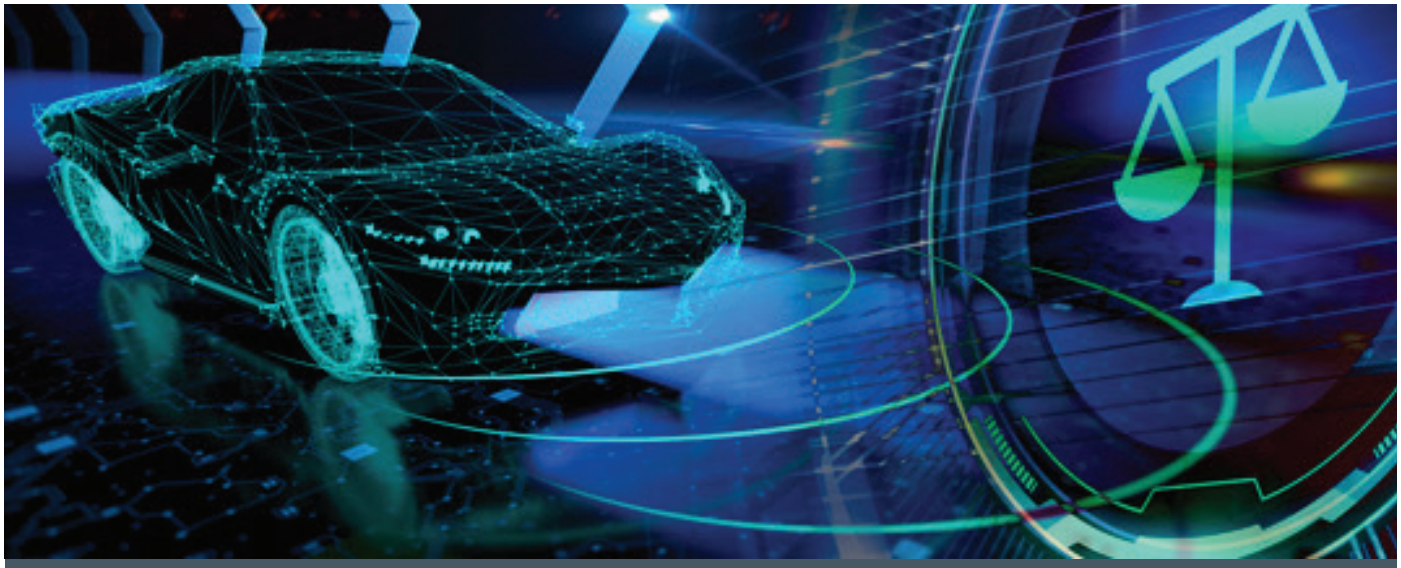
JONES DAY | One Firm Worldwide®



WHITE PAPER

October 2025

Who's Liable When AI Takes the Wheel? New Frontiers of Civil Liability and Risk Mitigation Strategies in the EU and the U.S.

The emergence of fully autonomous vehicles is fundamentally transforming the landscape of civil liability within the automotive industry. Significant regulatory advancements, evolving case law, and emergent tort doctrines in both the European Union and the United States are actively redefining liability allocation across the entire technology and manufacturing supply chain. This necessitates a proactive update of risk mitigation strategies and a reevaluation of vehicle owners' responsibilities.

The shift toward automated driving technologies is consequently redirecting civil liability exposure to technology providers, component suppliers, and automotive manufacturers. This evolution demands a comprehensive rethinking of traditional civil liability frameworks, with particular focus on four pivotal areas: liability for product and algorithmic defects, cybersecurity and data privacy concerns, the intricate interconnected ecosystem and associated third-party liabilities, and the emergence of new duties for vehicle owners.

Therefore, it is crucial for all automotive industry participants to adopt forward-looking risk mitigation strategies. By implementing robust quality controls, ensuring strict regulatory compliance, and cultivating transparent supply chain relationships, stakeholders can more effectively navigate the complexities of this new era. This approach will help guard against the multifaceted risks linked to automated driving systems, while simultaneously upholding accountability and safeguarding potential victims.

INTRODUCTION

The emergence of fully autonomous vehicles ("AVs") is fundamentally transforming the landscape of civil liability in the automotive sector.

The European Union ("EU") has responded—although indirectly—to these challenges thus far with the PLD (Directive (EU) 2024/2853 on Liability for Defective Products) and the AI Act (Regulation (EU) 2024/1689), while the proposal for an AI Liability Directive has been withdrawn in early 2025.

In contrast with the EU's (at least partial) regulatory response, the United States continues to lack a comprehensive federal regime governing civil liability in situations involving AVs. Instead, civil liability is predominantly governed by state law, primarily through traditional tort doctrines such as product liability and negligence. That said, emerging case law portends the development of a more robust regulatory response.

