RETHINKING INSURANCE COVERAGE FOR AUTONOMOUS VEHICLES

By Lorelie S. Masters, Walter J. Andrews, Paul T. Moura, and Sergio F. Oehninger

The autonomous vehicle industry is pressing forward, full speed ahead. In addition to providing convenience, safety, and cost-efficiency for passengers, these vehicles stand to completely transform the economic dynamics of the automotive industry. But while autonomous vehicles can lessen the costs of human error, they also can introduce new, potentially crippling technological risks. In turn, the rollout of these new vehicles—along with their concomitant risks—will require a significant revamp of the traditional functions of auto insurance and increase the role of other forms of insurance, such as product liability coverage, business interruption policies, and cyber insurance options.

Many predict that vehicle automation will generate billions of dollars for automotive companies and spur a diversity of new entrants into the industry, including suppliers of new technologies, digital services, and infrastructure developers. Car manufacturers like Tesla have hopped on the automated bandwagon in a race to develop their networks of self-driving vehicles.

Other companies are moving full-throttle to develop other niches in the autonomous vehicle space. For example, Lyft recently announced that it is creating a (new several-hundred-employee) "Level Five" unit focused on developing an open network for autonomous vehicles that automakers and technology companies can use. Consumers may soon find Google's Waymo vehicles or General Motors' Bolt model operating on the network. Others are taking the lead in developing the computer software, sensor technologies, and user interface that autonomous vehicles need to navigate.

Automation is expected to create numerous benefits for businesses and consumers: better safety, greater mobility, energy efficiency, and cost savings. In an attempt to keep up with this growth, many states are grappling with how to regulate these vehicles and industry players. In fact, some states have opted to reduce regulatory barriers in order to lure investment and innovation. The result, however, is a patchwork of regulations and uncertainties about where liabilities will land.

As vehicles become more "connected" to outside forces and controls, autonomous vehicle operators will need to focus on new areas of liability that previously may have had little place in the automotive industry—issues such as privacy, cyber security, and the Internet of Things (IoT). Going forward, auto insurance as we know it may lose its importance, and the "connected" nature of these vehicles will require greater consideration of other forms of insurance to address new liabilities.

Evolution of Risk in the Era of Autonomous Vehicles

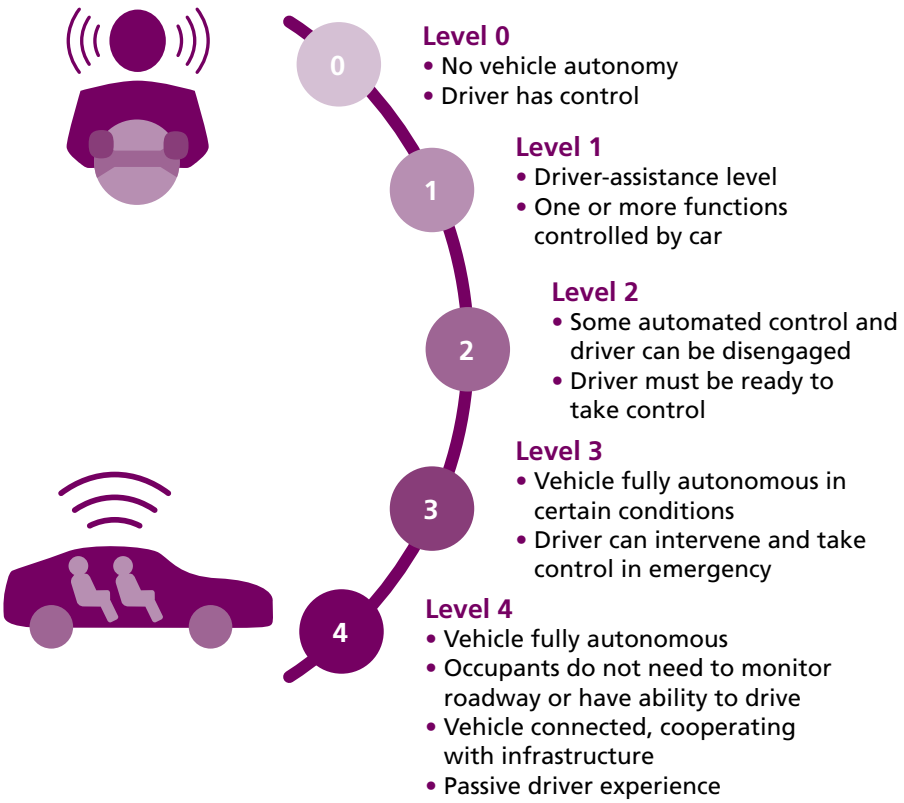
Autonomous vehicles can introduce new, potentially catastrophic risks—as well as questions about who should be responsible for them. For example, the first known fatality in an autonomous vehicle occurred on a divided highway in central Florida. While on autopilot mode, the vehicle collided with a tractor-trailer—reportedly due to a combination of flaws in the vehicle radar system settings, the weather, and the atypical height of the trailer. As this unfortunate event demonstrates, we may need to rethink the assignments of liability made by our test lab systems and how the law responds. Evolution of unmanned transportation and vehicle systems (collectively, UVS), artificial intelligence (AI), and other technologies may revolutionize liability insurance as well. For example, the existing auto insurance system, which has developed around the fact that a human driver controls the vehicle, will need to change as the technology changes and adoption of UVSs increase. Changes in liability and assignment and transfer of risk likely will increase the evolution of other forms of insurance, such as product liability coverage, business-interruption policies, and cyber insurance options.

