April 1, 2021

James C. Owens
National Highway Traffic Safety Administration
1200 New Jersey Avenue SE
Washington, DC 20590

RE: Comment on the Proposed Framework for Automated Driving System Safety [Docket No. NHTSA-2020-0106]

Dear Mr. Owens:

The National Highway Transportation Safety Administration (NHTSA) on December 3, 2020, published an Advance Notice of Proposed Rulemaking (ANPRM) on the development of a regulatory framework for Automated Driving System ("ADS") safety. ADS presents a unique opportunity to transform the safety of America's highways. Like other highway safety benchmarks, such as those for safety belts and airbags, correctly implemented rules set reasonable limits and expectations for manufacturers. If these rules are established early in the research and development process, they will prevent unnecessary waste and ensure that ADS develops in a way consistent with overall safety goals. These rules should be tech-neutral, allowing manufacturers flexibility to meet safety benchmarks using their technological expertise. Perhaps most importantly, NHTSA must coordinate with other agencies to address the critical weak point of cybersecurity in ADS. Altogether, these focus points will coalesce into the development of an effective ADS regulatory framework that safeguards the safety and prosperity of the American public.

Background

NHTSA plays a critical role in the safety of America's roads. The Administrator of NHTSA is empowered to carry out "duties and powers vested in the Secretary [of Transportation] . . . ."[1] Part of those duties is "to prescribe motor vehicle safety standards for motor vehicles and motor vehicle equipment in interstate commerce . . . ."[2] Critically, this duty is prescribed through a "5-year plan for testing standards" and according to all relevant available safety information, and these standards may be developed in cooperation with other federal and state agencies, whether public or private.[3] Although this far-reaching mandate touches all aspects of vehicle safety, it has an important limitation stemming from the integration of computers with motor vehicles.

That shortcoming is in cybersecurity. As mentioned in the ANPRM, the Federal Trade Commission (FTC) takes primary oversight of privacy policy, including as it relates to cybersecurity. But privacy is only one aspect of cybersecurity, and other concerns in this realm may be of greater importance. Touching on those other aspects is the Federal Communications Commission (FCC), which is empowered to regulate "wire and radio communication,"

[1] 49 U.S.C. § 105(c).
[2] § 30101.
[3] § 30111(a)–(e).

including, in the modern context, network security.[4] The FCC coordinates with federal partners, state and local officials, and private industry to develop best practices for use in all aspects of internet safety and security.[5] This dispersion of authority on cybersecurity impacts accountability and uniformity, and will be a critical challenge for NHTSA regulation of ADS.

NHTSA Should Establish Tech-Neutral, Fleet-Level Standards to Guide ADS Development

Highway safety is a field that currently faces a critical juncture centered on the vehicle operator. Through the National Motor Vehicle Safety Act and its requirement of various safety devices, the survivability of motor vehicle crashes has increased considerably over the past few decades.[6] However, safety devices can only help when they are used by vehicle occupants, and their effectiveness drops dramatically when drivers choose to speed or otherwise operate vehicles recklessly.[7] Also, pedestrians and cyclists remain at extreme risk, regardless of whether distracted, reckless drivers wear a seatbelt.[8] In fact, even though traffic decreased during the COVID-19 pandemic by forty-one percent nationwide, and more than sixty percent in urban areas, remaining drivers contributed to a spike of over thirteen percent in traffic fatalities during the summer of 2020.[9] This unexpected break in correlation between fatalities to decreased traffic speaks to the poor decision-making made every day by the average driver. Although driver education can correct some of these bad behaviors, few drivers are willing to devote the time required to adequately complete the training.[10] Worse, between 2009 and 2013, inadequately prepared, drowsy drivers caused "over 72,000 police-reported motor vehicle accidents."[11] Ultimately, the safety achievements made with the use of devices such as seatbelts and airbags are threatened by the poor decision-making of the human at the wheel.