These regulatory developments are redefining the allocation of liabilities throughout the technology and manufacturing supply chain, imposing new risk mitigation strategies and transforming the duties of vehicle owners.

DRIVING ACCOUNTABILITY: HOW EU AND U.S. LAWS ARE REDEFINING CIVIL LIABILITY FOR AUTONOMOUS VEHICLES

The emergence of fully AVs, particularly those at SAE Levels 4 and 5, is fundamentally transforming the landscape of civil liability in the automotive sector. As control shifts from human drivers to Automated Driving Systems ("ADS"), the traditional fault-based liability regime—centered on human error—becomes less applicable. This evolution places technology providers, component suppliers, and automotive manufacturers at the center of new and complex liability exposures, requiring a reallocation of risk and the development of robust risk mitigation strategies.

The EU has responded to these challenges with a two-pronged legislative approach thus far:

- **Directive (EU) 2024/2853 on Liability for Defective Products**. This directive establishes a harmonized product liability regime across the EU, directly impacting technology providers, component suppliers, and automotive manufacturers. It expands the definition of defect to include not only physical flaws but also digital and software-related failures, including those arising from AI and automated systems.
- **The AI Act (Regulation (EU) 2024/1689)**. The AI Act classifies AV systems as "high-risk" and imposes stringent requirements on manufacturers regarding data governance, transparency, and robustness. While noncompliance with these requirements can serve as evidence of fault in civil liability claims, the AI Act does not establish a specific set of rules regarding ADS and civil liability.
- Complementing the above regulatory framework would have been the *ex-post* (remedial) **AI Liability Directive** ("AILD"), had its proposal not been withdrawn in early 2025.

In the United States, AVs are regulated by a patchwork of federal and state regimes:

- The National Highway Traffic Safety Administration ("NHTSA") regulates the testing and safety of motor vehicles through the Federal Motor Vehicle Safety Standards ("FMVSS"), but these standards were designed for traditional vehicles and often assume the presence of a human driver. The Federal Autonomous Vehicle Acceleration Act of 2025 is currently under review by the Senate Commerce, Science, and Transportation Committee and instructs the Secretary of Transportation to update the FMVSS so that such assumptions do not impede the approval process for AVs. In August 2025, Amazon's Zoox robotaxis received the first exemption from the FMVSS under NHTSA's Automated Vehicle Exemption Program. Separately, NHTSA has also issued several guidance documents, such as Automated Driving Systems 2.0-4.0 and Standing General Orders requiring AV incident reporting.
- The Federal Motor Carrier Safety Administration sets safety standards for trucks, the Federal Motor Carrier Safety Regulations.
- The National Transportation Safety Board has authority to investigate vehicular accidents and make recommendations for improved safety, though it primarily focuses on civil aviation, trains, and trucking.
- States have traditionally regulated roadway safety by licensing drivers, registering motor vehicles, conducting safety inspections, enacting and enforcing traffic laws, providing the safety infrastructure, and regulating motor vehicle insurance and liability for vehicular accidents.

While most state laws governing AVs concern their development and operation, several states are beginning to address civil liability. For instance, laws in Michigan, Florida, and Nevada limit manufacturer liability where a non-OEM entity modifies the vehicle post-sale. *See*, e.g., Mich. Comp. Laws § 600.2949b; Nev. Rev. Stat. § 482A.090; Fla. Stat. § 316.86. Additionally, Tennessee recognizes the automated driving system as the legal driver of the vehicle for purposes of determining vehicle owner liability for injury, damage, or nonconformity with traffic laws. Tenn. Code Ann. § 55-30-106. Similarly, California's AV statute empowers law enforcement to cite AVs for traffic violations. Cal. Veh. Code. § 38752.

Also relevant to the current state of AV civil liability is the judiciary. Emerging case law demonstrates that the courts are grappling with the attribution of fault in accidents involving AVs. For example, a court in the Southern District of Florida recently held that a reasonable jury could find Tesla's Autopilot system defectively designed, marking a potential shift in judicial willingness to assign liability to AV manufacturers. *See, Benavides v. Tesla, Inc.* No. 21-cv-21940, 2025 WL 1768469 (S.D. Fla. Jun. 26, 2025). At trial, the jury found that Tesla's Autopilot was defective and was 33% at fault for the underlying crash, ultimately imposing $242.57 million in damages on Tesla, including $200 million in punitive damages. *Id.*, Dkt. No. 534. Following the case, a Tesla investor filed suit in the Western District of Texas alleging that Tesla overstated the capabilities of its self-driving technology despite knowing of its flaws and the associated risks, ultimately reducing the company's market value. *Morand v. Tesla, Inc.*, No. 1:25-cv-01213 (W.D. Tex. Aug. 4, 2025). Although juries in other cases have sided with Tesla, they have similarly found driver error to be the predominant cause of crashes, even when Autopilot was engaged. The evolving jurisprudence suggests that U.S. courts are beginning to distinguish between traditional human negligence and machine failure and suggests that regulatory action may be on the horizon.

