CONNECT CARS
RECENT LEGAL DEVELOPMENTS

FRANÇOISE GILBERT[1] AND RAFFAELE ZALLONE[2]

This paper will examine the (1) regulatory; (2) privacy and data protection; and (3) liability issues relating to connected and autonomous cars, and automated technology from a U.S. and European perspective.

1 – REGULATORY ISSUES

As car manufacturers and technology companies continue to innovate with respect to automated technology and autonomous vehicles, the legal and regulatory landscape both in the U.S. and throughout the European Union has struggled to keep pace with developments.

United States

In the United States, although the National Highway Traffic Safety Administration (NHTSA) is responsible for developing and setting federal motor vehicle standards and regulations, the current evolving regulatory framework regarding the testing and deployment of autonomous vehicles is essentially being driven at the state level. This patchwork approach to regulation, and

[1] © 2016 Gilbert + Zallone All rights reserved.

*Francoise Gilbert and Raffaele Zallone would like to recognize Joanne Kirk and Maneesh Mathur for their excellent contribution to this document. **Joanne Kirk**, CAPP/US/EU, is a privacy and cybersecurity professional, in the Cybersecurity, Privacy, and Crisis Management Group at Greenberg Traurig. **Maneesh Mathur**, JD, PhD, is a law clerk in the Corporate and Emerging Technologies Group at Greenberg Traurig Silicon Valley Office.*

***Françoise Gilbert** is a partner with Greenberg Traurig, a global law firm headquartered in the US and with offices on all continents. She practices in the firm's Silicon Valley office, located in East Palo Alto, California, where she advises public companies, emerging technology businesses and non-profit organizations, on the entire spectrum of domestic and international privacy and cyber security issues legal issues. Francoise has focused on information technologies for 30 years; she regularly deals with compliance challenges raised by cloud computing, connected objects, smart cities, big data, mobile applications, wearable devices, social media, and other cutting-edge developments. She is the author and editor of the two-volume treatise **Global Privacy and Security Law**, (Wolters Kluwer Publisher) which analyzes the data protection laws of 68 countries.*

[2] ***Raffaele Zallone** is an attorney in Milano, Italy, where in 1997 he founded Studio Legale Zallone, a niche firm focusing on IT and new technologies Law. From 2002 to 2008 Mr. Zallone was professor of IT Law at the University Luigi Bocconi of Milano, one of the most prestigious institutions in Italy. His main areas of activity of the firm include Data protection, New Technologies (robotics and biotech), IT contracts, e-Commerce and Internet law and regulation.*

lack of legal clarity, has created a lot of uncertainty for car manufacturers and technology companies.[3]

Developments at the State Level

Laws Regulating the Testing of Vehicles

California, District of Columbia, Florida, Michigan, and Nevada have laws that permit the testing of autonomous vehicles on public roads. They allow the use of vehicles for tests provided that an experienced human driver is at the wheel.

- **Nevada**

Nevada has been extremely active. NV SB 313, regarding autonomous vehicles, requires an autonomous vehicle that is being tested on a highway to meet certain conditions relating to a human operator. It requires proof of insurance and prohibits an autonomous vehicle from being registered in the state, or tested or operated on a highway within the state, unless it meets certain conditions. It also provides that the manufacturer of a vehicle that has been converted to be an autonomous vehicle by a third party is immune from liability for certain injuries.

Further, NV AB 511 authorizes operation of autonomous vehicles and a driver's license endorsement for operators of autonomous vehicles. It defines "autonomous vehicle" and directs state Department of Motor Vehicles (DMV) to adopt rules for license endorsement and for operation, including insurance, safety standards and testing.

Finally, NV SB 140 prohibits the use of cell phones or other handheld wireless communications devices while driving in certain circumstances, and makes it a crime to text or read data on a cellular phone while driving. However, it permits the use of such devices for persons in a legally operating autonomous vehicle. These persons are deemed not to be operating a motor vehicle for the purposes of this law.

- **Florida**

In Florida, FL HB 1207 defines "autonomous vehicle" and "autonomous technology." It also declares legislative intent to encourage the safe development, testing and operation of motor vehicles with autonomous technology on public roads of the state and finds that the state does not prohibit or specifically regulate the testing or operation of autonomous technology in motor vehicles on public roads.

The law authorizes a person who possesses a valid driver's license to operate an autonomous vehicle, specifying that the person who causes the vehicle's autonomous technology to engage is the operator. It also authorizes the operation of autonomous vehicles by certain persons for testing purposes under certain conditions and requires an instrument of insurance, surety bond or self-insurance prior to the testing of a vehicle. It directs the Department of Highway Safety and Motor Vehicles to prepare a report recommending additional legislative or regulatory action

[3] *See*, Testimony of Dr. Chris Urmson, Director, Self-Driving Cars Google [x], before Senate Committee on Commerce, Science and Technology Hearing: "Hands Off: The Future of Self-Driving Cars", March 15 2016, available at http://www.commerce.senate.gov/public/index.cfm/hearings?id=C1BE704F-8D6B-43C6-B472-858C6B457E86.

that may be required for the safe testing and operation of vehicles equipped with autonomous technology.

- **Michigan**

Michigan, a state that traditionally has had significant audible industry has also shown great interest in connected vehicles. MI S 169 defines "automated technology," "automated vehicle," "automated mode," expressly permits testing of automated vehicles by certain parties under certain conditions, defines the term "operator", addresses liability of the original manufacturer of a vehicle on which a third party has installed an automated system, and directs state DOT with Secretary of State to submit report by Feb. 1, 2016.

In addition, MI SB 663 (2013) limits liability of vehicle manufacturer or upfitter for damages in a product liability suit resulting from modifications made by a third party to an automated vehicle or automated vehicle technology under certain circumstances; relates to automated mode conversions.

- **California**

Among other things, California CA SB 1298 requires the Department of the California Highway Patrol to adopt safety standards and performance requirements to ensure the safe operation and testing of autonomous vehicles, as defined, on the public roads in this state. Permits autonomous vehicles to be operated or tested on the public roads in the state pending the adoption of safety standards and performance requirements that would be adopted under this bill.

- **Washington DC**

In the District of Colombia, DC B 19-0931 defines "autonomous vehicle" as "a vehicle capable of navigating District roadways and interpreting traffic-control devices without a driver actively operating any of the vehicle's control systems." It requires a human driver "prepared to take control of the autonomous vehicle at any moment." It also restricts conversion to recent vehicles, and addresses liability of the original manufacturer of a converted vehicle.

In 2015, both North Dakota and Tennessee enacted legislation pertaining to autonomous vehicles. In North Dakota, ND HB 1065 provides for a study of autonomous vehicles. It includes research into the degree that automated motor vehicles could reduce traffic fatalities and crashes by reducing or eliminating driver error and the degree that automated motor vehicles could reduce congestion and improve fuel economy. Finally, Tennessee's TN SB 598, which relates to motor vehicles, prohibits local governments from banning the use of motor vehicles equipped with autonomous technology.

During the course of 2015, at least sixteen states have introduced legislation related to autonomous cars.[4] In addition, some states, such as California, are currently drafting regulations for the deployment of autonomous vehicles on California roads.

Laws Regulating the Deployment of Vehicles

Section 38750 of the California Vehicle Code requires the California Department of Motor Vehicles (DMV) to adopt regulations establishing certain vehicle equipment requirements,

[4] *See,* http://www.ncsl.org/research/transportation/autonomous-vehicles-legislation.aspx

equipment performance standards, safety certifications and any other matters the DMV concludes necessary to ensure the safe operation of autonomous vehicles on public roads. The DMV elected to divide the drafting of the regulations into two separate phases: testing and deployment. The regulations for the testing of autonomous cars became effective in September 2014.

In December 2015, the DMV produced draft deployment regulations. These deployment regulations, once adopted, will establish the requirements that manufacturers must meet to enable the public to operate their autonomous vehicles on California roads.

Following the publication of the draft regulations, the DMV has held two public consultations in January and February 2016 to discuss the draft regulations and to receive input from the public, industry, consumer and public interest groups, and academic and research institutions. The California DMV has also asked California Partners for Advanced Transportation Technology (PATH)[5] to conduct a peer review of the behavioral competencies identified in the draft regulations.[6]

Summary of California DMV's Proposed Deployment Regulations

The California DMV has stated that the development of the draft deployment regulations raises complex questions that it had to consider regarding vehicle safety, certification approaches, operator responsibilities, licensing and registration requirements, and privacy and cyber security.