With careful application of engineering principles, ADS offers an option to correct this human safety limitation. Self-driving technology can be built into electric cars, gas cars, and even into tractor trailers.[12] Current iterations of this technology include a variety of sensors, including radar, lidar, suites of cameras, and ultrasonic obstacle sensors.[13] Onboard computers combine and analyze this data to produce a simulated representation of the world, which the computer

---

[4] 47 U.S.C. § 151; *Cyber Security and Network Reliability*, FED. COMMC'NS COMM'N, https://www.fcc.gov/general/cyber-security-and-network-reliability (last visited Apr. 1, 2021).
[5] *Cyber Security and Network Reliability*, *supra* note 4.
[6] *See Motor Vehicle Crash Deaths*, CTRS. FOR DISEASE CONTROL & PREVENTION (July 6, 2016), https://www.cdc.gov/vitalsigns/motor-vehicle-safety/index.html.
[7] *See id.*
[8] *See Take Steps to Avoid Injury or Death While Walking*, NAT'L SAFETY COUNCIL (2021), https://www.nsc.org/home-safety/safety-topics/distracted-walking.
[9] Jacob Baumgart, *Pandemic Revs Up Bad Driver Behavior in Maryland*, PATCH (Feb 12, 2021, 8:33 PM), https://patch.com/maryland/annapolis/pandemic-revs-bad-driver-behavior-Maryland.
[10] Andrew Emeonye, *Driver Education - Saving Lives Through Safe Driving*, DMVEDU.ORG (Mar. 28, 2021), https://www.dmvedu.org/drivers-ed-2021/driver-education/driver-education-saving-lives-through-safe-driving/.
[11] *Id.*
[12] See Michael Hicks & Michelle Fitzsimmons, *Self-Driving Cars: Your Complete Guide to Autonomous Vehicles*, TECHRADAR (June 7, 2019), https://www.techradar.com/news/self-driving-cars; Semi, Tesla (2021), https://www.tesla.com/semi.
[13] See *What is an Autonomous Car?*, SYNOPSYS (2021), https://www.synopsys.com/automotive/what-is-autonomous-car.html.

then uses to determine how to control the vehicle's steering, acceleration, and braking systems.[14] Each manufacturer implements these systems in varying ways, with some emphasizing, for instance, visual processing over radio ranging or vice versa. Each sensor has its strengths and weaknesses, but the overall system implementation is critical in determining the sensor's reliability. Although critics argue that current ADS have difficulty dealing with unusual driving circumstances, they acknowledge that driver assistance/replacement systems show great promise in preventing accidents that result from common situations like fatigue and distraction.[15] Also, in support of the comments submitted on the ANPRM by the League of American Bicyclists and its supporters, ADS can be implemented in a way that emphasizes pedestrian and cyclist safety, with consistency unachievable by human drivers alone. As such, the implementation of the system and its reliability should be the focus of NHTSA regulations, highlighting the need to achieve safety outcomes rather than limiting manufacturers to particular sensors.

Taking the system focus a step further, NHTSA must approach ADS not only at the vehicle level, but also at the fleet level. The vast data required to reliably implement ADS outstrips the available computing power onboard each vehicle, so manufacturers implement centralized processing systems to supplement vehicle processing.[16] Through artificially intelligent algorithms, these systems constantly train on real-world scenarios, improving vehicle performance across the fleet. As a result, NHTSA testing of vehicle performance cannot rely simply on a "crash test" model, where a single vehicle proceeds through each standard course of maneuvers.[17] Instead, NHTSA should develop a cooperative approach with manufacturers to provide oversight based on available fleet data. Realtime, aggregated performance data can be compared with safety benchmarks to verify achievement of milestones while preserving the anonymity of each customer. In fact, this approach would significantly enhance the picture of each vehicle's safety compared to reliance on only the "snapshot in time" available from the current "crash test" regime. Further, this constant oversight of fleet data would support the intent behind the comment to the ANPRM from the National Society of Professional Engineers, who contend that ADS data must be verified by third parties and approved through transparent decision-making. Availability of safety metrics based on actual operation would open a whole host of options for testing and verifying best practices and innovation in ADS technology. But while physical safety of vehicles is promoted through oversight of centralized data processing, NHTSA must also consider the resulting impact of modern cybersecurity threats attendant to the transmission of that data.