Levels of Vehicle Autonomy

In many instances, the ability of the driver to exert some degree of control over the vehicle may have the greatest impact on determining liability. The National Highway Transportation Safety Administration's (NHTSA) five levels of vehicle autonomy illustrate the spectrum of autonomous vehicle types, ranging from full driver control to total automation.

At Level Zero, the driver is in complete and sole control of the vehicle controls at all times and is

NATIONAL HIGHWAY SAFETY ADMINISTRATION LEVELS OF VEHICLE AUTONOMY



Source: National Highway Traffic Safety Administration: Automated Vehicles for Safety (https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety)

solely responsible for monitoring the roadway.

At Level One, automation involves one or more specific control functions, such as electronic stability control or precharged brakes. At Level Two, automation involves at least two primary control functions designed to work in unison to relieve the driver of control of those functions, such as adaptive cruise control in combination with lane centering. At Level Three, there is limited self-driving automation. Automation at this level allows the driver to refrain from monitoring the roadway and cede full control of all safety-critical functions, but returns control to the driver in certain conditions. At Level Four, the vehicle is fully autonomous. The vehicle can perform all operation and safety-critical driving functions for an entire trip.

Lorelie S. Masters *and* ***Walter J. Andrews*** *are partners and* ***Sergio F. Oehninger*** *is counsel in the Insurance Recovery Group of Hunton Andrews Kurth LLP in Washington, DC.* ***Paul T. Moura*** *is an associate in the group, practicing in the New York and Los Angeles offices.*

A New Era for Auto Insurance

These varying levels of autonomy present new challenges for traditional auto liability insurance, which developed in an era when Level Zero was the norm. With vehicles that use partial autonomy (Levels One through Three), the driver is still expected to monitor the roadway and have at least some control over the vehicle. In those situations, the driver should remain generally responsible for accidents because the driver retains ultimate control of the vehicle. These situations do not appear to require a reformation of the liability or tort system. Hence, it is reasonable to assume that the driver's own insurance should apply. Traditional bodily injury and property damage liability coverage, uninsured or underinsured motorist coverage, and no-fault coverage may not change significantly for these vehicles, though premium costs may decrease if the expected reduction in accidents materializes.

However, as vehicles on the market become truly autonomous (Level Four), the role of the individual driver disappears. Driving decisions will instead be based on artificial intelligence and through communication with other connected vehicles and surrounding infrastructure. In these circumstances, the potential liability of the manufacturers and technology developers will likely increase, while the liability of individual drivers will likely decrease. The allocation of liability among the potentially responsible actors can be difficult to determine when different technologies interoperate to collectively create an autonomous experience. For example, if an accident occurs in an auto manufacturer's self-driving vehicle that drives on a rideshare app's network and accepts data through a "SMART" city's connected road infrastructure, then liability will likely hinge on identifying which elements contributed to the accident amid this technological chain. Under these circumstances, insurance must evolve to cover the potential liabilities faced by all these new players in the industry, including suppliers of new technologies, digital services, and infrastructure developers.

Importantly, the risks posed by autonomous vehicles are not limited to traffic accidents. The sensors in autonomous vehicles constantly collect data and maintain identifying information about passengers and owners. Vehicles track individual drivers' safety habits and entertainment settings, as well as their movements and whereabouts. Voice recognition technologies used to operate the vehicle may also enable the vehicles to capture private communications by passengers. In addition,

technology now allows vehicles to download and use the owner's contact lists and social media accounts. Businesses and advertisers will surely capitalize on the ability to track passengers' personal interests and daily routine. Exposure of this sensitive information poses a number of risks for passengers—from embarrassment, to identity theft, to potential bodily injury if location data become accessible to stalkers or other wrongdoers. And if private user data are exposed on a large scale, then companies may face the risk of data breach response costs and regulatory sanctions.

Minimizing Liability Before It Occurs

For centuries, insurance has made innovation possible by spreading risk and protecting against injury and damage. Effective insurance programs can likewise be a foundation and facilitator for further innovation in the era of autonomous vehicles.