The DMV has also indicated that it expects that the deployment regulations will create a framework i) allowing manufacturers to transition from testing to deployment, ii) promoting the continued development of autonomous vehicle technology, and iii) ensuring that deployment of autonomous vehicle technology is carried out in a safe and responsible manner on public roads in California.[7]

A review of the key underlying aspects of the DMV's proposed approach to deployment of autonomous vehicles for use on public roads provide a useful summary of the regulatory issues that must be considered in this area.

[5] California Partners for Advanced Transportation Technology is a research and development program of the University of California, Berkeley. Founded in 1986, its mission is to develop solutions that address the challenges of California's transportation systems through advanced ideas and technologies. http://www.path.berkeley.edu.

[6] The proposed behavioral competencies identify the typical driving maneuvers that an autonomous vehicle would be expected to perform. The draft regulations define "behavioral competency" as the ability of the autonomous vehicle to operate in all of the driving situations that may be encountered while operating on public roads whereby the autonomous vehicle must respond to either, by performing a driving maneuver, or requiring the operator to take control.

[7] California Department of Motor Vehicles, Summary of Draft Autonomous Vehicles Deployment Regulations, December 16, 2015.

- **Manufacturer Safety Certifications and Third-Party Vehicle Demonstration Test**

Safety certifications from both the manufacturer and a third-party testing organization[8] would validate the deployment readiness of an autonomous vehicle. A manufacturer would be required to certify to its compliance with specific vehicle safety and performance requirements, including functional safety and behavioral competency requirements. In addition, a vehicle demonstration test conducted by a third-party testing organization [9] - defined in the regulations as a Third-Party Testing Organization for Autonomous Vehicle Demonstration Test - would provide independent verification of the ability to perform key driving maneuvers typically encountered in real-world driving conditions.[10]

- **Licensed Driver Required in the Vehicle**

In order to legally operate an autonomous vehicle, an individual would be required to hold a specific license issued by the DMV. Thus, all operators of autonomous vehicle would be licensed drivers with an autonomous vehicle operator certificate issued by the DMV.

The operator[11] would be responsible for monitoring the safe operation of the vehicle at all times and would be required to take over immediate control if the automated technology fails or there is another emergency. Under the draft regulations, the operator would be responsible for all traffic violations that occur while operating the autonomous vehicle.

Manufacturers would have to develop a consumer education plan and a behind the wheel training program to provide operators with an understanding of how the vehicle technology is engaged, used, monitored and disengaged.[12]

The draft regulations would exclude autonomous vehicles capable of operating without the presence of a driver. The DMV believes that manufacturers need to obtain more experience in testing driverless vehicles on public roads before their general deployment. However, it has indicated that it will address the unique safety, performance, and equipment requirements associated with fully autonomous vehicles without the presence of a driver in subsequent regulatory packages.

- **Provisional Deployment Permit with Ongoing Reporting Requirements**

In order to deploy autonomous vehicles on any public road, manufacturers would be required to submit an Application for a Permit to Deploy Autonomous Vehicles on Public Streets. In doing so, manufacturers would have to provide detailed information, as outlined in the draft

[8] "Third-Party Testing Organization" means the independent entity authorized by the manufacturer to conduct the vehicle demonstration test of the manufacturer's autonomous vehicle.

[9] *See*, CA Draft Autonomous Vehicles Deployment Regulations §227.58 Third-Party Vehicle Demonstration Test and §227.60 Third-Party Testing Organization Qualifications of draft regulations for further detail.

[10] *See*, Draft Autonomous Vehicles Deployment Regulations §227.56 for further detail on certification and testing requirements.

[11] "Operator" is defined as the person who possess the proper class of license and who has direct control over the operation of an autonomous vehicle and has engaged the autonomous technology while sitting in the driver seat of the vehicle.

[12] The draft regulations contain specific detail on the requirements that would have to be included in the education program.

regulations, to the DMV. For example, the information required would include: make and model of vehicles for deployment[13], and the areas of operation[14] in which the vehicles are designed to operate.[15]

Manufacturers approved for deployment would initially be granted a three-year deployment permit. A condition of the issuance of this provisional permit would be that autonomous vehicles can only be operated by the manufacturer or made available to the public on a leased basis only.

During the term of the permit, manufacturers would have to submit monthly reports regarding the performance, safety, and use of the vehicles. The draft regulations detail the data that would have to be submitted as part of the monthly report.[16] The DMV hopes that data collected through the permit term will provide an opportunity to evaluate the safety and real-world performance of the vehicles and inform subsequent regulatory actions.

A permit would be suspended or revoked if the manufacturer i) has failed to maintain financial responsibility as required by the Vehicle Code and the draft regulations, ii) has submitted incorrect or misleading information in its permit application, or iii) has failed to report any change to the information/certification provided as part of the application.[17]

- **Financial Requirements for Provisional Deployment Permit**

The draft regulations contain a number of provisions regarding financial requirements[18] that the manufacturer must fulfill to obtain a permit to deploy autonomous vehicles. These include, for example, demonstrative proof - by way of insurance, surety bond or self-insurance - that the manufacturer has the ability to respond to judgment(s) for damages arising from collisions or accidents caused by its autonomous vehicles.

- **Vehicle Performance Requirements**

A manufacturer would be required to report accidents that occurred while the vehicle was in autonomous mode. They would also have to report any safety-related defects in their autonomous technology. The Manufacturer would have to submit a Report of Traffic Accident Involving an Autonomous Vehicle form, within 10 days of the accident.

Autonomous vehicles would have to be equipped with an event data recorder that captures and stores autonomous technology sensor data for all vehicle functions controlled by the

[13] Known as "subject autonomous vehicle."

[14] An "area of operation" is defined as one of the following: i) urban, which is any developed contiguous area where there are more than 10,000 residents, ii) rural, which is all other areas of California not included in urban areas except for a freeway/highway, and iii) freeway/highway, where "freeway" is defined in Vehicle Code section 332. In its permit application, the manufacturer is required to certify that the vehicles are incapable of operating in autonomous mode in areas outside of the disclosed areas of operation.

[15] The permit application must be accompanied by a range of other documentation and certifications as outlined in CA Draft Autonomous Vehicles Deployment Regulations §227.56.

[16] CA Draft Autonomous Vehicles Deployment Regulations §227.689(d).

[17] CA Draft Autonomous Vehicles Deployment Regulations §227.74 Suspension/Revocation of Permit.

[18] *See*, CA Draft Autonomous Vehicles Deployment Regulations § 227.54.

autonomous technology at least 30 seconds before a collision with another vehicle, person or object while operating in autonomous mode. The captured data would have to be stored in a read only format capable of being accessed and retrieved by a commercially available tool.

When applying for a deployment permit the manufacturer would have to submit, amongst other documentation, certification that i) the autonomous vehicle performs the specified behavioral competencies and ii) the manufacturer adheres to an established functional safety plan.[19] In addition, the manufacturer would have to certify that its autonomous vehicles have self-diagnostic capabilities meeting current industry best practices and have the capability to detect and respond to cyber-attacks, unauthorized intrusions, and false or spurious messages, and that it have the capacity to alert the operator of the incident.

- **Vehicle Registration Requirements**

All autonomous vehicles would have a display certification label that details: manufacturer's name; date of manufacture; vehicle identification number, along with a certification statement that, *"The manufacturer of this autonomous vehicle has certified it conforms to State of California requirements for autonomous vehicles in effect on the date shown above."*

If a manufacturer installs autonomous technology in a vehicle after its original manufacture, so that it qualifies as an autonomous vehicle, it would be required to affix a certification label detailing: manufacturer/business name; date of manufacture; vehicle identification number, along with a certification statement that, *"This vehicle has been modified with the incorporation of autonomous technology that the manufacture has certified conforms to State of California requirements for autonomous vehicles in effect on the date shown above."*[20]

- **Privacy and Cyber-Security Requirements**

Manufacturers would be required to provide written disclosures to autonomous vehicle operators, of any information collected by the autonomous technology not necessary for the safe operation of the vehicle. Manufacturers would have to obtain written approval to collect the information.[21]

The vehicles would have to be equipped with self-diagnostic capabilities that meet industry best practices, and are capable of detecting, responding, and alerting the operator to cyber-attacks or other unauthorized intrusions. If such an alert occurs, the vehicle operator would have to be able to override the autonomous technology.

