JONES DAY | One Firm Worldwide®

WHITE PAPER

May 2021

Autonomous Vehicles: Legal and Regulatory Developments in the United States

The evolution of autonomous vehicle technology and its forthcoming widespread use have the potential for many societal benefits, including safer roads, greater economic productivity, and better fuel economy. Along with the innovations and industry growth, stakeholders in the industry will encounter a broad range of legal issues.

This Jones Day *White Paper* updates our prior publication regarding the legal and regulatory issues related to autonomous vehicles. It focuses on self-driving passenger automobiles and sets forth the developments in the areas of: (i) automated technology; (ii) state and federal regulations; (iii) product liability; and (iv) liability concerns related to cybersecurity and data privacy.

TABLE OF CONTENTS

Background 1

Degrees of Automation 2

Timelines to Automation 2

Remaining Technological Challenges 3

- Machine Learning 4
- Wireless Communications 4
- A Summary Model 5

Regulation 5

An Open Landscape 5

- Federal Regulation 6
- State Regulation 8

Legal Issues 8

Liability Considerations 9

- Collecting and Storing Electronic Data 9

Liability Paradigms 10

- Federal Preemption 10
- Strict Product Liability 11
- Breach of Warranty 14

Specific Liability Concerns Relating to Cybersecurity and Data Privacy 15

- Cybersecurity 15
- Data Privacy 16
- Self-Help—Uncertainty Should Not Prevent Action 17

Conclusion 18

Lawyer Contacts 19

Endnotes 19

Driverless vehicles are coming onto our horizon. As they are adopted for widespread use, they will promote efficiency and spur innovation in a number of industries and transportation infrastructures worldwide. At the same time, high levels of vehicle automation present unique safety, cybersecurity, and data privacy issues for manufacturers, suppliers, sellers, consumers, and the public.

The diverse technological options both in equipment and software have created a market full of competitors striving to prove their worth. The United States federal government, so far, has refrained from choosing a winning technology or implementing a comprehensive regulatory regime. While many states have passed laws addressing autonomous vehicles, they have generally taken a permissive approach that encourages development and testing. Therefore, the laws adopted to date are far from uniform and provide significant flexibility to companies investing in the research and technology that will drive the future of the highly automated vehicle ("HAV").

This *White Paper* updates the technological, regulatory, and liability developments in the United States since our last *White Paper* in November 2017. It will address product liability rules and regulations faced in the United States by HAV manufacturers, suppliers, and sellers, and also identify legal issues that likely will arise. At present, in the absence of comprehensive state or federal legislation, traditional tort liability principles will typically govern, while law professors and commentators wrestle with predicting future liability rules. Many expect decreasing emphasis on the common-law negligence of human drivers as they play less of a role, and eventually no role, in operating HAVs. The independent functioning of HAVs puts an increasing emphasis on product design as a cause of future accidents, and questions of product design invoke familiar concepts of product liability.

Product liability rules likely will continue to adapt, as they always have, to address the unique concerns that arise within the budding HAV sector. Federal preemption could play a substantial role in shaping tort liability, but to what degree and manner remain unresolved, because the federal government has not yet acted with defining legislation. The areas of cybersecurity and data privacy raise special concerns for manufacturers of autonomous vehicles and their suppliers, and some have called for federal legislation on these issues in particular. Without federal intervention, manufacturers and suppliers can engage in self-help through contractual risk allocation, indemnification agreements, limitation of warranties, consumer education and training, industry standards, and insurance. This *White Paper* aims to provide practical advice for HAV manufacturers, suppliers, and sellers to consider now to mitigate the risk of product liability claims.

BACKGROUND

Many vehicles on the roadway already are fitted with automated driving features, and fully autonomous cars are in development and testing. Other types of autonomous transportation, such as drones, trains, ships, shuttle buses, and trucks, will support a variety of industries. Already, certain retail vendors are testing the use of autonomous drones for home delivery of online purchases,[1] one company has begun delivering pizzas by robot,[2] and at least one shipping company is using partially automated trucks to haul cargo across the southwestern United States.[3] Truck platooning and driverless taxis and buses seem to be next. This emerging technology will affect even industries that do not directly deploy autonomous vehicles. The growth of autonomous transportation eventually will yield fewer roadway accidents; the growth of vehicle sharing will decrease demand for traditional parking; and the optimization of vehicle functions will reduce the consumption of fuel, lubricants, chemicals, and degradable materials.[4] The wide-ranging uses and applications of this technology raise too many issues across many industries to address in one *White Paper*. This *White Paper* focuses on self-driving passenger automobiles, their regulation, and the legal issues arising from an automated infrastructure.

Degrees of Automation

The Society of Automotive Engineers International ("SAE") defines vehicle automation along a spectrum (zero to five).[5]

SAE AUTOMATION LEVELS

No Automation

The full-time performance by the human driver of all aspects of the dynamic driving task, even when enhanced by warning or intervention systems.

Driver Assistance

The driving mode-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task.

Partial Automation

The driving mode-specific execution by one or more driver assistance systems of both steering or acceleration/deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task.

Conditional Automation

The driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task with the expectation that the human driver will respond appropriately to a request to intervene.

High Automation

The driving mode-specific performance by and automated driving system of all aspects of the dynamic driving task, even if a human does not respond appropriately to a request to intervene.

Full Automation

The full-time performance by an automated driving system of all aspects of the dynamic driving task under all roadway and environmental conditions that can be managed by a human driver.

A Note on Terminology

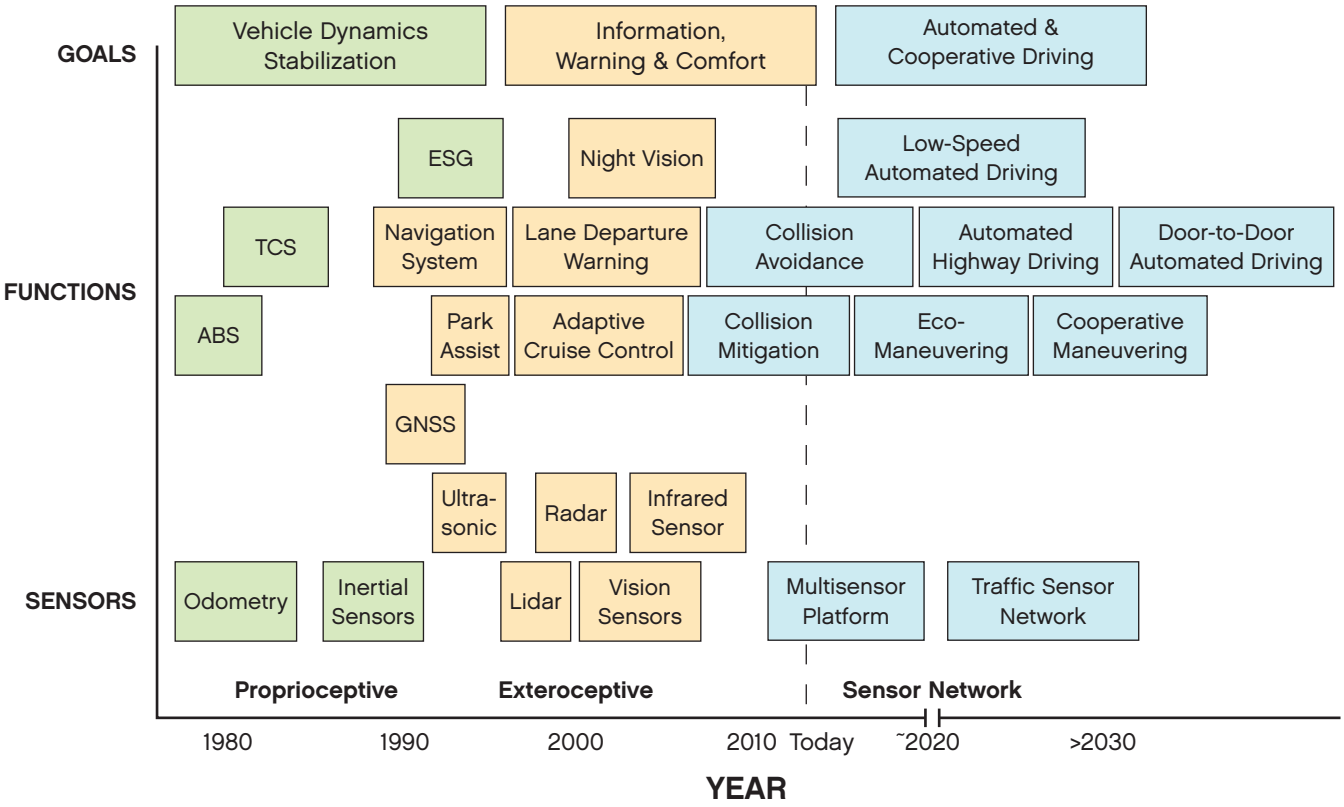
Clear and consistent definition and use of terminology is critical to advancing the discussion around automation. To date, a variety of terms (i.e., self-driving, autonomous, driverless, highly automated) have been used by industry, government, and observers to describe various forms of automation in surface transportation. While no terminology is correct or incorrect, this document uses "automation" and "automated vehicles" as general terms to broadly describe the topic, with more specific language, such as "Automated Driving System" or "ADS" used when appropriate.

SAE International, J3016__201806: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (Warrendale; SAE international, 15 June 2018), https://www.sae.org/standards/content j3016__201806/.

SAE 0 through SAE 2 vehicles employ a human driver. To the extent that driving functions are automated, the human driver is required to monitor and supervise those functions.[6] Features in this range of automation include visual warnings and driver-assist technologies that have been present in consumer vehicles for years. HAVs are categorized as SAE 3 through SAE 5. An automated system controls vehicle movement and decision-making.[7] Whereas lower-level HAVs may incorporate features like automatic parking systems, the higher levels are capable of fully autonomous driving for some or all driving parameters without any human interaction.

Timelines to Automation

SAE 0 through SAE 3 vehicles are on roadways throughout the United States. As illustrated in the diagram on the next page, familiar features of these vehicles include anti-lock brakes, traction control, accelerometers, navigation systems, rear-view and blind-spot cameras, parking assist, lane departure systems, adaptive cruise control, collision avoidance, eco-maneuvering, and automated highway driving.



Fully autonomous SAE 4 and SAE 5 vehicles are in development and testing, and real-world roadway testing has increased throughout the country.[8] Their experimental uses include driverless taxi services in Phoenix, Arizona; autonomous passenger vehicles connecting residential and business areas in central Florida;[9] and low-speed parking shuttles in Reston, Virginia.[10] Autonomous consumer vehicles have hit roadways as well. For example, Tesla has demonstrated "Smart Summons"—an automatic and driverless SAE 4 feature that retrieves a user's vehicle within parking lots when the user is nearby.[11] Zoox, a company owned by Amazon, is testing a "carriage-style" vehicle on roadways in Las Vegas, San Francisco, and Foster City that can serve as a robo-taxi or assist in package deliveries.[12]

While this progress results from millions of hours of vehicle simulations, testing, and optimization, the estimated timeline for full-scale deployment remains highly disputed. On one extreme, Apple co-founder Steve Wozniak believes that fully autonomous vehicles will not deploy for many decades.[13] On the other extreme, Tesla founder Elon Musk asserts that the hardware components required for full automation are used in the latest commercially available Tesla vehicles; the fleet merely awaits a "software update" to control and optimize driving commands.[14] Whatever happens, experience tells us that engineering feasibility will not be the only consideration. Public concerns, government decision-making, and ability to control for liability risk will be important factors, too.

Remaining Technological Challenges

From a hardware perspective, two types of sensors provide the backbone for fully autonomous vehicles: either (i) a suite of laser sensors, known as Light Detection and Ranging ("LiDAR"), or (ii) optical cameras. Although they are different technologies, each is designed to paint a comprehensive image of the vehicle's surrounding environment.[15] HAVs also incorporate a panoply of other sensor technologies used in features already found in commercial vehicles:

- Radio detection and ranging ("RADAR"), which emits and receives radio waves to measure distances as used in blind-spot detection and cross-traffic alert systems;
- Ultrasonic ranges, which measure the deflection of sound waves to identify objects during parking assist;
- Global positioning systems ("GPS"), which triangulate vehicle positions from orbital satellites to provide navigation and real-time traffic updates;

- Inertial measurement units, which use gyroscopes and accelerometers to detect changes in vehicle position and velocity independent of GPS;[16]
- Infrared cameras, which detect wavelengths that indicate heat and help identify people or animals in the roadway[17]; and
- Around-the-corner imaging, which identifies objects around the next bend in the road.[18]

Generally speaking, these hardware components are reported to be mature and ready for scaled deployment.

Machine Learning

Advances in software remain the single greatest obstacle to vehicle autonomy. HAV software analyzes all sensor data and makes vehicle-control decisions in a functionally analogous manner to a driver, though more rapidly. Because of the complex nature of driving, hard-coded rules cannot dictate software outputs. Instead, HAV software must implement "machine learning," which iteratively theorizes system parameters, models vehicle-control decisions, and updates them based on collected data, real-world test results, and lessons learned. Just as humans improve their decision-making based on cumulative life experience, HAV software continuously improves based on the sensor data collected and the success of its past vehicle-control decisions.

