JONES DAY | One Firm Worldwide℠

WHITE PAPER

November 2017

Legal Issues Related to the Development of Automated, Autonomous, and Connected Cars

As interest in autonomous vehicles accelerates, and as the related technologies evolve, the vehicles' manufacturers and their suppliers are preparing to encounter a broad range of legal issues.

This Jones Day *White Paper* provides an overview of autonomous vehicles, defines key terms, explains recent pertinent legislation, and summarizes the actions of regulatory authorities in the U.S. and other nations involved in autonomous vehicle development. Special attention is given the intellectual property, privacy and data protection, and product liability issues related to the introduction of these vehicles.

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

ADS	Automated Driving Systems
AEB	Automatic Emergency Braking System
AGL	Automotive Grade Linux
Auto-ISAC	Automotive Information Sharing and Analysis Center
AV START	The American Vision for Safer Transportation Through Advancement of Revolutionary Technologies
BSM	Basic Safety Administration
DMCA	Digital Millennium Copyright Act
DOT	Department of Transportation
DSRC	Dedicated Short-Range Communication
EDR	Electronic Data Recorder
EPC	The European Patent Convention
FCC	Federal Communications Commission
FMVSS	Federal Motor Vehicle Safety Standards
GDPR	EU's General Data Protection Regulation
HAVs	Highly Automated Vehicles
IP	Intellectual Property
NIST	National Institute of Standards and Technology
NTSB	National Transportation Safety Board
OEDR	Object and Event Detection and Response
ODD	Operational Design Domain
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
SAE	Society of Automotive Engineers International
SCMS	Security Credential Management System
SIPO	State Intellectual Property Office
V2I	Vehicle-to-Internet
V2V	Vehicle-to-Vehicle
VDA	The German Association of the Automotive Industry

I. INTRODUCTION

According to the National Highway Transportation Safety Administration ("NHTSA"), "[a]utomated vehicle technologies signal the next revolution in roadway safety. We see great potential in these technologies to save lives—more than 30,000 people die on our roads every year and we can tie 94 percent of crashes to human choice—transform personal mobility and open doors to communities that today have limited mobility options."

The anticipated societal and individual benefits from automated, autonomous, and connected vehicle technology have brought a global chorus of support, with words of caution, from governments, public interest organizations, standard-setting organizations, manufacturers, and consumers. In September 2017, the U.S. House of Representatives passed *unanimously* the "SELF-DRIVE" Act, which will allow 50,000 highly automated vehicles to take the road with an exemption from current safety standards (provided their safety is at least equal to current standards). The Senate is expected to pass a similar bill, called the "AV START Act," now under consideration. Other governments globally are also promoting the development of highly automated and connected vehicles in their countries.

As the technologies required for automated, autonomous, and connected vehicles evolve, vehicle manufacturers and their suppliers will face a panoply of new legal issues. This *White Paper* will address some of the key legal issues related to the development of those vehicles.

But first, we need some definitions. An "automated" vehicle has systems that automate certain functions, such as adaptive cruise control (which maintains a certain distance from the vehicle in front of the car) and automatic braking or, at the driver's direction, takes over driving subject to the driver retaking control if necessary. An "autonomous" vehicle drives itself in most or all conditions. This *White Paper* will refer to autonomous and automated cars together as highly automated vehicles ("HAVs"), to borrow NHTSA's terminology.

A "connected" vehicle can access the internet and is usually connected to a wireless network. It can communicate with other vehicles, traffic management infrastructure, manufacturers, and fleet operators, among others. These features allow the car to send and receive messages and data, which can be used for monitoring wear and tear of parts, navigation, collision avoidance, weather and traffic reports, entertainment, and accident and other emergency notifications.

II. EXECUTIVE SUMMARY

1. Governments around the world have concluded that HAVs will be safer, improve traffic conditions, save energy, be better for the environment, and provide mobility to disabled and senior citizens, among other benefits. They want their countries to lead the charge.

2. In the United States, the House of Representatives has passed a bill that will exempt 50,000 or more HAVs from current safety standards (as long as the technology provides a level of safety comparable to current standards) to allow them to take to the road. The legislation will also demarcate the roles of federal and state governmental agencies. It appears that the federal government will reserve to itself laws and regulations governing design, construction, and performance of HAVs. States will have authority over licensing, training, liability, insurance, and traffic safety. The Department of Transportation ("DOT") is directed to remove or update references to human drivers and occupants in the Federal Motor Vehicle Safety Standards ("FMVSS"). The Senate will soon consider a comparable bill.

3. In September 2017, NHTSA issued 12 new guidelines for automated driving systems ("ADS"). The guidance is voluntary and encourages technology development. As NHTSA explained, "regulatory efforts in this area must promote safety, remove any existing unnecessary barriers, remain technology neutral, and enable a pathway for innovation that has the potential to save lives. Any initiative in the regulatory realm will seek to remove regulatory barriers and burdens that could unnecessarily hinder the safe and efficient implementation of ADSs."[1]

4. Automated vehicles that are not fully autonomous present the "hand-off" problem: the technology itself is likely to make drivers less attentive and thus less likely to respond to a vehicle's notice of a potential problem. As a result, some automakers and Google favor proceeding directly

to autonomous cars. NHTSA's guidelines contemplate fully autonomous cars, but not in the near future.

5. NHTSA and many automakers appear committed to a standard dedicated short-range communication ("DSRC") protocol for vehicle-to-vehicle ("V2V") communications. NHTSA's proposed V2V rule is reportedly stalled.

6. NHTSA's proposed V2V communications standards leave some questions open. One is whether the focus on communications protocols will be sufficient if car manufacturers develop different hardware and software platforms. How are those cars to "cooperate" with one another? Moreover, NHTSA has not yet issued any specifications for applications.

7. HAV development has global appeal. The United Nations Economic Commission for Europe has approved amendments to the Vienna Convention on Road Traffic to allow automated driving—provided the driver can override or switch off the technologies.

8. The German government has proposed legislation that would allow automated vehicles—but not fully autonomous vehicles—on its roads.

9. Germany's Federal Ministry of Transport and Digital Infrastructure has issued the world's first ethical guidelines for partly and fully automated vehicles. The guidelines address, at a high level, decisions between human life and property damages (humans must be given priority) and the more difficult decision between one human life and another.

10. China's Ministry of Industry and Information Technology and China's Society of Automotive Engineers have issued a draft plan for HAVs. By 2030, China expects 10 percent of all cars sold to be fully autonomous. China's "Made in China 2025 Plan" targets artificial intelligence and other HAV technologies.

11. Japan and South Korea are investing large sums for HAV development.

12. A key question for companies is whether to develop the needed technologies on their own, jointly with others, or by licensing from others. How to form cooperative corporate, commercial, and supply relationships to facilitate development, sharing, and protection of proprietary technology, testing, deployment, and financing is a central issue.

13. Automakers and their technology suppliers will need to protect their intellectual property. Historically, there has been less intellectual property litigation in the automotive industry than in some other industries. As the automotive and technology industries converge, more litigation is expected.

14. Increasingly, innovations will be software, not hardware. The extent to which software innovations can be patented in the United States is uncertain. In other countries, patentability considerations are different. Companies will need an international intellectual property protection strategy. Trade secrets will also play a major role. Automakers and suppliers will face demands from China to disclose new technologies to Chinese joint venturers.

15. Much open source software will be used. Users will need to monitor their disclosure obligations under software licenses.

16. Another business question is who will own and who can use the data that HAVs and connected cars generate? Automakers will want to use the data to provide infotainment and other services and for research. In the United States, this issue likely can be addressed in purchase contracts and owners' manuals, provided full disclosure is made. The issue will be more difficult in Europe, especially if automakers want to move European consumers' data out of Europe. European regulators say that consent has to be freely given, specific, and informed, and the company must have a legitimate basis for processing the data.

17. There will be accidents and, therefore, injuries and fatalities leading to litigation. What law will apply? Some commentators favor strict liability coupled with an insurance regime. Automakers have told NHTSA that cooperative crash avoidance safety applications present an "unprecedented challenge to risk management"—in part because of the complexities added by the new technologies and in part because of concern that insurance will not be available. NHTSA has sought to minimize those concerns.

18. Some commentators predict that insurers will insure automakers, not drivers, in a strict liability regime. Germany's

new ethical guidelines take on this issue directly: "In the case of automated and connected driving systems, the accountability that previously was the sole preserve of the individual shifts from the motorist to the manufacturers and operators of the technological systems and to the bodies responsible for making infrastructure, policy and legal decisions." In the United States, Congress may leave tort liability and insurance to state laws and regulations. NHTSA has advised states to consider rules and laws allocating tort liability.

19. The application of traditional product liability law to HAVs and their software will be complicated. Plaintiffs may attempt to link software defects to hardware. Those claims often will be technically complex. Injured or dissatisfied plaintiffs may also assert failure to warn, breach of warranty, or consumer misrepresentation claims, perhaps as class actions.

20. With consumer expectations high, but knowledge and experience often low, consumer warnings, disclosures, training, and education on the proper operation, limitations, and risks of HAVs will be critically important for safety and avoiding liability.

21. As HAVs are designed, tested, and operated, manufacturers should pay close attention to their document retention policies.