The manufacturer's consumer education plan would have to provide information on how an operator can override unauthorized commands received by the autonomous technology in the event of a cyber-attack.

[19] Under the draft regulations, "functional safety plan" is defined as the process and procedures implemented by a manufacturer to identify and assess hazards associated with the operation of an autonomous vehicle's technology, and to develop and implement hazard mitigation strategies.

[20] It would not be possible to register an automated vehicle unless it displays a certification label (as above). The application for registration would have to clearly indicate when a vehicle has been equipped with autonomous technology by indicating, "MISC" followed by "AV." An autonomous vehicle would be identified on the registration card and any certificate of ownership.

[21] *See*, CA Draft Autonomous Vehicles Deployment Regulations § 227.76. Information Privacy

- **Exclusion of Commercial Vehicles**

Consistent with the testing regulations, commercial vehicles would be excluded from deployment.

Developments at the Federal Level

NHTSA/Department of Transport: (2016 Update)"Preliminary Statement of Policy Concerning Automated Vehicles"

NHTSA has been actively evaluating the field for several years. In May 2013, it released its "Preliminary Statement of Policy Concerning Automated Vehicles."[22] Among other things, this was intended to provide guidance to those states that were enacting regulations to permit the testing of autonomous cars.

In January 2016, the Department of Transport and NHTSA issued policy guidance updating the Preliminary Statement of Policy Concerning Automated Vehicles. The updated Statement of Policy detailed a number of initiatives, such as initiatives to:

- **Develop Best Practice Guidance for Deployment of Autonomous Vehicles**

NHTSA has committed to developing best-practice guidance for the safe deployment and operation of fully autonomous vehicles,[23] and to providing a common understanding of the performance characteristics necessary for the development and operation of fully autonomous vehicles and the testing and analysis methods used to assess them. NHTSA has committed to complete this guidance by July 2016.

- **Develop a Model State Policy on Automated Vehicles**

NHTSA has also committed that by July 2016, it will develop a model state policy on automated vehicles. This model policy will be intended to create a path to a consistent national policy. It will be developed in cooperation with state partners, the American Association of Motor Vehicle Administrators, and other stakeholders.

- **Encourage the Submission of Rule Interpretation Requests by Manufacturers**

NHTSA is also encouraging manufacturers to submit rule interpretation requests, where appropriate, to help enable innovation in the area of automated technologies and autonomous vehicles. For example, NHTSA has responded to such interpretation requests from BMW (confirming that BMW's remote self-parking system meets federal safety standards) and Google (in response to Google's request to interpret several provisions of the Federal Motor Vehicle Safety Standards as they apply to Google's described design for vehicles in developing and testing).

[22] See, http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+Department+of+Transportation+Releases+Policy+on+Automated+Vehicle+Development.

[23] Vehicles at Level 4 on the scale established in its 2013 preliminary policy statement.

- **Request for Use of the Agency's Exemption Authority**

NHTSA has also called on manufacturers to submit requests for use of the Agency's exemption authority to allow the deployment of fully autonomous vehicles. This exemption authority allows NHTSA to enable the deployment of up to 2500 vehicles for up to two years if it determines that an exemption would ease the development of new autonomous features.

- **Request New Statutory Authorities when Necessary**

The Department of Transport and NHTSA will consider seeking new statutory authorities when necessary to ensure that fully autonomous vehicles are deployable once their safety has been demonstrated. The US Transportation Secretary has emphasized that the administration will not seek to pre-empt state authority over highway safety with a single national policy, but will work with states to ensure a workable, consistent regulatory regime for autonomous vehicles.

NHTSA Response to Google's Request for Interpretation of the Federal Motor Vehicle Safety Standards (February 2016)

As already detailed, NHTSA has been actively encouraging manufacturers and technology companies to submit rule interpretation requests. In November 2015, Google submitted such an interpretation request to NHTSA requesting that the Agency interpret some provisions of the Federal Motor Vehicle Safety Standards (FMVSSs) as they apply to Google's described design for driverless motor vehicles that it is in the process of developing and testing.

The response issued by NHTSA highlights how, in some instances, the existing legal and regulatory framework may be ill equipped to deal with current and ongoing developments with the more sophisticated autonomous technology. A few of the interpretation requests and NHTSA's responses are reviewed below to give an illustrative overview of the current limitations of the regulatory framework with respect to driverless cars.

- **Background to Google's Interpretation Request**

According to Google, its self-driving vehicles (SDVs) are fully autonomous vehicles whose operations are controlled exclusively by a self-driving system (SDS). The SDS is an artificial intelligence driver, which is a computer designed into the motor vehicle itself that controls all aspects of driving by perceiving its environment and reacting to it. Therefore, Google maintains that its vehicles have no need for a human driver. As there is no requirement for a human driver, Google's design removes all conventional driver controls and interfaces (e.g., steering wheel, throttle pedal, brake pedal etc.…). The SDS controls all aspects of driving and, according to Google, the SDS will make the optimal decisions for the safety of the occupants of the SDV. Google is concerned that providing occupants with the ability to control steering, acceleration, braking or turn signals, or providing occupants with information about the vehicle's operation could be detrimental to safety as the occupants could attempt to override the SDS's decision.

In its response to Google's interpretation request, NHTSA detailed how Google's design choices for the SDV presented a number of unique challenges in applying the FMVSSs. The Agency outlined how the standards were drafted when it was reasonable to assume that all vehicles would require conventional driver controls, usually located at the front left seating position, and that these controls would all be operated by a human driver. However, NHTSA has found that for vehicles with an artificial intelligence driver that precludes an occupant from driving, these assumptions no longer hold.

As automated technology develops beyond what was envisioned when the FMVSSs were originally drafted and issued, NHTSA has stated that it may not be able to apply the same kind of test standards for determining compliance.

- **Overview of Main Aspects of Google's Interpretation Request**

The critical point of NHTSA's responses for many of the interpretation requests from Google is that defining the driver as the SDS (see below) does not end the inquiry or determine the result. NHTSA has made it clear that once the SDS is deemed to be the driver for the purposes of a particular standard or test, the next issue is whether and how Google could certify that the SDS meets a standard developed and designed to apply to a vehicle with a human driver.

Further, NHTSA's clarifies that there are limits with interpretation, even if the results of which might be sound policy. This is because an interpretation may not make a substantive change to the statutory or regulatory regime and it may not adopt a new position that is irreconcilable with or repudiates existing statutory or regulatory provisions.

➢ *Who/What is Considered to be the Driver of the SDV?*

49 CFR §571.3 defines the driver as the occupant of a motor vehicle seated immediately behind the steering control system. As Google's SDV does not have a conventional steering control system or does not permit occupants to drive, it is problematic for Google to determine how to certify its motor vehicle design to certain FMVSS provisions concerning the driver.

As a foundational starting point for the interpretation request, NHTSA agreed to interpret the driver as referring to the SDS and not to any of the vehicle occupants. NHTSA stated that no human occupant of the SDV could meet the definition of §571.3. It further acknowledged that, if no human occupant can actually drive the vehicle, it is more reasonable to identify the “driver” as “whatever is doing the driving,” i.e., the SDS that is actually driving the vehicle.

The remainder of Google's request to NHTSA concentrates on several interpretative issues related to the absence of a human driver. One of the main interpretative requests is covered below as an illustrative example.

➢ *Light Vehicle Break Systems*

FMVSS No. 135 contains requirements for service brakes and associated parking brake systems. Service brakes must be activated by means of a foot control, while the control of parking brakes must be independent of the service brake control and may be either a hand or a foot control.

Google's design does not include hand or foot controls for either brake. It argues that because the SDS will control all aspects of braking it would not be necessary or beneficial for safety for a human to be able to apply the brakes. Google requested that NHTSA interpret these provisions to be inapplicable to its described vehicle design and to allow the service brake system performance requirements to be met if the SDS activates the service brakes.

