DOT AND NHTSA RELEASE REVISED FRAMEWORK FOR AUTOMATED VEHICLES

Brita Strandberg, V. Shiva Goel, and Michael Carlson

Last September the federal Department of Transportation ("DOT") and National Highway Traffic Safety Administration ("NHTSA") released the first edition of their Federal Automated Vehicles Policy.

Version 2.0 hit the web on Tuesday. Dubbed *A Vision for Safety*, the new release continues to keep federal policy in beta mode—for now—by providing guidance rather than prescriptive regulation.

Think of the 2017 model as a mid-cycle facelift, not a redesign.

It continues to encourage companies to conduct a multi-point voluntary safety assessment unique to automated driving systems. It also continues to strictly divide state and federal responsibilities over regulation. Consistent with DOT's 2016 guidance, and the preemption provisions of the SELF-DRIVE Act passed by the House last week, the new guidance urges state officials to focus on insurance, licensing, and vehicle registration—and to leave safety design and performance considerations to DOT alone.

Comments on the new policy are due 60 days following publication in the Federal Register, or **November 14, 2017**, assuming the guidance is published tomorrow as expected.

A Less Regulatory Approach Under the Hood

Despite its resemblance to the 2016 policy, *A Vision for Safety* upgrades to a slimmer form factor in several key respects.

- **Safety assessment letters**. The 2016 guidance encouraged companies to comply with a voluntary safety assessment by submitting Safety Assessment Letters ("SALs") to NHTSA. But the old policy blurred the line between guidance and regulation by (1) encouraging states to require the submission of an SAL before permitting the testing and deployment of automated driving technologies, and (2) committing to initiate a rulemaking that would transform the voluntary assessment into a hard requirement.

  The new guidance eliminates both of these elements. More emphatically than before, DOT and NHTSA stress that their voluntary safety assessment remains just that—voluntary—and carries no expectation of agency review or submission.

  Of course, the new policy's lighter touch may not stop Congress from requiring a more regulatory approach in relatively short order. The House version of the SELF-DRIVE Act

would direct NHTSA to mandate safety assessment certifications within two years, and require companies developing automated driving technologies to submit less detailed SALs in the interim.

- **Privacy and data use**. The 2016 guidance devoted an entire component of the voluntary safety assessment exclusively to privacy matters. The new guidance eliminates privacy from the voluntary safety assessment completely. It also limits NHTSA's focus on data recording to crash data only, encouraging carmakers to collect and share collision information to improve automated driving technologies and facilitate emergency response in the event of an accident.

  NHTSA still encourages developers of automated vehicle systems to follow best practices on cybersecurity, which remains a part of the voluntary safety assessment, and builds on the agency's general cybersecurity guidance for all "modern vehicles," automated or not.

  The agency may revisit its approach to privacy and data sharing in the future. In the meantime, look for the FTC to step in, buoyed by its existing competence, recent selection as the primary vehicle privacy regulator under the current version of the proposed SELF-DRIVE Act, and existing powers to enforce privacy policies, including the Privacy Principles for Vehicle Technologies and Services adopted by leading automakers. States may enter the arena as well, although they are likely to proceed with caution in light of California's failed attempt to regulate vehicle data privacy in 2014.

- **Ethical considerations**. NHTSA eliminates ethical considerations from the voluntary safety assessment, citing the lack of consensus and poor understanding of the dilemmas raised by automated vehicles.

- **New statutory authority**. The 2016 guidance called on Congress to complement NHTSA's existing recall authority with expansive new powers, including the power to require pre-market approval of automated driving systems. The new guidance, however, eliminates the NHTSA's requests for expanded regulatory authority.

Communications and Information Technology Suppliers: Get Ready to Adapt, Especially on Privacy, Data Security, and Cybersecurity

Although DOT eased off the gas for 2017, it would be a mistake to assume that the new guidance signals a laissez-faire attitude toward the serious legal and policy concerns raised by automated vehicles. DOT's light-touch approach more likely reflects the agency's recognition that no one in government fully understands the problem before them, and that early-stage regulatory misfires could stall progress in a rapidly emerging part of the economy.

But a tipping point that favors rules over guidance may arrive soon enough. And given the prevalence of vehicle telematics systems today, regulators may act on rules to govern all connected cars, automated or not, well before they adopt specific provisions to regulate automated vehicles.

When new rules of the road do hit the market, their impact almost certainly will extend far beyond traditional carmakers and their original equipment manufacturers. Companies that provide connectivity, software, and IoT device management solutions easily could be swept in, too, especially on privacy, data security, and cybersecurity matters.

For example:

- The new automated vehicles policy encourages all "[e]ntities involved" with automated driving systems, and not just carmakers, to address vehicle cybersecurity by adopting a "coordinated vulnerability reporting/disclosure policy."

- Likewise, NHTSA's 2016 cybersecurity guidance for all modern vehicles expressly addresses the need to exert "fine-grained" control over a vehicle's access to wireless networks. It also addresses the need to control communications to back-end servers, and to limit access to vehicle control units, including the ECU. These and other cybersecurity best practices could affect how connectivity and IT suppliers design, sell, and integrate their products.

- In its current form, the proposed SELF-DRIVE Act would direct the FTC to broadly examine privacy policies for *all* entities in the automated vehicle "ecosystem"—not just automakers.

- This past June, NHTSA and the FTC convened a joint workshop on connected car privacy and data security issues, which explicitly explored the privacy practices of both automakers and their service providers. These workshops typically lead to agency staff reports, which can be highly influential in shaping emerging industry and regulatory norms.

- The proposed Spy Car Act, introduced in the Senate in 2015 and reintroduced just last March, would require all "driving data" to be "reasonably secured"—not just onboard the vehicle, but when "in transit" and "in any subsequent offboard storage or use."

The uncertain regulatory environment facing automated and connected vehicle technologies may invite a wait-and-see approach, especially from suppliers. With new rules potentially just around the corner, however, companies may be better served by building capacity early, monitoring developments closely, and negotiating flexibility or assigning risk appropriately in potentially affected long-term agreements.

* * * *

For more information on the regulation of connected cars or automated 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.

This advisory is not intended to convey legal advice. It is circulated to our clients and friends as a convenience, and is not intended to reflect or create an attorney-client relationship as to its subject matter.