FDCC Annual Meeting 2026
Lisbon, Portugal

Asleep at the Wheel: Assessing Liability and Risk when Technology is in the Driver's Seat

INTRODUCTION:

When machines make decisions traditionally made by humans, who bears responsibility when something goes wrong? From advanced driver-assistance systems (ADAS) to fully automated driving systems (ADS), technology increasingly performs tasks once reserved exclusively for human vehicle operators. Thus, what once involved relatively straightforward negligence claims against human drivers now presents complex, multi-party disputes potentially involving manufacturers, software developers, fleet operators, insurers, and technology vendors.

As vehicles increasingly rely on artificial intelligence, machine learning, sensors, and over-the-air software updates, the traditional distinction between "driver error" and "product defect" are less clear. Existing tort negligence and liability theories remain relevant, but they are increasingly strained by technologies that blur the line between human conduct and machine decision-making. As vehicles become more technologically autonomous it is less certain who ultimately bears the financial and legal consequences when technology fails.

AUTONOMOUS VEHICLE TECHNOLOGY:

An autonomous vehicle ("AV") is a vehicle equipped with technology capable of performing some or all driving functions without continuous human input. These systems rely on combinations of:

- Artificial intelligence (AI)
- Machine learning algorithms
- Cameras and computer vision systems
- Radar and LiDAR sensors
- GPS and mapping technologies
- Vehicle-to-vehicle (V2V) communication
- Vehicle-to-infrastructure (V2I) communication
- Real-time data processing systems

Most modern autonomous systems continuously collect and analyze environmental data in order to make operational driving decisions such as steering, braking, acceleration, lane positioning, obstacle avoidance, and route navigation.

Autonomous vehicle technology exists along a spectrum developed by the Society of Automotive Engineers (SAE). These levels of automation range from Level 0 (no automation) to Level 5 (full automation). Understanding the level of automation is important is understanding how liability exposure can change.

Levels of Automation:

Level 0 – No Automation. The human driver performs all driving tasks. Technology may provide warnings but does not actively control vehicle functions. (e.g. blind spot monitoring, lane departure warnings)

Level 1 – Driver Assistance. The vehicle can assist with either steering or acceleration/braking, but not both simultaneously. The driver remains fully responsible for vehicle operation. (e.g. adaptive cruise control, lane centering assistance)

Level 2 – Partial Automation. The vehicle can simultaneously control steering and acceleration/braking under certain conditions, but continuous human monitoring is still required. (e.g. highway autopilot systems, traffic jam assist systems, advanced lane centering technologies)

Level 3 – Conditional Automation. The vehicle can independently operate under certain conditions without constant human monitoring, but the drive must be available to intervene upon request.

Level 4 – High Automation. The vehicle can perform all driving functions within designated operational domains without human intervention.

Level 5 – Full Automation. The vehicle performs all driving functions under all conditions without any human involvement.

These classifications distinguish truly automated driving systems (ADS) from Advanced Driver-Assistance Systems (ADAS).

ADAS are technologies designed to assist human drivers—not replace them. ADAS systems support driving functions such as steering assistance, braking, speed, lane positioning, parking, and collision avoidance. ADAS vehicles still require constant driver oversight, attentiveness and intervention.

Unlike ADAS systems, ADS vehicles are intended to perceive environmental conditions independently, make operational driving decisions, and execute vehicle control functions without constant driver oversight. At the higher levels of automation, the system—not the human—becomes the primary operational decision-maker.

Most ADAS-equipped vehicles currently operate at SAE Levels 1 or 2 automation. True autonomous operation (ADS) generally begins at SAE Level 3 and expands significantly at Levels 4 and 5.

ADAS (Level 2)

Examples:

- Tesla Autopilot/FSD
- Ford BlueCruise
- GM/Cadillac Super Cruise

ADS (Levels 3–5)

Examples:

- Waymo robotaxis
- Mercedes Drive Pilot
- Cruise autonomous vehicles
- Zoox test fleet

RECENT LITIGATION AND LEGISLATION:

Although there is a growing number of much more highly publicized incidents and crashes involve ADS vehicles such as Waymo, currently the majority of reported AV crashes and resulting litigation involve Level 2 systems; however, there is still very limited guidance to date on how fault should be determined.