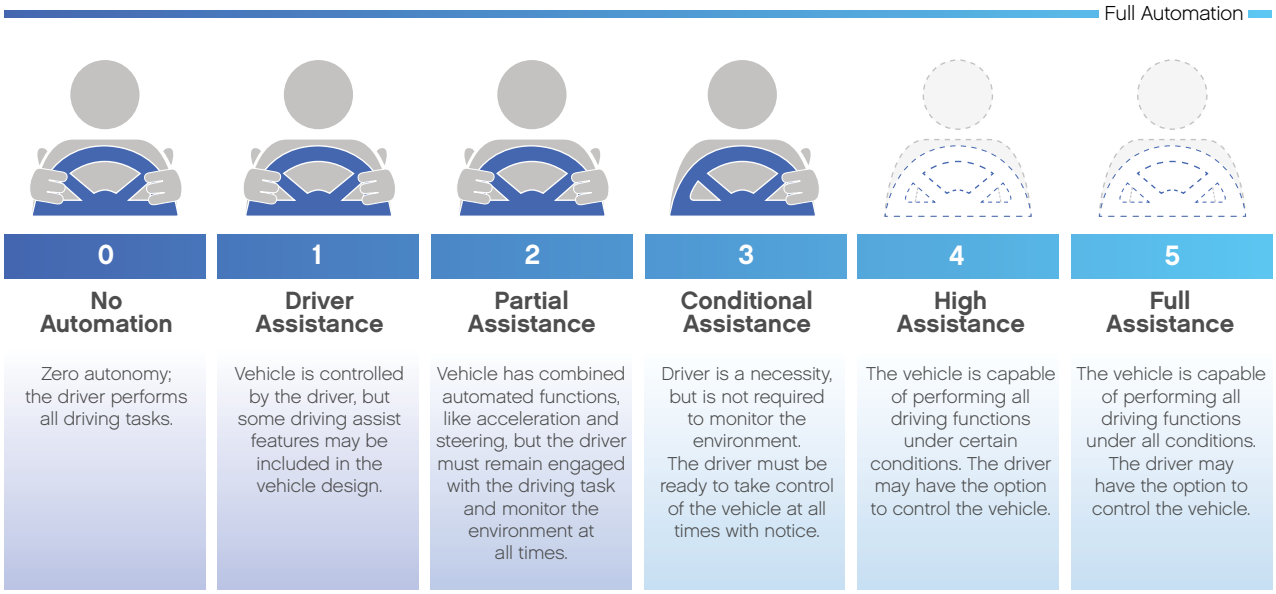
22. Contracting practices should be reviewed. For example, what indemnification, limitation of liability, and quality control provisions should be placed in supplier contracts or in contracts with fleet operators? Manufacturers, their suppliers, and their corporate customers have the opportunity to use their agreements to allocate responsibility, and to choose a preferred forum, law, and means for dispute resolution.

III. OVERVIEW OF AUTOMATED, AUTONOMOUS, AND CONNECTED CARS

A. Highly Automated and Autonomous Cars

Many cars already feature some automation, such as automated emergency braking, lane departure warning, or assisted parking, but otherwise the driver operates the car at all times. In future generations, the vehicle will take over some driver functions and ultimately drive itself. NHTSA has adopted the Society of Automotive Engineers International's ("SAE") definitions of levels of automation[2]:

SAE AUTOMATION LEVELS



Most vehicles today are at Levels 1 and 2. NHTSA has defined "highly automated vehicles" to include Levels 3, 4, and 5.[3] Tesla has achieved Level 3 automation. So has Audi, which plans to have a Level 4 vehicle on the road by 2020. With its acquisition of Mobileye, Intel says that it will begin road testing of Level 4 cars by year-end. Most major manufacturers have announced plans for introducing different levels over time.

Level 3 cars present the "hands-off" problem. Automotive engineers have not yet found a way to make a distracted driver respond to an alert and retake control of the car in a fraction of a second as required in an emergency. The danger is that technology may create new hazards by inducing drivers to pay even less attention to driving.

This is why Google and some car manufacturers are skipping Level 3 cars and developing Level 4 and 5 cars. In their view, the best way to proceed is to take the driver out of the equation. Other manufacturers will address the hands-off problem by design limitations. For example, Audi's Level 3 system for its 2018 A8 will function only at 35 mph or lower speeds.

At the 2017 Consumer Electronic Show, a Toyota representative indicated that "we're nowhere near close" to autonomous driving, which he described as SAE Level 5.[4] In addition to the need for millions more miles of on-the-road experience in unpredictable, real-world conditions, HAV development requires improvement in computational power and sensors.[5]

B. Connected Cars

Vehicle-to-vehicle ("V2V") and vehicle-to-internet ("V2I") communications will create a network of connected cars and infrastructure talking to each other. Cars will exchange their position, speed, and other information while receiving additional information from infrastructure, such as road conditions and traffic lights. Then all vehicles will react to avoid accidents and travel efficiently.[6]

Government and private research programs began at least 25 years ago. In 1999, the U.S. Federal Communications Commission ("FCC") dedicated 75 megahertz of valuable spectrum radio space for intelligent transportation systems, and a protocol named Dedicated Short Range Communication ("DSRC") was developed to support V2V and V2I communications.[7]

In 2012, the U.S. Department of Transportation funded a $31 million study called the Connected Vehicle Safety Pilot Model Deployment at the University of Michigan's Mobility Transportation Center. In 2014, NHTSA was ready to move forward with rulemaking.[8] Although NHTSA's rulemaking has stalled recently,[9] some automakers are using connected car technology for vehicle maintenance and infotainment. In 2012, Tesla began to market connected cars with technology used to access a vehicle's data and fix issues with over-the-air updates.[10] In May 2016, Ford and Microsoft announced a $253 million investment in Pivotal Software to develop predictive maintenance software.[11] Toyota is collaborating with Microsoft,[12] and General Motors is using V2V technology for Cadillac's CT6 model introduced in September 2017.

IV. LEGAL ISSUES

A. Regulation

1. U.S. Federal Government

(a) Automated and Autonomous Vehicles

(i) Legislation

On September 6, 2017, the House of Representatives unanimously passed HR 3388 titled "Safely Ensuring Lives Future Deployment and Research in Vehicle Evolution," or the "SELF-DRIVE," Act. The bill would allow as many as 50,000 HAVs to be exempted from current safety standards over two years as long as they provide safety at least equal to current standards.[13] After two years, the number of exemptions would jump to 100,000 cars. Among other provisions, not later than 30 months after the date of enactment, the Secretary of Transportation is required to (a) "issue a final rule requiring the submission of safety assessment certifications regarding how safety is being addressed," and (b) review FMVSS.[14]

Under the bill, "no State or political subdivision of a State may adopt, maintain, enforce, impose, or continue in effect any law, rule, regulation, duty, requirement, standard, or other provision having the force and effect of law related to the design, construction, mechanical systems, hardware and software systems, or communications systems of highly automated vehicles or automated driving system equipment," unless the state law "is identical to a standard presented under the

chapter." On the other hand, states may set rules for registration, licensing, liability, driving education and training, insurance, safety inspection, and traffic regulations unless the law is an unreasonable restriction on the design, construction, mechanical systems, hardware and software systems, or communications systems of HAVs.[15]

On September 28, 2017, Senator Thune, Chair of the Senate Committee on Commerce, Science, and Transportation, and other sponsors introduced "The American Vision for Safer Transportation Through Advancement of Revolutionary Technologies ("AV START") Act," S. 1885. Like the House bill, the AV START Act defines federal, state, and local roles. The federal government has exclusive authority over the design, construction, and performance of HAVs and their components. States retain traditional power over licensing, registration, insurance, law enforcement, traffic safety, franchising, and common law liability. The Secretary of Transportation is to remove, if practical, references in FMVSS to human drivers and occupants. It also provides for HAV testing, exemptions, manufacturer safety evaluation reports, manufacturer cybersecurity plans, and consumer education. The bill does not address trucks and buses.

(ii) NHTSA Policies and Guidelines

In September 2017, Transportation Secretary Elaine Chao announced the latest federal policy for ADS. It replaces the Federal Automated Vehicle Policy issued in September 2016. The Secretary's introductory message encourages "the safe deployment of automated vehicles."

The new policy has two sections: Voluntary Guidance for Automated Driving Systems and Technical Assistance to States—Best Practices for Legislatures and State Highway Safety Officials Regarding Automated Driving Systems.

The Voluntary Guidance focuses on vehicles with SAE Automation Levels 3-5. The Guidance recognizes that an ADS may have no human driver.

The Voluntary Guidance outlines 12 safety elements:

1. **System Safety**
   Design safety considerations should include design architecture, sensors, actuators, communication failure, potential software errors, reliability, potential inadequate control, undesirable control actions, potential collisions with environmental objects and other road users, potential collisions that could be caused by actions of an ADS, leaving the roadway, loss of traction or stability, and violation of traffic laws and deviations from normal (expected) driving practices.

2. **Operational Design Domain ("ODD")**
   The ODD defines where (such as roadway types and geographic areas and terrain) and when (under what conditions, such as speed, daylight, and weather limits) an ADS is designed to operate. The vehicle must also be able to move to a condition with minimal risk, such as stopping or returning control to the driver, when the ODD is exceeded.