THE JULY 2025 STUDY ON AI AND CIVIL LIABILITY COMMISSIONED BY THE EU PARLIAMENT AT THE REQUEST OF THE EU COMMISSION

Building on the revised PLD, a recent study commissioned by the EU Parliament at the request of the EU Commission ("Study") remarked that the notion of "defect"—still anchored in a lack-of-safety test—remains ill-suited for Level 4 and Level 5 ADS, whose failures are more often rooted in performance shortcomings, data opacity, and algorithmic drift than in classical safety faults.

The Study therefore urges lawmakers to decouple liability from a traditional defect inquiry and to move toward a functional, strict-liability model for "high-risk" AI systems, mirroring the high-risk tier of the AI Act. Such a model would allocate primary responsibility to a single operator—ideally, the economic actor that controls the automated driving system and derives revenue from its deployment—thereby eliminating overlapping causes of action and the litigation costs generated by today's multiparty claims.

The Study further cautions that, absent an EU-wide strict-liability framework, Member States are likely to enact divergent national statutes—Germany's Autonomous Driving Act and Italy's Law No. 132/2025 already illustrate this centrifugal trend—creating path dependencies that will be extremely difficult to harmonize *ex post*.

Over-regulation, the Study argues, does not stem from *too many* rules but from a patchwork of inconsistent ones; uniform, technology-specific liability rules would in fact lower compliance costs by transforming indeterminate risk into insurable, priced-in cost components.

Taken together, these findings strengthen the policy case for supplementing the updated PLD with a distinct, no-fault liability instrument targeted at high-risk automated driving systems, thereby safeguarding victim compensation, legal certainty, and cross-border market integration.

FOUR KEY ASPECTS

The subject requires a rethinking of the traditional legal categories of the attribution of civil liability, taking into account four key aspects:

1. **Product and Algorithmic Defect Liability**. Liability is now focused on those who design, manufacture, and integrate ADS and their components. Any accident or damage resulting from a malfunction—whether due to hardware failure, software bug, or algorithmic error—may be considered evidence of a product defect. This includes not only traditional

mechanical failures but also failures in AI decision-making, cybersecurity vulnerabilities, and errors in data processing or sensor fusion. Technology providers and component suppliers may be held liable if their systems do not meet the standard of a reasonably prudent human driver or fail to safely manage foreseeable situations, including ethical dilemmas programmed into the system.

2. **Cybersecurity and Data Privacy**. Modern AVs are not only cyber-physical machines, but also roaming data centers that ingest, process, and transmit vast volumes of sensor, geolocation, biometric, and behavioral information. As a result, civil liability now extends beyond physical-collision harms to include: (i) exposure from cybersecurity breaches that threaten vehicle safety, vehicle integrity, or the confidentiality, security, or integrity of any personal data processed, as well as (ii) privacy violations related to any such personal data. As part of the growing trend toward greater regulation of personal data, enforcers and regulators are increasingly focused on geolocation and biometric data, with several legislative regimes specifically regulating its collection, sharing, and sale (*See*, e.g., the General Data Protection Regulation, California Consumer Privacy Act, and Colorado Privacy Act). Accordingly, those parties collecting, processing, or maintaining such data may face civil liability exposure beyond that associated with non-autonomous vehicles.
3. **Interconnected Ecosystem and Third-Party Liability**. AVs operate as nodes within a highly interconnected digital ecosystem, relying on real-time data from infrastructure, other vehicles, and external service providers. Liability may extend to technology suppliers responsible for V2X (Vehicle-to-Everything) communications, map data, or cybersecurity. A failure in any part of this network—such as a corrupted software update, a compromised data stream, or a cybersecurity breach—can trigger liability for multiple parties, including infrastructure operators and telecommunications providers. The scope of liability is thus broadened, and all actors in the supply chain can be held jointly and severally liable for damages caused by defective products, regardless of whether the defect is mechanical, digital, or algorithmic in nature.
4. **New Duties for Vehicle Owners**. While the primary focus of liability shifts to manufacturers and technology providers, vehicle owners are not entirely absolved. Their responsibilities are redefined: Owners must act as technological custodians, ensuring timely software updates, compliance with safety recalls, and operation within the vehicle's specified operational design domain. Failure to meet these duties may result in liability under theories of negligent entrustment or breach of duty of care. The standard of "digital diligence" is emerging, requiring owners to actively maintain the technological integrity and legal compliance of their vehicles.