Software optimization through machine learning algorithms is time-consuming because driving tasks require massive data collection, synthesis, and rapid decision-making. Consider ridesharing. At first blush, the venture may seem simple, but the underlying tasks are quite complex—ensuring that a taxi has picked up the correct passenger is already difficult for an experienced human driver, and it is a unique challenge to identify the series of rules enabling an automated vehicle to find and verify the right passenger.[19] Consequently, machine learning is more efficient at theorizing tasks involving fewer variables, such as highway driving, than more complex scenarios, such as maneuvering a busy parking lot.[20] Real-world driving requires a great deal of intuition, finesse, and common sense—all of which are gained through experiential learning. But there is the rub. Real-world test cases are critical for amassing the data needed to automate complex driving tasks and improve safety, but safely performing that real-world testing is challenging before the collection of the data.[21]

HAV developers have come up with creative ways to advance the technology. Their strategies include accumulating testing data on digital platforms,[22] identifying nontraditional inferences that can be made from sensor data,[23] and upgrading the physical infrastructure on roadways to facilitate autonomous decision-making with machine-readable signs, lane indicators, and warnings.[24] Each of these techniques helps streamline the eventual timeline to market. But none is a complete substitute for lengthy real-world testing, so inevitable delays and uncertainties remain.

Wireless Communications

Wireless communication also plays a critical role in a fully autonomous infrastructure, because it reduces the inferential logic needed in HAV software. Developers seek "vehicle-to-everything" ("V2X") communications—sending and receiving information with nearby vehicles, the immediate roadway infrastructure, and a traffic control system regarding the speed and position of other vehicles, the status of roadway conditions, the presence of roadway obstacles, and traffic warnings. Two technologies have sought to achieve the V2X goal: Dedicated short range communications ("DSRC") and cellular-vehicle-to-everything ("C-V2X").[25] DSRC enables communication by emitting and receiving radio waves with frequencies in the 5.9 GHz band—a band dedicated to vehicle communication and safety by the Federal Communications Commission ("FCC").[26] C-V2X enables communication through cellular technology, relaying signals through cell towers and orbital satellites.[27]

Of the two technologies, DSRC was the first out of the gate and garnered substantial industry backing from many vehicle manufacturers.[28] C-V2X, however, is positioned to benefit substantially from the growth of 5G technology and its increased bandwidth, speed, and cellular connectivity.[29] This communications debate has delayed the timeline to fully automated deployment. But recent developments initiated by the FCC seemingly declared C-V2X the victor (*see* "Federal Communications Commission," *below*), and industry developers' design selections—at least for those that had yet to settle on a wireless communication technology—likely will be finalized as a result in the near future.

A Summary Model

At risk of oversimplifying, manufacturers, suppliers, and sellers have many factors to consider for mitigating liability risk.

SUMMARY MODEL
Industry Practices
Vehicle Functions
• Detection/perception of the vehicle's continually changing driving environment (e.g., weather, road conditions, other vehicles, traffic signals and signs, pedestrians, and the like); – Interpretation/understanding of those conditions; – Reaction time to respond to those conditions; – Response chosen to operate safely in those conditions; and • Crashworthiness in the event an accident cannot be avoided.
Vehicle Design and Operation
• Equipment and hardware, including both the vehicle component parts and its communications; • Location of equipment, such as sensors and cameras; • Software; • Recording and preservation of data for machine learning, updates, and reconstruction; and • Crashworthiness, such as compartment design and restraints.
Driver and Consumer Information, Education, and Training
• Operating manuals and other written information; • Warnings and alerts on board the vehicle; • Enhanced, additional education and training; and • Advertising.
Potential Liability Claims
• Design, including research, testing, and compliance with applicable laws, regulations, or industry standards; • Manufacturing, including quality control; • Warnings and instructions, both at the time of sale and post-sale; • Claims of false advertising or misrepresentations; and • Breach of warranties, express or implied.

As applied, this matrix shows the issues that a manufacturer, supplier, or seller may need to evaluate, both individually and holistically, to forecast and mitigate the potential liability risks associated with HAV development, manufacturing, and sales. The remainder of this *White Paper* will discuss current federal and state laws and regulations that set the legal framework for evaluation of potential liability risks and will analyze existing liability concepts and precedent that are applicable to HAV risk scenarios.

REGULATION

An Open Landscape

A comprehensive AV-specific regulatory structure has not yet emerged at either the federal or state level in the United States. The safety of passenger vehicles is traditionally regulated under a combined federal-state framework. Under the direction of Congress, the National Highway Traffic Safety Administration ("NHTSA") regulates the testing and safety of motor vehicles through the Federal Motor Vehicle Safety Standards ("FMVSS").[30] It enforces compliance, manages recalls for safety-related defects, and, together with the Environmental Protection Agency ("EPA"), regulates fuel economy and emissions. Similarly, the Federal Motor Carrier Safety Administration ("FMCSA") sets safety standards for trucks, known as the Federal Motor Carrier Safety Regulations ("FMCSR"). The National Transportation Safety Board ("NTSB") has authority to investigate vehicular accidents and make recommendations for improved safety, though it primarily focuses on civil aviation, trains, and trucking. States have traditionally also had a say in roadway safety by licensing drivers, registering motor vehicles, conducting safety inspections, enacting and enforcing traffic laws, providing the safety infrastructure, and regulating motor vehicle insurance and liability for vehicular accidents.

Vehicle and automotive component manufacturers take this entire framework into account when designing and testing their products. However, most of these regulations were drafted without contemplating driverless vehicles and their unique benefits, challenges, and risks. For example, FMVSS testing protocols for steering systems assume a human driver seated behind a steering wheel, neither of which is necessary in high-level HAVs.[31] SAE 4 and SAE 5 vehicles inherently are not designed to comply—and do not need to comply—with many of the FMVSS. The federal government is moving carefully to evaluate and develop an AV-specific regulatory structure—in part to avoid stifling the development of new technology and to allow further experience from roadway use and testing.[32] Absent an AV-specific regulatory structure, HAV

manufacturers must request a temporary exemption from NHTSA to bypass federal standards; NHTSA has issued some exemptions so far.[33]

So far, neither the federal nor the state governments have dictated HAV design parameters or technology in any comprehensive way. This latitude is allowing competition to proceed in the choice and testing of vehicle design, including the choice of safety equipment. Unlike the decisive regulation of the 5.9 GHz band and the 5G infrastructure (*see below*), there are no comprehensive federal requirements for roadway testing protocols, minimum safety criteria, or vehicle design to provide definitive guidance to HAV manufacturers or suppliers. Developers and investors remain free to back their preferred technologies, and to seek permission to test and prove those technologies on the nation's roads. State and local governments, too, have taken a generally permissive approach to driverless vehicle safety and testing, but numerous state-specific regulations have emerged, creating a patchwork regulatory scheme that differs state to state and changes nearly every month.

Federal Regulation

Unlike Europe and Japan, Congress has not enacted specific laws regulating HAV safety, cybersecurity, or data privacy.[34] In 2017, the House and the Senate considered competing bills,[35] and although the House passed its version, the SELF DRIVE Act, neither ultimately became law.[36] In September 2020, Representative Bob Latta, a member of the House Energy and Commerce Subcommittee on Communications and Technology, introduced a revised version of the SELF DRIVE Act.[37] Congress's latest attempt at enacting legislation regulating HAV safety, cybersecurity, or data privacy failed to garner the support needed to become law. The revised Act would have mandated updates to the FMVSS, and it aimed to have taken steps to provide specific safety standards for autonomous vehicles.

If it had been enacted, vehicle manufacturers would have been required to complete and submit "safety assessment certifications," and the Secretary of Transportation would have determined the regulatory requirements for those certifications within two years of the legislation's enactment.[38] By mandate, the Secretary's rules would have defined the "relevant test results, data, and other contents required to . . . demonstrate that such entity's vehicles are likely to maintain safety, and function as intended and contain fail safe features."[39] While this ultimately is a delegation of rulemaking authority rather than the passage of standards in and of themselves, this bill, if passed, might have set in motion a more comprehensive federal regulatory structure.

Moreover, in the two-year interim before final regulation, the bill would have authorized industry members to submit "safety assessment letters" for NHTSA's review.[40] This procedure would have formalized a standard avenue for HAV testing and deployment apart from the FMVSS exemption process currently in place. Similar to existing federal motor vehicle safety law, the revised SELF DRIVE Act would have created a uniform regime of federal HAV safety standards by prohibiting any state or local government from "effect[ing] any law or regulation regarding the design, construction, or performance of highly automated vehicles, automated driving systems, or components of automated driving systems unless such law or regulation is *identical* to a standard prescribed under this chapter."[41] Such a framework would have provided potential protection for manufacturers to implement nationwide testing and deployment of their HAVs.

The revised SELF DRIVE Act also would have added requirements for cybersecurity and data privacy. This latest bill would have required, among other things, that vehicle manufacturers develop a "written cybersecurity policy" that "identif[ies], assess[es], and mitigat[es] reasonably foreseeable vulnerabilities from cyber attacks or unauthorized intrusions, including false and spurious messages and malicious vehicle control commands." It also would have required companies to "tak[e] preventive and corrective action to mitigate against [such] vulnerabilities."[42] Likewise, vehicle manufacturers would have been required to develop a "written privacy plan" with respect to information "collection, use, sharing, and storage," as well as practices for "data minimization, de-identification, and retention about vehicle owners or occupants."[43] The revised Act's regulation of cybersecurity and data privacy remained deferential to industry choices.

Overall, the bill was aimed at fostering HAV innovation while beginning to address key questions about safety, cybersecurity, and data privacy. It would have allowed for greater HAV testing and deployment—first through individualized NHTSA safety assessments, followed soon thereafter by final agency regulations. The bill also would have prevented

the development of myriad disconnected and inconsistent state laws and regulations. However, it remains unclear if a new iteration of the SELF DRIVE Act will be introduced in this Congress or in the near future.[44] Until then, and in the absence of a Congressional directive, federal agencies have provided voluntary guidance.

Department of Transportation. Like Congress, DOT and its sub-agencies have only recently begun taking concrete steps toward comprehensive HAV regulations. DOT's overall approach has been to support state initiatives and encourage some level of self-regulation by the automotive industry itself. DOT has issued five guidance documents since 2016.[45] DOT has consistently made "prioritizing safety" the leading principle, along with fostering innovation and modernizing regulations. While early guidelines foregrounded the role that state and local governments can play, the most recent publications, "Automated Vehicles 4.0" and "Automated Vehicles: Comprehensive Plan," call for a "consistent federal approach."[46]

In June 2020, former U.S. Transportation Secretary Elaine L. Chao announced that DOT was "creating a formal platform for Federal, State, and local government to coordinate and share information in a standard way."[47] When the Automated Vehicle Transparency and Engagement for Safe Testing ("AV TEST") Initiative launched, it was a cooperative effort between DOT, nine private industry companies,[48] and eight states.[49] Now, 52 companies, state governments, and associations[50] are participating "to improve transparency and safety in the development and testing of automated driving systems" by publicly sharing automated testing activities and safety information.[51]

NHTSA has also taken preliminary steps by seeking industry and stakeholder comment for how HAV testing and safety should be regulated. In 2018, NHTSA sought comment regarding the factors it should consider,[52] and in 2019, both NHTSA and FMCSA sought comments regarding the obstacles presented by existing motor vehicle regulations when applied to HAV testing and deployment.[53] In 2020, NHTSA focused on the need to "modernize" the FMVSS to adapt to vehicles with higher degrees of automation.[54] In March 2020, NHTSA issued a notice of proposed rulemaking, which sought to "remove unnecessary barriers to Automated Driving System-equipped vehicles ("ADS-equipped vehicles") and the unconventional interior designs that are expected to accompany these vehicles, including the lack of driving controls."[55] Examples included modification of the FMVSS to alter definitions—which in turn govern safety requirements—related to driver air bags, steering control systems, and seating positions, particularly with an eye toward scenarios that do not arise with human drivers, such as vehicles without occupants or child-seating in the front compartment.[56]

These proposed changes would remove a regulatory barrier to HAV testing and deployment by no longer presupposing that all vehicles have human drivers. If adopted as a final rule, these standards could preempt many existing state-law safety standards.[57] The comment period on NHTSA's proposed rule has ended, but to date, the disposition of the proposed rule remains pending.[58]

In December 2020, NHTSA issued a notice of proposed rulemaking that sought comments on the development of a "governmental safety framework specifically tailored to ADS safety."[59] The resulting framework could encompass more than just formal regulations; it could "involve a range of actions by NHTSA, including guidance documents addressing best industry practices, providing information to consumers, and describing different approaches to research and summarizing the results of research, as well as more formal regulation, from rules requiring reporting and disclosure of information to the adoption of ADS-specific FMVSS."[60] NHTSA sought comments on how NHTSA should administer the framework.[61] The comment period on the proposed rule ended on April 1, 2021.[62]

Federal Communications Commission. Until recently, the FCC, which regulates the use of airwaves, had largely punted the largest regulatory decisions related to HAV: the preferred method of wireless vehicle communications. More than 20 years ago, the FCC allocated 75 megahertz in the 5.9 GHz frequency band to DSRC for vehicle safety purposes. Some automakers desired to use the upper portion of that band for HAV communications and petitioned the FCC for a waiver to do so.[63] However, the issue was in dispute because non-automotive industries want to use the band as well.