3. **Object and Event Detection and Response ("OEDR")**
   OEDR is the detection and response by the driver or ADS of any circumstance relevant to the immediate driving task. Based on its ODD, an ADS should be able to deal with control loss; crossing-path crashes; lane change/merge; head-on and opposite-direction travel; and rear-end, road departure, and parking maneuvers.

4. **Fallback (Minimal Risk Condition)**
   An ADS should detect that it has malfunctioned or is operating outside the ODD and then notify the driver to regain control of the vehicle or to return the vehicle to a minimal risk condition independently.

5. **Validation Methods**
   Testing may include simulation, test track, and on-road testing. It should demonstrate performance in normal operations, crash avoidance, and fallback strategies.

6. **Human-Machine Interface**
   The vehicle must accurately convey information to the driver or operator regarding intentions and vehicle performance. For example, in a Level 3 vehicle, the driver must always be ready for a request to take back driving.

7. **Vehicle Cybersecurity**
   Manufacturers and suppliers should minimize safety risks from hacking and should follow industry best practices, including response plans and reporting of incidents.

8. **Crashworthiness**
   Occupant protection must continue to meet performance standards, including for new seating and interior designs.

9. **Post-Crash ADS Behavior**
   An ADS should return the vehicle to a safe state and location after a crash.

10. **Data Recording**
    To promote continual learning, entities engaging in HAV testing or deployment should collect crash data. Crash event data recorders are recommended to collect and store accident data, including ADS status and driver role.

11. **Consumer Education and Training**
    Education and training of manufacturer representatives, dealers, distributors, and consumers is imperative for safety. Education and training programs should address the anticipated differences in the use and operation of ADSs from conventional vehicles, and the need for drivers to be prepared to take back control in an instant.

12. **Federal, State, and Local Laws**
    Entities developing ADSs are encouraged, but not required, to publish Voluntary Safety Self-Assessments. In addition to complying with traffic laws, an ADS must also be able to violate a traffic law temporarily when safety demands, such as crossing a double line to avoid a disabled vehicle or a bicycle. An ADS must also be updated as traffic laws change.

(b) Connected Vehicles

To facilitate safety and development of fully autonomous vehicles, NHTSA issued a Notice of Proposed Rulemaking in December 2016 requiring V2V technology in all cars and light trucks.[16] The proposal contains V2V communication performance requirements for the use of on-board DSRC devices, which will transmit Basic Safety Administration ("BSM") messages about a vehicle's speed, heading, brake status, and other information to nearby vehicles and receive the same information from them. Other technologies are permitted if compatible with DSRC.

For security reasons, vehicles should contain "firewalls" between the V2V modules and other vehicle modules connected to the data system.[17] Finally, V2V devices should allow periodic software updates.[18]

One obstacle to NHTSA's V2V rules is its tussle with the FCC over control of the spectrum radio space the FCC previously set aside for intelligent transportation communications but now may use for superfast Wi-Fi service. In addition, the FCC has received a petition to put off using V2V in the contested spectrum until cybersecurity standards are developed.[19]

Engineers have been working on specifications for DSRC devices for over a decade.[20] Yet some automakers, wireless carriers, and chip makers believe that cellular systems will better handle V2V communications on future 5G networks.[21] Ultimately, some combination of DSRC and 5G may be used. 5G is not expected until 2020. DSRC will likely come first.

2. United States

NHTSA's 2017 Guidance recommends best practices for state legislatures and highway safety officials. However, NHTSA first cautions the states "to allow DOT alone to regulate the safety design and performance aspects of ADS technology."

NHTSA defines its responsibilities and then the states' role[22]:

NHTSA'S RESPONSIBILITIES	STATES' RESPONSIBILITIES
• Setting Federal Motor Vehicle Safety Standards (FMVSSs) for new motor vehicles and motor vehicle equipment (with which manufacturers must certify compliance before they sell their vehicle)[33] • Enforcing compliance with FMVSSs • Investigating and managing the recall and remedy of non-compliances and safety-related motor vehicle defects nationwide • Communicating with and educating the public about motor vehicle safety issues	• Licensing human drivers and registering motor vehicles in their jurisdictions • Enacting and enforcing traffic laws and regulations • Conducting safety inspections, where states choose to do so • Regulating motor vehicle insurance and liability

NHTSA recommends several "Best Practices" for state legislatures:

- Provide a "technology-neutral" environment.
- Provide licensing and registration procedures, including insurance.
- Provide reporting and communications methods for public safety officials.
- Review traffic laws that may serve as barriers to ADS operation.

At least 41 states and the District of Columbia have considered legislation related to HAVs. Twenty-one states have adopted such legislation. The governors of four other states have issued executive orders. The National Conference of State Legislatures has a database of state HAV legislation.[23] Six states in particular tout their laws as facilitating the testing and deployment of HAVs: Arizona, California, Michigan, Nevada, Pennsylvania, and Texas.

3. International Regulation

The 1968 Vienna Convention on Road Traffic is an accord among 74 participating members of the United Nations (including Brazil, China, Mexico, and most European countries, but not the United States). One fundamental principle of the Convention has been that a driver is always fully in control of and responsible for the behavior of the car in traffic.

In March 2016, the United Nations Economic Commission for Europe ("UNECE") amended the Vienna Convention on Road Traffic to allow automated vehicles, provided that the technologies conform with U.N. vehicle regulations and the driver can override or switch off the technology.[24]

Germany. After the Vienna Convention was updated, the German government prepared a "Strategy for Automated and Connected Driving." In May 2017, the government passed a bill to allow the use of automated vehicles, provided that the driver is able to regain control without undue delay. The legislation does not provide for autonomous vehicles.

This legislation does not change general liability under German law. Both the driver and "owner" remain liable even if the vehicle is in automated driving mode, but the driver may avoid liability if he or she lawfully used the automated driving mode.

Also in June 2017, Germany's Federal Ministry of Transport and Digital Infrastructure issued the world's first ethical guidelines for partly and fully automated vehicles. Key guidelines, in brief, include:

- The protection of individuals takes precedence.
- The public sector is responsible for guaranteeing the safety of the automated and connected systems.
- Automated and connected technology should prevent accidents wherever possible.
- Genuine dilemma decisions, such as a decision between one human life and another, depend on the specific situation and "unpredictable" behavior; therefore, no ethical rule can be set or programmed. Technological systems cannot

replace or anticipate the decision of a responsible driver with the moral capacity to make correct judgments.
- In the event of unavoidable accidents, any distinction based on personal features (age, gender, physical or mental status) is prohibited.
- Accountability shifts from the motorist to the manufacturers and operators of the automated and connected driving systems, and to the entities responsible for infrastructure, policy, and legal decisions.
- Liability for damage is governed by the same rules as other product liability.
- Vehicle owners and users decide the use of their vehicle data.
- Self-learning systems are allowed if, and to the extent that, they improve safety.

The German federal government plans to shape the guidelines' principles into law.

The United Kingdom. In 2017, a proposed Vehicle Technology and Aviation Bill set forth how liability for accidents involving automated vehicles should be apportioned, including whether vehicle owners have made unauthorized alterations to or failed to accept updates to the vehicles' software. Insurers would have default liability for death, personal injury, or property damages resulting from accidents caused by HAVs while in self-driving mode, but insurers may attempt to recover their payments from vehicle manufacturers. Insurers would not have any liability when the accident involving an HAV was caused by the owner's "negligence in allowing the vehicle to drive itself when it was not appropriate to do so."[25]

China. China also is accelerating its development of HAV and connected car technology. In 2015, the State Council, the chief administrative authority of the People's Republic of China, announced a new 10-year plan for China—titled "Made in China 2025"—with the goal of making the country an innovation hub in numerous industries, including the automotive industry.

In December 2016, the Ministry and China's Society of Automotive Engineers issued a 450-page draft plan for autonomous vehicles titled "The Technology Road Map for Energy Saving and New Energy Vehicles." "'Partially autonomous' cars (think driver assist) are to account for 50 percent of sales by 2020. 'Highly automated' cars (not quite fully autonomous) will take 15 percent of sales in 2025. By 2030, fully autonomous vehicles are expected to feature in 10 percent of sales."[26]

Two of China's largest technology companies are pushing to develop platforms for connected cars: Baidu and Alibaba.[27] Other partnerships, some with U.S. and European companies, illustrate China's interest in and market for connected cars. The 2016 Plan did not establish any standard for cars to communicate with each other or with infrastructure. As it did with telecommunications, China may select a different communications standard to favor its companies.[28]

China has limited the amount of mapping that foreign companies can perform in China. Foreign companies must work with a Chinese company licensed for surveying and mapping.[29] Foreign companies may also face challenges to gaining approval to test HAVs in China.[30]

Baidu plans to have a fully automated platform ready for commercial application by 2019 and production by 2021.[31] Another potentially important development is that Baidu has open-sourced its software.[32] Ironically, to accomplish its goals, Baidu has formed a self-driving research team in Silicon Valley.

Some start-up Chinese automakers are also coming to the United States. NIO, the Chinese-backed start-up formerly known as NextEV, plans to bring a Level 4 autonomous electric car to the United States by 2020.[33] NIO will partner with Israel-based Mobileye, which develops camera-based systems to help drivers avoid collisions, Nvidia, and NXP Semiconductors, the world's largest chip supplier to the automotive industry. Nvidia has developed an artificial intelligence computing platform that Audi and others are using to deploy autonomous vehicles. In October 2016, the California Department of Motor Vehicles issued NIO an autonomous vehicle testing permit.