---

[14] See, e.g., *Future of Driving*, TESLA (2021), https://www.tesla.com/autopilot (visualizing the car's recognition of objects in the world, as compared to the driver's view); Dirty Tesla, *FSD Beta Gets Updated with V8.2 Software– First Impressions Downtown | 2021.4.11.1*, YOUTUBE (Mar. 5, 2021), https://youtu.be/EPg_mi15mls (demonstrating capability of the most-recent Tesla beta release of autonomous driving software, including many examples of reactions to poor human driving and degraded road infrastructure).

[15] See Peter Hancock, *Are Autonomous Cars Really Safer than Human Drivers?*, SCI. AM. (Feb. 3, 2018), https://www.scientificamerican.com/article/are-autonomous-cars-really-safer-than-human-drivers/.

[16] See Maarten Vinkhuyzen, *Tesla Dojo Supercomputer Explained—How to Make Full Self-Driving AI*, CLEANTECHNICA (Nov. 21, 2020), https://cleantechnica.com/2020/11/21/tesla-dojo-supercomputer-explained-how-to-make-full-self-driving-ai/ (describing Tesla's use of a supercomputer to process data from its global fleet of customer-owned vehicles).

[17] Nick Kurczewski, *NHTSA and IIHS Crash Test Safety Ratings Explained*, CAR & DRIVER (Feb. 27, 2021), https://www.caranddriver.com/features/g35634275/what-to-know-about-the-wrecks-behind-the-ratings-feature/.

NHTSA Must Coordinate Cybersecurity Efforts with Other Agencies

ADS operation requires consistent and secure communications between vehicles and fleet data processing centers, placing cybersecurity at the center of the ADS safety issue. The most important cybersecurity threat to ADS stems from the potential for malicious interference with the physical operation of vehicles.[18] Even simple systems such as basic vehicle telematics have been shown to present a route for hackers to take control of vehicles, even those that lack any advanced ADS at all.[19] But NHTSA lacks the authority or expertise to establish network security protocols. Instead, like tech-neutral rules for vehicle system design benchmarks, NHTSA should establish minimum-acceptable security concepts that rely on implementation under other-agency authorities.

Cybersecurity is a relatively new realm with shared responsibility among multiple federal agencies. The ANPRM acknowledges FTC's role in regulating privacy. To be sure, the ubiquity of location data and driving habits in ADS data raises privacy as a serious concern. But as discussed above, physical security stemming from cyber vulnerability is the primary concern in the ADS space. The agency with primary responsibility over network security, and therefore the one with the most experience in combatting this type of threat, is the FCC.[20] Unfortunately, even that agency approaches cybersecurity more generally, engaging in efforts such as spectrum availability for transportation and internet of things devices.[21] Since FCC's mandate is broader than transportation, its rules and policies do not adequately address the heightened threat of hackers taking control of vehicles, insertion of malicious code or bad data into control algorithms, or any number of other possibilities. As such, NHTSA must work with FCC and FTC, as well as with the experts employed by manufacturers themselves, to place greater emphasis on cybersecurity regulation.

Conclusion

America's highways are a dangerous place, resulting in far too many deaths due to distracted and drowsy driving. ADS promises a way to allow drivers to safely engage in activities other than driving. By implementing safety benchmarks in the current early phase of industry implementation and with input from manufacturers finding success on the bleeding edge of this technology, NHTSA has the opportunity to transform the safety of our roads.

Sincerely,

Kyle E. Durch

---

[18] *See* Rahul Razdan, *Tesla Decepticons? Is Automotive Cybersecurity a National Defense Issue?*, FORBES (May 2, 2020, 7:33 AM), https://www.forbes.com/sites/rahulrazdan/2020/05/02/is-automotive-cybersecurity-a-national-defense-issue-/?sh=245c3aea1b75 (recounting demonstration of hacker control of a Jeep through its telematics system).

[19] *See id.*

[20] See Jennifer Johnson & Thomas Parisi, *IoT Update: FCC Proposes New Spectrum Plan for Vehicle Safety and Unlicensed Uses*, INSIDE TECH MEDIA (Dec. 4, 2019), https://www.insidetechmedia.com/2019/12/04/iot-update-fcc-proposes-new-spectrum-plan-for-vehicle-safety-and-unlicensed-uses/.

[21] *Id.*