HWG | HARRIS, WILTSHIRE & GRANNIS LLP

CLIENT ADVISORY
SEPTEMBER 2016

DOT RELEASES REGULATORY FRAMEWORK FOR AUTONOMOUS VEHICLES

Brita Strandberg, V. Shiva Goel and Michael Carlson

On September 20, 2016, the Department of Transportation (DOT) released the first edition of its Federal Automated Vehicles Policy (the "Policy"). The Policy attempts to translate the many legal questions surrounding highly autonomous vehicles (HAVs)—including driverless cars—into "early guidance" for auto manufacturers, technology companies, ridesharing services and others involved in the development, use and delivery of HAV systems. DOT seeks comments on the Policy and expects to revise it annually. Comments are due November 22, 2016.

As reported in the press and introduced by President Obama, the Policy warmly welcomes HAV deployment. DOT clearly understands the value of HAV systems and their ability to bring transformative improvements in safety, mobility and efficiency. Underscoring the cordial reception is DOT's decision not to propose prescriptive rules at this time. In fact, by publishing a model state policy for oversight of HAV systems, DOT hopes to reduce regulatory barriers by promoting uniform nationwide rules of the road.

Nevertheless, it would be a mistake to ignore the regulatory implications swept beneath the agency's red carpet. As DOT explains, the Policy will serve as "a foundation and framework upon which future Agency action will occur." The Policy is also sure to impact the regulatory initiatives of other agencies. As the Nation's primary transportation regulator, and as the first-mover in establishing a comprehensive federal policy, DOT maintains a strong position of influence over officials within the Federal Communications Commission (FCC), Federal Trade Commission (FTC), Department of Energy (DOE), and other agencies that will shape the legal landscape affecting HAVs.

Summary of the Policy

The Policy contains four parts:

- Vehicle performance guidance, which includes a 15-point safety assessment covering crashworthiness, cybersecurity, privacy, data recording and sharing, the human machine interface, ethical dilemmas, and other areas.

- A Model State Policy designed to promote interstate travel and minimize burdens on HAV manufacturers, while also recognizing the role state and local governments will serve to regulate traffic, licensing and registration, insurance and liability.

- Guidance on the current regulatory tools of the National Highway Traffic Safety Administration (NHTSA, a DOT department), including exemptions, letters of interpretation, rulemakings, recalls and enforcement actions.

- Discussion of new regulatory tools and authorities, including pre-market review and approval, post-sale software regulation, cease-and-desist orders, expanded exemptions, record-keeping and reporting requirements, and enhanced data collections.

Concerns for Manufacturers, Technology Companies and Telecommunications Providers

Our initial review of the Policy raises a number of key questions for industry, a few of which we discuss below. Critically, the Policy also makes clear that DOT regulatory actions could affect companies that do not typically engage with DOT or its departments, including technology and telecommunications companies whose platforms power existing telematics systems and will serve as the backbone of tomorrow's connected vehicles.

Privacy, Data Security and Cybersecurity

- Will DOT choose to adopt substantive privacy, data security, and cybersecurity requirements? If so, will auto manufacturers, ride-sharing companies, telecommunications providers, and technology companies face overlapping—or worse, conflicting—requirements?

Acknowledging the value of machine learning, the Policy strongly encourages that HAV systems collect, record, and share data for operational, testing, event reconstruction, and other purposes. At the same time, the Policy calls for the protection of such information and urges companies to ensure that data is collected, recorded, stored and shared "in accordance with privacy and security agreements and notices applicable to the vehicle." But the Policy does not stop there. It goes on to identify the substantive elements DOT would like to see in HAV-related privacy practices, including transparency, consumer choice, and contextual use limitations.

In addition, the Policy encourages companies handling HAV data to adopt minimization and de-identification practices, ensure appropriate levels of data security, maintain data integrity and consumer access to data, and promote accountability through audits and evaluation. The Policy also recognizes the cybersecurity threats posed by connected cars, and encourages companies to address vulnerabilities by incorporating design principles published by regulators, industry groups and standards-setting bodies.

DOT's attention to privacy, data security, and cybersecurity issues raises the prospect of having yet another regulator on the loose—and complicating efforts to leverage HAV data for beneficial ends. Right now, auto manufacturers that self-provision or resell wireless communications services may be subject to regulation by the FCC, whose Chairman has emphasized the need to promote cybersecurity for 5G wireless applications, including "autonomous vehicles." At the same time, companies other than auto manufacturers—such as the telecommunications and technology platform providers that make the Internet-of-Things work today—are likely to handle HAV data. As a result, all of these companies may find themselves forced to comply with both FCC and DOT directives, either directly as a result of their participation in HAV or telecommunications service delivery, or indirectly by contract. In addition, the FTC, which published an Internet-of-Things report in 2015 highlighting the privacy and cybersecurity implications of connected vehicles, will provide an overlay of regulatory authority where it has jurisdiction.

Note, however, that the present landscape remains incredibly dynamic—and could be modified heavily by Congress before DOT steps in (if it chooses to do so). Indeed, the SPY Car Act, which aims to require the FTC and the DOT (through NHTSA) to establish uniform privacy and network security rules for motor vehicles, is currently in committee.

Production v. Testing

- Will DOT provide sufficient flexibility to develop and test HAV systems and components without facing heavy regulation?

To promote innovation, legal regimes must minimize regulatory burdens during the design and testing phase of production. DOT suggests that agencies should distinguish between HAV systems in "testing" and HAV systems in "production" on the basis of whether an employee or agent operates the vehicle—which may not account for all necessary testing scenarios.

Accessibility Obligations for Target Beneficiaries

- Will DOT adopt affirmative accessibility requirements?

As the Policy recognizes, HAVs stand to revolutionize mobility for disabled and elderly populations. Accordingly, "DOT encourages manufacturers and other entities to consider the full array of users and their specific needs during the development process." If this encouragement evolves into hard requirements, regulated entities will need to ensure that the rules provide sufficient flexibility to serve all populations without compromising the design of HAV systems.

Software Updates and Red-Tape

- Would DOT's safety assessment program, and post-sale regulation of software, discourage over-the-air updates to HAV systems and their components?

The Policy asks companies to submit a voluntary 15-point safety assessment documenting their efforts to ensure HAV safety. Critically, DOT recommends that a manufacturer or other regulated entity submit a new assessment with every "significant update" to a vehicle or HAV system. A "significant update" includes "software or hardware updates" that "materially change" the way in which the vehicle complies with any one of the 15 elements of the proposed safety assessment. DOT also asserts that it has existing authority to regulate software changes affecting compliance after vehicles enter the market.

Prompt over-the-air updates are critical to improving user experience, safety and security, and will be essential to the HAV technologies developed by carmakers, transportation service providers and network operators. Companies that participate in the safety assessment or are regulated by motor vehicle safety standards—and suppliers that sell services to those entities—will want to ensure that agency rules and procedure accommodate these updates.

* * * *

For more information on the regulatory landscape affecting autonomous vehicles, please contact Brita Strandberg (202 730-1346), V. Shiva Goel (202 730-1304), Michael Carlson (202 730-1331) or the HWG lawyer with whom you regularly work.