Auto manufacturers, service providers, technology-platform developers, transit authorities, and businesses developing and selling AI and UVS technologies have a number of options. These players will need to look to broader commercial auto and liability insurance options to help minimize the potentially crippling costs caused by autonomous vehicle mishaps. However, in doing so, policyholders are well-advised to reconsider common policy exclusions that may limit, inappropriately, the protection innovators need. For example, traditional weather-related policy exclusions may need revision to account for the effects weather may have on sensors or cellular signals.[1]

In addition, traditional auto policies contain audio, visual, and data/electronic equipment coverage exclusions originally devised to limit coverage for sound systems and communications devices.[2] Likewise, other traditional insurance products may not respond to risks arising from the collection of data and personal information[3] or the processing of credit-card or other financial data.[4] In fact, even today, very broad "Y2K exclusions" find their way into some final policies, with terms that create gaps in coverage large enough for an "autonomous Mack Truck." Because visual and data signals are critical components of autonomous vehicles and UVSs, businesses should be sure to negotiate exceptions to these exclusions in order to preserve necessary coverage.

Given the increased risk of hacking or other exposure of private data transmitted using autonomous vehicle technologies, the developing AI and UVS industries will require other coverages that previously played no role in the automotive industry. Relying only on traditional commercial general liability insurance will likely leave significant coverage gaps for autonomous vehicle businesses that rely heavily on data transmission and processing.[5] Dedicated cyber liability, crime, and related coverages can provide necessary protection against liability to cover dishonest third-party acts, such as employee theft, forgery or alteration, computer fraud and funds transfer fraud, and cyber extortion.[6] Because the policies written for these coverages, unlike those providing commercial general liability (CGL) and first-party property insurance, are not at all "standardized," careful consideration of their terms, and possible "gaps" between such coverages, is essential. Businesses and others also need to consider whether addition of social-engineering[7] and kidnap and ransom coverage may be necessary in order to protect against the constantly evolving risks.

Increasing reliance on AI and other such technologies also creates prospects for liability from system failure and outages. Businesses exposed to these risks should consider whether their property and related coverages are prepared to respond. For example, appropriately structured business-interruption coverages can protect against cyber events that cause outages or interruptions in autonomous vehicles' delivery and transportation schedules even when there has been no actual physical damage to the vehicles (and certainly when there has).[8]

Additionally, companies will want to carefully consider supply-chain risks posed by UVS's component parts, products, and suppliers. To that end, companies can consider purchasing product liability and recall insurance to cover liabilities associated with the technical components of autonomous vehicles, such as faulty sensors and communications devices.

Finally, given the significant media attention on the autonomous vehicle industry, companies should consider coverages for reputational or business-income losses that stem from accidents, recalls, hacking, or other unanticipated events and risks. These consequential losses arising from highly publicized autonomous vehicle accidents may not be covered as under basic cyber and related coverages.[9]

New Insurance Products

The insurance industry already is offering new specialized policies for autonomous vehicles. In 2016, U.K. insurer Adrian Flux introduced the first "driverless car" insurance policy. The Flux policy provides limited coverage for losses arising from hacking or attempted hacking of vehicle software, as well as losses arising from collisions caused by a failure to install updates to the car's operating systems within a certain period of time. The Flux policy covers losses from satellite failures or other outages that affect technical navigation systems. Other companies are also selling driverless car insurance with their vehicles. Tesla, for example, has bundled QBE-provided insurance along with the driverless cars it sells in Asia and Australia.

These new insurance products are tailored to individuals who own semi-autonomous cars. As a result, this may not be the right product for businesses in these developing industries. Companies operating autonomous vehicles, third parties that develop technologies or services that provide information or commands to the vehicles, or developers of connected road infrastructure need to consider proposed policy terms carefully. These organizations should consider broader commercial auto

and liability insurance, and possibly other new insurance options, to cover the cyber, product liability, business-interruption, and reputational risks described above. Although the market offers insurance options to help cover these risks, we expect insurance companies to begin offering more specialized products aimed at companies that provide technologies and services that interoperate with autonomous vehicles. All of those new products will require analysis of the coverage offered and how the terms of those policies may be affected or interact with traditional insurance concepts and policy terms.

New Insurance Paradigms

Autonomous driving technologies may first take hold in specific industries, such as rideshare operations, trucking companies, and delivery services. These services will likely need a new paradigm in vehicle insurance and protection. For companies in these spaces, a reconfiguration of existing forms of commercial auto insurance may be key, but with an ongoing focus on insuring the heightened risks that may develop as the software becomes the "driver." For example, accidents may decrease in frequency but could still rise in severity, as connected cars rely on technology that primarily anticipates foreseeable situations. Coverages also may need to be flexible to account for the possibility of driving on roads that are not equipped or are less equipped to support autonomous vehicles. Similarly, first-party insurance or auto insurance coverages may need to be restructured to address higher maintenance and repair costs associated with the more complex component parts of autonomous vehicles.