Japan. The Japanese government is a proponent of automated and connected cars. Its goal is for Japanese automakers to introduce autonomous acceleration, steering, and braking in time for the Tokyo Summer Olympic Games in 2020.[34]

Car manufacturers soon will be able to test autonomous cars on Japan's roads. To get a testing license, the police must examine autonomous cars, and they must take a test drive.

The person in control of the vehicle does not need to sit inside the car under Japanese rules.

South Korea. The South Korean Ministry of Land, Infrastructure, and Transport encourages the development of HAV technologies. Also, private Korean companies are promoting automated driving. South Korea is building a large test facility for HAVs.

Samsung, a large smart phone manufacturer, recently received approval to test self-driving cars on public roads. Hyundai, South Korea's top-selling automaker, has also been pitching its self-driving, all-electric Ioniq as an affordable driverless car.

B. Intellectual Property[35]

Companies developing HAV technology will need to protect their intellectual property ("IP") rights through patents or the confidentiality of trade secrets. They will also need to protect themselves against IP claims by others. IP due diligence will have an increasingly important role with regard to joint development agreements, mergers, and acquisitions. Litigation over technology rights is also more likely to occur.

Some of the key technologies relevant to the development of HAVs and connected cars include:

- Automated automotive technologies, including automatic parking and braking systems and automotive engine control circuitry.
- Collision-avoidance technologies, including blind spot detection and lane control systems.
- Digital cameras, including the capture of analog images, conversion to digital signals, processing of those signals for display on a screen, and image processing algorithms for object detection.
- LiDAR and radar.
- Telecommunications, including DSRC technology for V2V communications and 5G.
- Artificial intelligence and machine learning, including cybersecurity for vehicles and object detection and characterization in digital images.
- Sensors and mesh networking technology, including distributed sensor networks and weight-sensing technologies.
- Diagnostic trouble code, data analytics, and telematics.

Thousands of patents have already been issued to auto manufacturers, technology companies, and auto suppliers for technology related to HAVs and connected cars.

1. Patents

(a) Are Artificial Intelligence and Machine Learning Innovations Patent Eligible?

The number of artificial intelligence patents issued in the United States increased significantly in 2016. Some observers are surprised given the U.S. Supreme Court's decision in *Alice Corp. Pty. Ltd. v. CLS Bank International*, 134 S.Ct. 2347 (2014), which established standards for patents that are difficult for some software innovations to meet.

(i) Validity of Software Patents in the United States

The U.S. Supreme Court has long held that "[l]aws of nature, natural phenomena, and abstract ideas are not patentable."[36] "[M]onopolization of those tools through the grant of a patent might tend to impede innovation more than it would tend to promote it."[37]

The Supreme Court has set forth a two-part framework for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts:

> First, we determine whether the claims at issue are directed to one of those patent ineligible concepts. If so, we ask, [w]hat else is there in the claims before us?[38]

The second step is a search for an "inventive concept," meaning an element or combination of elements that is "sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself."[39]

In *Alice,* the Supreme Court found the claims were directed to an abstract idea, because the use of a third party to mitigate risk in banking transactions was "a fundamental economic practice long prevalent in our system of commerce."[40] The Court then found that the method claims, which merely required generic computer implementation, failed to transform

the abstract idea into a patent-eligible invention.[41] An improvement to the functioning of a computer or a technological process is required for patent eligibility.[42]

After *Alice*, federal courts found that many claimed software or computer-implemented inventions were not patent eligible. One example was a Mercedes-Benz patent premised on using one or more "expert systems" to screen equipment and vehicle operators for medical or emotional impairment or intoxication.[43] The Federal Circuit affirmed the invalidity of the patent, reasoning that, "in the absence of any details about how the 'expert system' works, the claims at issue are drawn to a patent-ineligible abstract idea…."[44] The court also found no support for an inventive concept: "But markedly absent from the '932 patent is any explanation of how the methods at issue can be embedded into these existing modules."[45]

More recently, claims directed to using artificial intelligence to analyze data through predictive analytics were held ineligible for patent protection.[46] "[J]ust because a computer can make calculations more quickly than a human does, does not render a method patent eligible."[47] Moreover, the "claims do not describe specific system architecture, and references to generic 'modules' do not provide any further specificity."[48]

One Federal Circuit opinion upholding a patent directed to a "self-referential" database has provided software patent owners some hope.[49] The Federal Circuit concluded that specific functional improvements meant the claims were not an abstract idea.[50] The fact that the invention ran on a general purpose computer did not doom the claims. The Court of Appeals explained:

> We thus see no reason to conclude that all claims directed to improvements in computer-related technology, including those directed to software, are abstract and necessarily analyzed at the second step of *Alice,* nor do we believe that *Alice* so directs. Therefore, we find it relevant to ask whether the claims are directed to an improvement to computer functionality versus being directed to an abstract idea, even at the first step of the *Alic*e analysis.[51]

Two conclusions emerge from the case law:

- Software patents must carefully claim and show how the invention improves the operation of a computer or advances a technology; and
- The "expert system" must be programmed to perform functions in a particular way, and how it decides upon a course of action must be disclosed.

(ii) Validity of Software Patents in Other Countries

Europe. The European Patent Convention does not allow patents for discoveries, scientific theories, and mathematical methods;[52] schemes, rules, and methods for performing mental acts, playing games, or doing business; and programs for computers, "as such."[53] This exclusion for computer programs "as such" can be avoided as long as some other technical subject matter is defined in the claim.[54] In practice, features incorporating technical computer implementation of software, such as an AI-equipped surgical robot system, will pass the test.

Japan. Japan has no subject matter eligibility exclusion directed to software. A software invention that defines tangible components of computer implementation qualifies for patent protection.[55] A mathematical algorithm per se is not patent eligible in Japan but should be eligible if defined with reference to implementation by computer hardware.

China. In China, computer programs per se are considered rules and methods for mental activities and thus are not eligible for patent protection under Article 25 of Chinese Patent Law. An invention relating to computer programs is eligible for patent protection only if it constitutes a technical solution.[56] Defining a software invention in terms of computer implementation is typically sufficient to satisfy patent eligibility. Accordingly, computer-implemented AI inventions are likely to be patent eligible. AI patents in China have grown rapidly.[57]

(b) Standard-Setting Bodies and Patent Pools

Some commentators have predicted that HAV technologies could become subject to the patent licensing policies of industry standard-setting bodies.[58] At IAM's 2017 "IP in the Automotive Industry" Conference, in-house counsel for several major automakers reported requests to join patent pools. Patent pools raise numerous issues, including:

- Are all major players in a given technology willing to participate?

- What is the required scope of contribution of patents, and is that consistent with the company's strategy?
- What is the cost?
- How will the pool be administered?
- Are there any antitrust issues?

2. Trade Secrets

Trade secret claims may arise when a car manufacturer or supplier hires a competitor's employees.[59] The most highly publicized example is the lawsuit that Waymo LLC—the autonomous car business Google has spun off—filed against Uber Technologies, Inc., Ottomotto LLC, and Otto Trucking LLC. Waymo accuses defendants of stealing its trade secrets related to LiDAR by hiring a senior engineer away from Waymo.[60] The engineer downloaded more than 14,000 confidential files immediately before departing Waymo. Uber is now allegedly using the LiDAR system that Waymo developed. This case highlights some of the issues that can arise in a trade secret suit.

Other lessons for potential plaintiffs and defendants in trade secret disputes include:

Potential plaintiffs:

- On important projects, consider preparing lists of trade secrets and having key employees sign them.
- Have good off-boarding procedures, such as having employees sign statements that they have not taken any confidential information.
- To obtain expedited discovery, temporary restraining orders, and preliminary injunctions, consider filing in state court.
- When describing the trade secrets in issue, make them specific. Do not make overly broad claims.
- Do not rush into injunctive proceedings and trials unless you have evidence of defendants' use.
- Consider carefully whether to sue individuals.

Potential defendants:

- Emphasize IP due diligence during acquisitions. Get representations and warranties by sellers.
- Have good on-boarding procedures for key technical employees. Have them sign representations that they are not bringing and will not use prior employers' IP.
- In litigation, if applicable law does not require early identification of trade secrets (as does California law), push for an early statement and discovery of trade secrets.
- Pick fights regarding discovery requests carefully, especially when the plaintiff has evidence someone took its trade secrets. Perceived discovery misconduct can affect resolution of the merits, as can overly broad assertions of privilege.
- Evaluate carefully whether key employees involved—especially if new—should have their own counsel.
- Take into consideration possible criminal proceedings.

3. Patent Protection v. Trade Secret Protection

Companies have long debated whether to patent their innovations or rely on trade secret law to protect them. There are many considerations.

Factors favoring patents:

- Patents are presumed to be valid.
- Patents do not require elaborate confidentiality precautions.
- Patents protect innovations against reverse engineering and even independent development.
- Patents put competitors on notice.
- Patents are more commonly licensed and thus monetized.
- Patents are preferred by providers of funding.

Factors favoring trade secrets:

- There is no subject matter limitation.
- Confidentiality protections can be established much faster than a patent application can be prosecuted.
- It is less expensive to establish and maintain trade secrets.
- Theoretically, trade secrets can last forever.
- Trade secrets are more flexible in litigation, because they can be defined in litigation, and misappropriation can be proved by access, substantial similarity, and circumstantial evidence.
- Trade secrets do not give road maps to competitors.

