LOS ANGELES
Daily Journal
www.dailyjournal.com
WEDNESDAY, NOVEMEBR 9, 2016

PERSPECTIVE

It's the end of [automobile insurance] as we know it

By Laurie Lo and Patice Gore

Many have predicted the rise of autonomous vehicles (AVs) will initiate the end of the automobile insurance industry. By eliminating the number one cause of vehicle collisions, driver error, AVs are expected to herald a golden age of vehicle safety and effectively eliminate automobile liability. However, the more likely scenario is that the automobile insurance industry will change as AVs become more commonplace.

One way the automobile industry may change is shifting its focus to addressing cybersecurity liability. With a high level of connectivity, AVs will be particularly vulnerable to cybersecurity issues and risks. A recent experiment is illustrative of the potential "hacking" risks of vehicles (both AVs and non-AVs). In July 2015, two researchers successfully hacked a Jeep Cherokee, a non-AV. The hackers used the vehicle's cellular connection to remotely access its internal computer network, allowing them to control the vehicle's physical components. The experiment conjures the once far-fetched idea of a machine run amok — transformed into a mobile weapon of destruction.

Automobile liability insurance policies typically cover liabilities arising out of the insured's ownership, maintenance, or use of a motor vehicle. Current automobile liability insurance policies are not tailored to address the unique risks carried by AVs, particularly cyber risks.

Ownership: Generally, an automobile liability policy covers liability arising from the insured's ownership of a vehicle. The cybersecurity risks associated with the ownership of an AV differ greatly from the risks of a conventional, non-AV. AVs require internet connectivity to maintain the functionality of the autonomous technology. Vulnerabilities, or security gaps can arise from this increased interconnectedness and can be exploited to create damage or injury. Ownership of an AV can expose the owner, and its insurer, to increased liability and costs as a result of a cyber-attack.

Shutterstock

With a high level of connectivity, AVs will be particularly vulnerable to cybersecurity issues and risks.

Maintenance: Automobile liability policies also cover an insured's liability arising from the vehicle's maintenance. AVs carry unique liability risks arising from the maintenance of, or failure to maintain, those vehicles. This is because AVs are primarily operated by a computer. Data recorded and collected from the operation of the AV is expected to be used by AV manufacturers and other groups, to develop software updates to improve the reliability and safety of AVs. These software updates will include security patches to address potential security vulnerabilities. If an owner fails to update the AV's software, the AV may be susceptible to a cyberattack. Additionally, the software updates could actually be used as a way to conduct a cyberattack. Consequently, the simple act of maintaining the AV may in fact create cybersecurity liability.

Use: Automobile liability insurance policies also generally cover liabilities arising from an insured's operation and the loading or unloading of an insured vehicle. AVs would not pose an additional risk with respect to the loading and unloading of the vehicle beyond a traditional vehicle, however, they do pose unique risks with respect to their "operation." Traditionally, the "operation" of a vehicle relates to the act of driving by a human operator. This does not apply in the AV context, where a computer, not a human, is expected to control the vehicle. Nevertheless, liability can arise from the "use" or "operation" of an AV in instances where the human operator or occupant should disengage the autonomous technology and take control of the AV. For a cybersecurity event, disengaging the autonomous technology may be needed in order to defeat the attack. However, some commentators have predicted that AV operators will be lulled into a false sense of security and will not be prepared to disengage the autonomous technology when needed. Human error, or inattention, will still be a source of automobile liability for AVs.

Insureds and insurers should consider the first-party and third-party coverages needed to fully address a potential AV cyber threat. First-party coverage will focus on the damage to the insured including physical damage to the AV as well as intangible damage, such as the insured's business interruption attributable to the cyberattack. Additionally, coverage for the costs of a forensic investigation to determine the cause and extent of the breach, and an appropriate solution to the security vulnerability will be an important aspect of AV insurance. Third-party coverage will focus on controlling and limiting liability exposures from the "machine run amok," which would include the defense of inevitable third-party lawsuits.

Insurers and insureds will also need to thoughtfully consider the potential exclusions which could minimize exposure with respect to AVs. Any insurance policy covering AVs should include an exclusion or condition of coverage aimed at sustaining a requisite level of maintenance of the AV's physical components and necessary software updates in order to ensure the safe operation of the AV. AV insurance policies will also need to address, either in the form of a policy condition or exclusion, the allocation of liability between AV manufacturers and suppliers and the AV operator or owner. Manufacturers and suppliers will presumably bear more responsibility as vehicle automation increases. Right now, both state and federal law do not sufficiently address how liability will be allocated between AV operators and manufacturers outside of the testing context. Nevertheless, insurers should be ready to align their products to reflect legal developments pertaining to AVs.

AV technology is developing more quickly than anyone can predict, and it will precipitate a change in all aspects of our lives, particularly insurance. Companies and individuals who intend to utilize AVs and the insurance companies who insure them should assess their risk management needs to make sure they are adequately protected in this rapidly growing area of automation.

Laurie Lo *and* **Patice Gore** *are attorneys with Haight Brown & Bonesteel LLP, one of California's leading law firms since 1937. Lo and Gore's practice focuses on risk management and insurance law. Lo can be reached at (213) 542-8064 or llo@hbblaw.com; Gore can be reached at (213) 542-8088 or pgore@hbblaw.com.*

LO

PATICE GORE