NHTSA responded that the fact that the SDS may be programmed to perform the tests enumerated in FMVSS No. 135 does not overcome the language of S5.3.1, which plainly states that service breaks shall be activated by means of a foot control.

In order to satisfy Google's request, NHTSA advised that it would need to commence a rulemaking to consider how FMVSS No. 135 might be amended to ensure that vehicles that control all braking through an artificial driver have a way to comply with the standard. In the interim, the Agency suggested that Google might wish to consider petitioning for an exemption from these provisions.

However, in its response to Google, NHTSA did recognize that it could take a substantial period of time to develop final rules and that many of its interpretation do not fully resolve all of the issues Google raised in its original request. Consequently, NHTSA has suggested that Google may wish to explore the interim step of seeking exemptions. Exemptions are available for manufacturers that are able to demonstrate that features of their product provide equivalent levels of safety to those required by the FMVSS.[24]

Europe

Regulatory and Legal Framework for Automated Vehicles

Over the past decade, the European Union (EU) has begun taking steps to evaluate the changes it needs to ensure that its regulatory and legal framework are capable of dealing with the increased risks posed by automated vehicles. Part of the challenge faced by the EU is that different national jurisdictions may implement differing or conflicting regulations that could hinder the development and deployment of new technologies for traffic systems or vehicles. The EU recognizes this challenge and has committed several million euros to funding research projects aimed at evaluating various automated technologies, determining the feasibility of the deployment of such technologies on European road systems, assessing the relevant legal issues (such as product liability, road traffic laws, regulatory laws, data privacy and data security) resulting from automation of traffic systems and vehicles, and determining guidelines for implementing a uniform regulatory framework for all EU member states.

In September 2015 the Transport ministers of the G7 states (Canada, France, Germany, Great Britain, Italy, Japan, and the US) and the European Commissioner for Transport agreed on a declaration on automated and connected driving. As a result of the declaration, it became apparent that appropriate steps must be taken by the world transportation authorities in order to establish a harmonized regulatory framework for automated traffic systems and vehicles, which would enable the safe deployment of these technologies across national borders.

EU Initiatives and Research Programs

Pursuant to this need for harmonization, the EU has implemented various directives[25] to give the EU Commission the power to adopt the necessary regulatory provisions for automated

[24] 49 U.S.C. 30114 and 49 CFR Part 55.

[25] E.g., the ITS Directive (Directive 2010/40/EC), which gives power to the EU Commission to adopt functional, technical, organizational and service provision specifications for the compatibility, interoperability and continuity of Intelligent Transport Systems throughout the European Union.

traffic systems and vehicles, and various initiatives[26] aimed at, i) conducting research on the impact of automated technologies on the public road systems, and ii) developing legal standards for ensuring public safety.

In the 7th Framework Program for Research and Technological Development, the EU Commission initiated several research projects focused on assessing automated vehicle technology and developing strategies, technologies and integration of the automated systems into current regulatory frameworks. One such EU funded project, AdaptIVe,[27] is a 42-month EU funded project designed to address the major challenges of automated driving. By December 2016, the project will have defined the legal aspects of automation on EU public roadways, with final project results to be presented in June 2017. The goals of the project are to demonstrate the feasibility of automated driving, provide guidelines for cooperative controls and define and validate new methodologies for safety evaluation. Further, AdaptIVe will assess any impact automation has on road transport and will evaluate the legal framework with regard to barriers to implementation.

Expanding on the notion that automated vehicles can include more than just personal passenger vehicles, the 7th Framework Program also funds projects looking to automate public transportation systems (buses, taxis, etc.). CityMobil2[28] is an EU funded project that is working to develop a prototype automated transport system for urban areas with low passenger numbers. Automated transport systems are made up of multiple vehicles operating without a driver in what is known as collective mode. These vehicles will operate on-demand, in the same fashion as an elevator, and allowed to run in dedicated areas of the city; pedestrian areas, car parks, private sites such as a hospital or a college campus, or on dedicated lanes (such as bus lanes when they are not in use). The goal of this project is to determine the feasibility of implanting such a system in urban areas throughout Europe, and to gather useful data to help develop new regulations and/or modify the current legislation as they relate to automated vehicles in order to relax the current constraints.

E-call Initiative

In early 2009, the European Parliament, in its resolution on the Intelligent Transport Systems Action Plan (ITS Action Plan),[29] underlined the importance of digital technologies for safer and more secure, cleaner and more efficient transport in the EU. Among the first priorities of the ITS Action Plan was the "eCall" emergency system. The purpose of the eCall initiative is to bring rapid assistance to motorists involved in traffic collisions anywhere in the EU. In the event of a vehicle-involved accident, an eCall-equipped vehicle will automatically call the nearest emergency center. The eCall system is a partially automated system that will automatically send a minimum set of data whenever an accident occurs. This data will include the exact location of

[26] *See*, iMobility Forum (http://www.imobilitysupport.eu/) and the C-ITS Platform (http://ec.europa.eu/transport/themes/its/news/c-its-deployment-platform_en.htm), which bring together private and public stakeholders to coordinate technical developments on European level and to ensure interoperability and coherent deployment of the automated traffic and vehicle systems.

[27] *See*, https://www.adaptive-ip.eu/.

[28] *See*, http://www.citymobil2.eu/en/.

[29] *See*, European Parliament resolution of 23 April 2009 on Intelligent Transport Systems Action Plan (2008/2216(INI)).

the accident, type of vehicle involved, and other important vehicle statistics, so that first responders can be deployed to the accident location even if all passengers of a vehicle are unable to speak to a live emergency center operator. The eCall system will significantly cut emergency response times, thus potentially saving hundreds of lives in the EU every year. The eCall regulation requires all new cars to be equipped with eCall technology beginning April 2018.

Evaluation of EU Member State Existing Regulations

Despite the EU's efforts to harmonize the regulation of automated vehicles on European roads, many of the EU Member States have begun proactively assessing their current regulations and legislation to determine what additions or modifications are needed to account for automated vehicles on their public roads.

United Kingdom

In the United Kingdom, the Department for Transport (DT), recognizing the potential benefits of driverless and automated technologies to reduce vehicle related fatalities and improve overall road safety, has developed a Code of Practice (CoP) for those technology companies wishing to test their automated vehicles on public roads.[30] CoP is expected to provide preliminary standards for using automated vehicles on public roads. Any data acquired from such testing will be used to enhance existing regulations. The DT conducted a detailed review of its existing legislation to establish the regulatory framework with respect to testing of automated vehicles and their longer-term introduction to the market. It concluded that "real-world testing of automated technologies is possible in the UK today, [provided] a test driver is present, and takes responsibility for the safe operation of the vehicle; and that the vehicle can be used compatibly with road traffic law."[31] Following the testing of automated vehicles on UK public roads, the DT will establish and clarify the necessary changes to its legislation in order to allow these technologies to come to market.

Germany

The German Ministry of Transport and Digital Infrastructure (BMVI) is hoping to utilize the same type of automated vehicle testing programs to transform Germany into the leader of Europe's automated traffic systems and vehicles. The Ministry believes that by 2020, it will be able to bring highly automated vehicles to German roads that are i) capable of driving in structured, less complex traffic environments, such as on the Autobahn, and ii) capable of driving at low speeds in places such as car parks.

The German government has identified areas in which existing regulations need to be modified. These include adjusting the term "driver" as currently defined to include "systems with full control over a vehicle." This is important from a liability standpoint, as discussed below, because one of the biggest questions with driverless vehicles is who is responsible in the case of an accident, the human occupant, or the car? Further potential modifications to existing regulations include allowing for automatic lane changes at a high rate of speed, and enabling automated and connected drive systems to participate in road traffic.

[30] *The Pathway to Driverless Cars: A Code of Practice for testing*, Department for Transport, UK (2015).

[31] *The Pathway to Driverless Cars*, Department for Transport, UK (Feb. 2015)

2 –PRIVACY AND DATA PROTECTION

Connected cars and automated vehicle technology provide consumers with a customized and personalized driving experience. However, in order to tailor such an experience a significant amount of data is collected and transmitted. This data can include information about the exact location of the vehicle, or information about how a driver operates his car. This raises significant questions for not only legislators and regulators but also car manufacturers and technology companies, such as Google and Apple.