Of course, the debate is only warranted if an innovation is patentable. Even U.S. decisions allowing software innovations to be patent eligible have impacted the cost-benefit analysis of seeking patent protection because they require much greater disclosure of how the software improves computers or advances a given technology.

4. Copyrights

(a) Open-Source Software

Some automakers are using open-source software, principally for infotainment. In early 2009, BMW, PSA Peugeot Citroen, and GM and suppliers Delphi, Magneti-Marelli and Visteon, and Intel and Wind River announced the formation of the GENIVI® Alliance. Today, more than 180 members are collaborating on in-vehicle infotainment software based on the GENIVI Linux platform.

On May 31, 2017, Toyota announced that its Camry infotainment system will run in the United States on a Linux-based open-source technology platform. Toyota has worked with 10 global automakers—including Mazda, Suzuki, and Daimler—to develop this Automotive Grade Linux ("AGL") system software.[61]

Most automakers and developers of HAV technology have been reluctant to share their proprietary automated and autonomous vehicle technology. Yet, on April 19, 2017, Baidu—China's largest search engine company and a developer of artificial intelligence—revealed its "Apollo" project for autonomous driving. Baidu plans to open-source its autonomous driving technology in steps: (i) in July 2017, it would share its technology for "restricted environment" driving; (ii) by year-end, it would share its technology for autonomous driving in simple urban road conditions; and (iii) by 2020, it would make available "fully autonomous driving capabilities on highways and open city road."[62] Baidu has not said how it will share its technology, only that it will "open source code."[63] Moreover, Baidu said developers will have access to driving simulation tools and services vital for training artificial intelligence systems for autonomous driving.[64]

Microsoft will also make its Ariel Informatics and Robotics Platform[65] available on an open-source basis.[66] This simulation software will allow designers and developers to test autonomous navigation software in realistic virtual environments.

While open-source software provides source code, it can impose unanticipated development, testing, debugging, implementation, administration, and support costs. There is likely no manual. Moreover, while there is usually no license fee, there is a license, and the terms can be onerous to administer. Open-source software licenses require procedures for notice of proposed use of open-source software, approval of such use, and assurance of compliance with licenses. Failure to comply with open-source licenses can lead to a lawsuit by the licensor for copyright infringement[67] and breach of contract.[68]

(b) Other Copyright Issues

Invoking the Digital Millennium Copyright Act ("DMCA"), the Alliance for Automobile Manufacturers and two manufacturers have tried to limit or prevent users of vehicles from accessing or making alterations to computer programs in vehicles for purposes of personalization or diagnostics and repair. The Librarian of Congress, however, has exempted from the DMCA the acts of accessing computer programs for purposes of diagnosis, repair, and modification of vehicles.[69] The exemption excludes electronic control units that are chiefly designed to operate vehicle entertainment and telematics systems.[70]

C. Privacy and Data Protection

HAV and connected cars require the collection, transmittal, and use of data. The data can include information about the exact location of vehicles as well as how and where drivers operate their cars. This data collection raises important privacy and data protection issues.

1. United States

(a) Self-Regulation

The Alliance of Automobile Manufacturers and the Association of Global Automakers published "Consumer Privacy Protection Principles for Vehicle Technologies and Services" in November 2014.[71] Participating members commit to seven principles:

- Transparency, including notice about their collection, use, and sharing of covered information.
- Choice for owners and registered users.
- Respect for context in which data were originally collected.
- Data minimization, de-identification, and retention only as needed for legitimate business purposes.
- Data security against unauthorized use or access.
- Integrity and owner access to maintain the accuracy of covered and personal subscription information.
- Accountability of members.

As of January 2016, all participating members became accountable to the Federal Trade Commission and to state attorneys general for implementation of these principles.

In 2015, the Alliance of Automobile Manufacturers and the Association of Global Automakers established the Automotive Information Sharing and Analysis Center to share intelligence about vehicle cybersecurity threats. Early in 2016, these bodies published a Cybersecurity Best Practices Framework.[72]

(b) New 2017 Federal Policies

NHTSA's 2017 guidelines discuss vehicle cybersecurity in general. They encourage manufacturers "to consider and incorporate voluntary guidance, best practices, and design principles published by National Institute of Standards and Technology (NIST), NHTSA, SAE International, the Alliance of Automobile Manufacturers, the Association of Global Automakers, the Automotive Information Sharing and Analysis Center (Auto-ISAC), and other relevant organizations, as appropriate."[73] Manufacturers "are encouraged to report to the Auto-ISAC all discovered incidents, exploits, threats and vulnerabilities from internal testing, consumer reporting, or external security research…."[74] Incident response plans and an industry coordinated disclosure policy are suggested. [75]

NHTSA has also issued proposed guidance titled "Cybersecurity Best Practices for Modern Vehicles." The guidance includes a list of "fundamental vehicle cybersecurity protections," such as the control of keys and passwords, and control of access for vehicle maintenance diagnostics.

(c) NHTSA V2V Privacy Safeguards

According to NHTSA, privacy and security are fundamental to the design of DSRC systems. DSRC communications for V2V are designed not to collect or transmit Personally Identifiable Information ("PII"), as the FCC has proposed to define that term.[76] Moreover, a Public Key Infrastructure ("PKI")-based security system, known as a Security Credential Management System ("SCMS"), has been designed to protect DSRC security. NHTSA V2V regulation plans to require the use of this system.[77]

A fundamental regulatory issue is: Who owns the data? Under U.S. federal law, drivers own data stored in event data recorders, and police and insurers need drivers' consent or a court order to get those data. But no law specifically addresses ownership of data collected by automakers through vehicle internet connections. Thus, contracts and owner's manuals may be able to address this issue.

Another question is: To what extent is data collected from a vehicle's "personal data" attributable to a specific individual and, therefore, subject to the FTC's Fair Information Practice Principles? Assuming that some data collected from intelligent vehicles are "personal data," numerous issues can arise, such as processing and notice, consent, choice, access by third parties, and security.

NHTSA did not resolve the data ownership issue in its proposed rule requiring V2V technology:

> NHTSA feels strongly that in the context of a V2V system based on broadcast messages, the critical consumer privacy issue is not that of data ownership, but that of data access and use—ensuring that the consumer has clear, understandable and transparent notice of the makeup of the V2V message broadcast by mandated V2V equipment, who may access V2V messages emanating from a consumer's motor vehicle, and how the data in V2V messages may be collected and used. For this reason, NHTSA proposes that motor vehicle manufacturers, at a minimum, include the following standard V2V Privacy Statement in all owner's manuals (regardless of media) and on a publicly-accessible web location that current and future owners may search by make/model/year to obtain the data access and privacy policies applicable to their motor vehicle, including those specifically addressing V2V data and functions.[78]

2. International Conference of Data Protection and Privacy Commissioners

At the 39th International Conference of Data Protection and Privacy Commissioners in Hong Kong on September 25-29, 2017, data privacy and security guidance on the development of automated and connected car technologies was approved.[79] The Commissioners recommended that vehicle manufacturers and others take several steps:

- Use anonymization measures to "minimize the amount of personal data or use pseudonymization when the former is not feasible";

- Minimize collection and retention of personal data;
- Implement easy-to-use privacy controls for vehicle users, enabling them to grant or withhold access to different data categories, where appropriate;
- Implement secure data storage technologies;
- Develop and implement technologies to prevent unauthorized access to and interception of collected personal data;
- Provide safeguards against unlawful tracking of drivers, and limit the possibility of illegitimate vehicle tracking and driver identification;
- Have an independent third party assess potential discriminatory automated decisions arising from self-learning algorithms; and
- Assess the impact of new, innovative, or risky data technologies.

The U.S. Federal Trade Commission abstained—leaving open whether the resolution applies in the United States.

3. Europe

(a) Self-Regulation

As an example of self-regulation in the European Union, the German Association of the Automotive Industry ("VDA") published Data Protection Principles for Connected Vehicles in November 2014.[80] VDA members allow customers to determine the processing and use of personal data. Through contractual provisions, consents, optional features, and choices, customers can activate or deactivate services, unless the processing is regulated by law.

(b) Current EU Privacy Law and HAV and Connected Cars

When applicable, EU data protection laws require any person who wishes to collect and process identifying personal data to inform the individual (defined under the law as "data subject") [81] of its identity, the fact that it is going to process the data, the reasons for the processing, and any other information to ensure processing is "fair." There must be a legitimate purpose for processing. In certain cases, the data subject's consent will be necessary; in other cases, it will not—for example, if data are necessary to perform a contract, processing is in the legitimate interests of the controller or other person, or if a legal obligation requires processing.[82] The consent has to be freely given, specific, and informed. These same principles may apply to personal data generated by an HAV or connected car.

The Article 29 Working Party has addressed the rules for processing data from mobile smart devices.[83] The Article 29 Working Party requires the informed consent of users to process the location of, as well as to supply value-added services to, users.[84] Its opinion could serve as a basis for HAV and connected cars.

EU privacy laws require security measures to protect personal data. Under EU law, the obligation to protect the data may become the responsibility of the car manufacturer, the manufacturers of the digital devices and software, or perhaps all.