On August 1, 2025, in Benavides v. Tesla, Case No. 21-cv-21940, in the U.S. District Court for the Southern District of Florida, a jury found Tesla partially liable for a fatal crash involving its "Autopilot" system and awarded approximately $243 million in compensatory and punitive damages. The accident occurred while the driver was operating a Tesla Model S with Autopilot engaged. The vehicle failed to stop at a T-intersection and fatally struck one pedestrian and seriously injured another. Both the driver and Tesla were named as defendants. The defendant driver admitted he was distracted by his phone at the time of the crash and settled out. Tesla denied responsibility. Plaintiffs argued Tesla's Autopilot system could be activated in unsafe conditions; that the driver monitoring measures were insufficient to assure a driver remained engaged; and that Tesla's marketing overstated Autopilot's capabilities and encouraged overreliance on the system.

The jury agreed that Tesla was independently negligent and apportioned fault between the driver and Tesla, assigning approximately one-third of the liability to Tesla, making this one of the first major jury verdicts imposing substantial liability on the vehicle manufacturer based on failure to warn and design defects based, in part on consumer expectations. The case is also notable for the award of significant punitive damages due to Tesla's statements and marketing materials that jurors clearly believed was evidence of corporate indifference to driver safety. Until this case, Tesla and other manufacturers had successfully defended claims taking the position that the driver alone bears responsibility for Level 2 automation systems. Post trial motions have been filed and further appeals are expected.

Accidents involving AVs are also being scrutinized by state and federal regulatory and administrative authorities for safety concerns, but there is still limited focus on fault allocation for accidents.

At about the same time the verdict in Benavides was rendered in August 2025, a federal class action alleging deceptive marketing of Tesla's "Full Self Driving" (FSD) package was certified in California in In re Tesla Advanced Driver Assistance Systems Litigation, Case No. 22-cv-05240, in the U.S. District Court for the Northern District of California. The certified class covers California residents who purchased or leased a Tesla and paid separately for the Full Self Driving package between May 19, 2017 and July 31, 2024. and is still in the early stages.

Most recently on March 31, 2026, the National Transportation Safety Board (NTSB) completed an investigation into two fatal crashes in 2024 and concluded that Ford Motor Company's hands-free partial automation system, Blue Cruise, contributed to both crashes and made recommendations to the US Department of Transportation and Ford calling for stronger federal guidelines and performance standard, crash data recording and automatic notification requirements, improved driver monitoring systems to detect distraction and changes to the Ford's Blue Cruise system to reduce excessive speeding and improve driver attention.

In early May 2026 the National Highway Traffic and Safety Administration (NHSTA) opened a probe into 16 crashes involving Avrides's autonomous delivery vehicles and robotaxis which operate on the Uber platform in Texas concerning allegations of aggressive/assertive behaviors and failure to avoid obstacles.

Several states, such as Colorado, Mississippi and California, have passed legislation governing various aspects of autonomous vehicles. However, Utah Senate Bill 292 was signed into law by the Governor on March 23, 2026 and provides the most detailed attempt at legislating responsibility for motor vehicle accidents involving AVs. The bill generally restricts actions against the ADS (Level 4 or 5) manufacturer to two paths. The first is the special "driverless operation liability", an exclusive remedy for claims against the owner and dispatcher which is limited to $100,000. The plaintiff must prove that the ADS was engaged, and that the ADS was the proximate cause of the injury. Larger claims would have to pursue a product liability claim, which would be limited to $1million, but the plaintiff would have to prove that a reasonable alternative design exists, and that ADS use causes more injuries than human drivers. The law became effective on May 6, 2026. Many other states and the federal government also have numerous proposed legislative changes that are under consideration.

EVOLVING THEORIES OF LIABILITY AND RISK:

Automobile litigation has historically centered only on driver conduct and traditional tort negligence principles. As automation expands, liability analysis and exposure shifts from solely human conduct toward system performance and technological reliability and liability may turn less on the collision itself and more on the system architecture, software design decisions, human-machine interaction, and possible consumer expectations created by marketing and

branding. Therefore, when an AV is on the road, liability may be shared or entirely transferred to many potential parties in addition to the driver such as manufacturers, software developers, fleet operators, component parts manufacturers and suppliers, or third party data providers. For insurers and defense counsel, AV claims may no longer resemble traditional motor vehicle accidents. Instead, they are evolving into hybrid cases also involving products liability, cybersecurity, and technology litigation.

Moreover, new coverage questions and challenges are presented as parties seek to understand what coverage may be implicated and what policy provisions or exclusions may apply, potentially under automobile, general liability, cyber, product liability, or other coverage.