In 2019, the FCC proposed a rule attempting to accommodate both. It proposed "unlicensed operations" for "the lower 45 megahertz of the band," while "reserv[ing] the upper 30 megahertz band" for vehicle communications.[64] Within the band reserved for vehicle communications, the agency further proposed allocating two-thirds for the C-V2X solution, and

sought comments regarding whether the remainder should remain reserved for DSRC.[65] Considering that the entire band had been reserved for DSRC over the past two decades, the FCC's proposal marked a dramatic change in thinking. In addition to debate within the industry, the proposal faced opposition within the federal government. DOT opposed the plan,[66] as did several members of the House Committee on Transportation and Infrastructure.[67]

In late October 2020, former FCC Chairman Ajit Pai released statements favoring the C-V2X solution over DSRC, and the FCC released a draft order proposing final rules to repurpose the 5.9 GHz band between dedicated ranges for Wi-Fi and C-V2X vehicle communications.[68] The decision came because of marked success of the spectrum's use during the early days of the COVID-19 pandemic (after the FCC had granted a special temporary authority permitting internet providers to use the 5.9 GHz band).[69] On November 18, 2020, the FCC approved a report and order splitting the band 45-30 between unlicensed Wi-Fi uses and C-V2X technology to enhance automobile safety.[70] The FCC envisions the order as opening the pathway for C-V2X to expand its capabilities "to provide direct communications between vehicles and obstacles like other vehicles, cyclists, pedestrians, and road workers, and to receive safety information from roadside transmitters."[71] This FCC order aims to facilitate HAV deployment.

State Regulation

As long as the federal government declines to take on a preemptive role, state and local governments will have more latitude to regulate.[72]

Currently, 37 states and D.C. have enacted some sort of HAV-related legislation.[73] Several governors have issued related executive orders as well. Some of these regulations are minimal, simply authorizing platooning or establishing advisory councils to conduct research.[74] At least 29 states have issued policies or regulations related to HAV testing,[75] mostly by executive order.[76]

State approaches vary greatly. For example, California regulates extensively.[77] The state has a regulatory code dedicated to the testing and deployment of HAVs.[78] As of February 25, 2021, the state had issued 56 permits for HAV testing with a driver, six permits for driverless testing, and has authorized the deployment of autonomous vehicles from only one entity.[79]

In California, any testing permit requires the manufacturer, among other requirements, to demonstrate substantial collateral against potential liability judgments.[80] Additionally, drivers must complete a training program before certain types of HAV testing, and if a vehicle manufacturer desires a driverless test, the company must adhere to further specific procedural requirements.[81]

The same is true in states like Arizona, where driverless testing requires certification that the vehicle complies with the FMVSS, that it implements collision mitigation, that the test will adhere to all traffic laws, and that the HAV meets registration and insurance requirements.[82] However, after a fatal accident in Arizona in 2018, the NTSB recommended that Arizona and other states expand regulations to require detailed testing and safety plans, including mitigating the risk for operator inattention.[83] In response, some states like Pennsylvania (which allows for platooning generally[84]) have adopted additional regulations limiting driverless testing and imposing additional application and review processes before any roadway HAV testing.[85]

Most states have striven to create a welcoming environment for HAV development. However, the lack of consistency complicates manufacturer compliance and can result in redundant certification requirements. States also have not yet addressed industry questions related to cybersecurity and data privacy in any comprehensive way.[86] Although individual cities[87] and states will always retain some authority to create differing physical and regulatory environments at the local level, it appears that some state and local governments are waiting for federal intervention to resolve overarching questions in equipment testing protocols, cybersecurity, and data privacy.

LEGAL ISSUES

Given the limited mandatory regulation to date,[88] HAV manufacturers and suppliers have significant freedom to choose how to manage their potential liability.

Unless a more comprehensive federal or state regulatory framework materializes, traditional state tort and warranty rules will usually govern civil liability arising out of HAV accidents. Courts will need to consider whether to modify those rules to adapt to HAVs at different levels of automation. Existing liability schemes and rules, with likely modifications creating new

precedent, will sort out the potential liability of manufacturers, suppliers, and sellers to injured persons, as well as the potential apportionment of liability among manufacturers, suppliers, and sellers.[89]

Under a theory of negligence, the plaintiff must demonstrate that the defendant breached a duty owed to the plaintiff, causing injury and damages. As it relates to HAVs, many questions remain open, including *who* can and should be held liable. Drivers traditionally are liable for car accidents, absent mechanical failure. Without a driver in control of a vehicle (depending on the level of automation), neglected maintenance of the vehicle, or the driver's ability to resume control when circumstances demand, driver fault may no longer be at issue in numerous accidents. Indeed, the long-term goal of HAVs is to remove drivers, who reportedly cause 94% of accidents, from control.[90]

Depending on state law, negligence principles still could apply to evaluate the fault of HAV manufacturers and suppliers for defects in manufacture, insufficient testing or quality control, unreasonable design choices, inaccurate representations, or inadequate warnings.[91] It remains to be seen: (i) whether negligence duties will extend to sellers for inadequate warnings, defective manufacturing of automated systems, or improper or inadequate training or education of vehicle owners; (ii) how any such duties may or may not extend to passengers in the owner's or other vehicles, or to bystanders; and (iii) the extent to which passengers and pedestrians are deemed to assume their own risk. In considering negligence liability, the circumstances and causes of an accident will remain relevant. Again, the vehicle's level of automation will influence the liability analysis, with the most complexity in the liability analyses occurring before full automation is reached.

Early commentators predicted that the principal rules governing the liability of HAV manufacturers, suppliers, and sellers will be strict product liability, premised on defects in manufacturing, design, or warnings. That already is the case. Plaintiffs can be expected, as now, to include, when possible, common-law and statutory claims for fraud and misrepresentation. Contract-based claims, such as breach of warranty, may also apply. But if and when the federal government enacts HAV regulations, its actions may preempt some or all state common-law claims.

Absent federal intervention and guidance, manufacturers may also face additional liabilities arising out of cybersecurity and data privacy. Accordingly, manufacturers, suppliers, and sellers may protect themselves through indemnification agreements, allocation of risk by contractual arrangements, disclaimer of warranties (to the extent permitted by state law), helping to set industry standards, preservation of electronic data from the vehicle and its systems, and insurance.[92]

Liability Considerations

Collecting and Storing Electronic Data

As a threshold matter, autonomous technology and its mass collection of data will fundamentally impact traditional litigation. For example, in the event of an alleged mechanical failure, ownership and access to vehicle data will become a critical issue that stakeholders will need to resolve. E-discovery can help identify relevant data needed to prove facts related to causation and liability. Federal Rule of Civil Procedure 37 and parallel state rules were amended to reflect the availability of electronic data and to provide curative measures for data that are not preserved.[93]

Accordingly, manufacturers will need to evaluate the types of data to collect from the vehicle and accident surroundings. Regulations or industry standards might dictate a minimum.[94] Then, manufacturers can assess their needs for purposes of liability or product improvement, adapt, and understand how to use and preserve the types of data collected by autonomous vehicles in order to evaluate the circumstances and causes of accidents.[95] Data collection also will help to improve the design of HAVs based on real-world performance in a variety of conditions as well as suggest whether improvements to infrastructure are needed.

For HAV collisions, data can reveal the speed and position of vehicles, as well as which automated functions were operational at the time of the accident (i.e., brakes, accelerator, steering, and detection). Data will be critical in determining what the vehicle's sensors detected and how the vehicle interpreted the circumstances perceived. Recorded data also could show whether a driver took over control of the vehicle's functions, or whether the vehicle warned the driver to take over control. If so, then the driver's actions or failure to act might

require consideration, not just the manufacturer's conduct and the vehicle's design if the vehicle were operating in its autonomous mode during a collision.

In the fatal accident in Arizona in 2018 (see "State Regulation," *above*), electronically stored information showed the automatic braking system was turned off, and the backup driver failed to intervene. Moreover, data from the driver's online media account showed that she was streaming a television show just before the accident and, therefore, was likely not paying proper attention.[96] Third-party sources of data could shed light on the causes of an accident, and those sources in turn may raise issues of data privacy.

The types of data to record and store turn on pre-accident decisions by manufacturers, suppliers, regulators, and insurers. Electronic data and preservation of evidence will shape tort litigation even more so in a fully automated infrastructure. A party's ability to access or preserve this type of electronic data may transform the litigation narrative regarding driver negligence, third-party fault, or product defect.

Liability Paradigms

Federal Preemption

Looming over all aspects of liability is the open legal issue of federal preemption and whether individuals can bring state law actions based on injuries arising out of HAV accidents. Existing law already lays the groundwork for federal preemption of certain HAV-related state tort claims.[97] In *Geier v. American Honda Motor Co., Inc.*,[98] the United States Supreme Court considered express and implied preemption under the Federal Motor Vehicle Safety Act ("FMVSA") and 1984 FMVSS. Federal regulation required cars to be equipped with passive restraints, but did not specify the type of restraint—manufacturers could choose which type of restraint to include. The regulation reflected a deliberate government policy to permit manufacturers to use different types of passive restraints while regulators and the industry accumulated needed data and experience on the effectiveness of each type under diverse accident circumstances. The plaintiff, who was injured in a collision while wearing a seatbelt, argued that the manufacturer should have equipped the car with airbags. The Supreme Court held that this type of claim, while not expressly preempted, conflicted with the federal government's policy of manufacturer choice and, therefore, was impliedly preempted.

In contrast, in the subsequent case *Williamson v. Mazda Motor of America, Inc.*,[99] a newer version of the FMVSS permitted manufacturers to equip rear seats with either lap-only or lap-and-shoulder belts. The plaintiff alleged that, under state law, manufacturers owed a duty of care to install lap-and-shoulder belts. The Court distinguished *Geier* and found no express or implied preemption, because there was no clear federal policy in favor of allowing manufacturers a design choice.

Under the current statute and the *Geier*/*Williamson* paradigm, if federal regulators deliberately pursue a path of allowing AV manufacturers to choose among different safety-enhancing technologies while the industry develops, that could arguably preempt state common-law causes of action. But after *Williamson*, more is required than simply refraining from action, as the federal government has done so far—regulators must adopt a deliberate policy of manufacturer choice.

Congress could also choose to establish a separate preemption paradigm for HAVs. Representative Latta's bill would have prohibited any state or local government from "effect[ing] any law or regulation regarding the design, construction, or performance of highly automated vehicles, automated driving systems, or components of automated driving systems unless such law or regulation is identical to a standard prescribed under this chapter."[100] And it contained a saving clause.[101] Both of these measures, while AV-specific, track similar language in the FMVSA and would not likely have substantially changed the *Geier*/*Williamson* paradigm for federal preemption.

But there are other models for preemption. For example, under the Federal Railway Safety Act, where a federal regulation "subsumes" an area of safety regulation, a state tort claim can proceed only if it alleges a violation of the federal standard or of the defendant's own self-imposed safety standard.[102] Such an approach could scale back the impact of state tort law. Congress could also choose to target preemption at design choices or performance criteria, but leave in place tort law claims based on inadequate warnings, common-law or statutory fraud, or misrepresentations.[103] Or, if the federal government takes the European approach,[104] and adopts rudimentary safety standards[105] such as requiring vehicles to be equipped with a functional self-check and a data recorder, arguably no preemptive effect will attach, because these features merely aid in determining subsequent liability. They do not in and of themselves prevent the states from instituting safety standards

to which manufacturers must adhere. As always, the scope of federal preemption will depend not only on applicable statutory language but on subsequent judicial interpretation.

One specific area of controversy until the federal government adopts HAV-specific rules may be the preemptive effect of interim approvals such as those contemplated by previously proposed federal legislation, which would have required NHTSA to approve safety assessments of HAV manufacturers during the two-year period between the legislation's enactment and the agency's issuance of comprehensive safety regulations. The exemptions that NHTSA is currently authorized to provide could create similar issues. Existing law provides some support for preemption in such cases, because: (i) a federal statute mandates the approvals, and (ii) agency exemptions from federal regulations can have the same preemptive effect as the regulations themselves. For example, in *Rollins v. Bombardier Recreational Products, Inc.*,[106] the U.S. Coast Guard exempted a personal watercraft from a ventilation system required by the Federal Boat Safety Act of 1971. Because the Coast Guard's exemption was granted pursuant to express Congressional authority, the court held that the plaintiff's state product liability claim, which conflicted with that exemption, was preempted.[107]

The future of federal preemption remains an open question. As long as NHTSA and FMCSA continue to implement deferential standards or merely require industry members to develop and document their own safety protocols and testing procedures, the preemptive effect of their rules will be questionable, and those industry members would have more risk of state-law liability. Because federal agencies have indicated a desire for some degree of self-regulation by the HAV industry, however, manufacturers and suppliers can help shape the development of industry-accepted standards that could become a federal preemptive standard. Industry safety initiatives may determine—at least, partially—how federal agencies ultimately decide to regulate.

Strict Product Liability

Unless and until the federal government steps forward, state law has a significant role to play, beginning with strict product liability. Common-law strict product liability recognizes claims against manufacturers, suppliers, and sellers to recover for personal injuries or property damage arising from product defects in design, manufacturing, or warnings or instructions. For HAVs, some commentators anticipate a decreasing role for negligence liability, and perhaps a move toward a no-fault system of liability. They argue that fully automated HAVs are supposedly designed to prevent most accidents; therefore, any accident likely results from some vehicle defect for which the manufacturer, component supplier, or seller is liable.[108] While the apportionment of liability between a manufacturer, supplier, or seller might remain in dispute, their liability to the injured persons is presumed under this theory, so that a no-fault system imposing liability on HAV manufacturers and, when appropriate, component suppliers and HAV sellers would be both fair and most efficient. However, we are many years away from roadways mostly populated by fully automated HAVs, and the underlying premises of the "no fault" theory are subject to debate. In the meantime, the traditional strict product liability framework likely will govern the determination of liability in HAV accidents.[109]

Under the product liability framework, HAV manufacturers, component part suppliers, and sellers may be held liable for selling defective products to consumers even if they exercised reasonable care.[110] They are not liable for substantial changes in the condition of the vehicle after sale, such as after-market equipment or owner's lack of maintenance. This strict liability framework is quite familiar and applied daily to auto accidents. What, then, are the challenging new issues that HAVs likely will present?

