involving first generation autonomous cars, these so-called “peripheral” defendants may include local governments that failed to repair unsafe roads, or government entities improperly maintaining or operating communications infrastructure used by autonomous cars that are also connected vehicles. Sovereign immunity to civil liability does not apply in states where government liability presumes the existence of a “ministerial” as opposed to a “discretionary” government responsibility with regard to such matters as road maintenance.

On the one hand, designing roads or, potentially, vehicle communications systems, is usually regarded as requiring the exercise of significant discretion by government agencies in most states so that sovereign immunity applies. On the other hand, in many of these same states, government liability law presumes the existence of a “ministerial” duty (as opposed to a “discretionary” obligation) on the part of state or local governments with regard to maintaining roadway infrastructure. As a ministerial duty, upkeep does not give rise to sovereign immunity that would otherwise protect a state or local government transportation agency against civil liability in tort actions. When harm in whole or in part results from deficient roadway upkeep or inadequate infrastructure maintenance (presumably including Connected Vehicle communications systems), sovereign immunity may not shield the government entity from liability. Either federal enactment of liability limitations or state laws specifically restoring sovereign immunity would be possible; but such legislation has not been enacted.
In the face of these uncertainties about civil liability, some autonomous car policy mavens have suggested a comprehensive strict liability system that places all risks and losses on vehicle manufacturers that assemble autonomous cars. Then the manufacturers would include these risks of damages and injuries in the price of each autonomous vehicle. Legislation establishing such a strict liability system that would apply to first generation autonomous cars has not yet been introduced.

2. Criminal Law and Procedure

When first generation autonomous cars begin to operate on public roads, most existing criminal offenses, such as driving the wrong way on a one-way street or blocking fire lanes, will apply to these autonomous cars, just as they do to conventional cars. In other contexts, first generation autonomous cars will challenge traditional criminal law concepts and applications. They also may generate entirely new criminal activity.

To the extent that first generation autonomous vehicles are programmed to comply with all traffic laws, citations of autonomous vehicles for traffic law infractions could well be almost non-existent. Of course, if an operator or owner of an autonomous car deliberately programmed the autonomous vehicle to disregard or to violate traffic laws, the operator/programmer logically might be liable for traffic infractions that result. But such criminal liability has not been widely discussed, much less enacted.

Overall, widespread use of autonomous vehicles presumably programmed to comply with traffic laws and rules of the road should eventually lead to crime-reduction. First generation autonomous vehicles would plausibly prevent such criminal behavior as driving under the influence and most vehicular manslaughter. Moreover, to the extent that first generation autonomous cars incorporate technologies that prevent vehicle theft and vehicle tampering, incidence of such existing crimes would also be reduced.

In some cases, autonomous vehicles may create difficult issues of criminal-law policy, such as whether and when criminal penalties should apply to programming decisions that produce avoidable crashes or other socially undesirable consequences. Moreover, first generation autonomous cars will stimulate changes in the existing model of local traffic law regulation that relies on enforcement of low-level traffic infractions for deterrence of a wide spectrum of anti-social behavior.

Autonomous cars may also lead to legislation creating new crimes. For example, legislative enactments may prohibit autonomous cars to operate at certain times or places or permit autonomous car operation only in other places or at other times. For the most part, violations of such restrictions would likely entail very limited mens rea requirements, carry low penalties, and be enforced by
local or possibly state governments. The federal government could also enact specific offenses related to autonomous cars. For example, a federal statute might be enacted to penalize manufacture of curtain dangerous types of autonomous cars. Other federal criminal statutes might prohibit unauthorized collection or use of information generated by autonomous cars.

Additional crimes may emerge with regard to misuse of autonomous cars in the commission of other crimes. Indeed, the use of an autonomous car in criminal activities may be the object of special criminal prohibitions, just as the use of firearms may be both a crime and also provide grounds for enhancement of criminal penalties for other crimes. Indeed, the FBI has already cautioned that autonomous cars may be used to facilitate acts of terrorism.