For example, to what extent is data collected from a vehicle "personal data," i.e. attributable to a specific individual and, as such, subject to the Fair Information Practice Principles? Assuming that some of the data collected from or through the intelligent vehicle qualify as "personal data," numerous issues arise, such as:

- **Processing and notice:**
  Who is the controller of the processing of such data and how to inform individuals of the nature of the collection, processing or dissemination of personal data?

- **Consent:**
  How can the driver and the passengers express their consent or objection to the collection of data produced by their vehicle?

- **Choice:**
  How can individuals control whether or when their personal data is collected or used?

- **Access by third parties:**
  When and in which circumstances may the personal data be shared with third parties or reused for purposes other than the original purpose (e.g., in liability cases?)

- **Security:**
  Connected vehicles and intelligent vehicles rely on a vast ecosystem of specialized entities such as vendors, service providers, outsourcers, hosting companies, internet service providers that furnish the content, the data, and the connections, that are necessary for the vehicle to move safely, interact with the traffic, suggest or make decisions to and perform its primary functions. How is it possible to ensure data security in such a complex and co-dependent environment?

USA

The Rise of Self-Regulation

The Alliance of Automobile Manufacturers and the Association of Global Automakers have been proactive in this area and have taken self-regulatory measures with the publication of

"Consumer Privacy Protection Principles for Vehicle Technologies and Services" in November 2014.[32]

The Principles provide a framework for the protection of personal information through in-car technologies. They are not intended to replace applicable laws and regulations, where they exist. In this context, the Principles should be interpreted as subject to and superseded by applicable laws and regulations.

The Principles apply to the collection, use and sharing of covered information[33] in association with "vehicle technologies and services"[34] available on cars and lights trucks sold or leased to individual consumers for personal use in the United States. Participating Members commit to seven principles regarding:

- **Transparency:**
  Members have committed to providing car owners and registered users with access to clear and meaning full notice about their collection, use and sharing of covered information.

- **Choice:**
  Owners and registered users will be provided with certain choices regarding the collection, use and sharing of covered information.

- **Respect for Context:**
  Members have committed to using and sharing covered information in ways consistent with the context in which it was originally collected, taking into account the likely impact on owners and registered users.

- **Data Minimization, De-identification and Retention:**
  Covered information will be collected only as needed for legitimate business purposes, and it will be retained for no longer than the Member determines necessary for legitimate business purposes.

[32] A copy of the Privacy Protection Principles is available at http://www.globalautomakers.org/system/files/document/attachments/Global%27s%20and%20the%20Alliance%27s%20FTC%20Letter%20Committment%20and%20Privacy%20Principles%20%282%29.pdf.

[33] "Covered Information" is defined in the Principles as information that is linked or linkable to i) the vehicle from which the information is retrieved; ii) the owner of that vehicle; or iii) a registered user of that vehicle's technologies and services. Further, covered information is information that vehicles collect, generate, record or store in an electronic format that is retrieved from the vehicles by or on behalf of a participating member in connection with Vehicle Technologies and Services; or Personal Subscription Information provided by individuals subscribing or registering for Vehicle Technologies and Services. Covered information includes biometric, driver behavior, and geolocation Information.

[34] Vehicle Technologies and Services is defined as referring to technologies and services provided by, made available through, or offered on behalf of participating members that involve the collection, use, or sharing of information that is collected, generated or recorded or stored by a vehicle.

- **Data Security**
  Members are committed to implementing reasonable measures to protect covered information against unauthorized use or access.

- **Integrity and Access:**
  Members will implement reasonable security measures to maintain the accuracy of covered information. They have committed to offering owners and registered users reasonable means to review and correct personal subscription information provided during the subscription or registration process for vehicle technologies and services.[35]

- **Accountability:**
  Members have committed to taking reasonable steps to ensure that they and other entities that received covered information adhere to the Principles.[36]

Members committed to meeting or exceeding the above commitments for new vehicles manufactured no later than Model Year 2017, and for vehicle technologies and services subscriptions that are initiated or renewed on or after January 2016. As of January 2016, all Participating Members are accountable to the Federal Trade Commission for their implementation of these principles.

In 2015, the Alliance of Automobile Manufacturers and the Association of Global Automakers established the Automotive Information Sharing and Analysis Center (Auto-ISAC) to share intelligence about vehicle cybersecurity threats. Early in 2016, these bodies published a Cybersecurity Best Practice Framework[37]and they are currently working together to develop automotive cybersecurity best practices that will be modeled on the aforementioned framework.

Proposed Federal Legislation

Throughout the course of 2015, a number of bills were published at the federal level dealing with the data privacy and security implications of connected cars and automated vehicle technology.

- **Security and Privacy in Your Car Act 2015**

In July 2015, Senator Edward Markey and Senator Richard Blumenthal proposed legislation, namely the Security and Privacy in Your Car Act ("SPY Car Act")[38], directing NHTSA and the

[35] Personal subscription information is information that individuals provide during the subscription or registration process that on its own or in combination with other information can identify a person, such as a name, address, credit card number, telephone number or email address.

[36] In this respect, Members that use a third-party service provider to provide some or all of their vehicle technologies and services have committed to taking reasonable steps to ensure that the service provider adheres to the Principles.

[37] See, https://www.globalautomakers.org/system/files/document/attachments/framework_auto_cyber_best_practices_14jan2016_id_10376.pdf

[38] S1806 is based on the findings of Senator Markey's 2015 Report, Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk, available at http://www.markey.senate.gov/imo/media/doc/2015-02-

Federal Trade Commission to conduct rulemaking to implement cybersecurity standards for vehicle systems and for driving data security, such as location data and driving history.

The current draft of the bill would direct NHTSA to issue regulations requiring that motor vehicles manufactured for sale in the U.S. to protect against unauthorized access to i) electronic controls or driving data, inclusive of information about vehicle location, speed, owner, driver or passengers; or ii) driving data collected by electronic systems integrated in the vehicle while that date is stored onboard the vehicle, in transit to another location or subsequently stored or used off-board the vehicle. Under the SPY Car Act, the NHTSA regulations would have to require that vehicles with accessible data or control signals be capable of detecting, reporting, and stopping attempts to intercept driving data or to attempts to control the vehicle itself. The SPY Car Act would also direct NHTSA to issue regulations requiring manufacturers to affix a "cyber dashboard" display to a vehicle in order to inform consumers about the extent to which a vehicle protects an individual's cybersecurity and privacy under the Act.

Under the SPY Car Act, the FTC would have to draft regulations to i) require the notification of owners/lessees about the collection, transmission, retention, and use of driving date; ii) provide owners/lessees with an option to terminate such data collection and retention[39] without losing navigation tools or other features; and iii) prohibit manufacturers from collecting information for advertising or marketing purposes without consent. Violations of these provisions would be treated as unfair and deceptive acts or practices under the Federal Trade Commission Act. The SPY Car Act was referred to the Committee on Commerce, Science, and Transportation.

- **The Security and Privacy in Your Car Study Act 2015**

In November 2015, Representatives Ted Lieu and Joe Wilson proposed legislation[40] that would require NHTSA to conduct a one year study, consulting with the FTC, Department of Defense, National Institutes of Standards and Technology, and industry leaders and higher education institutions, to recommend a framework for regulating car automated software safety, cybersecurity and privacy regulations.

- **Autonomous Vehicle Privacy Protection Act of 2015**

In November 2015, Representative Grace Meng introduced a bill aiming to protect consumer privacy during the development and use of autonomous vehicle technologies. H.R.3876[41] proposes that the US Comptroller General be required to make available to the public a report that assesses the organizational readiness of the DoT to address vehicle technology challenges, including consumer privacy protection.

06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf. A copy of the bill is available at https://www.markey.senate.gov/imo/media/doc/SPY%20Car%20legislation.pdf.

[39] There is an exemption for onboard safety systems required for post incident investigations, emissions, crash avoidance, and other regulatory compliance programs.

[40] *See*, https://lieu.house.gov/sites/lieu.house.gov/files/documents/SPY%20Car%20Study%20Act.pdf.

[41] *Available at* https://www.congress.gov/bill/114th-congress/house-bill/3876/text.

