April 1, 2021

Sara R. Bennett, Attorney Advisor
c/o Docket Management Facility, M-30
U.S. Department of Transportation
West Building, Ground Floor, Room W12-140
1200 New Jersey Avenue SE
Washington, DC 20590

Re: Framework for Automated Driving System Safety, 85 Fed. Reg. 78058 (Dec. 3, 2020) [Docket ID NHTSA-2020-0106]

Dear Attorney Advisor Sara Bennett:

I am a current law student submitting comments in response to the request from the U.S. Department of Transportation, National Highway Traffic Safety Administration (NHTSA), on its Advanced Notice of Proposed Rulemaking to establish a safety framework, best practice, or a more formal regulation for Automated Driving System safety. I am writing this comment because it is clear that the automotive and technology industries will strive to develop and use Society of Automotive Engineers Automation Level 5 (full automation) on public streets, which we must keep safe.[1]

"RELIABILITY" SHOULD BE ADDED TO THE CORE ELEMENTS

This section proposes the addition of "reliability" to the NHTSA's four core elements for automated driving systems. In short, adding "reliability" will ensure that each of the NHTSA's four core elements *will* actually work under all circumstances by having redundant systems and a proper cybersecurity contingency plan.

The four core elements are indeed designed and considered to ensure public safety; however, as they stand right now, they are treated as separate elements of a whole. There needs to be something that explicitly brings all four elements together: "reliability." Adding the element of "reliability" to the NHTSA's core elements will explicitly help to ensure public safety through the use of redundant systems and a proper cybersecurity contingency plan.

[1] *Automated Vehicles for Safety*, NHTSA, https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety.

I. Redundant Systems

Sensors fail; whether they be vehicle oxygen sensors, tire pressure sensors, or even home security sensors.[2] Sensors fail. The reliability of sensors should be the number one priority of the NHTSA.[3]

Understandably, the NHTSA plans to have redundant systems for each of the four core elements; perhaps, by having a team responsible for redundancy within each of the four core elements. This comment proposes an oversight team that oversees each of the other four core elements. Having a dedicated team that ensures redundancy will not only help to ensure there are redundant measures for each sensor, but will also allow the coordination between core elements should a sensor fail to mitigate public safety concerns.

II. Safety-Related Cybersecurity Team

Although the NHTSA has contingency plans, such as fail-safe and limp-home modes, there is not much mention of a cybersecurity contingency plan.[4] Cybersecurity was mentioned in the form of privacy and reporting concerns, but only barely touched upon safety-related cybersecurity risks.[5]

Computers get hacked, the government gets hacked, and vehicles get hacked.[6] Hackers can jam the vehicle's signals, insert false inputs, or even directly control the vehicle.[7] As mentioned, "general privacy and cybersecurity unrelated to safety" do not fall under the NHTSA's authority, but safety-related cybersecurity risks do.[8] This comment proposes the NHTSA to create a safety-related cybersecurity team and to adopt the latest cybersecurity measures under the National

---

[2] *Sensors: When to Replace Them*, KNOW YOUR PARTS, https://www.knowyourparts.com/technical-resources/electrical/sensors-and-when-to-replace-them (referencing vehicle oxygen sensors); Lance B. Eliot, *Going Blind: When Sensors Fail on Self-Driving Cars*, AI TRENDS (May 23, 2017), https://www.aitrends.com/ai-insider/going-blind-sensors-fail-self-driving-cars (referencing tire pressure sensors); Krista Bruton, *Addressing a Sensor Failure*, BRINKS HOME (Sept. 22, 2020), https://brinkshome.com/smartcenter/addressing-a-sensor-failure (referencing home security sensors).

[3] *See* Eliot, *supra* note 2; Manish Gupta, *Self-Driving Cars: Reliability Challenges, Solutions, and Social Adoption*, DESIGN NEWS (June 22, 2018), https://www.designnews.com/electronics-test/self-driving-cars-reliability-challenges-solutions-and-social-adoption.

[4] 85 Fed. Reg. 78064; *see generally* Joao Salvado et al., *Contingency Planning for Automated Vehicles*, RSJ INTERNATIONAL CONFERENCE ON INTELLIGENT ROBOTS AND SYSTEMS (Oct. 9-14, 2016), https://www.researchgate.net/publication/312096989_Contingency_Planning_for_Automated_Vehicles.

[5] 85 Fed. Reg. 78064 (citing *Protecting Consumer Privacy and Security*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security).