Law enforcement interaction with first generation autonomous cars may also generate some novel Fourth Amendment search-and-seizure issues. For example, no court has decided whether a warrant would be required before a law enforcement agency could send a signal to an autonomous vehicle’s automated systems that would jam these systems or cause the vehicle to come to a safe stop at a given location. In *United States v. Jones*, 132 S. Ct. 945 (2012), the United States Supreme Court recognized that a Fourth Amendment “search” occurred when the government attached a GPS device to a vehicle and then used the device to track the movements of a suspect’s vehicle over the course of a month. In her concurring opinion, Justice Sotomayor noted that it remains unclear whether a similar search rule would apply if the GPS device had already been in the vehicle, as will be the case with most, if not all, first generation autonomous vehicles. Subsequently, in *Riley v. California*, 134 S. Ct. 2473 (2014), the United States Supreme Court required a warrant before law enforcement officers could search the internal files of a smart phone. Whether an autonomous car’s information systems are similarly protected against warrantless law enforcement searches as those of a smart phone is among the criminal law issues first generation autonomous cars will raise.

3. **Insurance**

Since NHTSA estimates that at least 93% or more of car crashes are caused by human error, first generation autonomous cars, which have no human drivers, might appear to be excellent insurance risks. Nevertheless, autonomous cars that drive themselves will present difficult challenges under present insurance laws and models.

It is uncertain how, if at all, injured parties could be compensated under most automobile insurance policies, if no driver is found to be at fault. Moreover, in states where automobile insurance is mandatory for drivers (but not for motor vehicles), it is unclear whether autonomous cars (without drivers) will be required to purchase insurance. If autonomous car insurance is required, what that
insurance should cost, or cover remains unclear. As insurance matters now stand, the liability provisions of standard automobile policies insure against liability due to the fault of drivers. Uninsured/underinsured coverage usually insures drivers against damages caused by the fault of an uninsured or underinsured driver. None of these standard insurance models takes account of autonomous cars which have no human drivers. In short, automobile insurance will need to evolve to accommodate autonomous cars, which will require a different type of insurance that does not depend on human driving behavior.

Even if a basis for autonomous car insurance can be established, first generation autonomous cars will contend with at least fifty different forms of state motor vehicle insurance laws. Because the federal government ceded most insurance regulation to the states in 1945 under the McCarran-Ferguson Act, 15 U.S. Code § 1011, insurance laws and regulations that will affect first generation autonomous cars will be mostly in the form of state law. To the extent that first generation autonomous cars would be used for livery purposes, such as taxis, limousines, and on-demand ridesharing, various state public utilities commissions may also regulate them and require minimum levels of commercial insurance.

A 1944 United States Supreme Court decision, United States v. South-Eastern Underwriters Association 322 U.S. 533 (1944), confirmed that the federal government has authority to regulate insurance as an aspect of interstate commerce. Since federal law requires minimum insurance levels for commercial vehicles that travel interstate, autonomous commercial vehicles traveling in interstate commerce would be subject to federal minimum insurance levels. However, passenger cars, such as first generation autonomous cars, will be subject only to state laws regarding automobile insurance, unless federal law establishes a unified national insurance system for autonomous cars (or for autonomous vehicles in general). Such a federalized car insurance system seems unlikely in light of longstanding automobile insurance regulation under state law.

All states except New Hampshire have adopted some form of mandatory automobile insurance. However, various states have different models for regulating automobile insurance, policy terms, cost rating factors, liability limits, and uninsured/underinsured motorist coverage. In California, the insurance situation facing first generation autonomous cars in California is particularly dire. That is because state initiative legislation (Proposition 103, adopted in 1988) requires automobile insurance rates to be based on risk factors related to drivers (the driver’s driving record, the number of miles the driver drives annually, and the driver’s number of years of driving experience – as well as a required 20% discount for drivers with good driving records). Given the absence of these factors in the case of an autonomous car, it is unclear what risk factors can be the basis for calculating the cost of mandatory automobile insurance for an autonomous car. To make matters worse, these initiative-adopted automobile
insurance restrictions can be changed only through a vote of the entire state’s electorate.

In other states, first generation autonomous cars will also pose challenges with regard to automobile insurance costs because insurance is priced based on past experience with losses. The very first generation of autonomous cars will have no loss experience from which to project insurance costs. Moreover, because the artificial intelligence controlling an autonomous car is self-learning, autonomous car losses should diminish over time as machine learning adapts vehicle controls to avoid crashes. Insurance cost models based on past losses may not be accurate predictors of future losses from autonomous cars. One solution to this problem would be for state law to authorize insurance rates based on assuming that liability for injuries and damages will be placed on owners or operators of autonomous cars (as vicariously responsible equivalents of “drivers”) and require those autonomous car owners or operators to purchase automobile insurance the cost of which would be based on anticipated losses.