RISK MITIGATION STRATEGIES

Risk mitigation strategies are numerous and include the following:

- **Quality Assurance and Testing**. Implement comprehensive testing protocols for both hardware and software, including rigorous validation of AI models and real-world scenario simulations. Continuous monitoring and post-market surveillance are essential to detect and address emerging defects.
- **Privacy, Cybersecurity, and Data Integrity**. Establish strong privacy and cybersecurity frameworks to accommodate individual's privacy rights and protect against unauthorized access, data corruption, and malicious attacks. Regularly update security protocols and conduct vulnerability assessments to ensure the integrity of all digital systems.
- **Regulatory Compliance and Documentation**. Ensure strict adherence to all relevant EU regulations, including the AI Act and Directive (EU) 2024/2853. Maintain detailed records of design, testing, and compliance activities to facilitate defense in the event of litigation.
- **Supply Chain Management**. Define contractual arrangements that clearly allocate liability and indemnification obligations among technology providers, component suppliers, and manufacturers. This includes specifying responsibilities for software updates, data management, and post-sale support.
- **Proactive Recall and Update Management**. Develop efficient mechanisms for issuing recalls, deploying software patches, and communicating safety-critical information to vehicle owners and operators. Prompt action in response to identified defects can limit exposure to liability.
- **Insurance and Risk Transfer**. Secure appropriate insurance coverage tailored to the unique risks of automated driving technologies, including coverage for product liability, cyber incidents, and third-party claims.
- **Evidentiary Facilitation Inspired by the AILD**. Even though the AILD was not adopted, its approach to easing the

evidentiary burden for victims—by introducing a rebuttable presumption of causation in cases of regulatory noncompliance—remains a reference point for future reforms and risk mitigation strategies. Stakeholders should monitor ongoing policy discussions, as similar mechanisms may be incorporated into future legislative or regulatory initiatives.

ALTERNATIVE THEORIES OF LIABILITY

Some scholars advocate for no-fault insurance or compensation fund models, which would provide swift compensation to accident victims without requiring proof of fault, funded by levies on manufacturers and owners. While this approach prioritizes efficiency and victim compensation, it may sacrifice individualized justice and accountability. On the criminal law front, liability remains challenging, as algorithms cannot bear criminal responsibility. Prosecutors must trace accountability to specific human actions or omissions within the corporate structure, such as reckless management decisions or grossly negligent programming. The complexity of AV systems and the opacity of AI decision-making (the so-called "black box" problem) further complicate the attribution of criminal liability.

Although civil liability in the United States primarily involves theories of negligence, strict liability may arise under product liability doctrines where a defective product causes harm regardless of fault. While U.S. courts have traditionally applied these doctrines to tangible goods, recent decisions have recognized AI software as a "product" to which these doctrines may apply, in the context of social media platforms. *See*, e.g., *Garcia v. Character Techs., Inc.*, No. 6:24-CV-1903-ACC-UAM, 2025 WL 1461721 (M.D. Fla. May 21, 2025); *see* also, Restatement (Third) of Torts: Prod. Liab. § 19 (1998). The willingness of courts to allow product liability claims to proceed against social media platforms using AI technologies that evolve post-sale suggests a potential willingness to view AI-related software as a product in other contexts, such as AVs.

CONCLUSIONS

The transition to automated driving technologies brings significant shifts in civil liability exposure for technology providers, component suppliers, and automotive manufacturers. The interplay between emerging EU legislation—particularly Directive (EU) 2024/2853 and the AI Act—and the technical realities of AVs demands a proactive, multilayered approach to risk management.

In the United States, while AVs are governed by a patchwork of state and federal laws, emerging trends in state laws, ongoing AV litigation, and product liability reflect the continuing transition in how liability is attributed and potentially foreshadow the development of a more robust regulatory regime.

By implementing robust quality controls, ensuring regulatory compliance, and fostering transparent supply chain relationships, stakeholders can better navigate the challenges of this new era and safeguard against the complex risks associated with automated driving systems, while ensuring accountability and protection for potential victims. The evolving legal landscape requires continuous adaptation and vigilance, as the boundaries of liability, responsibility, and risk continue to be tested by technological innovation.

LAWYER CONTACTS

Sion Richards
Practice Leader
London
+44.20.7039.5139
srichards@jonesday.com

Eric Barbier de La Serre
Paris
+33.1.56.59.38.11
ebarbierdelaserre@jonesday.com

Arthur O'Reilly
Detroit
+1.313.230.7925
atoreilly@jonesday.com

Lamberto Schiona
Milan
+39.02.7645.4001
lschiona@jonesday.com

Ozan Akyurek
Paris
+33.1.56.59.39.39
oakyurek@jonesday.com

Dr. Jacob Guhn
Düsseldorf
+49.211.5406.5500
jguhn@jonesday.com

Philip Pfeffer
New York
+1.212.326.3688
ppfeffer@jonesday.com

Associates Margherita Farina, Landon Kane, Michael McFerran, Lara Stojanov, and summer associate Kelsey Ford contributed to this White Paper.