H.R. 3876 seems to stem from specific provisions in H.R. 22 Fixing America's Surface Transportation Act[42], which was also issued in 2015. Section 6025 of which provides that, not later than 2 years after the enactment of H.R. 22, the Comptroller General will submit a report to Congress that will:

- Assess the status of autonomous technology policy developed by public entities in the US;
- Assess the organizational readiness of the DoT to address autonomous vehicle technology challenges, including consumer privacy protections; and
- Recommend implementation paths for autonomous transportation technology, applications, and policies.

Europe

eCall Initiative and Privacy

The European Commission adopted Regulation (EU) 2015/758 [43], which establishes the rules of the eCall initiative. Section 6 of the Regulation lays down specific provisions related to the privacy of the personal data of the users (i.e., owners of the car) of the eCall system. Essentially, the provisions follow the data protection principles laid down in EU Data Protection Directive 95/46/EC .For example, under the Regulation, the data must be used only to handle emergencies.

In terms of data retention, the Regulation requires that data must be deleted as soon as they are no longer necessary for such purposes. In other words, if no accident occurs, the data must be cancelled right away.

Manufacturers must ensure that the 112-based eCall system[44] is not traceable and not subject to constant tracking. The data in the system (i.e., in the memory installed in the cars) must be automatically removed, with one exception: the last three locations recorded can be kept, only as long as it is necessary to understand the exact location and the direction the car was traveling at the time of the accident. In addition, no individual outside the eCall system may have access to the data, and privacy enhancing technologies must be used to minimize risks of privacy violations and misuse. EU Privacy Law[45] requires that due notice of data processing must be given to the data subject (i.e. the person whose data are being processed). In the case of eCall, the manufacturers have such obligation. This information is to be provided for in the owner manual.

Regulation (EU) 2015/758 is a good starting point to address the more general issue of privacy in autonomous cars, just as in any other electronic device (like navigators) being used in connection with the use of the car.

[42] *Available at* https://www.congress.gov/bill/114th-congress/house-bill/22/text.

[43] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0758&from=EN.

[44] 112 is the uniform emergency number used in all of Europe.

[45] See, e.g., Data Protection Directive 95/46/EC which currently serves as the basis for the data protection laws of the 31 member states of the European Economic Area.

Current EU Privacy Law and Autonomous Cars

The current data protection laws in effect in the European Union generally require that if any person wishes to collect and process the personal data of any given natural person, it must inform this individual (defined under the law as "data subject") that it is going to process such data, and provide the individual with the reasons for the processing. In certain cases, the consent of the data subject will be necessary, in other cases it will not, for example, if the data are necessary to perform a contract, or if the data have to be processed to comply with a legal obligation.[46]

These same principles should apply in the case of personal data that is being processed by an autonomous car. In this respect, one of the major issues is the processing of geo-location data. Assuming the car has a navigation system that memorizes the different locations the driver has visited; this creates certain privacy issues, which are similar to those that arise with smartphones or smart devices in general.

The rules on the processing of data from mobile smart devices have been clearly addressed by the Article 29 Working Party, [47] in a document published in 2011. [48] The Article 29 Working Party opinion could serve as a basis for a similar analysis to be applied to the connected car or intelligent car market. In 2011 opinion, the Article 29 Working Party stated that the data controller can be the subject that controls and manages the ITC infrastructure, or the provider of the geo-localization services, or the developer of the operating system (although this latter only when and if it interacts directly with the user). By analogy, one can conclude that the maker of the IT system of the car can be regarded as one of the possible controllers of the data processing.

The Article 29 Working Party has taken the position that the informed consent of the user must be obtained to process the location, as well as to supply value-added services to the users.[49] Location data and data about driving habits are of immense value for insurance companies; the knowledge that a car driver frequently is present in certain areas may be an indication of higher potential for the car (or some of its devices) to be stolen, with obvious consequences. In certain EU Member States, geo-localization services require prior notification to the local Data Protection Authority.

Another potential privacy issue is breaches of security that compromises personal data. In general, EU privacy laws require that security measures be taken to protect personal data. In the

[46] Section 7 of the EU Directive 95/46/EC indicates the criteria for legitimate processing of personal data http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en.

[47] The WP 29 is a working party established by Section 29 of EU Data Protection Directive 95/46/EC. It is an independent body, composed by members of the EU Member State Data Protection Authorities, with consulting powers.

[48] WP 185; Opinion 13/2011 on Geo-localization on Smart Mobile Devices, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf.

[49] Given the sensitivity of the processing of (patterns of) location data, *prior informed consent* is the main applicable ground for legitimizing the data processing of the locations of a smart mobile device in the context of information society services, WP 185, Sec. 5.3.1, page 13, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf

context of autonomous cars, this means a significant effort to prevent the autonomous technology from being hacked and the data being stolen. Under EU law, the security of personal data is a major obligation of the controller. In terms of autonomous cars, the obligation to protect the data is likely to be the responsibility of the manufacturer of the car or that of the manufacturer of the digital devices and software, or perhaps both.

Under the upcoming EU General Data Protection Regulation, entities that suffer a breach of security that exposes or compromises personal data will be required to inform the local Data Protection Authority[50] and, in some instances, the data subject. In the case of a data breach impacting an autonomous car, the obligation to report the data breach would likely rest with the data controller, who may not be aware of the theft and, therefore may not be in the condition to file the report within the given timeframe. One possible workaround may be to contractually agree that, in case of theft, there must be a way for the car owner to inform the data controller, so that he may fulfill its obligation to report the data breach.

Can the personal data collected with car usage be communicated to third parties, and if so, what data may be communicated? Regulation (EU) 2015/758 prohibits any use of the data of the eCall system other than for emergencies. Thus, such data cannot be used for any other purpose. Data collected by separate, different devices can be communicated to third parties only subject to the previous informed consent of the owner of the car. This could be the typical method to supply or offer value added services to the owner of the car.

The amount of personal data that can be recorded, stored, and processed from the use of an autonomous car is potentially enormous. The number and variety of services that could be offered is equally very high. It should be expect that businesses will try with every possible means to gather as much data as they possibly can. Once again, the collection of such data would have to be balanced and verified in the light of the relevance and adequacy test called for by European privacy law. If they exceed the purposes for which the data is collected (that must have been clearly stated in the privacy notice to be provided to the data subject) any processing for additional or new purposes may be illegal and subject to significant sanctions.

3 – LIABILITY ISSUES

In the United States, the regime of liability for defective products (product liability law) is very complex. It involves concepts of contract law (contract law) and the law of torts and torts (tort law). For manufacturers of connected cars, product liability law will have a significant impact on their strategy to bring their products to market. The legal precedents that have been established for product liability law will provide manufacturers with a strong incentive to ensure that every connected car that they build will be as safe as possible for consumers.[51]

Driverless cars, for example, pose the greatest risk that accidents involving these vehicles could be attributable in whole or in part to defects in the automation systems. In a recent case, researchers have demonstrated that certain connected cars can be hacked and that hackers can remotely control vehicle functionality by exploiting security defects in the vehicle's software.

[50] Under section 31 of the new EU General Data Protection Regulation data breaches will have to be reported to the relevant Data Protection Authority within 72 hours

[51] *See* Restatement (Second) of Torts § 402A.

This susceptibility of the connected car to malfunction or to be remotely accessed is a legitimate and important concern that can be addressed with a thorough understanding of current product liability law, which is a combination of tort law and contract law.

Products liability jurisprudence pertaining to the sale and operation of vehicles abounds. However, the operation of intelligent cars, driverless cars, connected cars and the like brings new interesting twists that remain to be explored. It is not clear how the artificial intelligence aspect of the operation of the new vehicles of the 21st century will be treated in the application of centuries old products liability law.

Overview of United States Products Liability Law

When a defective product (or misrepresentations about a product) causes harm to persons or property, products liability law can be the conduit for seeking remedies against manufacturers of the defective product. Involving a mixture of tort law and contract law, products liability provides victims with redress for their injuries through lawsuits seeking damages.

Tort law can focus on strict liability, negligence, or misrepresentation, while contract law is implicated by the commercial nature of product marketing and sales (e.g. through explicit and implicit warranties with respect to the quality of a product). If a product fails to meet sufficient quality standards, and that failure is the cause of an injury to a consumer who uses the product reasonably, the seller could be liable for breach of warranty.