Design Defects. Courts typically use one of two tests to determine if a design defect exists. The historically first, but now minority, test is the consumer-expectations test.[111] It asks whether the HAV or a component part functioned as a reasonable consumer in the general public would expect. Because the courts have recognized that consumers have little conception of how complex technology is supposed to function, this test has fallen into disfavor. In the HAV context, this test could invite a "reasonable consumer" to expect that the vehicle can avoid all or almost all accidents.

For example, in a recent tragic case, a design defect was alleged for a vehicle's rear-view camera system after a father inadvertently backed over his child in the driveway. The lawsuit alleged that the camera's rear-view visibility failed to identify individuals—particularly children and persons with disabilities—located directly behind the vehicle.[112] Because identifying persons behind the moving vehicle was one of the primary

functions of the technology and one that consumers would expect from a vehicle's rear-view camera, the manufacturer was found to be liable.

What will consumers reasonably expect from HAV technology? Manufacturers, suppliers, and sellers can expect to confront a broad range of consumer attitudes.[113] The knee-jerk instinct of some consumers and jurors will be to fear technology that takes control away from them and that they do not understand. Human tendency is to assign more risk to things that they cannot perceive, such as nuclear radiation, and cannot control, such as flying. They are not likely to understand the limitations of the technology, particularly before HAVs reach full automation level 5. Yet, at the other end of the spectrum will be consumers and jurors who embrace the technology, but expect too much—that the technology will be foolproof and able to prevent all accidents and injuries.

As always, manufacturers and suppliers will need to evaluate reasonably foreseeable uses and misuses of HAV vehicles and technology, including reasonably foreseeable failure modes, subject to the limitations of applicable law. They would be well served to comprehensively document the robust design, testing, and safety procedures used, as well as the reasons supporting their design choices. And, importantly, they will need to be able to demonstrate that the machine continued to learn and improve as intended.

As the competing technologies show, manufacturers and suppliers will face many technology choices from the type of sensors and their placement, the trade-offs in the design of compartments between occupant safety as opposed to comfort and convenience, the types of restraints to use, the communication systems, the ability (if any) of the driver to take over control of the vehicle, and the software design. These technological choices are beyond the ken of most consumers. However, it will be critically important for vehicle and component manufacturers to provide manuals or other written information describing the technology incorporated in the HAVs accurately, explaining its functions and limitations, discussing the risks, and emphasizing the continuing responsibilities of owners and drivers. Competitors likely will continue to promote the design choices in their vehicles as superior to others, but at the same time also provide a range of choice and safety reflected by different price points and consumer preferences. Because consumers are dealing with new technology, manufacturers, suppliers, and sellers can play an important role in informing and managing public expectations and the perception of their technology. HAV manufacturers, suppliers, and sellers can mitigate their liability risk by underpromising, but overdelivering.

However, like the Restatement (Third) of Torts: Products Liability, most state courts have moved away from the consumer-expectations test to the risk-utility test.[114] Under the risk-utility test, courts balance the product's utility with its risk of harm. The latest Restatement also requires proof of a reasonable alternative design. While public perception of risk still matters, this test puts more weight on more objective factors, such as the feasibility, risks, costs, and benefits of alternative technology at the time of manufacture and sale.

Cases involving automated vehicle technologies are instructive. In *Honda of Am. Mfg., Inc. v. Norman*, a driver died after accidentally driving her vehicle into a body of water when a mechanically automated seatbelt shoulder strap failed to disengage allegedly due to a design defect.[115] Applying the risk-utility test, the court required plaintiffs to show through expert testimony that a reasonable design alternative "was both *technologically* and *economically* feasible."[116] When plaintiffs failed to do so, the court determined that the automatic seatbelt was not unreasonably dangerous or defectively designed.[117] Helping the manufacturer's defense were the facts that the automated restraint system "was the most expensive seatbelt system in use at the time [the] car was manufactured," and there was "no evidence that a reasonably safer alternative design existed for Honda's passive restraint system when the car was manufactured."[118]

Under this test, liability should turn on an objective, scientific analysis of the reasonableness of the design choices made by the manufacturer or supplier compared to available, alternative technology. While the circumstances of the particular accident and its foreseeability provide the context for the lawsuit, the liability analysis more broadly considers the benefits of the design choice against reasonably foreseeable risks across all anticipated accident scenarios. A favorable safety comparison between human-driver accidents and HAV accidents also may be relevant to calibrate and offset the inherent risk of harm presented by the budding technology, particularly when design alternatives remain limited. Testing and simulations of various design alternatives, a rigorous failure mode

engineering analysis, and carefully documented decision-making will remain important to the defense.

Manufacturing Defects. Manufacturing defects arise at the production line, where an unreasonable danger is introduced into an otherwise safe design. Errors in the manufacturing process can cause defects that result in a product or part not meeting its design specifications. For example, in *Fitzpatrick v. Currie*, an automated airbag system deployed and split open, releasing gases that caused the plaintiff trauma and chemical burns.[119] A witness had "observed a vertical slit or tear in the underside of the airbag," which the plaintiff attributed to a manufacturing defect.[120] The court ultimately ruled in favor of the vehicle manufacturer, because it made a prima facie showing that the airbag was free of manufacturing defects when it left its control, and because the plaintiff failed to introduce any evidence that a defect in the airbag caused his injuries.[121]

As always, high levels of quality control, both with parts and materials as well as the finished product, are important to mitigate the risk of manufacturing errors. And because the technology is so complex and integrated, manufacturers and suppliers may want to consider system designs that include self-diagnostics to report functional loss or faulty components. Detecting software errors will be much more complex than hardware and equipment and may require a system to collect and respond to field reports and customer complaints to detect those errors.

An emerging, potential legal risk for manufacturing defect liability will include manufacturing defects that are created after HAVs leave the manufacturer's factory. Because HAVs are expected to continually learn from experience and to receive software updates, their software and decision-making inevitably will be different than when they left the factory. But the same liability analysis will apply: Was there a design defect that resulted in faulty software decision-making?

Failure to Warn. Inadequate warnings or instructions may also give rise to a strict liability defect claim. The increasing complexity of the HAV technology along with its limitations, particularly before level 5 automation is reached, may provide more fodder for claims of accidents arising from driver and consumer ignorance or confusion.[122] Especially while the technology is new and unfamiliar to the public, and the level of automation requires some driver control or monitoring, vehicle and component manufacturers may consider providing robust driver and consumer information, education, and training, as well as on-board warnings and alerts.

Cases involving HAV-related technologies are somewhat instructive for how this will impact component manufacturers. In one case, a court found that a GPS company did not fail to warn a woman, who was injured by a negligent driver while crossing a rural highway, in part because the company had no legal duty to protect her from the negligence of a third party.[123] This contrasts with another case, where passengers were injured after their bus collided with a bridge when the GPS failed to identify that bridge as height-restricted.[124] The passengers sued, among others, TomTom and Garmin for breach of implied warranty of merchantability, negligence, and strict liability.[125] These cases illustrate how plaintiffs may allege that component manufacturers owe end-users some duty to provide accurate warnings and safe instructions for use.

The same principle applies beyond components to a vehicle's automated driving features. In a case involving an aircraft's autopilot technology, a court found that the airplane manufacturer did not have a duty to train the pilot in the autopilot system's use, but it did have a duty to provide adequate instructions for safe use.[126] Accordingly, courts will consider whether vehicle manufacturers provided adequate safety instructions either onboard or in the user and owner's manuals. Moreover, depending on the level of technical sophistication in the HAV design, a manufacturer or seller may consider consumer training—in addition to a manual.[127] A typical operator of an HAV may be distinguished from an airplane pilot in terms of expertise and training that reasonably can be expected. The expectation a manufacturer can reasonably have in an HAV operator's ability to understand and comply with owner's manual instructions will likely emerge as an important factor in determining manufacturer liability under failure to warn theories of liability.[128]

Few lawsuits involve fully or near fully automated vehicles, and those cases are either pending[129] or have been settled without a judgment.[130] But, while fully automated vehicles have yet to deploy in significant numbers, courts and commentators already have begun to explore how traditional tort concepts will adapt to determine liability in a fully automated world in which human drivers have no or far less interaction with the technology and less opportunity for negligence. Before then

and before a system of no-fault liability, determinations of common-law tort liability will remain a complicated battle of expert opinions and juror expectations, and the common law will need to adapt.

Post-Sale Duties. With ordinary consumer products, the common-law tort duty of manufacturers, suppliers, and sellers is measured at the time of sale—and ends at the time of sale. However, the common law in some states has imposed continuing, post-sale duties in some circumstances for specialized heavy equipment or machinery sold to particular purchasers whom the manufacturer or seller can identify and with whom the manufacturer or seller can communicate after sale.[131] While there is seldom a duty to retrofit or upgrade a product that was reasonably safe when sold, the common law is evolving to fit the circumstances of particular products with identifiable purchasers.

There is a real possibility of post-sale duties arising for HAV manufacturers, because HAVs can be tracked, and manufacturers and suppliers are developing ways to upgrade vehicle software based on additional experience and testing after sale. Some HAV manufacturers may volunteer to provide those software upgrades to enhance consumer satisfaction, to persuade consumers to purchase their vehicles, and to mitigate litigation risk. To date, those upgrades appear to be limited to software, much like software upgrades are routinely supplied for cell phones. Whether upgrades expand to hardware and equipment remains to be seen, but actions by manufacturers promising those upgrades or disclaiming any duty to supply equipment or software upgrades could impact whether that expansion occurs. Post-sale duties may include warning of newly discovered, product-related risks,[132] updating software decision-making to include safer algorithms, or recalling a product found to have some defect causing serious injury.[133]

Of course, HAV manufacturers, like current auto manufacturers, will undoubtedly continue to have the regulatory duty to report and recall vehicles with hazardous safety defects. An interesting and difficult decision-making point for manufacturers will be whether and under what circumstances to provide algorithmic safety updates as part of an ongoing, free-of-charge service or whether to charge for updates, as well as what promises to make to consumers about providing those updates. Whether tort law, regulations, or industry standards and practices develop to provide guidance on this complex question remains to be seen.

Under strict liability rules, HAV component part suppliers may have defenses not available to HAV manufacturers, if the parts were not defective when sold. For example, bulk suppliers of parts to sophisticated users typically have no duty to warn the end-product purchasers.[134] The obligation to warn consumers rests on the end-product manufacturers. Also, suppliers of nondefective parts that end-product manufacturers then use or modify improperly to create a hazard typically are not liable either to the end-product manufacturers or consumers, if the component suppliers were not aware of the improper use or modification,[135] or did not take part in integrating their parts into the end products.[136] Whether those defenses arise depends in part on how suppliers structure their relationships with manufacturers, both in their contracts, promises (or their absence), and conduct. Additionally, different analysis may occur when the component part involves artificial intelligence that is intended to learn and change over time.

Breach of Warranty

Claims for breach of warranty arise under contract law. These types of claims come in three flavors: express warranty, implied warranty of fitness for a particular purpose, and implied warranty of merchantability.[137] Under the Uniform Commercial Code, an express warranty is made through an affirmation, description of the product, or a sample.[138] Consequently, the product manufacturer, supplier, or seller can control whether any express warranty is made. The implied warranties hinge on particular buyer and market expectations for a product.

While the state of the art may be new, the legal analysis of warranties arising in HAV business dealings likely will remain comparable to those of any automated technology industry. For example, in *Auto-Teria, Inc. v. Ahern*, a brochure described an automated car-washing system as "Automatic—Coin Operated—No Hand Wash Labor."[139] After the coin meter broke, the system's buyer disconnected it and manned the system with an operator.[140] The court found the broken coin meter to have violated the express warranty mandated by the system's brochure.[141] Moreover, the court determined that the automated brushing function violated implied warranties of merchantability and fitness, because the system failed to "effectively wash automobiles without knocking off their exterior accessories."[142]

To protect from breach of warranty actions, HAV manufacturers, component suppliers, and sellers can carefully consider the scope of functions claimed and promises made in their advertising, marketing literature, sales materials, operating manuals, and contracts with consumers. In addition to the express functions claimed, advertising, marketing, and sales materials can be tailored to match the technology's capabilities and limitations. Manufacturers also can check state statutes, regulations, and common law to determine the types of statements that are deemed to be express warranties, as well as the legal requirements and constraints for disclaiming implied warranties and for limiting available remedies and legal procedures for obtaining relief. If systems require maintenance or periodic safety checks, these can be communicated to consumers, and manufacturers can consider automated safety checks that report back to the manufacturer. Additionally, manufacturers and sellers will need to account for machine learning and consider how to ensure that the system is learning and performing as warranted.

Specific Liability Concerns Relating to Cybersecurity and Data Privacy

In addition to tort and contract liability for on-the-road accidents, the HAV technology presents liability risks arising out of cybersecurity and data privacy.

Cybersecurity

Cyber threats have been raised as concerns for the safety and security of autonomous vehicles.[143] If manufacturers fail to reasonably address these risks, they could incur liability from security and data breaches, like those related to hacking or vehicle theft. As with the Internet of Things ("IoT"), these risks at present are theoretical, but the fact that engineers and commentators can envision these types of risks raises legislative, regulatory, and public concerns calling for evaluation and prevention of those risks. Several years ago, a journalist demonstrated cyber risks in a carefully designed vignette where hackers remotely toyed with onboard displays and vehicle functions, before finally cutting power to a vehicle on the highway—all while its driver was still at the wheel.[144] While this was a carefully contrived demonstration, and the risk of similar hacking is likely remote absent physical access to a vehicle, manufacturers may contemplate ways to prevent these hypothetical risks and may warn about those risks that they cannot fully prevent.

