JONES DAY

MARCH 2017

COMMENTARY

Automated Vehicles Will Revolutionize the Automotive Industry

But Survival of this Magnificent Technology Will Require the Creation of Robust Best Practices to Protect Against Inevitable Attack by Potential Third Parties Who Prey on Visionaries

A renaissance of epic proportion is quietly underway in the United States, where 4,000-pound objects will soon be motoring alongside us on freeways, through intersections, crosswalks, and school zones without a driver. Ground zero for this marvel centers around the creation of digital hardware and associated software that will propel these vehicles among us, while simultaneously increasing safety and roadway efficiency. It will herald a fundamental change in how our society functions, similar to the creation of the automobile, airplane, and cell phone. The U.S. government, noting that 94 percent of fatal road accidents—killing 30,000 people annually—are caused by human choice or error, sees "great potential" in this new frontier to save lives. In fact, the U.S. Department of Transportation ("DOT") has defined autonomous vehicles as "the archetype of our future transportation."

Labeled "highly automated vehicles" ("HAV") by DOT, these vehicles will operate through a network of highly sophisticated technology carefully developed by reputable manufacturers who see the vision of the future. California, Michigan, and other states will play a significant role in the development of HAVs; as of February 9, 2017, the California Department of Motor Vehicles ("Cal. DMV") has issued autonomous vehicle testing permits to, among others, Volkswagen, Mercedes Benz, Google, Delphi Motors, Tesla, Bosch, Nissan, General Motors, BMW, Honda, and Ford. Several other states have raced to follow suit with similar legislation, passing preliminary regulations governing the testing of HAVs. California, however, will no doubt play a significant role in paving the way for safe HAV testing and deployment, and Cal. DMV has already taken steps to do so. Effective September 16, 2014, it successfully passed regulations governing the testing of HAVs. (See California Code of Regulations, Title 13, Division 1, Chapter 1, Article 3.7).

Federal and State Regulations Remain Inadequate to Protect the Industry

While manufacturers are anxiously working to deploy HAVs, California has not yet passed (but has carefully

proposed) regulations governing deployment. These regulations are currently undergoing intense scrutiny by the public, public interest groups, and the automotive industry at large. Cal. DMV's proposed regulations are in turn heavily influenced by the National Highway Traffic Safety Administration's ("NHSTA") recent release of its "Federal Automated Vehicles Policy" ("Policy"). NHSTA enthusiastically defines its Policy as "(a)ccelerating the next revolution in roadway safety." The Policy also adopts autonomous vehicle categories created by SAE International ("SAE") based on the level of interaction of the driver. For example, SAE Level 1-2 defines semi-autonomous vehicle interaction ("AV") where the *driver* maintains primary responsibility for monitoring the driving environment. DOT classifies HAVs as those utilizing technology within SAE Level 3-5, where automated technology primarily controls the operation of the vehicle. The Policy offers a 15-point guidance recommending best practices for the "pre-deployment design, development and testing of HAVs." However, *no* federal regulations yet exist pertaining to testing or deployment. The space is literally that new, evolving right before our eyes.

The Short Term May Be the Most Dangerous for Industry

However, like releasing baby seals into the ocean, those with fins on their backs await. It is imperative that general counsel of the automated car industry ready for the potential onslaught of litigation that may follow after the first HAV makes a misstep. Ironically, greater product liability risk likely exists with the implementation of *lesser* automated technology that is set to enter the market first. How can this be? While industry is quickly evolving HAV technology, our government(s) have assumed the seemingly practical approach of requiring that industry first develop, test, and then safely implement AV technology. That is, technology where the automobile can operate without the active interaction of a driver, *but where* the driver may (must) retake control when an emergency occurs. Cal. DMV (as an example) is not yet ready to allow fully autonomous HAVs on its roadways, and it has excluded them from its draft regulations. This has led to an interesting and dangerous paradox: while AVs will first take to the roads—relying on a human driver to intervene when the automated system so needs or requests—that technology requires the human driver to be attentive, but reliance on automated systems may create the *opposite* effect.