As ownership of vehicles loses its importance and consumers and companies instead begin relying on commercial providers of autonomous vehicle fleets and transportation systems, the need for broader, multifaceted, and more creative commercial auto and liability insurance options will increase. For these providers, along with the manufacturers and technology developers that control the vehicles, additional types of liability insurance will be critical to cover risks posed by vehicles operating under Level Four autonomy. As discussed above, product liability, recall, cyber liability, business-interruption, contingent business-interruption, and reputational loss coverages should all be considered as part of a company's insurance framework. Companies should also explore other creative solutions, such as captive insurance and Insurtech options that can be tailored toward their particular products, services, and risk profile.

All of these coverages will be important to the industry sector. However, those who create and implement public policy should consider the ramifications of these technologies for both the insurance and the developing UVS and technology industries that support UVSs. In this "fourth industrial revolution," insurance can, as it has in past such revolutions, be part of the engine of change and innovation.

* * *

Autonomous technologies promise to change driving as we know it. Many businesses are sure to thrive on the efficiencies that driverless vehicles bring. Nevertheless, embracing autonomous technologies also can create new cracks and potholes in traditional risk management frameworks. Experienced coverage counsel can advise on how to fill those gaps—including by analyzing policy language in light of new risks and partnering with brokers to negotiate endorsements to fit a company's unique needs. ◆

Endnotes

1. *See* Small v. King, 915 P.2d 1192, 1193 (Wyo. 1996) (no coverage under CGL policy due to exclusion for weather-related damage).

2. *Cf.* Md. Cas. Co. v. Integration Concepts, Inc., 119 F. Supp. 3d 1322, 1328 (S.D. Fla. 2015) (electronic data exclusions barred coverage for bodily injuries from defects in software designed to conduct flow measurements); Clark v. Clarendon Ins. Co., 841 So. 2d 1039, 1044 (La. Ct. App. 2003) (excluding coverage for losses to CDs and cassettes under audio, visual, or data electronic devices exclusion).

3. *E.g.,* Innovak Int'l, Inc. v. Hanover Ins. Co., 280 F. Supp. 3d 1340 (M.D. Fla. 2017) (court rejected coverage under CGL insurance for disclosure of employees' personal information, including Social Security numbers, exposed as a result of software developed by the policyholder).

4. *See, e.g.*, Spec's Family Partners, Ltd. v. Hanover Ins. Co., No. H–16–438, 2017 WL 3278060 (S.D. Tex. Mar. 15, 2017), *reversed and remanded by* 739 F. App'x 233 (5th Cir. 2018) (insured's alleged liability to credit-card processor was not barred by exclusion in liability policy).

5. *See, e.g.*, Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., 103 F. Supp. 3d 1297 (D. Utah 2015) (court rejected coverage under cyber liability policy, finding that unauthorized withholding of data was not an "error, omission, or negligent act" as required under the policy).

6. *See, e.g.*, Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa., 691 F.3d 821 (6th Cir. 2012) (upheld coverage for millions of dollars of loss from data breach under crime policy); State Bank of Bellingham v. BancInsure, Inc., 823 F.3d 456, 460–61 (8th Cir. 2016) (upheld coverage for a hacking incident under a financial institution bond and rejected arguments that coverage did not apply because employee mistakenly left one of three security measures disabled and computers running overnight).

7. *See, e.g.*, Medidata Solutions, Inc. v. Fed. Ins. Co., 268 F. Supp. 3d 471 (S.D.N.Y. 2017), *aff'd*, 729 F. App'x 117 (2d Cir. 2018) (finding that manipulation of code in e-mail messages qualified as the kind of fraud necessary to trigger computer-fraud and funds-transfer coverage in crime policy).

8. *Compare* Am. Guar. & Liab. Ins. Co. v. Ingram Micro Inc., No. 99-185 (TUC/ACM), 2000 WL 726789 (D. Ariz. Apr. 19, 2000) (loss of computer data found to constitute "physical loss" to "tangible property" under general liability policy); *with* Vonage Holdings Corp. v. Hartford Fire Ins. Co., No. 11-6187, 2012 WL 1067694 (D.N.J. Mar. 29, 2012) (no coverage for business losses resulting from corruption of servers because no "physical damage" to "tangible property").

9. *See, e.g.*, P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., No. 2:15-cv-1322 (SMM), 2016 WL 3055111 (D. Ariz. May 31, 2016) (rejecting coverage for consequential damages resulting from hacking event under cyber risk policy).