Under such an owner/operator insurance model, insurers of autonomous cars (instead of drivers) would likely seek to pass losses up the retail chain to manufacturers and commercial suppliers of autonomous cars and autonomous car components. If, under products liability law, discussed above, autonomous vehicle sellers and suppliers are held strictly responsible, then autonomous vehicle insurance against injuries and property damage will shift from being “personal” insurance to being a type of commercial risk insurance. Such a shift would raise a number of issues, such as whether autonomous car insurance should be mandatory; whether there is a potential for an autonomous car manufacturer becoming insolvent; and whether alternatives to insurance, such as no-fault, self-insurance or bonding might be preferable.

The existing fault-based, driver-centric system of car insurance appears inappropriate in the context of autonomous cars. Other ways to assure compensation for losses associated with autonomous cars may work better, including both other forms of insurance or financial responsibility measures such as no-fault. Moreover, as noted earlier, it is likely that some autonomous vehicles will be “connected vehicles.” Such an interactive “connected vehicle” infrastructure in which at least some first generation autonomous vehicles are likely to emerge, may render determinations, such as of fault or causation, so technologically complex that fault and causation are for most practical purposes illusory. Transaction costs of determining cause and fault may suggest spreading autonomous car insurance burdens for injuries and losses associated with autonomous vehicles more broadly among autonomous vehicle users, or even the public.
4. Land Use and Environment

First generation autonomous cars will have minor impacts on land use and the environment because they will be relatively few in number. Over time, autonomous cars will probably affect longer-term changes in land use patterns and the environment. Whether, in the long run autonomous cars will help lead to sustainable patterns of land use and enhance environmental quality is a matter of considerable debate.

A recent Rand study, “Autonomous Vehicle Technology” (2014), suggests that the potential effects of autonomous vehicles on aggregate vehicle miles traveled (VMT - a transportation measure of environmental impact) remain unclear. Nevertheless, this study concluded that it seems likely autonomous vehicles will lead to more total travel, rather than less. On the one hand, the convenience of autonomous vehicles for commuting between home and work may lead to more scattered residential development in rural areas, away from urban centers. The ability to use commuting time in one’s autonomous car for other purposes, such as work, rest or recreation, may make longer commute times and distances less burdensome for autonomous car users. If so, autonomous car users may be encouraged to live in rural or semi-rural areas and thereby contribute to sprawl.

As a result, many land planners are concerned that the availability of autonomous cars that provide more convenient commuting will result in longer commute patterns. These longer journeys could both exacerbate environmental problems such as air pollution and contribute to land development sprawl. On the other hand, first generation of autonomous cars may be deployed as low-speed zero emission vehicles that are not so useful for long highway commutes. In such a case, first generation autonomous cars might account for fewer vehicle miles traveled and be more environmentally benign. To the extent that higher speed autonomous cars use better, cleaner power technology, they may be more environmentally benign.

The total number of miles expected to be traveled by first generation autonomous cars is difficult to estimate. A study by the University of Michigan Transportation Research Institute considered the “Potential Impact of Self-Driving Vehicles on Household Vehicle Demand and Usage”. The results of this study seem to show that autonomous cars would likely lead to fewer cars being owned by the average household. At the same time, each vehicle would be used more intensely (travelling more miles over a given time period) so that roughly the same mileage would be covered by fewer cars.

a. Air Pollution Reduction

In several respects, first generation autonomous cars may contribute to sustainable community goals of reducing air pollution and greenhouse gas emissions. Although first generation autonomous vehicles could be powered by
any type of engine, including internal combustion engines burning fossil fuels, it would be possible to require first generation autonomous cars to be zero emission vehicles. Irrespective of their fuel or energy source, first generation autonomous cars are expected to reduce air pollution through avoiding congestion and intelligent routing. Autonomous vehicle automatic crash-avoidance capacities should ultimately lead to reductions in vehicle weight that will require less fuel to move the vehicle. Indeed, passive safety equipment such as heavy bumpers will eventually be no longer be necessary for occupant and vehicle safety in crash-avoiding autonomous cars that can be built using lighter materials.

b. Land Development Patterns

As noted above, it remains uncertain whether first generation autonomous cars will lead to denser, mixed use sustainable communities. For example, it would be possible to require that first generation autonomous cars only take the form of low-speed vehicles and only operate in urban areas. Such an urbanized-areas-only strategy for first generation autonomous cars might provide an incentive for residing in more dense urbanized areas. It would likely prove particularly beneficial to elderly and disabled persons who live in urbanized areas and face unusual personal mobility challenges.