Industry sources have thus expressed concern that this initial phase of automated development may actually be the most dangerous period for this technology. In a recent study by Stanford University, the authors questioned whether semi-autonomous vehicles are sustainable, because as drivers become more confident in autonomous systems, they are less likely to pay attention and may become even more dangerous than those who do not use such systems. On June 30, 2016, Joshua Brown was killed as he allegedly watched a Harry Potter movie while relying on Tesla semi-automated technology. The technology did not stop his vehicle, and Mr. Brown's vehicle struck a flatbed truck that had turned in his path. Mr. Brown could have taken control, but his reliance on the technology took his eyes and attention from the road.

Lawsuits Are Inevitable, but Industry Has the Luxury (for Now) of Anticipating Them

Further accidents like this are inevitable as this new frontier is further developed and explored. And, human error is but one pitfall facing the future of automated vehicles. Thieves and terrorists also join the mix. Consequently, cybersecurity measures appear in DOT's and Cal. DMV's guidance (and proposed regulations) as well. HAVs will present two new avenues for cyberattack: the theft of abundant personal information contained within these highly sophisticated vehicles and hacking designed to disrupt, incapacitate, or even crash HAVs as a basis for coercion, ransom, or just to harm others. Criminals are likely already plotting to steal data from or commandeer automated vehicles. But NHSTA is wary of this intent. Just months ago, it released further guidance for industry with its publication "Cybersecurity Best Practices for Modern Vehicles." The government's guidance urges manufacturers to develop technology not just to identify cyberattacks but, where such attacks are successful, to develop mechanisms for immediate response, mitigation, and resumption of control.

NHSTA Guidance Will Protect Industry but May also Define the Battlefield for Litigants in the Future

Enter now, stage left, two of the most popular "vehicles" for class action lawsuits that likely await the launch of automated vehicles: product liability and cybersecurity-based claims. How can general counsel prepare their companies

from these inevitable attacks made by those looking to exploit the technology for potential gain? In this instance, a litigation avoidance strategy to protect AVs and HAVs is, for many companies, a matter of first impression. Counsel must therefore envision and anticipate the bases for the attack(s) and create a robust internal protocol that relies on the Policy, which in turn complements the Federal Motor Vehicle Safety Standards and is furthered by NHSTA advice on cybersecurity.

The federal government's guidance on operational design, object event detection and response, fallback response, post-crash behavior, and validation methods should form the templates upon which industry can rely—if they comply. The government is expecting from industry detailed processes and plans pertaining to each of its guidance points and will request manufacturers' written compliance with them. Corporations that push down (and ensure compliance with) these requirements throughout the relevant sectors of their AV and HAV programs will best defend against later efforts against them to establish negligence.

Plaintiffs' lawyers will be looking at the same guidance to find oversights to exploit in the courtroom. An example: NHSTA recommends that manufacturers create a "documented process" for testing, validation, and collection of events, incidents, and crash data to improve the technology. Cal. DMV will also require this transparency from manufacturers prior to permitting HAVs to operate on its roads. Plaintiffs' lawyers will search for failure(s) to adhere to guidance like this and use it as a basis to establish negligence with a manufacturer's crash avoidance or cybersecurity systems. Robust compliance by manufacturers will have the opposite effect, and *help* insulate them from harm.

General counsel involved in the development and sale of AVs and HAVs have thus found themselves in the enviable and exciting position of becoming the gatekeepers for the most significant development in transportation since the creation of the automobile itself. The future explosion of this technology into taxi cabs and 18-wheelers, and to help our disabled and elderly who can no longer drive, is limitless. But industry must not let automated vehicle technology face the litigation challenges that contributed to the demise of three-wheeled off-road motorbikes in the 1980s, or the more recent misguided attack(s) on compact recreational off-highway vehicles that have redefined off-roading. Planning ahead will be key.

Conclusion

Legal departments of the automated vehicle industry are strongly encouraged *now* to take on the complex task of devising, implementing, monitoring, and enforcing internal protocols and procedures that mirror the guidance by NHSTA (and others) and will form the tools for outside counsel to successfully defend this marvelous industry when the time comes.

Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

Paul F. Rafferty
Irvine
+1.949.553.7588
pfrafferty@jonesday.com

Jeffrey J. Jones
Detroit/Columbus
+1.313.230.7950/+1.614.281.3950
jjjones@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Charles H. Moellenberg Jr.
Pittsburgh
+1.412.394.7917
chmoellenberg@jonesday.com