Typically, plaintiffs in product liability suits cite multiple theories of liability in order to maximize the odds of prevailing and obtaining a damages award. This paper will discuss strict liability, negligence, misrepresentation, and breach of warranty, as they appear to be the most applicable to the automotive industry and connected cars.

Applicability of United States Strict Products Liability

Of the theories of products liability likely to be brought by consumers against manufacturers of connected cars, strict products liability would provide the best theory for recovery for an injured consumer. Under a strict product liability theory, even if a manufacturer exercises the highest level of care in its attempt to build a safe product, if the product that is ultimately shipped to the consumer contains an unsafe defect, and such defect causes an injury to the user of that product, the manufacturer would be strictly liable for all resulting and foreseeable damages.

Strict liability is essentially based on the consumer's expectations that the product should not be unreasonably dangerous. In general, a consumer who claims that a manufacturer is strictly liable for the harm caused by a defective product will argue that the product suffered from a manufacturing defect, a design defect, or that the product lacked a specific warning for the type of injury that resulted from use (or misuse) of the product.

Under the Restatement (Second) of Torts, a manufacturer is liable for the sale of a product containing an "unreasonably dangerous" defect even if the manufacturer has "exercised all possible care in the preparation and sale" of the product. Further, even if the user of the product "has not bought the product from or entered into any contractual relation with the seller," strict liability can apply.[52]

Consequently, any entity (i.e. manufacturer, wholesaler, dealer, retailer, etc.) in the product distribution chain can be held strictly liable,[53] and the user need not have purchased the product at all. The rationale for holding these entities liable is based on the economic benefit that they derive from the sales of the products.

A strict liability argument may take several forms. It can be based on a manufacturing defect, a design defect, or the use of inadequate warning.

Manufacturing Defect

A manufacturer, or any entity in the chain of distribution, may incur liability if it fails to discover a flaw in the product it is manufacturing or selling. To successfully bring a claim of strict products liability for a manufacturing defect, the plaintiff must show, by a preponderance of the evidence, that the product left the manufacturer in a defective condition that was unreasonably dangerous to the user or consumer, and that such defect was the actual and proximate cause of his injuries.[54]

Recently, several car manufacturers, such as Mercedes-Benz, Volvo, and General Motors, have developed advanced software systems that automatically apply the vehicle's brakes in order to avoid a front-end collision. Such technology would undoubtedly be included in connected cars and driverless cars.

Suppose that a manufacturer of an autonomous vehicle, who performs all the necessary safety and quality control tests on its vehicles, accidentally ships one vehicle with faulty braking software. Suppose further, that this vehicle becomes involved in an accident, and such accident is attributable to the fault in the braking software. If the driver, passenger, or bystander is injured in the accident, they could raise a claim for strict liability arising from this manufacturing defect. The manufacturer could be found strictly liable for the dangerous software fault, even though it exercised all possible care in preparing and shipping the product.

Design Defect

A manufacturer could also be subject to liability if the design of the product itself is defective in nature. If a product has a defective design, the defect that causes injury to the consumer is inherent in every product that leaves the manufacturer.

To successfully bring a claim of strict products liability for a design defect, the plaintiff must establish that the product's defective design was the actual and proximate cause of his injuries.

[52] *Id.* Strict liability will also apply if "the seller engaged in the business of selling such a product." Thus, a private individual who sells a used car would not be liable for a manufacturing defect it might contain.

[53] While any entity in the distribution chain could be held liable for a consumer's injury, ultimately, those entities will seek indemnification from the manufacturer.

[54] *Colon ex rel. Molina v. BIC USA, Inc.*, 199 F. Supp. 2d 53, 85 (S.D.N.Y. 2001) ("[T]he plaintiff must show that a specific product unit was defective as a result of 'some mishap in the manufacturing process itself, improper workmanship, or because defective materials were used in construction,' and that defect was the cause of plaintiff's injury.").

Further, the manufacturer must show that benefits of the design outweighed the risk of danger posed by such design.

Under this risk/benefit test, a product's design is evaluated by considering the gravity of the danger posed by the design, the likelihood such danger would occur, the feasibility of a safer alternative design, the financial cost of an improved design, and the adverse consequences to the consumer resulting from an alternative design. In the context of connected cars and autonomous vehicles, liability complaints alleging design defects will likely arise in connection with the shared responsibilities between the vehicle and the human occupant/driver.

The National Highway Traffic Safety Administration (NHTSA) has developed five levels of automation for connected cars and automated vehicles. Under automation Level 2, for example, the vehicle would have systems where there exists "automation of at least two primary control functions designed to work in unison to relieve the driver of control of those functions." Further, the "driver [would still be] responsible for monitoring the roadway and [for] safe operation and is expected to be available for control at all times and on short notice."[55]

If a manufacturer markets and sells an automated vehicle that it claims has NHTSA level two automation, and an accident occurs involving this vehicle because the system failed to provide the required "short notice" advanced warning, then an injured party would likely bring a design defect cause of action. The plaintiff would argue that the vehicle should have been designed to provide more advanced warning that the driver should assume control. The manufacturer might counter this argument by stating i) that the system provided sufficient warning, but the driver did not react timely, ii) that modifying or altering the system to provide even more warning would necessitate adding costly sensors or equipment to the vehicle, and iii) that even if such alterations or modifications were feasible at the time of manufacture, the increase in warning time would be marginal and not make a practical difference in the drivers ability to react.

Inadequate Warnings

A manufacturer may also be liable for failure to warn consumers about a danger or hazard when it knows or should have known about an inherent danger or hazard regarding its product. In order to minimize exposure to liability, manufacturers are becoming more conservative with the warnings that they provide.

For example, Mercedes-Benz manufactures some of its cars with an automatic cruise control system it calls "Distronic Plus." This system utilizes a radar system that automatically maintains a safe distance from the vehicle in front and during highway driving and in stop-start traffic. The system applies the brakes automatically to help reduce the risk and severity of front-end collisions. In its warning, Mercedes-Benz states "[a]lways pay attention to traffic conditions even when DISTRONIC PLUS is activated. Otherwise you may fail to recognize dangers in time, cause an accident and injure yourself and others."[56] With the advent of new forms of vehicle automation, and with the driverless vehicles, manufacturers will no doubt include warnings related to these new systems.

[55] *See*, Press Release, NHTSA, U.S. Department of Transportation Release Policy on Automated Vehicle Development (May 30, 2013).

[56] *See*, Mercedes-Benz E-class owner's manual.

Interestingly, with respect to autonomous vehicles, the failure to provide adequate warnings to the consumers may arise post-sale when and if the manufacturer discovers new risks with the operation of its vehicles. Under the Third restatement, manufacturers have a duty and clear responsibility to provide adequate warnings to consumers regarding newly discovered risks.[57] As a result of the inclusion of this post-sale requirement to provide warning, many states have adopted new requirements regarding a manufacturer's responsibility to provide post-sale warnings with regard to newly discovered risks.

It is likely that future litigation for product defects resulting from inadequate warnings would be mitigated by the government's attention to consumer safety and protection. NHTSA, for example, conducts investigations for defects and administers safety recalls related to various defects it discovers. Manufacturers would, thus, be able to address any potential defects before actual injury occurs.

Manufacturers of connected cars and automated vehicles may also be required under post-sale safety notification regulations to provide software upgrades for the vehicles. As the manufacturer becomes more aware of potentially risky software problems, it will need to quickly provide updates to resolve the issues, while ensuring that the new software update is appropriately tested and safe to use before its release.

Applicability of United States Negligence Law

If a consumer is injured by a defect with a connected car or autonomous vehicle, and strict liability is not available as a cause of action, the consumer may seek redress for his damages through a claim of negligence. Under a negligence theory of products liability, the plaintiff must show that:

- The manufacturer had a duty to exercise the appropriate standard of care in designing the product;
- The manufacturer breached that duty, and
- The manufacturer's breach of that duty was the actual and proximate cause of the plaintiffs' injuries.

Product manufacturers have a duty to exercise a reasonable degree of care in designing their products so that they are safe when the consumer uses the product in reasonably foreseeable ways. A manufacturer of automated vehicles has a duty to design its vehicles with at least the same care as a "reasonable manufacturer" would under similar circumstances.