On May 25, 2018, the European Union's General Data Protection Regulation ("GDPR") takes effect.[85] When a breach of security exposes personal data, entities must inform the local Data Protection Authority where feasible within 72 hours of awareness of the breach and, in some instances, notify the data subjects.[86] The GDPR will increase the maximum penalty for breach to the greater of €20 million or four percent of global turnover.

(c) The UK Government's New Cybersecurity Guidance for Automated and Connected Cars

On August 6, 2017, the UK government released "The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles."[87] It prescribes minimum, nonbinding cybersecurity protections for connected and HAV vehicles.

D. Product Liability Issues

1. General Considerations for HAVs[88]

A half century ago, the auto industry was evolving from lap belts into new technologies of passive restraints. Several options were available, depending on technical feasibility, market acceptance, field performance, cost, and regulation. Manufacturers faced nationwide lawsuits for not using available technology, yet also faced liability for technology that consumers could defeat, that did not meet consumer expectations in every accident scenario, or that introduced risk in some situations. A combination of favorable federal regulation with preemptive effect, public safety campaigns, sound engineering principles, ample testing, warnings and instructions in

product manuals, and cautious introduction of new technology helped to mitigate liability and to allow the technology to continue to improve.

Product liability law provides remedies for personal injury or property damage against manufacturers of a defective product under the tort doctrines of strict liability, negligence, and misrepresentation. Also, contract law provides remedies for breaches of contract, promises made in advertising, or express and implied warranties pertaining to product quality or features.

Product liability will need to evolve to the new world of HAVs. The interaction of driver, vehicle, and other drivers and vehicles will become more technically complex with automated and connected cars. If, for example, a manufacturer designs and sells a vehicle with Level 3 automation and an accident occurs, manufacturers may face a design defect, failure to warn, or misrepresentation claim. The plaintiff may argue that the vehicle should have been designed to provide more advance warning to allow the driver to assume control, or the car should have been designed to avoid the accident, or the car did not live up to the manufacturer's promise that the car was safe, able to drive itself, and able to avoid accidents.

Component and software suppliers are also at risk, and quality control over supply chains may become more complicated. New product liability rules for software may develop. Allocating responsibility for damages will be difficult because of the complex hardware and software, along with a diverse spectrum of automated functions and novel vehicle designs.

Liability in accidents involving fully autonomous cars is uncertain, too. Occupants may not face traditional driver liability, but they may face liability as an "operator" under state law. Insurance rules and state regulation may vary across states, affecting state tort law liability.[89] Allocation of responsibility may also be resolved by contract among operators, suppliers, and manufacturers.[90]

There have been few product liability claims to date. One accident has been closely followed. On May 7, 2016, an owner of a 2015 Tesla Model S was killed while the car was using the Autopilot feature. His car crashed into a tractor-trailer that crossed the road in front of his car. The automatic emergency braking system ("AEB") did not provide any warning. Neither Autopilot nor the driver applied the car's brakes.[91]

NHTSA's initial investigation did not identify any defects in the Autopilot or AEB systems.[92] But on September 12, 2017, the National Transportation Safety Board ("NTSB") issued new findings. The NTSB indicated that the crash was probably caused by the truck driver's failure to yield the right of way and the car driver's inattention due to over-reliance on vehicle automation. The NTSB determined that the vehicle design permitted the driver's over-reliance on the automation, because it allowed prolonged driver disengagement and use inconsistent with manufacturer guidance and warnings. According to the NTSB, "[s]ystem safeguards, that should have prevented the Tesla's driver from using the car's automation system on certain roadways, were lacking and the combined effects of human error and the lack of sufficient system safeguards resulted in a fatal collision that should not have happened."[93]

NTSB's safety recommendations address the need to capture event data on new vehicles equipped with automated vehicle control systems, system safeguards to restrict the use of automated control systems to their design conditions, and new applications to sense a driver's inattention and send an alert.

NHTSA has also cautioned automakers not to give consumers the impression they can let their cars drive themselves. NHTSA has sought to reinforce a manufacturer's duty to warn and train consumers about the safe operation and the limitations of HAVs and connected vehicles.[94] Watch for whether courts or regulators require real-time warnings and instructions, quickly understandable for immediate action.

In some cases, an obligation to provide additional warnings to HAV users may arise after sale when a manufacturer discovers new risks.[95] Some manufacturers of HAVs and connected cars may also be required under post-sale notification regulations to provide upgrades for software defects.

2. Negligence

Negligence is "conduct which falls below the standard established by law for the protection of others against unreasonable risk of harm."[96] Judges and juries will be asked to answer questions such as: Should a human "driver" be held liable for negligence if design, marketing, and warning information does not require attentiveness? Is driver inattention a foreseeable misuse making the manufacturer or software supplier liable under a strict liability theory? Was the driver, even if warned,

capable of avoiding the accident given the short amount of time to react and the stress of the situation?[97]

Government policies and regulation as well as insurance rules may also affect the analysis of duty and liability. Of course, many of the complicated liability issues may be reduced once vehicles are fully autonomous.

3. Misrepresentation

Manufacturers' disclosures to consumers regarding the capabilities and risks of HAV and connected car technologies should be carefully prepared. In the event of an accident or even consumer dissatisfaction, plaintiffs may assert either a misstatement or material omission. In light of federal and state consumer protection laws, plaintiffs' attorneys can be expected to scrutinize manufacturer disclosures, manuals, training materials, and advertising word by word. For example, an HAV manufacturer may find itself sued for misrepresentation if it stated that the driver would only "very rarely" be required to take control if in fact the vehicle alerts the driver to take control every few minutes.

Can a manufacturer, seller, or lessor of Level 3–4 HAVs tout the benefits of reading email, getting work done, or watching movies? (In the 2016 fatal crash involving Tesla's Autopilot, the driver was reportedly watching a Harry Potter movie.) What evidentiary support must manufacturers compile to support claims that their automation is "safe" or "safer"? Expect litigation over these issues based on traditional misrepresentation and consumer fraud.

4. Breach of Warranty

An express warranty may be created through promises made by a seller to a buyer of goods.[98] HAV manufacturers will likely provide buyers with contractual limited warranties and disclaim all other warranties. But, the HAV manufacturer or component supplier may be found to have provided express warranties or to have made representations through its advertising or sales pitch. In addition, unless there is an explicit disclaimer or exclusion (e.g., sold "as is"), there may be an implied warranty that the HAVs are "merchantable." There is no meaningful experience yet on how the courts or consumer protection agencies will interpret the scope and effect of those implied warranties and disclaimer, or any representations made, for HAVs or connected cars.

5. Potential Defenses to Product Liability Actions

The defenses typically available in a product liability action include contributory negligence and comparative fault, misuse, assumption of risk, and state of the art.[99] The key issue is whether the driver or another person should have taken some step to prevent or minimize the accident.[100]

The unforeseeable misuse[101] defense may turn on violation of a government regulation, disregard of explicit training and warnings, unauthorized modification of the HAV causing the technology to malfunction, or failure to accept an update.

An assumption of risk defense reduces or eliminates liability where the plaintiff understood and voluntarily accepted the product's risk.[102] Thus, one issue for litigation may be the extent to which the manufacturer has explained the potential risks, or the risks are otherwise known or obvious.[103]

A state of the art defense focuses on the feasibility of alternate designs at the time the product was designed and sold. It precludes liability where a manufacturer's ability to address a risk was limited by the available technology or by market or financial constraints.[104]

6. Insurance

(a) General Considerations[105]

HAVs may lead to a shift from driver responsibility toward increased responsibility of, among others, manufacturers or suppliers, which may then require additional insurance. Irrespective of whether this shift happens, basic risk pooling principles suggest that insurers will treat product liability insurance separately for HAVs. Standard coverage forms might also respond.

Manufacturers, parts suppliers, delivery services, fleet operators, and individuals will need to consider how their current insurance might cover (or not) losses that could result from their use of HAVs. Some of the important insurance issues (drawn from existing product liability and recall insurance) include:

- What are your disclosure and notice rights and obligations, particularly as to pre-loss information?
- Can you "batch" or "integrate" multiple individual occurrences to treat them as a single occurrence and, therefore, subject to a single self-insured retention?

- How does your insurance treat losses for products sold after a batch or integrated occurrence is notified, or losses that arise after a risk of loss is known?
- How does your insurance address the "sistership" situation, in which an alleged defect in one unit raises concern with a family of units? How does your insurance define a "recall," do you have recall coverage, and if so, for what territory?
- How will your insurance respond to a "primary" recall (i.e., one you initiate for your own product) versus a "secondary" recall (i.e., one initiated by a third party, such as the seller of a product containing a component from your company)?
- How will your insurance react to a governmental order requiring a recall, and does your insurance provide a defense against allegedly unlawful or inappropriate recall orders?
- Do your supply agreements arrange rights, responsibilities, and indemnities to optimize the potential for coverage, such as by way of additional insured status?
- Does your insurance cover consequential losses, such as business interruption?
- How does your insurance treat civil penalties or punitive damages?
- How would your cyber insurance (if any) respond to a potential claim, and should you have such insurance?

HAVs may also create new, "just-in-time" insurance for renters or users of ride-sharing or delivery services, as well as real-time risk calculations.