In addition, legal restrictions could require first generation autonomous cars to operate only in urbanized areas as personal-mobility-as-service (ridesharing). Such an urban amenity could encourage more people to live in sustainable developments instead of suburban sprawl. In fact, ridesharing or taxi applications of autonomous cars would probably need relatively high population densities to be economically feasible.

Restriction of first generation autonomous cars to urban areas could also include transportation planning regulations that permit the use of autonomous cars only in designated parts of urban areas. In areas of older cities where roadways are narrow and difficult to navigate, the only passenger vehicles allowed to operate might rationally be first generation autonomous cars. Chronically congested areas also could be zoned for autonomous-transport-only.

c. Infrastructure

With regard to infrastructure impacts, most transportation experts expect that first generation of autonomous cars will have to cope with existing roadways shared with mixed traffic including many kinds of conventional, human-driven vehicles. However, by the time first generation autonomous cars are launched within the next decade, two factors may improve the make-up of this mixed traffic. First, NHTSA predicts that over the next few years, conventional vehicles are almost certain to become increasingly automated. Second, NHTSA has announced its intention to require “connected vehicle” technologies in new
passenger vehicles. This requirement is intended to make cooperative interaction and collision warning among vehicles pervasive.

It is theoretically possible to designate existing roadway or highway lanes for autonomous car use. For example, an exclusive autonomous car lane might be marked as a “star” lane, to distinguish it from existing diamond lanes for conventional carpool vehicles, electric vehicles, and vehicles paying tolls. Autonomous cars can safely travel faster on narrower lanes with greater throughput than ordinary roadways or travel lanes. Moreover, the availability of such “star” lanes could incentivize consumer acceptance of first generation autonomous cars, just as admission to high-occupancy lanes was used to incentivize purchase of electric vehicles. Such proposals would almost certainly generate significant political opposition, as was the case with carpool lanes making electric vehicles eligible for free use of carpool or High Occupancy Toll (HOT) lanes. In the more distant future, segregated portions of roadways (dedicated lanes) or entirely segregated roads may be restricted to use only by automated, connected or autonomous vehicles.

If “connected vehicle” technologies are used by first generation autonomous vehicles, additional infrastructure in the form of antennas and roadside units may be needed. At present, NHTSA has insisted that DSRC vehicle connectivity will rely only on V2V communications for which needed infrastructure is entirely within vehicles. However, to the extent that V2V becomes also V2I or V2X, additional communications infrastructure will be needed in the form of antennae and roadside processing units. Moreover, if autonomous vehicles rely on beacons or sensor reflectors placed along roadsides or embedded in pavement, such additional equipment would also add to the land use footprint of infrastructure used by first generation autonomous vehicles.

5. Privacy and Security Laws

A wide variety of privacy laws and security standards will apply to first generation autonomous cars. Privacy laws are now both more numerous and more varied than legal requirements regarding security. By the time first generation autonomous cars are on the road in the United States, increased complexity with regard to both applicable privacy laws and security requirements is nearly certain.

a. Privacy Laws

First generation autonomous vehicles will need to comply with three types of privacy laws: personal information protections, communications privacy laws and surveillance resections. All of these privacy laws are interrelated. But each has a distinct focus.
First generation autonomous vehicles will encounter a number of personal information laws. Because the usual function of passenger cars is to move individual people, autonomous cars will inevitably have considerable personal information associated with them. Examples of personal information associated with first generation autonomous cars will include car ownership and registration information, insurance information and autonomous car usage data including a person’s location information and that individual’s travel patterns.

Scores of existing state and federal personal information laws, both federal and state, will apply to first generation autonomous cars as they generate, collect and use personal information. An interesting example of federal privacy statutes that will govern personal information associated with first generation autonomous cars is the Federal Drivers Privacy Protection Act, 18 U.S. Code §§ 2721-2725, (known as the DPPA). The DPPA is a federal law that protects an individual’s personal information contained in motor vehicle registration and licensing records held by state motor vehicle departments. Disclosure of this personal information without the written consent of the individual is prohibited unless an exception applies. In 2013 the United States Supreme Court reaffirmed the important privacy protection purposes of the DPPA in a case involving plaintiffs’ lawyers who improperly obtained DMV registration records containing vehicle purchasers’ names and addresses. The lawyers illegally used that information in sending direct mail advertisements to potential plaintiffs in a class action against car dealers. Maracich v. Spears, 133 S. Ct. 2191 (2013). Many states have enacted laws similar to the DPPA to protect personal information held by DMVs even more extensively than DPPA.

