LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Autonomous Car, Drone Cos. Navigate New Compliance Risks

By **Linda Chiem**

Law360 (January 29, 2019, 3:12 PM EST) -- As self-driving vehicles and unmanned aircraft systems hit the nation's roads and skies, the companies, developers and other stakeholders invested in these new technologies are grappling with still-evolving safety and regulatory concerns that will open them up to new compliance and legal risks, like accident liability and data security.

Automakers and technology companies will have to figure out how to manage the treasure troves of information they'll collect on consumer behavior and preferences and examine what their liability risks might be as their self-driving cars and drones eventually go mainstream. Meanwhile, federal and state governments are still ironing out comprehensive rules for how to regulate self-driving or connected cars and drones, so there's quite a bit of murkiness when it comes to compliance, experts say.

Here, Law360 examines some of the compliance concerns linked to emerging technology in the transportation sector.

Self-Driving Cars

The U.S. Department of Transportation's National Highway Traffic Safety Administration has made it clear that it will take the wheel on developing safety standards for the design and performance of autonomous or self-driving cars, sometimes called automated driving systems.

NHTSA in October 2018 issued an updated policy, "Preparing for the Future of Transportation: Automated Vehicles 3.0," on how auto manufacturers, technology giants, artificial intelligence developers and other companies should go about testing their automated car technologies before they make their debut on public roads.

"The first question you have to ask yourself, if you're in this space, is: What do I have to comply with and what regulations do I have to comply with?" Foley & Lardner LLP partner Jeff Soble told Law360. "What’s my capital investment to comply with them, and what's my return on my capital investment, considering that I don't know two years from now, or a year from now, whether those will change or [whether] there's any consistency?"

The AV 3.0 federal guidance is the starting point, experts say, offering additional regulatory clarity to companies, but notably steering clear of hard-line rules that might hinder the fast-evolving automated car technology. So there's been a dance between automakers that have long been accustomed to the rigid Federal Motor Vehicle Safety Standards, or FMVSS, and technology companies that are more used to freely designing products unencumbered by stringent federal rules.

"Technology companies often are quick to the market, they put technology out there and they understand they may have to send updates shortly thereafter to crack bug fixes and the like," Mayer Brown LLP partner Linda Rhodes told Law360. "Whereas an automotive manufacturer has a complete understanding of the NHTSA regulatory scheme and the need to design their vehicles for safety, so you have to develop relationships that are going to work on both sides."

It's something that regulators are getting used to as well.

"There are a lot of companies with no history with any of the automotive industry regulators who are now in this industry, so these tech companies are more willing to be disruptive in how they deal with regulators," Soble said. "The regulators are not necessarily used to that."

Another big compliance concern that autonomous vehicle manufacturers are wrapping their heads around is how to responsibly manage the mountains of consumer location and travel data that will be generated from the cars.

"You have new regulatory concerns because now you're collecting vast amounts of data combined with the mass computing power to fuel the industry to build the artificial intelligence and to really make autonomous vehicles successful," Rhodes said. "When you start putting this technology into a vehicle where you now have risk of physical harm to persons or even death, the consequences of not getting it right are much greater."

For now, companies in the self-driving car space are relying on best practices from The Automotive Information Sharing and Analysis Center, or Auto ISAC, the nonprofit information-sharing organization that is owned and operated by automotive manufacturers and suppliers.

"They have the insight and the technical expertise to develop practices that are going to work in real life," Rhodes said.

Given how quickly self-driving cars are being designed and developed, experts say cybersecurity and privacy will be key areas that regulators will focus their rulemaking efforts on in the future.

"It would not surprise me if we start to see the federal government move away from voluntary [guidance] to 'we need something more uniform here' across the nation so we don't have this sort of patchwork approach," Foley & Lardner partner Mike Overly said.

Drones

As the commercial use of unmanned aircraft systems, or drones, expands in the U.S., drone manufacturers and operators are still pinpointing what their product liability risks are, what safety standards they have to follow and what limits are placed on their drone flights and operations.

The federal government has addressed at least some of those legal questions with rulemaking from the Federal Aviation Administration, which finalized a rule in June 2016 governing the commercial use of small drones weighing up to 55 pounds. That rule, known as Part 107, took effect in August 2016 and established a set of guidelines for drone operations, but prohibits drone flights over people, nighttime operations and flights that aren't within an operator's visual line of sight, among other restrictions. Operators can apply for waivers from those restrictions.

The FAA is currently working on finalizing new proposed rules that could be released in 2019. They include rules concerning the remote identification and tracking of drones in flight and rules allowing for drone flights over people and at night.

Earlier this month, the FAA said it was preparing to publish a notice of proposed rulemaking that for the first time will allow drones to fly over people or at night without having to obtain a special waiver. But officials said the rules allowing those additional drone operations are contingent on the FAA finalizing another set of regulations to remotely track and identify drones, which the industry considers essential for keeping tabs on drone users and curbing any rogue or illicit activities. The remote ID rule is still in the works.

Additionally, a White House drone integration pilot program — 10 state- and local-backed projects testing different ways for flying drones — is expected to generate more data for regulators on alternative uses for drones.

Drones are currently being used for limited commercial purposes that include media and entertainment, energy, agriculture, real estate, telecommunications, shipping, construction, and disaster aid and recovery efforts. It's important for companies to get familiar with various drones to be sure they're the right models for any given task or operation, experts say.

"It's not a one-size-fits-all, so it's making sure the aircraft is tailored to the specific operation you're doing and doing your due diligence on that," Jennifer Richter, a partner with Akin Gump Strauss Hauer & Feld LLP, told Law360. "We know that a lot of contractors out there are using recreational drones that you can just buy off the shelf … [but] we like to suggest that that is not commercial-grade and that really needs to be rethought."

For example, recreational drones aren't designed with the security and reliability that's needed of a drone flying over critical assets such as pipelines or transmission lines, Richter explained.

"Many types of recreational drones are operated on unlicensed bands, which aren't secure. You can lose link and lose your drone and if it crashes into your infrastructure, whatever that might be, that's a problem for you," she said.

It's also important for companies to have the right operational plans and manuals in place, running through those plans for any given task or mission using the drone, and getting their IT departments involved early on to work through privacy and data security practices concerning data collected from the drone, Richter said. That includes figuring out what to do with data, especially if the information happens to be personally identifiable, and assessing whether there's enough server or cloud capacity to store that data.

A solid resource is the U.S. Department of Commerce's National Telecommunications and Information Administration, which came up with best practices addressing privacy, transparency and accountability issues related to the commercial and recreational use of drones.

"If you have corporate data policies, corporate privacy policies, those are the sorts of considerations that one needs to think through where you don’t necessarily need to write a privacy policy that’s specific just to drones. It’s more so just about the data that the drones are collecting," Akin Gump senior policy adviser Mark Aitken said.

--Editing by Pamela Wilkinson and Katherine Rautenberg.