The level of scrutiny that courts and regulators will apply in the HAV cybersecurity context remains to be seen. In a civil suit in California, plaintiffs alleged Ford, GM, and Toyota equipped their vehicles with computer technology susceptible to hacking.[145] The court dismissed the case for lack of standing, ruling that "potential" hacking is not an injury-in-fact. After this decision, California passed the country's first IoT law requiring manufacturers of *connected devices* to equip the device with a reasonable security feature or features that are appropriate (i) to the nature and function of the device, and the information the device may collect, contain, or transmit, and (ii) designed to protect the *device* and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.[146] The broad definition of *devices* would likely encompass HAV components that depend on Internet connectivity. Presumably, in the short term and in the absence of additional statutes, regulations, or warranties, traditional common-law rules for negligence, product liability, and consumer protection laws will adapt to govern manufacturer liability in the cybersecurity context.

Under the negligence framework in the cybersecurity context, a cause of action must demonstrate that the vehicle manufacturer violated its duty of reasonable care (sometimes called duty of ordinary care) owed to an individual injured by a security breach. The metes and bounds of that objective duty of reasonable care remain unclear absent federal or state regulation or voluntary industry standards setting minimum cybersecurity standards. To date, most cybersecurity efforts have been *voluntary*, so there are few required security standards for manufacturers to adopt.

Under the most recently proposed federal legislation—which represents Congress's most in-depth foray into regulating HAV cybersecurity risks—the key cybersecurity provisions primarily would have required manufacturers to "limit access to automated driving systems," designate a cybersecurity officer, and train employees with regard to cybersecurity.[147] Although the then-pending federal bill would have required manufacturers to develop their own cybersecurity plans to "detect[] and respond[] to cyber attacks, unauthorized intrusions, and false and spurious messages or vehicle control commands," the specificity of those plans was left to the manufacturers.[148] Congressman Latta's bill would have mandated that cybersecurity policies include: (i) "a process for identifying, assessing, and mitigating reasonably foreseeable vulnerabilities";

and (ii) "a process for taking preventive and corrective action to mitigate against [those] vulnerabilities."[149] For now in the United States, there is little specific, binding guidance for manufacturers on what actions they must take.

Also, without additional Federal legislation on HAV cybersecurity, industry cybersecurity and data privacy practices will be subject to consumer protection enforcement by the Federal Trade Commission ("FTC") under Section 5 of the Federal Trade Commission Act ("Section 5"), and by State Attorneys General with similar enforcement authority under their analogous state laws. Section 5 could be used to prohibit businesses from engaging in unfair or deceptive practices involving inadequate HAV cybersecurity or protection of consumers' personal data or deceptive "promises" concerning such matters.[150] The FTC also has authority to enforce a variety of sector-specific privacy laws that it could potentially apply to HAV issues.[151] The FTC could use this authority to address deceptive security and data privacy "promises" by providers of connected devices, including HAVs.[152]

Absent additional requirements in U.S. laws or regulations, potential plaintiffs might look to guidance in foreign countries. Accordingly, it is advisable for manufacturers and suppliers to monitor pertinent foreign laws, regulations, and standards for HAV cybersecurity and data privacy. Manufacturers and suppliers may also monitor NHTSA's nonbinding guidance on best practices concerning vehicle cybersecurity.[153]

If additional federal standards are promulgated, industry participants will want to ensure compliance with, and documentation satisfying, all cybersecurity requirements. Because autonomous systems within these vehicles will continue to learn and adapt after deployment, without robust reporting and documentation it will be difficult to establish the status of the vehicle's coded infrastructure, vulnerabilities, and breaches for any particular moment in time when a liability is alleged.

Data Privacy

Data privacy is another potential concern for future HAV consumers, because the technology can collect, store, and analyze significant sensitive information. During a recent NHTSA workshop, industry participants discussed the types of data collected and the purposes those data serve.[154] Some data are collected in the aggregate, such as information on car functions, to provide end-user services. Geolocation data can be used for traffic management or emergency response. All of these data—particularly locational data—may be sensitive in nature, but the more delicate information identifies the preferences or behavior of individual end-users and owners. Individuals' music preferences or internet browsing, for example, may be collected and sold to third-party advertisers. With HAVs, moreover, the personal information collected may be the driver's fingerprints or iris patterns. While data can be used to improve product functionality or implement safety measures, the breadth and detail of the data collected is potentially very valuable. Indeed, McKinsey & Co. found that the potential revenue pool from car data monetization will be $750 billion by 2030 globally.[155]

The data's value and personal nature raise fundamental legal issues: (i) what data should be permissible to collect; (ii) who owns the data and who can monetize the data, under what conditions; and (iii) how should industry members store and protect data to ensure privacy—whether from monetization, hacking, or identity theft. Consumers presumably will want to retain control over their personal information, and manufacturers will want, at a minimum, to access certain information for integration and optimization of their HAVs. To resolve this conflict, parties may agree to release data in exchange for certain features or compensation, or HAV data ownership may be allocated in vendor contracts, sales contracts, or even vehicle owner's manuals and privacy notices.[156] But the ultimate question of who owns the data has yet to be resolved in any uniform way and will likely be contested.[157]

Regardless of who owns the data, liability can ensue from data use in contravention of privacy policies and self-regulatory codes of privacy practices, data loss, and identity theft. Civil liability can also arise from failures to comply with state laws applicable to personal information collection and protection, prohibition on data sales, or failure to honor the exercise of consumer rights to access their personal information, have their personal information corrected or deleted where required, or failure to honor opt-outs to the sale of their data.[158] Accordingly, companies will need to consider corporate policies and practices with respect to data collection, retention, sharing, and loss prevention.

Formal data privacy standards exist internationally and, in some locales, at the state level. For example, in the European

Union and the European Economic Area, individuals' right to privacy includes a human right and property interest over their personal data, and companies must adhere to specific standards for protecting those interests.[159]

Domestically some states have also attempted to regulate similar privacy concerns. For example, California's Consumer Privacy Act gives private rights of action for data breaches.[160] Its protections cover certain data breaches involving specific, personal information. Moreover, companies are given the opportunity to cure a violation before consumers are entitled to damages. But California's data privacy right of action marks a substantial litigation risk for companies, because the state itself may bring actions for civil penalties.[161] Although data privacy laws in other states are more narrow,[162] the differing approaches under state law create uncertainty and a lack of uniformity for HAV manufacturers and sellers.[163]

The federal government has yet to regulate data privacy concerns arising from vehicles. The SELF DRIVE Act would have required companies to develop written plans regarding information "collection, use, sharing, and storage," as well as practices for "data minimization, de-identification, and retention about vehicle owners or occupants."[164] But those requirements, if they were adopted, would not have resolved other questions regarding who owns the data. Accordingly, in the United States, the data privacy issues will continue to evolve.

Self-Help—Uncertainty Should Not Prevent Action

Despite the uncertainties surrounding liability, vehicle and component manufacturers and sellers can take steps to protect themselves.

Indemnification Agreements with Suppliers. HAV manufacturers and suppliers may seek to define and apportion their liability among themselves through indemnification agreements. For vehicle manufacturers and suppliers, this contractual definition and assignment of liability can streamline litigation and lower litigation costs. For example, if a camera malfunctions, causing an accident, an indemnification agreement may allow the vehicle manufacturer to tender the claim to the camera manufacturer to defend, or require the camera manufacturer to cooperate and assist in the defense, or allow the vehicle manufacturer to recover its litigation expenses for defending the lawsuit.

Component providers can likewise seek indemnification from vehicle manufacturers for the use and integration of any of their parts, and they can attempt to limit any indemnification that they provide to purchasers of their parts. The Restatement (Third) of Torts: Products Liability[165] and state law provide guidance for component parts manufacturers on ways to avoid or limit potential liability. Component providers face a tradeoff: They can minimize their risk of liability by not "substantially participat[ing] in the integration of [their] components into the design of the other products,"[166] but business needs may risk liability by requiring them to collaborate with manufacturers to "design a component that will perform specifically as part of the integrated product" or even to "assist in modifying the design of the integrated product to accept the seller's component."[167]

For component providers of HAVs, the tradeoff may include considering how to foster technological innovation, product improvement, and future sales by partnering with end-product manufacturers in product design and development, while mitigating the accompanying risk of liability. This is particularly complicated by the fact that an HAV's capabilities to perform continue to change after it leaves a manufacturer. Accordingly, indemnification or supplier agreements may allow companies to control, at least in part, their tolerance for future liability risk.

Contractual Considerations. Manufacturers may also seek to reallocate risk by including certain terms and conditions in the sales agreement or owner's manuals so that vehicle owners assume certain risks during vehicle use. As HAVs develop through the early levels of automation, the sales agreement can require a buyer's consent not to use the vehicle in certain roadway or weather conditions or in higher-risk populated areas or to maintain control or attention during those conditions. Limited uses and capabilities of vehicle features could likewise be outlined and disclaimed in the owner's manual. Moreover, the owner's manual can limit liabilities associated with certain unsafe vehicle uses, such as driving over unmarked, unpaved roads, or require periodic maintenance.

For example, the vehicle manufacturer can require the owner to have the vehicle's sensors regularly tested to ensure proper functionality, and it can mandate that the owner regularly update the system software to optimize vehicle safety or patch

a security vulnerability. An owner's failure to comply with regular maintenance or software updates could shield liability, limit damages, or void warranties.[168] In *Carter*, a truck owner alleged breach of contract against the vehicle manufacturer after his truck broke down.[169] But the court attributed the truck's failure to the owner's "abuse of the vehicle," rather than "any defect exist[ing] . . . prior to [its] purchase," because the owner failed to adhere to the "regular maintenance" outlined in the owner's manual and likewise exceeded the truck's load capacity as limited in the operator's manual.[170] Key to reliance on this type of legal precedent will be clear notice to and consent by the consumer of the obligations.

Insurance. Securing insurance can protect the financial interests of a litigant that may face liability arising from HAV technology—hardware, software, cybersecurity, and data management. Although insurance companies may require preventive measures in exchange for coverage, they likely will "bas[e] premiums on an insured's level of self-protection," allowing flexibility in the coverage of liabilities for both drivers and manufacturers.[171] For drivers, insuring HAVs is expected to become less expensive over time because most highway accidents are caused by driver error rather than mechanical failure.[172] The new market has spurred venture capitalists and entrepreneurs to lay the groundwork for HAV insurance companies, with some major manufacturers intending to offer the insurance themselves.[173] All of that, of course, applies to the vehicle owner's liability insurance, not insurance against the manufacturer's potential liabilities under the broader product liability framework.

The level and manner in which vehicle manufacturers will be insured remains unclear, but the insurance industry has already identified the opportunity as a growth area.[174] The availability and cost of insurance for HAV manufacturers, suppliers, and sellers will turn in part on the legal liability rules that will apply. Scholars and commentators already are writing about potential terms of insurance.[175] HAV manufacturers, suppliers, and sellers are well-advised to monitor developments in the terms of insurance and review their policies carefully for HAV coverage, when the need arises.

Industry Standards. Regulatory gaps leave room for manufacturers, suppliers, and sellers to join with other stakeholders to develop voluntary standards, which then can serve as the basis for regulations. So far, the Department of Transportation has encouraged development of industry standards because no one knows the capabilities and limitations of technology better than manufacturers and suppliers. Furthermore, manufacturers and suppliers are in the best position to determine what is technologically feasible and economically advantageous. Industry standards can also help guide common-law liability, although those standards are not dispositive. Ultimately, manufacturers and suppliers should seize on this opportunity to shape their own future and the future of HAVs.[176]

CONCLUSION

While the HAV sector further develops in the absence of comprehensive state laws and controlling federal laws and regulations, HAV manufacturers, suppliers, and sellers may consider several ways to mitigate the risk of product liability claims:

- Chart out contractual obligations, responsibilities, representations, and warranties to pinpoint potential risks among those interacting with one's component part or end product;
- Join with stakeholders to develop industry standards and federal, state, and local regulations that will facilitate deployment and testing;
- Survey consumers concerning their views regarding product uses, advertising, and representations to understand their expectations as well as unintended, potential misunderstandings;
- Develop automatic enrollment systems for product alerts, including post-sale warnings and recalls, so important communication is streamlined to consumers directly;
- Monitor the development of state liability law and, when necessary, intervene to foster common-law rules favorable to deployment and testing of HAVs;
- Monitor the development of foreign laws, regulations, and guidance for applicability in the United States;
- Obtain robust insurance coverage for foreseeable risks; and
- Establish federal and state compliance rules for cybersecurity and data privacy issues underlying product development and consumer usage.

LAWYER CONTACTS

Barbara M. Harding
Washington
+1.202.879.4681
bharding@jonesday.com

Jeffrey J. Jones
Detroit/Columbus
+1.313.230.7950/+1.614.281.3950
jjjones@jonesday.com

Charles H. Moellenberg Jr.
Pittsburgh
+1.412.394.7917
chmoellenberg@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Jeff Rabkin
San Francisco/Silicon Valley
+1.415.875.5850/+1.650.739.3954
jrabkin@jonesday.com

Charlotte H. Taylor
Washington
+1.202.879.3872
ctaylor@jonesday.com

Keeton H. Christian, Autumn Hamit Patterson, and Stephen C. Scott assisted in the preparation of this White Paper.