Other state privacy statues require fair information practices as part of consumer protection laws. Forty-seven states have enacted privacy breach statutes. These statutes, which may be called “data breach”, “security breach” or “privacy breach” laws, typically protect “personal information” such as a person’s name combined with SSN, driver’s license or state ID number, account numbers, or other personal information. Protection extends to improper disclosures of this personal information through unauthorized access, such as hacking, and other types of data losses, including negligence. Encrypted personal information is frequently exempt. If personal information is improperly disclosed, each individual whose personal information was disclosed must be notified. The impact of such privacy breach notifications, both in terms of notification costs and in terms of business reputation losses, can be substantial. These laws will affect first generation autonomous car manufacturers, sellers, ride-sharing-service companies, and indeed, anyone who has personal information associated with first generation autonomous vehicles.
Communications Privacy Laws

A number of federal communications statutes will protect the privacy of communications to and from first generation autonomous cars, depending on the technologies used in first generation autonomous cars. For example, the Electronic Communications Privacy Act, 18 U.S.C. § 2511 (2012), (sometimes called the Wiretap Act) will prohibit unauthorized interception of most electronic communications to and from autonomous vehicles.

In addition, section 222 of the Telecommunications Act of 1996, 47 U.S.C. 222, will protect the privacy of consumer proprietary network information (CPNI) to the extent that first generation autonomous cars use Connected Vehicle Mobility Applications over mobile wireless networks. CPNI includes “information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship,” as well as telephone bills. 47 U.S.C. 222(h)(1)(A). The Federal Communications Commission (FCC) has been aggressive in enforcing CPNI protections. For example, in 2014 Verizon agreed to a Consent Decree amounting to $7,400,000 to settle FCC complaints about misuse of customer’s private information. In the Matter of Verizon, FCC Order File No.: EB-TCD-13-00007027 (Sept. 2, 2014).

By the time first generation autonomous cars become available, there is likely to be additional personal information privacy legislation, particularly with regard to the location of individuals. Even now, Fiscal Year 2015 Consolidated and Further Continuing Appropriation Legislation, Pub. L. 113-235, Div. K, § 417, already restricts the Department of Transportation from using funds “to mandate global positioning system (GPS) tracking in private passenger motor vehicles without providing full and appropriate consideration of privacy concerns” under the Administrative Procedure Act. This law restricts the use of federal funds for certain aspects of autonomous car development if they involve location tracking using GPS signals. Since most experimental autonomous cars already use GPS systems, the provision appears to apply to existing autonomous car funding.

Other laws permitting law enforcement access to personal information and communications would also likely apply to first generation autonomous vehicle communications. For example, the Electronic Communications Privacy Act, 18 U.S.C. § 2511 (2012), (sometimes called the Wiretap Act) prohibits interception of electronic communications. But the same statute permits law enforcement access to autonomous vehicle communications with a warrant. To the extent that autonomous vehicle information is stored by communications providers, by manufacturers or by others, the Stored Communications Act, 18 U.S.C. §§ 2701–12 (2012), would apply. Access to such stored data by law enforcement often
requires only a subpoena or possibly a “2703(d) order” based on the reasonable fact-based belief that the records are relevant and material to a criminal investigation. Litigation regarding law enforcement access to mobile device information held by telecommunications carriers under the Stored Communications Act has been the subject of widely varied court rulings, some of them more protective of individual privacy than other rulings.

(3) Surveillance Laws

Ironically, many laws protecting communications privacy also authorize government interception and surveillance, provided a warrant is secured. For example, despite the Electronic Communications Privacy Act protections for wireless communications, mobile wireless communications (Connected Vehicle Mobility Applications) to and from first generation autonomous cars can be monitored by law enforcement under the Communications Assistance for Law Enforcement Act (CALEA). 47 U.S.C. § 1002(a)(1). CALEA requires telecommunications carriers to facilitate law enforcement access to telecommunications networks for the purpose of intercepting communications. In 2005, the FCC, which has jurisdiction over CALEA requirements, extended the reach of CALEA requirements to VoIP and facilities based broadband. In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services, 20 FCC Rcd. 14989, 14993, (Sep. 23, 2005). First generation autonomous vehicles using Connected Vehicle Mobility Applications will need to include CALEA access. As a result, connected vehicle mobility applications will have less privacy protection against law enforcement interception than V2V Connected Vehicle Safety Applications using only DSRC, which involves closed ad hoc networks probably not subject to CALEA.