As mentioned above, suppose Mercedes-Benz designed its Distronic Plus system to be fully automated in that no driver intervention was needed. Suppose further that Mercedes-Benz only tested its Distronic Plus system on vehicles driven on a dry, uniformly paved, test circuit. If it is later discovered that the system fails to properly and reliably engage on uneven surfaces or in wet weather conditions, and a person is injured as a result of this failure, then Mercedes-Benz would be liable for negligence in implementing and equipping its vehicles with the system. The injured person would be able to argue that his injuries were directly attributable to Mercedes-

[57] *See*, Restatement (Third) of Torts § 10, 'Liability of Commercial Product Seller or Distributor for Harm Caused by Post-Sale Failure to Warn."

Benz's negligence and that it was reasonably foreseeable that a car equipped with the Distronic Plus system would be used on uneven or wet roads.

Potential Application of Misrepresentation Law

Under US products liability cases may also include claims of misrepresentation regarding the quality of the product. A tortious misrepresentation involves the communication of false or misleading information. Liability for misrepresentation can occur when a person reasonably relies on the misrepresented information and suffers some harm.

There are several subcategories of misrepresentation; including:

- Fraudulent misrepresentation (where a party knowingly provides false or misleading information that causes harm);
- Negligent misrepresentation (where a party providing the information knew or should have known that the information was false), and
- Strict liability for misrepresentation (where it need not be shown whether the defendant knew that the information was false).

It is important to note that misrepresentation does not always involve a product defect, and would not arise from a manufacturing or design defect, but from the distribution of misleading information about the vehicle's capabilities when it was conveyed to the buyer.

In the context of an automated vehicle, a manufacturer could be liable for misrepresentation if it stated that the driver would only "very rarely" be required to take control of the vehicle (e.g., during the use of the Distronic Plus system), when in fact the driver is alerted by the vehicle to take control every few minutes. The consumer of this vehicle could bring a claim for damages based on the manufacturer's misrepresentation of how often the driver would need to take control of the vehicle.

Breach of Warranty

Strict liability, negligence, and misrepresentation are all causes of actions that could be brought under tort law. As stated above, products liability involves contract law through the warranties a manufacturer creates by marketing and selling its products. Warranties are assurances, which can be either explicit or implicit, that the goods being sold are of sufficient quality for the consumer. If the product is proven to not meet this standard of quality, and an injury results, then the injured party will be able to bring a claim for breach of warranty.

Product warranties are governed by the Uniform Commercial Code (UCC), which provides a uniform code of law with respect to commercial transactions, and has been adopted, sometimes with modification, by all the states and territories, but some states have not adopted Article 2 on Sales, which would govern most of the issues discussed here. Indeed Louisiana and Puerto Trico opted to retain their own codes, which take their roots in civil law systems. In the context of products liability, the UCC addresses express and implied warranties.

An express warranty is created through promises made by a seller to a prospective buyer in association with the sale of goods.[58] For automated vehicles, it is likely that the manufacturer

[58] UCC §§ 2-313(1)(a), (b) and (c).

would provide the buyer with actual vehicle warranties at the time of purchase. In addition, the manufacturer of automated vehicles may provide express warranties through its advertising. Unless there is an explicit disclaimer or exclusion (e.g., through a disclaimer of being sold "as is") goods are sold with implied warranties that they are "merchantable,"[59] meaning that the product is of a high enough quality to make it fit for sale. In addition, implicit in the sale of goods is a warranty that the goods will be fit for the purpose for which they are sold.

Several new, luxury vehicles have introduced a self-parking system. Lexus is one such manufacturer. Suppose that Lexus advertised that the automated parking system functions at night as well as it does during the day, but a consumer discovers that the system fails to park successfully at night time. The consumer could bring a claim that Lexus had breached an express warranty.

Further, suppose that Lexus never advertised the automated parking system's beneficial capabilities, but instead most consumers assumed that the system was designed to aid the driver in parallel parking the car. If the system instead created a situation by rotating the steering wheel such that a collision was inevitable, then, unless it had disclaimed implied warranties, Lexus would be liable for a breach of the implied warranty of merchantability because the system was not helpful to the driver.

Recent Issues Regarding Connected Cars and Automated Vehicles in the United States

Although the above theories of liabilities are applicable to products liability in general, not all are likely to apply at the same time to connected cars or automated vehicles in any one given situation. So far, case law is virtually non-existent when it comes to products liability claims against manufacturers of automated vehicles and connected cars.

Toyota, Ford and General Motors

In March 2015, a class action lawsuit was filed against Toyota, Ford and General Motors in the U.S. District Court of California, alleging that the manufacturers knowingly put consumers at risk by selling connected cars that are susceptible to hackers looking to remotely control vehicle functionality. The claim that the plaintiffs brought against the manufacturers was under a theory of product liability (strict liability and negligence) for a defect in the car's electronic systems.

The plaintiffs argued that because the car's computer systems lacked necessary security measures, basic vehicle functions could be controlled by individuals outside of the car, which would endanger the safety of the vehicle occupants. On November 25, 2015, U.S. District Judge William H. Orrick, dismissed the case stating that the class action lawsuit's allegations were "too speculative." No cars listed in the complaint had actually been hacked, there was no "impending" harm, and the allegations of possible future injury were not sufficient to maintain the case against the manufacturers. Because no member of the class suffered actual harm, there was no viable cause of action for product liability.

[59] UCC § 2-314(1), even in the absence of an exclusion, the implied warranty of merchantability only applies to goods sold by "a merchant with respect to goods of that kind."

Jeep Cherokee

Following the March 2015 filing of the class action lawsuit against Toyota, Ford, and General Motors, other vehicles were investigated for the potential of "being hacked" by remote individuals. In a controlled experiment conducted by Wired Magazine, hackers Charlie Miller and Chris Valasek successfully infiltrated the software system of a Jeep Cherokee and took control of internal functions such as the climate control system, the radio, windshield wipers, steering, brakes, and transmission.

Since the Jeep is a connected car, it is continuously transmitting information to, and gathering information from the Internet. It is through this capability that the hackers were able to introduce their malicious code and take control of the vehicle. Similar to the class action against Toyota, Ford and General Motors, it would be unlikely that a consumer who owns a similar model of Jeep Cherokee could bring a products liability claim against the manufacturer and succeed. This is because, to date, there have been no instances in which a Jeep, or any other connected car, has been hijacked by a hacker remotely.

However, assuming that these manufacturers, knowing that a defect in their software exists, do nothing to patch this exploitation and a consumer is injured as a result of being remotely hijacked, then such consumer could bring a products liability claim against the manufacturer if he suffers an injury. In this example, if Jeep does nothing to fix the holes in its software code that allowed for remote hacking, then it could be strictly liable for any injuries that result from the hacking. The software is allegedly clearly defective, and if the same code appears in the software on all Jeep Cherokees manufactured and sold, then there might be a design defect.

Should the consumer fail in bringing a claim for strict product liability, then it might be apparent that the manufacturer was negligent in not ensuring that the software was free from defect before shipping to the consumer, as well as negligent for not taking necessary actions to remedy the problem.

Finally, Jeep may be liable for breach of the implied warranty of merchantability. A consumer who purchases this particular model of car would expect that the automated and connected systems would be impervious to outside attack. Because the vehicle would be seemingly unfit to use due to the potential for remote hacking, the purchaser of the vehicle could assert that the implied warranty accompanying the sale of the vehicle had been breached.

So far, there have been no reported instances of actual remote hacking of vehicles, outside of the tests conducted by Wired Magazine and others. Because no person has been injured by defects of this type, it is unlikely that a products liability cause of action based on this event would be successful.

Vehicle Data as Evidence

In addition, in case of accidents, all the data deriving from these systems may be required as evidence. All of it is in digital form: appropriate forensic tools and techniques are required to access and subsequently produced as acceptable evidence.

The production of connected cars that use sophisticated Internet technologies to transmit data to the manufacturers' system is still very limited, and as a result, there are no reported cases that fully analyze the issues in this set of circumstances. However, in a not too long distant future it is likely that one of the vehicles that rely on sophisticated computing technologies will suffer a hack or will encounter an error that might damage property or cause injuries to individuals. In that case, there presence of an injury would likely result in the complaint not being rejected, and the case moving through. At that time, the court may have to carefully evaluate the fact to determine whether the situation fits within existing models or the presence of computer technologies justify new analysis.