ENDNOTES

1 Jillian D'Onfro, *Amazon's New Delivery Drone Will Start Shipping Packages 'In a Matter of Months'*, FORBES (June 5, 2019). In anticipation of a future with aerial home deliveries, the Federal Aviation Administration published new rules in January 2021. The rules require remote identification of drones and allow small drones to fly over people and at night under some conditions. Operation of Small Unmanned Aircraft Systems Over People, 86 Fed. Reg. 4314 (Jan. 15, 2021); Remote Identification of Unmanned Aircrafts, 86 Fed. Reg. 4390 (Jan. 15, 2021).

2 Kim Lyons, *Nuro's Self-Driving Robot Will Deliver Domino's Pizza Orders to Customers in Houston*, THE VERGE (Apr. 12, 2021) (In April 2021, Domino's began offering customers living in one neighborhood in Houston the option of having their pizzas delivered by a robot.).

3 Sean O'Kane, *UPS Has Been Quietly Delivering Cargo Using Self-Driving Trucks*, THE VERGE (Aug. 15, 2019).

4 Shay Eliaz, Robert Krumpf, & Tom Aldred, *Making the Future of Mobility: Chemicals and Specialty Materials in Electric, Autonomous, and Shared Vehicles*, DELOITTE (Apr. 19, 2018).

5 *SAE International Releases Updated Visual Chart for Its "Levels of Driving Automation" Standard for Self-Driving Vehicles*, SAE INTERNATIONAL (Dec. 11, 2018).

6 *Id.*

7 *Id.*

8 Roadway testing has also increased across the globe. For example, Volvo launched its Drive Me project in Sweden. *Drive Me, the World's Most Ambitious and Advanced Public Autonomous Driving Experiment, Starts Today*, VOLVO (Sept. 9, 2016). Shanghai became the first city in China to issue licenses for self-driving cars. Ryan Daws, *Shanghai Becomes the First Chinese City to License Self-Driving Cars to Carry Passengers*, IOTNEWS (Sept. 19, 2019). And South Korea has built a town, which covers approximately 89 acres, for self-driving car experimentation. Will Sabel Courtney, *South Korea Building an Entire Town for Testing Self-Driving Cars*, THE DRIVE (May 9, 2017).

9 *Move Nona*, BEEP (last visited Mar. 12, 2021); Alan Ohnsman, *Waymo Says More of Its Self-Driving Cars Operating 'Rider Only' with No One at Wheel*, FORBES (Oct. 28, 2019). Autonomous shuttles are set to launch in Yellowstone National Park in May 2021. Brandi Vincent, *The National Park Service is Exploring Emerging, Autonomous Technologies Through a New Pilot Program that the Public Can Opt to Participate in*, NEXTGOV (Oct. 30, 2020); *see also* David Welch, *GM-Backed Cruise Will Run Driverless Taxis in Dubai in 2023*, BLOOMBERG (Apr. 12, 2021). (In 2023, Cruise will begin operating self-driving taxis in Dubai, and the company expects the fleet to grow to include 4,000 driverless shuttles by 2030.).

10 Ian Duncan, *Autonomous Shuttles in Northern Virginia Suburb Show Why the Future of Robot Cars Might Be Slow*, WASH. POST. (Oct. 12, 2019).

11 Kevin Todd, *When Technology Is Unpredictable, Can Regulators Keep Up?*, MICH. L. (Oct. 7, 2019).

12 Tim Levin, *Amazon's Autonomous Vehicle Startup Zoox Just Unveiled a Robotaxi EV Without a Steering Wheel that Can Go 16 Hours Without Charging — See What It Looks Like*, BUS. INSIDER (Dec. 14, 2020).

13 Joshua Dowling, *Apple Co-founder Steve Wozniak Slams Autonomous Cars, Predicts They May Not Happen "in My Lifetime,"* CAR ADVICE (Oct. 29, 2019).

14 Aarian Marshall, *Elon Musk Promises a Really Truly Self-Driving Tesla in 2020*, WIRED (Feb. 19, 2019). In December 2020, Tesla described its Autopilot and Full Self-Driving features as representative of SAE 2 automation, and stated that it expects "functionality to remain largely unchanged" in the near future. Timothy B. Lee, *Tesla: "Full Self-Driving Beta" Isn't Designed for Full Self-Driving*, ARS TECHNICA (Mar. 9, 2021). In February 2021, NTSB recommended that NHTSA regulate safeguards that ensure drivers do not use automated driving systems beyond the conditions in which the systems are intended to operate. Letter from Robert L. Sumwalt, III, NTSB Chairman, to NHTSA (Feb. 1, 2021).

15 Steve Crowe, *Researchers Back Tesla's Non-LiDAR Approach to Self-Driving Cars*, THE ROBOT REPORT (Apr. 25, 2019).

16 Shahian-Jahromi Babak *et al.*, *Control of Autonomous Ground Vehicles: A Brief Technical Review*, 2017 IOP CONF. SER.: MATER. SCI. ENG. 224 012029, 4 (2017).

17 John R. Quain, *These High-Tech Sensors May Be the Key to Autonomous Cars*, N.Y. TIMES (Sept. 26, 2019); *see also* Chris Wiltz, *FLIR's Thermal Sensors Are Coming to Self-Driving Cars in 2021*, DESIGNNEWS (Nov. 6, 2019).

18 Ryan Whitwam, *MIT Taught Self-Driving Cars to See Around Corners with Shadows*, EXTREME TECH (Oct. 29, 2019).

19 Arun Ganesan, *Will Facial Recognition Protect Our Data in the Age of Autonomous Cars?*, INFO. SEC. BUZZ (May 30, 2018).

20 Aarian Marshall, *Why Are Parking Lots So Tricky for Self-Driving Cars?*, WIRED (Oct. 28, 2019).

21 China is rapidly expanding its testing of autonomous vehicles. Meghan Han, *Beijing Self-Driving Vehicle Road Tests Topped One*

Million Km in 2019, SYNCED (Mar. 14, 2020). This year, one company in China also obtained permission to test fully driverless cars on public roads. *Baidu Tops Beijing Autonomous Vehicles Road Test Report for the Third Consecutive Year*, PR NEWSWIRE (Feb. 5, 2021).

22 Allie Arp, *Researchers Develop Platform for Scalable Testing of Autonomous Vehicle Safety*, TECH XPLORE (Oct. 25, 2019).

23 Darrell Etherington, *MIT Uses Shadows to Help Autonomous Vehicles See Around Corners*, TECH CRUNCH (Oct. 28, 2019).

24 Tom Stone, *TTI Trialing New Machine-Readable Road Signs that Provide Driver Information*, TRAFFIC TECH. TODAY (Dec. 21, 2017). Companies are working toward developing infrastructure that can help HAVs more easily process driving scenarios, but some critics doubt the feasibility and prudence of replacing existing infrastructure if HAV software can adapt without the costly upgrades. Matt McFarland, *Your Self-Driving Car Still Isn't Ready. Smarter Roads Might Change That*, CNN (Mar. 5, 2021).

25 Gary Elinoff, *Is C-V2X Overtaking DSRC in Vehicle-to-Vehicle Communications?*, ALL ABOUT CIRCUITS (Mar. 5, 2019).

26 *Id.*

27 *See id.*

28 *DSRC vs. C-V2X for Safety Applications*, AUTOTALKS (last visited Mar. 15, 2021).

29 *See id.*; *see also* Sieeka Khan, *Verizon and Honda to Team Up and Develop Safe Driving Measures Using 5G and Mobile Edge Computing*, TECH TIMES (Apr. 8, 2021 1:23 PM EDT) (Honda and Verizon research partnership on the use of 5G and mobile edge computing for connected and autonomous vehicles to create improved, faster communication among pedestrians, vehicles, and infrastructure). Although growth of 5G technology is ongoing, 6G already is envisioned as the next advancement.

30 *See generally Laws and Regulations*, NHTSA (last visited Mar. 15, 2021).

31 *See, e.g.*, NHTSA, *Laboratory Test Procedure for FMVSS 203: Impact Protection for the Driver from the Steering Control System*, DOT TP-203-02 (May 4, 1990).

32 NHTSA requires self-certification with federal safety and testing standards, but also allows for exemptions. *See* 49 C.F.R. §§ 555.1–555.18; *see also* Laura Fraade-Blanar & Nidhi Kalra, *Autonomous Vehicles and Federal Safety Standards: An Exemption to the Rule?*, RAND CORP. (2017).

33 *See Autonomous Vehicle Exemptions to NHTSA's FMVSS*, SHARED-USE MOBILITY CENTER (Feb. 1, 2020).

34 For example, with regard to autonomous safety standards, the United Nations' European Commission for Europe held a World Forum for Harmonization of Vehicle Regulations within the last year that undertook and approved specific regulations for varying degrees of vehicle autonomy. *See, e.g.*, Provisional Agenda, *Proposal for a New UN Regulation on Uniform Provisions Concerning the Approval of Vehicles with Regards to Automated Lane Keeping System*, ECON. COMM'N FOR EUROPE, UNITED NATIONS (Apr. 6, 2020). Although Europe does not adhere to the SAE definitions of autonomy, these regulations primarily governed SAE 3 and SAE 4 equivalent vehicles. One of these regulations included new safety standards requiring operation only on roadways without pedestrians, the use of a backup driver, and implementation of design features such as a functional self-check on automated systems and a data recorder to help deduce fault in the event of an accident. *See id.* Likewise, Japan issued revisions to its Road Transport Vehicle Act to regulate vehicles equivalent of SAE 3 and up. *See* Takeyoshi Imai, *Legal Regulation of Autonomous Driving Technology: Current Conditions and Issues in Japan*, 43 INT'L ASS'N of Traffic and Safety Scis. 263 (2019). These revisions implement minimum safety standards for use and deployment, limit conditions of use for those autonomous systems (specifically, roadway, environmental, and geographic limitations), require regular maintenance to ensure that sensors and autonomous systems remain functional, and mandate access protocols that require manufacturer authorization before a user can modify vehicle systems or telecommunication functions. *See id.*

With regard to cybersecurity and data protection, other nations have implemented formal processes to which companies must adhere in order to protect consumers. Under the European Union's General Data Protection Regulation, for example, these processes include mandatory data inventory and the mapping of data flows, formal processes to erase individual personal information upon request, disclosure of data privacy practices, and written contracts with service providers. *See generally* Jacob M. Victor, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 YALE L.J. 513 (2013); *California Consumer Privacy Act Fact Sheet*, CAL. DEP'T OF JUST. An independent group of analysts, on behalf of the European Commission, has published a report outlining 20 ethical recommendations for the future development of automated vehicles. *See* EUROPEAN COMM'N, *Ethics of Connected and Automated Vehicles* (Sept. 2020). The report, which concerns, in part, privacy and data protection, encourages stakeholders to collaborate on how to best implement these recommendations. *See* JONES DAY, *European Commission Expert Group Issues Connected and Automated Vehicle Privacy Recommendations* (Apr. 2021).

Secretary Pete Buttigieg has argued that, unlike other countries that have developed "very robust strategies," "the policy framework in the U.S. has not really caught up with the technology platforms or some of the things that are becoming capable." *See The Administration's Priorities for Transportation Infrastructure*, at 52:11–30, 117th Cong. (2021) (testimony of Pete Buttigieg, Sec'y, U.S. Dep't of Transp.).

35 *See* H.R. 3388, 115th Cong. (2017); S. 1885, 115th Cong. (2017).

36 *H.R.3388 - SELF DRIVE Act*, CONG. (last visited Mar. 21, 2021); *S. 1885 - AV START Act*, CONG. (last visited Mar. 21, 2021).

37 *See* H.R. 8350, 116th Cong. (2020).

38 *See id.*

39 *See id.*

40 *See id.*

41 *See id.* (emphasis added).

42 *See id.*

43 *See id.*

44 Senator Thune (R-S.D.) and Senator Peters (D-Mich.), who previously co-sponsored autonomous vehicle legislation, have both expressed an interest in advancing bipartisan legislation again in this Congress. Maggie Miller, *Congress Makes Renewed Push on Self-Driving Cars Bill*, THE HILL (Feb. 17, 2021).

45 DOT, *Automated Vehicles: Comprehensive Plan* (Jan. 2021); National Science & Technology Council and DOT, *Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0* (Jan. 2020); DOT, *Automated Vehicles 3.0: Preparing for the Future of Transportation* (Oct. 2018); DOT and NHTSA, *Automated Drive Systems 2.0: A Vision for Safety* (Sept. 2017); DOT and NHTSA, *Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety* (Sept. 2016).

46 *Vehicles 4.0*, *supra* note 45, at 5; *Comprehensive Plan*, *supra* note 45, at 4.

47 *U.S. Transportation Secretary Elaine L. Chao Announces First Participants in New Automated Vehicle Initiative Web Pilot to Improve Safety, Testing, Public Engagement*, NHTSA (June 15, 2020).

48 Beep, Cruise, Fiat Chrysler Automobiles, Local Motors, Navya, Nuro, Toyota, Uber, and Waymo were the companies that initially participated in the AV TEST Initiative. *See id.*

49 California, Florida, Maryland, Michigan, Ohio, Pennsylvania, Texas, and Utah are participating in the AV TEST Initiative. *See id.*

50 *U.S. Department of Transportation Announces Expansion of AV TEST Initiative*, NHTSA (Jan. 11, 2021).