Similarly, if first generation autonomous vehicles communicate only over V2V applications of DSRC technologies, they will be able to avoid having to comply with CALEA access by law enforcement, unless the public interest requires access. The reason is because, as currently designed, V2V communications take place over ad hoc private closed networks that do not interconnect with public telephone systems or the Internet. If these same communications are sent as V2I communications so that they are interconnected with the public Internet or telephone systems to carry vehicle data to traffic management centers or other users, then those Connected Vehicle Safety applications would probably be subject to CALEA requirements.

Additional legislation has been introduced both in Congress and in state legislatures to enhance individual privacy protection from surveillance in the form of being tracked through the vehicles they use. Not only law enforcement agencies, but also private sector stalkers, and others seeking to track individuals in real time would be likely to find autonomous cars particularly useful tools. The
potential for surveillance of a person using an autonomous car through the car’s electronic systems will depend both on what technologies and applications are used by first generation autonomous vehicles and on legal restraints against such surveillance.

b. Security Laws

Among the many unknowns about laws that will apply to first generation autonomous cars, among the most elusive are security laws. Surprisingly little is known about technical aspects of autonomous vehicle systems security, although security measures appear to be under development.

Autonomous vehicles will depend on automated control systems that are particularly vulnerable to sophisticated malware such as Stuxnet that was used against Iranian network control software in 2010. Such security threats can jam as well as intercept autonomous vehicle communications. Sensors and actuators can be disabled. Hackers and attackers are likely to try just about anything and everything to take control of autonomous vehicle systems. Although policy questions about how best to provide security for autonomous cars are beginning to be asked, answers, in the form of appropriate legislation and regulation, will be essential before first generation autonomous cars move onto public roads.

The Federal Trade Commission (FTC) has enforced security requirements in the context of personal information. For example, the FTC has brought a series of groundbreaking “unfair trade practices” enforcement actions against companies that collected personal information but failed to secure it. Because first generation autonomous cars will be consumer products, they are susceptible to similar FTC scrutiny with regard to their security practices with regard to personally identifiable information.

In addition to securing personal information generated, collected, or used by first generation autonomous vehicles, security of vehicle communications security to and from autonomous cars will be important. If autonomous vehicles rely on V2V DSRC safety communications, specific security requirements for the resulting V2V ad hoc communications networks will be essential. Unfortunately, NHTSA’s 2014 advance notice of proposed rulemaking (ANPRM), with regard to requiring V2V over DSRC in all new passenger cars and light trucks, only sketched a limited PKI security certificate management system (SMS) for V2V. This SMS lacks essential detail. Moreover, broader concerns about the security of V2V data transmissions to and from heavy trucks and busses are not addressed at all. Robust communications security requirements are vital before first generation autonomous cars should be required to engage in V2V communications with other connected vehicles.

In addition to communications security, the potential for external control over and manipulation of autonomous cars presents somewhat different security
challenges. Recent “ethical hacker” experiments have gained remote access to automated vehicle functions, including engine control, in conventional vehicles. Familiar security hacks include (1) providing bogus input-information that misdirects an autonomous car to take a particular action or actions; or (2) taking over autonomous car operations through implanting malware that enables external access to and control. Technical research is under way regarding these and other autonomous car security issues. But legal requirements for security standards also need to be developed.

Because first generation autonomous cars will become part of the nation’s critical transportation infrastructure, legal requirements both for privacy and for cybersecurity need to be in place before first generation autonomous cars can emerge safely onto the nation’s roadways.

VI. LEGAL OUTLOOK DOWN THE ROAD

Autonomous cars appear to be developing in diverse ways and in diverse places under relatively low levels of regulation or standardization. Whether and how first generation autonomous cars will deliver anticipated safety, convenience, and environmental respect in personal mobility will unfold over the next decade. How soon and how smoothly first generation autonomous cars will emerge onto United States roads and highways will depend, in part, on how the legal system resolves some of the many legal issues explored in this discussion.