(b) NHTSA's Recommendation to States Regarding Liability and Insurance Issues

NHTSA's 2017 voluntary guidelines advise the states on liability and insurance:

a. Begin to consider how to allocate liability among ADS owners, operators, passengers, manufacturers, and other entities when a crash occurs.
b. For insurance purposes, determine who (owner, operator, passenger, manufacturer, other entity, etc.) must carry motor vehicle insurance.
c. States could begin to consider rules and laws allocating tort liability.[106]

To date, NHTSA has set aside industry concerns for liability arising from V2V technology and the possible lack of insurance.[107]

7. Preservation of Evidence

NHTSA strongly recommends that automakers create a documented process for design, testing, validation, and collection of events, incidents, and crash data. Some states have or have proposed data retention requirements.

Moreover, in certain cases where manufacturers reasonably anticipate litigation, they may have to preserve data collected from HAVs and connected vehicles as evidence. The electronic data recorder will have speed, braking, throttle control, air bag, and other data. Manufacturers of HAVs and connected vehicles should therefore evaluate their document retention policies to evaluate the types of documents and data that should be collected and stored to support continuous product improvement, satisfy regulators, and defend litigation.

V. CONCLUSION

The race is on across the globe. As HAV technology rapidly evolves, so must the law. As new ways of raising capital and doing business develop, so must the law adapt. Creative legal problem-solving will be needed to navigate the road through global, national, state, and local laws, regulations, and policies, and to guide industry standards and best practices for HAVs and connected cars.[108]

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

AUTHORS

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

Robert W. Kantner
Dallas
+1.214.969.3737
rwkantner@jonesday.com

Jonathon Little
London
+44.20.7039.5224
jrlittle@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

Paul F. Rafferty
Irvine
+1.949.553.7588
pfrafferty@jonesday.com

Dorothée M. Weber-Bruls
Frankfurt
+49.69.9726.3960
dweber@jonesday.com

ADDITIONAL CONTACTS

Chris J. Ahern
Sydney
+61.73085.7030
cahern@jonesday.com

Shogo Asaji
Tokyo
+81.3.6744.1612
sasaji@jonesday.com

Peter J. Biersteker
Washington
+1.202.879.3755
pbiersteker@jonesday.com

John E. Iole
Pittsburgh
+1.412.394.7914
jeiole@jonesday.com

David C. Kiernan
San Francisco
+1.415.875.5745
dkiernan@jonesday.com

Carl A. Kukkonen
San Diego / Silicon Valley
+1.858.314.1178 / +1.650.687.4178
ckukkonen@jonesday.com

Joseph Melnik
Silicon Valley
+1.650.687.4151
jmelnik@jonesday.com

Daniel R. Mitz
Silicon Valley
+1.650.739.3918
drmitz@jonesday.com

Yeah Sil Moon
New York
+1.212.326.3778
ymoon@jonesday.com

John R. Phillips
London
+44.20.7039.5215
jrphillips@jonesday.com

Jeffrey Rabkin
San Francisco
+1.415.875.5850
jrabkin@jonesday.com

John M. Saada, Jr.
Cleveland
+1.216.586.7089
johnmsaada@jonesday.com

David B. Sikes
Silicon Valley / San Francisco
+1.650.687.4192 / +1.415.875.5853
dsikes@jonesday.com

Adriane U. Sturm
Munich
+49.89.20.60.42.219
austurm@jonesday.com

Craig A. Waldman
San Francisco / Silicon Valley
+1.415.875.5765 / +1.650.739.3939
cwaldman@jonesday.com

Jennifer A. Bunting-Graden, an associate in the Atlanta Office, assisted in the preparation of this White Paper.

PRACTICAL CHECKLIST

Federal Regulation

- Pending federal legislation and proposed agency rulemaking
- Applicable FMVSS
- Exemption from FMVSS as needed
- NHTSA policy guidance for HAVs
- NHTSA pending proposed rule for V2V communications, including privacy and cybersecurity
- Applicable industry standards, principles, and best practices for HAVs, privacy, and cybersecurity
- Industry trade groups and coalitions

State Regulation

- Licensing of drivers/operators and registration of vehicles
- Safety inspections, if required
- Approval to operate or test on public roads with or without driver
- Satisfy insurance requirements
- Review traffic laws

International Regulation: By Jurisdiction

- Rules for licensing, testing, and operating on public roads,
- with or without driver
- Rules for V2V communications
- Data privacy and cybersecurity rules

Intellectual Property

- Worldwide strategy and plan to protect technology: patents and trade secrets
- Eligibility in United States and other countries for patent protection for software and AI
- List of countries in which you have employees, contractors, licensees, and purchasers using confidential technology and trade secrets
- Assessment of advantages and disadvantages of protecting confidential technology through patents or as trade secrets
- Procedures in place to designate certain information and data as confidential and as trade secrets
- Procedures in place to protect confidential business information and trade secrets, including at employee hiring and departure
- Due diligence to avoid patent infringement, including during corporate acquisitions
- Procedures to avoid unlawful acquisition of others' trade secrets, including during hiring of new employees
- Strategy and program to license patents and technology and to ensure compliance
- Procedures to comply with licenses of technology from others or open source
- Procedures to monitor work performed under joint development agreements
- Procedures or agreements with fleet operators, vehicle purchasers, and users as needed to protect licenses, patents, and trade secrets

Product Risk Mitigation

- Sound engineering design and testing procedures, including applicable industry standards, principles, and best practices
- Compliance with applicable FMVSS and NHTSA guidance
- Document retention and file review policies and audit of compliance
- Compliance with state licensing, registration, inspection, and traffic laws
- Analysis of insurance coverage, including HAVs and product recalls and investigations
- Quality control procedures and agreements for suppliers
- Sale or use agreements with fleet operators, ride-sharing companies, and others
- Dispute resolution procedures for suppliers, ride-sharing companies, and fleet operators, including forum, choice of law, and mechanism
- Review of warranties and disclaimers specific to HAVs and new technology
- Procedures for software and other technology updates and notifications

- Policies and procedures for education and training of sales representatives and consumers
- Review of advertising and representations pertaining to HAV technology
- Product manuals, instructions, and warnings, including software alerts and on-vehicle cautions
- Policies for data collection and use, and disclosure of those policies to owners and users
- Consumer agreements regarding data ownership, disclosure and use, where permissible
- Procedures for accident reporting and investigations, including procedures for NTSB and NHTSA reporting requirements and investigations
- Policies and procedures for preservation of evidence when litigation is anticipated
- Procedure for post-sale warnings and notifications, when necessary

ENDNOTES

1 U.S. Dep't. of Transp., NHTSA, Automated Driving Systems: A Vision for Safety," Notice of Public Availability and Request for Comments, at 1 (Sept. 12, 2017) ("NHTSA 2017 Guidance").

2 NHTSA 2017 Guidance, at 4 (Sept. 2017).

3 NHTSA, U.S. Dep't of Transp., Federal Automated Vehicles Policy, at 9-10 (2016)("NHTSA 2016 Policy").

4 "Toyota's Research Institute head says full autonomous driving is 'not even close."

5 "Toyota's Gill Pratt on Self-Driving Cars and the Reality of Full Autonomy," January 23, 2017.

6 "The future of auto safety is seat belts, airbags and network technology," *Network World*.

7 *Id.*

8 *Id. See* Federated Motor Vehicle Safety Standards – Vehicle-to-Vehicle (V2V) Communications, Docket No. NHTSA-2014-0022, August 20, 2014; "Vehicle-to-vehicle communication rule finally proposed by the government," December 14, 2016; NHTSA, "Vehicle-to-Vehicle Communications and Readiness of V2V Technology for Application" (2016).

9 David Welch *et al.*, "Trump Regulation Approach Likely to Stall Connected Vehicles" (Sept. 28, 2017).

10 "Tesla was just the beginning: Introducing the connected car landscape," *Venture Beat*, May 11, 2016.

11 *Id.*

12 Bloomberg, "Toyota, Microsoft Team Up on Connected-Car Technologies," April 4, 2016.

13 For a discussion of the difficulty in defining and proving equivalent safety, *see* L. Fraade-Blanar and N. Kalra, "Autonomous Vehicles and Federal Safety Standards: An Exemption to the Rule?" (Rand Corp. 2017).

14 For a preliminary review, *see* Anita Kim *et al*., "Review of Federal Motor Vehicle Safety Standards (FMVSS) for Automated Vehicles," (U.S. Dep't of Transp., John A. Volpe National Transportation Systems Center, March 2016). It concludes that automated vehicles with a conventional design (steering wheel, pedals, and seating) can comply with most FMVSS. Innovative, new designs would not.

15 For more information, please see Jones Day *Alert*, "Blind Spots Remain as SELF DRIVE Act Passes House" (Sept. 2017).

16 "Federal Motor Vehicle Safety Standards; V2V Communications, Docket No. NHTSA-2016-0126, RIN 2127, AL55 ("FMVSS V2V").

17 *Id.* at 3856-7.

18 *Id.* at 3914.

19 "Public Knowledge Responds to Department of Transportation's Connected Vehicles Proposal," Public Knowledge Press Release, December 13, 2016.

20 *Id.*

21 *Id.*

22 NHTSA 2017 Guidance, at 20.

23 National Conference of State Legislatures, "Autonomous Vehicles/Self-Driving Vehicles Enacted Legislation," 9/21/17.

24 "UNECE updates Vienna Convention on Road Traffic to allow automated vehicles."