51 *New Automated Vehicle Initiative*, *supra* note 47; *see also* James Owens, Deputy Administrator, *AV TEST Initiative Launch Remarks*, NHTSA (June 15, 2020). The public can view participants' testing information using an interactive test tracking tool. *AV Test Initiative: Test Tracking Tool*, NHTSA (last visited Mar. 15, 2021).

52 NHTSA, Pilot Program for Collaborative Research on Motor Vehicles with High or Full Driving Automation; Extension of Comment Period, 83 Fed. Reg. 59353 (Nov. 23, 2018).

53 FMCSA, Safe Integration of Automated Driving Systems-Equipped Commercial Vehicles, 84 Fed. Reg. 24449 (May 28, 2019); NHTSA,

Removing Regulatory Barriers for Vehicles with Automated Driving Systems, 84 Fed. Reg. 24433 (May 28, 2019).

54 *See, e.g.*, DOT, Occupant Protection for Automated Driving Systems, 85 Fed. Reg. 17,624 (Mar. 30, 2020).

55 *See id.*

56 *See id.*

57 *See infra* Part II(A)(2)(a).

58 *NHTSA Issues First-Ever Proposal to Modernize Occupant Protection Safety Standards for Vehicles Without Manual Controls*, NHTSA (last visited Mar. 17, 2021) (disposition labeled "pending").

59 NHTSA, Framework for Automated Driving System Safety, 85 Fed. Reg. 78058 (Dec. 3, 2020).

60 *Id.*

61 *Id.*

62 NHTSA, Framework for Automated Driving System Safety; Extension of Comment Period, 85 Fed. Reg. 78058 (Jan. 29, 2021). U.S. Transportation Secretary Pete Buttigieg has signaled support for the development of autonomous vehicles and expressed his perceived need for further regulation in the area. At his confirmation hearing, Secretary Buttigieg stated, "Automated vehicle technology is coming; it's advancing very quickly . . . It is something that holds the potential to be transformative[,] and I think in many ways policy has not kept up." Luke Bellos, *Transportation Secretary Nominee Pete Buttigieg Promotes Emerging Tech for Infrastructure Policies*, IOT EVOLUTION (Jan. 25, 2021). Later, before the House Committee on Transportation and Infrastructure, Secretary Buttigieg clarified that he prioritizes establishing "regulatory certainty and safety infrastructure for consumers and companies alike to know what to expect so that kind of technology meets its fullest potential." *See The Administration's Priorities for Transportation Infrastructure, supra* note 34, at 3:42:24–36.

63 *See* 5GAA Petition for Waiver, *In re: Petition for Wavier to Allow Deployment of Intelligent Transportation System Cellular Vehicle to Everything (C-V2X) Technology*, Docket No. 18-357 (Nov. 21, 2018); Letter from Ford to FCC regarding Petition for Waiver (Jan. 24, 2019).

64 FCC, Notice of Proposed Rulemaking in re: Use of the 5.850-5.925 GHz Band, Docket No. 19-138, ¶ 11 (adopted Dec. 12, 2019).

65 *Id*. at ¶ 28.

66 Letter from Elaine Chao, Secretary, DOT, to Ajit Pai, Chairman, FCC (Nov. 20, 2019); *see also* David Shepardson, *Government Agencies Question FCC Plan to Shift Auto Spectrum to Wi-Fi*, AUTOMOTIVE NEWS (Oct. 29, 2020). Secretary Pete Buttigieg testified before the House Committee on Transportation and Infrastructure that he shares the bipartisan concern regarding the 5.9 GHz band reorganization and plans to engage across the administration on how to best handle and share the spectrum consistent with safety, as well as current and future forms of communication. *See The Administration's Priorities for Transportation Infrastructure, supra* note 34, at 31:00–39.

67 Letter from Members of the House to Ajit Pai, Chairman of FCC, and Commissioners (Jan. 22, 2020).

68 *See* Monica Alleven, *FCC Moves to Authorize C-V2X in 5.9 GHz Band*, FIERCE WIRELESS (Oct. 29, 2020).

69 *See id.*

70 FCC, First Report and Order, Further Notice of Proposed Rulemaking, and Order of Proposed Modification in re: Use of the 5.850-5.925 GHz Band, Docket No. 19-138, ¶ 11 (adopted Nov. 18, 2020).

71 *See FCC Modernizes 5.9 GHz Band for Wi-Fi and Auto Safety*, FCC (Nov. 18, 2020).

72 Existing federal law does place some limitations on state regulation in the HAV space. The Federal Aviation Administration Authorization Act ("FAAAA"), for example, preempts states from passing legislation related "to a price, route, or service . . . of any motor carrier . . . with respect to the transportation of property." 49 U.S.C. § 14501(c)(1). Courts have interpreted this preemption provision broadly to include provisions having an "indirect" impact on motor carrier prices, routes, and services. *Rowe v. New Hampshire Motor Transp. Ass'n*, 552 U.S. 364, 370 (2008) (quoting *Morales v. Trans World Airlines, Inc.*, 504 U.S. 374, 386 (1992)). However, the FAAAA expressly permits state regulation of safety, insurance requirements, and the "size or weight of the motor vehicle or the hazardous nature of [its] cargo." 49 U.S.C. § 14501(c)(2).

73 *Autonomous Vehicles State Bill Tracking Database*, NAT'L CONF. OF STATE LEGISLATURES (Mar. 15, 2021).

74 *See, e.g.*, Okla. Stat. tit. 47, § 11-310 (e), (f) (exempting "motor vehicles traveling in a unified manner at electronically coordinated speeds" from tailgating prohibition); Executive Order 19-18 from Tim Walz, Governor of Minnesota (Apr. 8, 2019) (establishing the "Governor's Advisory Council on Connected and Automated Vehicles").

75 *Highway Accident Report: Collison Between Vehicle Controlled by Developmental Automated Driving System and Pedestrian, Tempe, Arizona, March 18, 2018*, NAT'L TRANSP. SAFETY BD. 55 (Nov. 19, 2019).

76 *See Autonomous Vehicles State Bill Tracking Database*, *supra* note 73 (showing that 11 states have passed legislation relating to the testing of HAVs).

77 *See id.* (listing 10 AV-related bills California has passed, including several related to testing).

78 *See* Cal. Veh. Code § 38750(d) (authorizing the California Department of Motor Vehicles to adopt regulations regarding autonomous vehicles); Cal. Code Regs. tit. 13, §§ 227.00–227.54 (testing of autonomous vehicles); Cal. Code Regs. tit. 13, §§ 228.00–28 (deployment of autonomous vehicles).

79 Permit Holders (Testing with a Driver), CAL. DEP'T OF MOTOR VEH.; Permit Holders (Driverless Testing), CAL. DEP'T OF MOTOR VEH.; Permit Holders (Deployment), CAL. DEP'T OF MOTOR VEH.

80 Cal. Veh. Code § 38750(b)(3); Cal. Code Regs. tit. 13, §§ 227.04(c); 227.30(a)(1) (fee for up to 10 HAVs and 20 drivers).

81 Cal. Code Regs. tit. 13, §§ 227.32, 227.34, 227.36, 227.38.

82 Executive Order 2018-04: Advancing Autonomous Vehicle Testing and Operating; Prioritizing Public Safety; *Autonomous Vehicles Testing and Operating WITHOUT Driver*, ARIZ. DEP'T OF TRANSP.

83 *Highway Accident Report*, *supra* note 75, at 55–59.

84 *See* 75 Pa. Stat. and Cons. Stat. §§ 102, 3317.

85 *Automated Vehicle Testing Guidance*, PENN. DEP'T OF TRANSP. 2 (July 23, 2018). Uber created an area outside of Pittsburgh to test self-driving-car technology. Lisa Eadicicco, *Uber Just Quietly Bought 600 Acres of Land to Build a New Test Track for Self-Driving Cars in Pittsburgh*, INSIDER (Dec. 26, 2019). Several other companies, including Aptiv, Argo AI, and Aurora, and Carnegie Mellon University, are testing driverless cars in Pittsburgh. Kyle Wiggers, *Companies Are Testing 55 Self-Driving Cars in Pittsburgh*, VENTURE BEAT (Apr. 26, 2019).

86 *See generally, e.g.*, Statement of Volvo Car Corp. before the House Committee on Energy & Commerce regarding Self-Driving Cars: Road to Deployment (Feb. 14, 2017); Daniel A. Crane et. al., *A Survey of Legal Issues Arising from the Deployment of Autonomous and Connected Vehicles*, 23 MICH. TELECOMM. & TECH. L. REV. 191, 222 (2017) (collecting statements regarding the desire for uniformity).

87 States traditionally leave certain roadway regulation to local governments, such as zoning, road signage, traffic signals, speed limits, traffic light cameras, and maintaining roadways. These local issues can impact HAV manufacturers. For example, a zoning ordinance in Chandler, Arizona, was used to incentivize local property owners to provide HAV parking areas. *See* Katherine Shaver, *City Planners Eye Self-Driving Vehicles to Correct Mistakes of the 20th-Century Auto*, WASH. POST (July 20, 2019); Aarlan Marshall, *32 Hours in Chandler, Arizona, the Self-Driving Capital of the World*, WIRED (Dec. 8, 2018); *Chandler First in the Nation to Include Autonomous Vehicles and Ride Sharing in Zoning Code*, CHANDLER, ARIZ. (Apr. 27, 2018). Beyond incentivizing or deterring HAVs, local regulation can also have a significant impact on testing and deployment. Pittsburgh, for example, has entered into a number of informal agreements with HAV manufacturers to allow for testing without substantial oversight. *See* Lucy Perkins, *et al.*, *Autonomous Vehicle Pilots Across America: Municipal Action Guide*, NAT'L LEAGUE OF CITIES 26–27 (2018). Other cities, such as Boston, expressly limit the timing and location of testing within the city, and require formal application and review before any testing may occur. *See* Executive Order Establishing a Policy for Autonomous Vehicles in the City of Boston, CITY OF BOSTON (Oct. 20,

2016); *Autonomous Vehicles: Boston's Approach*, CITY OF BOSTON (Jan. 19, 2021; *see also* Template Memorandum of Understanding for Autonomous Vehicle Testing in Boston (Jan. 20, 2017).

88 Secretary Buttigieg has acknowledged that many current safety regulations are not compatible with HAVs because they assume that a human driver is operating a vehicle. *See The Administration's Priorities for Transportation Infrastructure, supra* note 34, at 3:41:31–42:00.

89 Of course, other persons or entities may be liable for causing HAV accidents, such as those who performed faulty maintenance or failed to install a software upgrade.

90 At present, however, some legislators have insisted that HAVs permit drivers to take over control at their discretion. John Bonazzo, *Senate Hits the Brakes on Self-Driving Car Legislation Over Safety Concerns*, OBSERVER (Feb. 12, 2018, 4:38 PM).

91 *See Legal Issues Related to the Development of Automated, Autonomous, and Connected Cars*, JONES DAY (Nov. 2017) (discussing driver training, which could affect this analysis in states that use a consumer expectation test for strict liability).

92 Each of these methods of protection requires a thorough analysis of applicable federal and state law that is beyond the scope of the overview presented in this *White Paper*. The availability and terms of insurance coverage and state law requirements for insurance raise complex issues that the marketplace and regulators will need to sort out. *See The Road to Autonomous Vehicles: A Look at Insurance Implications*, JONES DAY (Apr. 2017) (outlining some of the key insurance issues concerning autonomous vehicle industry participants' potential product liability).

93 Michael J. Miles & Jeffrey E. Jakob, *Discovery Sanctions under Amended Rule 37(e): A Safe(r) Harbor*, AM. BAR ASS'N (Aug. 30, 2016).

94 In a guidance document, published in 2016, NHTSA stated that "vehicles should record, at a minimum, all information relevant to the [crash] event and the performance of the system, so that the circumstances of the event can be reconstructed." *Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety, supra* note 45. In March 2021, the British Standards Institute published "requirements for the collection, curation, storage and sharing of information during automated vehicle trials" in the United Kingdom. *PAS 1882:2021 Data Collection and Management for Automated Vehicle Trials for the Purpose of Incident Investigation – Specification*, BSI (Mar. 2021).

95 *See, e.g., Event Data Recorder*, NHTSA (last visited Mar. 13, 2021) (discussing the multifaceted use of a vehicular Event Data Recorder based on its complexity).

96 Jonathan Sperling, *Arizona Uber Driver Was Streaming 'The Voice' on Hulu Before Fatal Self-Driving Car Crash*, FORTUNE (June 22, 2018, 9:43 AM). Although this *White Paper* focuses on civil liabilities, the Arizona accident further demonstrates that criminal liability can arise in certain instances. The backup driver from that accident was charged with negligent homicide and was scheduled for trial on February 2021. Jay Ramey, *Uber Driver Charged in Fatal 2018 Autonomous Car Crash*, AUTOWEEK (Sept. 16, 2020). The backup driver's negligent homicide charge remains pending without a final disposition. *See State of Arizona v. Rafael Stuart Vasquez*, No. CR2020-001853-001 (Ariz. Super. Ct.), (last visited Mar. 13, 2021). France has begun drafting legislation to assign criminal liability among drivers and manufacturers in HAV-related accidents, like the Arizona accident. *See France Plans on Adopting New Rules for Self-Driving Cars*, JONES DAY (Apr. 2021).

97 *See* 49 U.S.C. § 30103.

98 529 U.S. 861 (2000).

99 562 U.S. 323 (2011).

100 *See* H.R. 8350, 116th Cong. (2020) (emphasis added).