Traditional comparative negligence frameworks become more complicated when autonomous systems share operational control with human drivers. In some cases, defense counsel may argue that inattentive drivers remain the primary proximate cause. Plaintiffs, however, may contend that the system itself induced foreseeable driver complacency. Additionally, a major challenge involves distinguishing between human and machine responsibility. Human drivers remain susceptible to distraction, fatigue, intoxication, and poor judgment. Autonomous systems, by contrast, may fail because of programming limitations, sensor inaccuracies, or algorithmic bias.

The recent verdict in Benavides, illustrates that this tension has already emerged in litigation involving ADAS where manufacturers market features with names implying full autonomy despite requiring human attention. Courts may increasingly examine whether marketing practices create unreasonable consumer reliance on automation.

AVs also present unique challenges because software behavior can evolve after deployment through updates and machine learning. Unlike static mechanical components, AI systems may adapt unpredictably over time.

For example, if an autonomous driving system misidentifies a pedestrian or fails to respond appropriately to road conditions, plaintiffs may argue that the software was defectively designed. Manufacturers, however, may contend that the driver ignored instructions requiring continued supervision.

Cybersecurity and Data privacy risks are also present. Autonomous vehicles depend heavily on interconnected software systems, cloud computing, GPS, and wireless communication. This dependence creates substantial cyber threats such as remote hacking of vehicle controls, GPs, spoofing, ransomware attacks on transportation systems, GPS spoofing, or data breaches. Further insurance companies may gain access to extensive driving data, enabling more precise evaluation of risk but also raising privacy concerns.

Cybersecurity failures could expose manufacturers and service providers to negligence claims if reasonable safeguards were not implemented. Additionally, questions arise regarding ownership and privacy of the vast amounts of data generated by autonomous vehicles.

Governments and regulators increasingly recognize cybersecurity as essential to transportation safety. However, regulation of autonomous vehicles remains fragmented and inconsistent. Federal, state, and international authorities continue to develop standards governing testing, deployment, and safety compliance. Regulators face the difficult task of balancing innovation with public safety. Overregulation may slow technological progress, while insufficient regulation could expose the public to unacceptable risks.

Autonomous vehicles also raise ethical concerns extending beyond traditional legal analysis. AI systems may face unavoidable crash scenarios requiring programmed decision-making about harm allocation. Although these dilemmas are statistically rare, they highlight the broader societal implications of delegating life-and-death decisions to machines.

Finally, traditional auto insurance focuses primarily on driver behavior. However, autonomous vehicle claims present significant insurance coverage uncertainties that existing policy language may not adequately address and auto insurers will likely seek to push risk to the manufacturer's insurance, cybersecurity coverage, or other policies. Insurers may also seek to revise policy language such as AV operation endorsements or exclusions or AI and technology or software related exclusions or limitations.

ACCIDENT INVESTIGATION AND LITIGATION CHALLENGES:

Autonomous vehicle claims and litigation introduce substantial discovery complexities.

Critical evidence may include:

- Vehicle telemetry data
- Event data recorder ("black box") information
- Sensor recordings
- Internal software logs
- AI decision-making pathways
- Over-the-air update histories
- Driver monitoring system data

However, these types of data create potentially thorny discovery and admissibility issues. Disputes over preservation or potential spoliation of evidence are possible. Potential issues involving authentication or protection of trade secrets and proprietary software and source codes are also likely. As litigation over autonomous vehicles develops, courts will increasingly confront disputes over discoverability of algorithmic decision-making processes and the extent to which manufacturers must disclose proprietary AI systems.

Early preservation of data and engagement of experts such as an accident reconstructionist, software engineers, human factors specialists, cybersecurity professionals, and even coverage counsel is highly likely and frequently critical for insurers and defense counsel to effectively assess and defend AV claims and litigation.

CONCLUSION:

Autonomous vehicles claims are changing the landscape of automobile accident claims. As the technology provides more features and more active control over the operation of a vehicle, the liability analysis becomes murky. Litigation increasingly resembles traditional product defect litigation rather than ordinary automobile negligence case including theories regarding defective design and failure to warn. It encompasses not only whether there was negligent vehicle operation but also determinations regarding the role of new or emerging technology and the potential fault of new and different parties such as manufacturers, programmers, designers and distributors.

Uncertainty abounds. Who is covered? Is the loss an auto accident or a product failure? Who was the driver? Does software constitute a product? Could liability rest with a rogue agent? Because autonomous vehicles depend heavily on interconnected software and wireless communications substantial cyber exposure may exist such as remote hacking, AI manipulation, data breaches, or ransomware attacks, leaving further uncertainty about who is at fault when technology takes the wheel.