25 "New UK laws address driverless cars insurance and liability," Feb. 24, 2017; UK Government Press Release, dated September 7, 2017

26 Michael J. Dunne, "China Aims to Be No. 1 Globally in EUs, Autonomous Cars by 2030."

27 PricewaterhouseCooper's Connected Car Report 2016 – Opportunities, Risk and Turmoil on the Road to Autonomous Vehicles, at 44.

28 "China to Set Communication Standard for Autonomous Cars After 2018," March 21, 2017.

29 "Roadblock: China's Grip on Maps," *The Wall Street Journal*, July 14, 2017.

30 *Id.*

31 *Id.*

32 Will Knight, "The Self-Driving Project that Could Help China leaping the West," July 5, 2017.

33 Kristen Koroscic, "This Chinese-Backed Startup Will Start Sell-Driving Electric Cars by 2020," March 10, 2017.

34 "Japan's Plan to Speed Self-Driving Cars"; "Japan's Olympic Dream: Driverless Cars on the Road for 2020."

35 *See also* Jones Day *Commentary*, "New Intellectual Property Considerations and Risks for Autonomous Vehicles" (May 2017).

36 *Association for Molecular Pathology v. Myriad Genetics, Inc.*, 133 S.Ct. 2107, 2116 (2013).

37 *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, 132 S.Ct. 1289, 1923 (2012).

38 *Id.* at 1297.

39 *Id.* at 1294.

40 *Id.* at 2356 (citing *Bilski v. Kappos*, 561 U.S. 593, 609, 130 S.Ct. 3218 (2010)).

41 *Id.* at 2357.

42 *Id.* (citing *Diamond v. Diehr*, 450 U.S. 175, 178-179 101 S. Ct. 1048 (1981), which involved a computer-implemented process for curing rubber).

43 *Vehicle Intelligence and Safety LLC v. Mercedes-Benz USA, LLC* 78 F.Supp. 3d 884 (N.D. Ill.), *aff'd*, 635 Fed. Appx. 914 (Fed. Cir. 2015).

44 *Vehicle Intelligence and Safety LLC v. Mercedes-Benz USA, LLC*, 635 Fed. Appx. 914, 918 (Fed. Cir. 2015).

45 *Id.* at 919.

46 *Purepredictive, Inc. v. H2O.AI, Inc.*, Case No. 17-cv-030409-WHO, Doc. 31 (N.D. Cal. Aug. 29, 2017).

47 *Id.* at *8.

48 *Id.* at *11-12.

49 *Enfish, LLC v. Microsoft Corporation*, 822 F.3d 1327 (Fed. Cir. 2016)

50 *Id.* at 1366.

51 *Id.* at 1335.

52 European Patent Convention ("EPC"), Article 52, paragraph 2.

53 *Id.*, Paragraph 3.

54 EPO Decision T 154/04 of November 15, 2006, Reasons 12.

55 JPO Guidelines, Part III Chapter 1 Eligibility for Patent and Industrial Applicability.

56 Guidelines of April 7, 2017, on Examination of Patents (promulgated by Order No. 74 of the State Intellectual Property Office ("SIPO")).

57 *See* "How China became an AI leader," World Economic Forum, June 26, 2017.

58 "As Autonomous Vehicles Gain Traction, Industry Needs One Standard, Experts Urge," *Automotive News*, September 25, 2013. In 2015, the IEEE amended its policy to require that all participants identify their essential patents and, for such patents, provide a letter of assurance that they will license on fair, reasonable, and nondiscriminatory terms or royalty free—subject to requesting a reciprocal license. Moreover, the royalty is to be on the smallest saleable unit.

59 "Tesla Sues Ex-Autopilot Director Over Recruiting," *The Wall Street Journal*, January 27, 2017.

60 *Waymo, LLC v. Uber Technologies, Inc., et al.*; Case No. 3:17-cv-00939-WHA (N.D. Cal.).

61 "Toyota uses upon source software in new in-car tech," Reuters, June 1, 2017.

62 Charles Glover and Sherry Fri Ju, "Baidu to open-source its autonomous driving technology," April 19, 2017.

63 Katyanna Quach, "Q. Why is Baidu Sharing Its Secret Self-Driving Service? A. To Help China Corner the Market," April 21, 2017.

64 Alan Ohnsman, "Baidu Enlists More Than 50 Companies for Driverless Tech Project," July 5, 2017.

65 Microsoft, "Aerial Informatics and Robotics Platform."

66 "Microsoft Made Its Autonomous Navigation Software Open Source, So What?" March 2017.

67 *Jacobsen v. Katzer*, 535 F.3d 1373 (Fed. Cir. 2008).

68 *Artifax Software, Inc. v. Hansom, Inc.*, No. 16-cv-06982-JSC, 2019 U.S. Dist. LEXIS 62815, Doc. 32 (N.D. Cal. Apr. 25, 2017).

69 37 C.F.R. Part 201 (Docket No. 2014-07) – Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, pp. 77-78.

70 *Id.* at 42.

71 *See* the Privacy Protection Principles.

72 Global Automakers, Press Release, "Automakers Develop Framework for Automotive Cybersecurity Best Practices," Jan. 19, 2016.

73 *Id*.

74 *Id*.

75 *Id*.

76 *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Red 2500 ¶¶ 60-66 (2016) ("Broadband Privacy NPRM").

77 *See* NHTSA, *Vehicle-to-Vehicle Security Credential Management System*, Request for Information, 79 Fed. Reg. 61927 at 61929 (2014).

78 NHTSA Notice of Rule Making, at 3926.

79 39th International Conference of Data Protection and Privacy Commissioners, Hong Kong, 25-29 September 2017, "Resolution on Data Protection on Automated and Connected Vehicles."

80 *Verband der Automobilindustrie* ("VDA"), "Data Protection Principles for Connected Vehicles."

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

82 Section 7 of the EU Directive 95/46/EC indicates the criteria for legitimate processing of personal data.

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

84 WP 185; Opinion 13/2011 on Geo-localization on Smart Mobile Devices.

85 *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

86 *See* section 31 of the EU General Data Protection Regulation.

87 UK Government Guidance, "The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles," published 6 August 2017,.

88 *See also* Jones Day *Commentary*, "Eyes on the Road Ahead: Product Liability Outlook for Autonomous Vehicles" (May 2017).

89 *See, e.g.*, California Acts, Chapter 570 of 2012, 2001-2012, 81; NAC Chapter 482A.020 (Nevada).

90 Currine Iozzio, "Who's Responsible When a Self-Driving Car Crashes?" May 1, 2016.

91 "ODI Resume cited NHTSA's full final investigation into Tesla's Autopilot shows 40% crash rate reduction," TechCrunch, January 19, 2017.

92 *Id.*

93 NTSB Press Release, "Driver Errors, Overreliance on Automation, Lack of Safeguards, Led to Fatal Tesla Crash," September 12, 2017.

94 For a more detailed discussion of how to manage consumer expectations and ways in which to inform and train drivers of HAVs, please *see* Charles H. Moellenberg, Jr., "Managing Consumer Expectations For Autonomous Vehicles," (August 28, 2107).

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

96 RESTATEMENT (SECOND) OF TORTS § 281 (1965).

97 Manufacturers cannot avoid liability just with warnings. *See* David G. Owen, *The Puzzle of Comment J.* 55 HASTINGS L.J. 1377, 1377.1, 1394-95 (2004). Manufacturers are responsible for using a "safer design [when it] can reasonably be implemented and risks can reasonably be designed out of a product…. Warnings are not … a substitute for the provision of a reasonably safe design." RESTATEMENT (THIRD) OF TORTS PROD. LIAB. § 2 cmt. 1 (1998). Warnings also need to protect consumers against foreseeable misuse. *See Rivera v. Phillip Morris, Inc.*, 209 P.3d 271 (Nev. 2009). *See* Andrew P. Garza, "*Look Ma, No Hands!*": *Wrinkles and Wrecks in the Age of Autonomous Vehicles*, 46 NEW ENG. L. REV. 581 (2012), for a more in-depth strict liability analysis of HAVs.

98 UCC §§ 2-313(1)(a), (b) and (c).

99 *See* Roy Alan Cohen, *Self-Driving Technology and Autonomous Vehicles: A Whole New World for Potential Product Liability Discussion*, 82 Def. Couns. J. 328, 333 (2015).

100 Jeffrey K. Gurney, *Sue My Car Not Me: Products Liability and Accidents Involving Autonomous Vehicles*, U. Ill. J.L. Tech. & Pol'y, Fall 2013, at 247, 267.

101 *See* Am. L. Prod. Liab., *supra*, at § 39:4.

102 *See* Am. L. Prod. Liab., *supra* § 39:3.

103 *Id.*; Gurney, J., *supra*, at 247, 269.

104 Gurney, J., *supra,* at 247, 268-9.

105 For a more detailed analysis, please see Jones Day *Commentary*, "The Road to Autonomous Vehicles: A Look at Insurance Implications" (April 2017).

106 NHTSA 2017 Guidance at 24.

107 NHTSA Notice of Proposed Rulemaking, *supra.* at 3967. NHTSA also cautioned against using contractual use agreements to limit liability to consumers. *Id*.

108 For another Jones Day publication, please see Jones Day *Commentary*, "Automated Vehicles Will Revolutionize the Automotive Industry" (March 2017).