101 *See id.*

102 *See* 49 U.S.C. §§ 20106(b)(1)(A), (B); *Ryder v. Union Pac. R.R. Co*., 945 F.3d 194, 203 (5th Cir. 2019).

103 *See generally, e.g.*, *Cipollone v. Liggett Grp., Inc*., 505 U.S. 504 (1992).

104 *See supra* note 34.

105 *See, e.g.*, ECON. COMM'N FOR EUROPE, *supra* note 34.

106 366 P.3d 33 (Wash. App. 2015).

107 *Id.* at 36–39.

108 Kenneth S. Abraham & Robert L. Rabin, *Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era*, 105 VA. L. REV. 127 (2019).

109 The move toward strict liability began in the early 1900s in the context of automobile accidents. *See, e.g.*, *Macpherson v. Buick Motor Co.*, 111 N.E. 1050 (N.Y. 1916). Strict liability has proven to be capable of adapting to changes in technology and resulting accidents and injuries.

110 *See* Restatement (Second) of Torts § 402A (AM. L. INST. 1965); Restatement (Third) of Torts: Prods. Liab. §2 (AM. L. INST. 1998); *see also, e.g.*, *Zamora v. Mobil Corp.*, 704 P.2d 584 (Wash. 1985) (reasoning that these principles are rooted in the theory that sellers and manufacturers are the least cost avoiders and in the best position to ensure design safety and functionality).

111 *See Consumer Expectations Test*, LEGAL INFO. INST., CORNELL L. SCH. (last visited Mar. 13, 2021).

112 Andrea Dearden, *Suit Blames Ford's Rear-View System for Toddler's Driveway Death*, SE. TEX. RECORD (Sept. 10, 2014).

113 Many states have limited product liability for sellers of consumer packaged goods. It is uncertain whether HAVs, like current automobiles, will fall within the scope of that limitation. However, dealer agreements or the common law may give sellers rights of indemnification against manufacturers. *See* 2 FRUMER & FRIEDMAN, PROD. LIAB. § 15.03(1)(e) (Matthew Bender, Rev. ed. 2021) (discussing the availability of common-law indemnification in each state). Because sellers may continue to have the direct contact with HAV purchasers and users, they can also play a role in educating consumers about the HAV technology and its limitations, as well as owner and driver responsibilities. Sellers can point out the various technology options on different vehicles. They also can deliver the limitations on warranties. Sellers may also create the factual basis for liability claims through their own advertising and representations to purchasers. *See* 2 James B. Astrachan *et al*., THE L. OF ADVERT. § 14.03 (Matthew Bender 2021) (outlining areas of potential liability concerning seller advertising statements). Some auto manufacturers are also contemplating a future model of direct sales to consumers that may include new forms of disseminating information. *See, e.g.,* Aria Alamalhodaei, *EV Rivals Tesla, Rivian Unite to Target Direct Sales Legislation*, TECHCRUNCH (Mar. 3, 2021 11:59 AM) (discussing companies incorporating a direct-to-consumers sales model and lobbying for direct sales legislation in all 50 states).

114 Cami Perkins, *The Increasing Acceptance of the Restatement (Third) Risk Utility Analysis in Design Defect Claims*, 4 NEV. L.J. 609 (2004).

115 104 S.W.3d 600, 602–03 (Tex. App. 2003).

116 *See id.* at 605 (emphasis added).

117 *See id.* at 608–09.

118 *See id.* at 603, 608–09.

119 861 N.Y.S.2d 431, 432–33 (N.Y. App. Div. 2008).

120 *See id.*

121 *See id.* at 434.

122 Claims of consumer confusion or misunderstanding also may give rise to claims under state consumer protection laws against a manufacturer or seller for fraudulent or deceptive conduct. *See Gregg v. Ameriprise Fin., Inc*., No. 29 WAP 2019, 2021 WL 607486 (Pa. Feb. 17, 2021). Some states, in addition, have false advertising statutes to protect consumers. *See, e.g.,* Cal. False Advert. L, Cal. Bus. & Prof. Code §§ 17500 *et seq*.

123 *Rosenberg v. Harwood*, No. 100916536, 2011 WL 3153314 (D. Utah Dist. Ct. May 27, 2011).

124 Jo Ciavaglia, *$15M Suit Blames GPS for Boston Bus Accident that Injured Students, Chaperones*, BUCKS CNTY COURIER TIMES (Jan. 26, 2015).

125 *Cruz v. Talmadge*, 15-0222 (Mass. Super. Ct. Jan. 23, 2015).

126 *Glorvigen v. Cirrus Design Corp.*, 796 N.W.2d 541 (Minn. Ct. App. 2011).

127 It also remains to be seen whether states will revise their driver's license requirements for HAVs, such as a requirement to pass a driving test with an HAV before operating one. *See Jurisdictional*

Guidelines for the Safe Testing and Deployment of Highly Automated Vehicles 29–31, Autonomous Vehicles Best Practices Working Grp., AM. ASS'N OF MOTOR VEHICLE ADM'RS (May 2018) (discussing standardized procedures for driver's license examinations for automated vehicles, depending on their level of automation); Ben Husch and Anne Teigen, *Regulating Autonomous Vehicles*, NAT'L CONF. OF STATE LEGISLATURES (Apr. 2017) (noting Florida is the first state permitting operation of an autonomous vehicle with a valid driver's license under its current driver's licensing requirements); Mark Harris, *Will You Need a New License to Operate a Self-Driving Car?*, IEE SPECTRUM (Mar. 2, 2015 15:00 GMT) (explaining that potential revisions to driver's license requirements for HAVs may include "lessons on the abilities and limitations of autonomous technologies, computer simulations of failures," "disengagements" practice, and autonomous vehicle setup and system deactivation tutorials).

128 *See Glorvigen*, 796 N.W.2d at 552 (explaining that it is unprecedented for the duty to provide adequate instructions for safe use to include "an obligation to train the end user to *proficiency*") (emphasis added).

129 *See, e.g.*, *Hudson v. Tesla, Inc*., 2018-CA-011812-O (Fla. Cir. Ct. Oct. 30, 2018) (involving an accident where a vehicle on autopilot collided with a disabled vehicle that stalled in its lane of travel).

130 *See, e.g.*, *Nilsson v. Gen. Motors LLC*, 4:18-cv-00471 (N.D. Cal. Jan. 22, 2018) (involving a vehicle in self-driving mode that abandoned an initial attempt to merge lanes, ultimately colliding with a motorcycle and injuring its driver).

131 *See, e.g.*, *Kozlowski v. John E. Smith's Sons Co*., 275 N.W.2d 915 (Wis. 1979).

132 *See* Restatement (Third) of Torts: Prods. Liab. §10 (AM. L. INST. 1998) (Liability of Commercial Product Seller or Distributor for Harm Caused by Post-Sale Failure to Warn); *see also id.* at § 13 (Liability of Successor for Harm Caused by Successor's Own Post-Sale Failure to Warn).

133 *See id.* at § 11 (Liability of Commercial Product Seller or Distributor for Harm Caused by Post-Sale Failure to Recall Product).

134 Restatement (Third) of Torts: Prods. Liab. § 5 cmt. a (AM. L. INST. 1998) (discussing the "bulk sales/sophisticated purchaser rule" that recognizes "component sellers who do not participate in the integration of the component into the design of the product should not be liable merely because the integration of the component causes the product to become dangerously defective").

135 *See id.* at § 5 cmt. e ("A component seller who simply designs a component to its buyer's specifications, and does not substantially participate in the integration of the component into the design of the product, is not liable. . .").

136 *See id.*

137 Sean P. Wajert, *Product Liability Claims, Defenses, and Remedies*, PRAC. LAW LITIG. (last visited Mar. 13, 2021); *see also* Stephanie E. Niehaus & Huu Nguyen, *Artificial Intelligence and Tort Liability: The Evolving Landscape*, PRAC. LAW LITIG. (last visited Mar. 13, 2021).

138 U.C.C. § 2-313 (AM. L. INST. & UNIF. L. COMM'N 2020 ed.).

139 352 N.E.2d 774, 777 (Ind. Ct. App. 1976).

140 *See id.* at 778.

141 *See id.* at 781.

142 *See id.* at 781–82.

143 Secretary Buttigieg has explained that the Department of Transportation will be "at the table" in addressing cyber and data privacy concerns and threats. *See The Administration's Priorities for Transportation Infrastructure*, *supra* note 34, at 1:35:00–14.

144 Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, WIRED (July 21, 2015).

145 *Cahen v. Toyota Motor Co*., 147 F. Supp. 3d 955, 958 (N.D. Cal. 2015), aff'd, 717 F. App'x 720 (9th Cir. 2017).

146 Cal. Civ. Code §§ 1798.91.

147 *See* H.R. 8350, 116th Cong. (2020).

148 *See id.*

149 *See id.*

150 15 U.S.C. § 45(a)(2).

151 For example, the FTC has authority to enforce non-compliance with the Controlling the Assault of Non-Solicited Pornography and Marketing, CAN-SPAM Act, applicable to direct digital marketing, and the Children's Online Privacy Protection Act, applicable to online personal data collection from children. 15 U.S.C. § 7706; 15 U.S.C. § 6505.

152 *See Vehicle Data Privacy*, NHTSA (last visited May 4, 2021) ("Although NHTSA has broad regulatory authority over the safety of passenger vehicles, it is the FTC that is the primary Federal agency responsible for protecting consumer privacy."); *see also Privacy Principles for Vehicle Technologies & Services*, GLOBAL AUTOMAKERS (Nov. 2014).

153 *See Cybersecurity Best Practices for Modern Vehicles*, NHTSA (Oct. 2016); *see also NHTSA Seeks Comment on Cybersecurity Best Practices for the Safety of Modern Vehicles*, NHTSA (Jan. 8, 2021) (announcing public comment on draft updating Cybersecurity Best Practices for Modern Vehicles).

154 *Connected Cars Workshop*, FED. TRADE COMM'N (Jan. 2018).

155 *Monetizing Car Data*, MCKINSEY & CO. (Sept. 2016).

156 *See* Sylvia Zhang, *Who Owns the Data Generated by Your Smart Car?*, 32 HARVARD J.L. & TECH. 299, 311–12 (2018); *Legal Issues Related to the Development of Automated, Autonomous, and Connected Cars*, *supra* note 91.

157 *See* Zhang, *supra* note 156.

158 *See* Cal. Civ. Code §§ 1798.100 *et seq.*; *see also* VA S.B. 1392 § 59.1-571 et seq.

159 *See also* Victor, *supra* note 34 (discussing how the European Union's General Data Protection Regulation mandates standard data inventory, mapping of data flows, opt-out processes, and disclosure and contract requirements).

160 *See* Cal. Civ. Code §§ 1798.100 *et seq.*; *California Consumer Privacy Act Fact Sheet*, *supra* note 34.

161 *See* Cal. Civ. Code § 1798.155(b) (version effective until Jan. 1, 2023) (providing, in part, "a *civil penalty* of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought . . . by the Attorney General."); *But see id.* at § 1798.155(a) (version operative Jan. 1, 2023) (providing, in part, the same except for an *administrative fine* and $7,500 for each intentional violation *or* "violations involving the personal information of consumers whom the business, service provider, contractor, or other person has actual knowledge are under 16 years of age.").

162 *2019 Consumer Data Privacy Legislation*, NAT'L CONF. OF STATE LEGISLATURES (Jan. 3, 2020).

163 While manufacturers and sellers do not have to comply with standards imposed by California or Europe for product sales elsewhere, courts considering common-law claims might turn to these standards to assess whether a manufacturer or seller acted reasonably.

164 *See* H.R. 8350, 116th Cong. (2020).

165 *See* Restatement (Third) of Torts: Prods. Liab. §5 (AM. L. INST. 1998).

166 *Id.* at § 5 cmt. a.

167 *Id.* at § 5 cmt. e.

168 *See, e.g.*, *Lawrence v. S. Recreations, LLC*, 304 So. 3d 128, 134 (La. Ct. App. 2020); *Carter v. Chrysler Motors Corp.*, 384 So. 2d 838, 842–43 (La. Ct. App. 1980).

169 *See Carter*, 384 So. 2d at 839–41.

170 *See id*. at 842–43.

171 *See, e.g.*, *Cybersecurity Insurance*, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY (last visited Apr. 9, 2021).

172 *See* Eric Schneider, *Insurance for Autonomous Vehicles & Self-Driving Cars*, FOUNDER SHIELD (July 23, 2019).

173 *See id.*

174 *See* Accenture & Stevens Institute of Technology, *Insuring Autonomous Vehicles an $81 Billion Opportunity Between Now and 2025*, ACCENTURE (2017).

175 *Id.*

176 *See Vehicles 4.0, supra* note 45 (outlining the federal government's coordination efforts with industry and governmental authorities in developing and implementing standards and regulatory policies); *SAE International Announces the Formation of the Cooperative Automation Driving System Committee*, SAE INT'L (Nov. 24, 2020) (announcing committee developing standards concerning the communication between autonomous vehicles and their surroundings, including pedestrians, other motorists, and infrastructure); *see also Safe Drive Initiative The Autonomous Vehicle Governance Ecosystem: Guide for Decision-Makers*, WORLD ECON. FORUM (Apr. 2021) (the white paper provides a "landscape of relevant industry alliances, consortia and other groups" and "[highlights] the activities of key standards bodies."); Laura Fraade-Blanar *et al.*, RAND CORP., *Measuring Automated Vehicle Safety: Forging a Framework* (2018) (providing a safety measurement framework for highly automated vehicles for public and private stakeholders).