[6] Roger A. Grimes, *15 Signs You've Been Hacked – And How to Fight Back*, CSO (Aug. 6, 2020), https://www.csoonline.com/article/2457873/signs-youve-been-hacked-and-how-to-fight-back.html; Isabella Jibilian & Katie Canales, *Here's a Simple Explanation of How the Massive SolarWinds Hack Happened and Why it's Such a Big Deal*, INSIDER (Feb. 25, 2021), https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12; Brandon Myers, *11 Ways Your Car Can Be Hacked – And 8 Ways You Can Prevent Car Hacking*, DEFENSIVE DRIVING (Mar. 23, 2021), https://www.defensivedriving.org/dmv-handbook/11-ways-your-car-can-be-hacked.

[7] Kyle Durch, *Dr. Skynet or: How I Learned to Stop Worrying and Love Autonomous Vehicles*, RICH. J.L. & TECH. BLOG (Mar. 24, 2021), https://jolt.richmond.edu/2021/03/24/dr-skynet-or-how-i-learned-to-stop-worrying-and-love-autonomous-vehicles.

[8] 85 Fed. Reg. 78064.

Institute of Standards and Technology.[9] This comment recognizes the need for the NHTSA to implement safety-related cybersecurity measures in cooperation with other agencies for their expertise in cybersecurity-related matters.[10]

A vehicle can be considered a deadly weapon; in the wrong hands, vehicles can do massive damage. The world has already seen the dead left behind after the 2016 Nice Truck Attack in France, where a terrorist intentionally hit multiple people with a truck resulting in more than 80 deaths.[11] Imagine the amount of damage terrorists or hackers would do if they controlled fleets of remotely controlled autonomous vehicles. Imagine the amount of damage hostile countries would do if they controlled fleets of remotely controlled autonomous vehicles. Thus, having a dedicated safety-related cybersecurity team utilizing the latest cybersecurity measures under the National Institute of Standards and Technology will help to mitigate public safety concerns.

STANDARDS-BASED REGULATIONS ALIGN WITH NHTSA'S LEGAL OBLIGATIONS

I. Tech-Specific Framework that Doubles as a Tech-Neutral Framework that Will Not Prevent Technological Innovation for Safety

The NHTSA should take care not to impose regulations early in the development of Automated Driving Systems that may result in forgone safety benefits; however, the NHTSA should still create regulations early in the development of Automated Driving Systems. In short, tech-specific regulations that double as tech-neutral regulations should be implemented as a form of framework or guidance for safety innovation, a kind of standards-based regulations specifically tailored to Automated Driving Systems.

Automated Driving Systems are unlike anything previously regulated; thus, regulations specifically pertaining to Automated Driving Systems are warranted – tech-specific regulations. However, in reality, tech-specific regulations may distort paths of technological development in ways that may result in foregone safety benefits.[12]

To resolve this issue, the tech-specific regulations may be drafted as tech-neutral regulations that speak only to Automated Driving Systems (tech-specific regulations that double as tech-neutral regulations). These regulations should act as a framework or guidance for the *encouragement* of safety innovation such as standards-based regulations, rather than as a framework or guidance that *restricts* technological development.[13]

---

[9] *Cybersecurity Framework*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, https://www.nist.gov/cyberframework.
[10] 49 U.S.C. § 30111(c) (2021).
[11] *Nice Attack: At Least 84 Killed by Lorry at Bastille Day Celebrations*, BBC (July 15, 2016), https://www.bbc.com/news/world-europe-36800730; *see also London Attack: Seven Killed in Vehicle and Stabbing Incidents*, BBC (June 4, 2017), https://www.bbc.com/news/uk-40146916.
[12] 85 Fed. Reg. 78073 (question #8).
[13] Lisa Quest & Anthony Charrie, *The Right Way to Regulate the Tech Industry*, MIT SLOAN MANAGEMENT REVIEW (Sept. 19, 2019), https://sloanreview.mit.edu/article/the-right-way-to-regulate-the-tech-industry.

With standards-based regulations specifically tailored to Automated Driving Systems, engineers and researchers will understand the baseline safety features required by the NHTSA. This allows the NHTSA to regulate the technological development of Automated Driving Systems while encouraging innovation and holding engineers and researchers accountable for any breaches of safety regulations.[14] Furthermore, having some sort of standard or goal to reach encourages competition between the engineers and researchers developing Automated Driving Systems.[15]

The NHTSA is careful to remind manufacturers to "comply with existing mandates applicable to conventional vehicles."[16] This means a minimum standard for the safety of motor vehicle performance, as mandated in Section 30102(a)(9)-(10) of Title 49 of the United States Code.[17] With this minimum standard for safety in mind, any standards-based regulations imposed for Automated Driving Systems will align with the NHTSA's legal obligations.[18]

II. NHTSA's Legal Obligations

"Bicycles are probably the most difficult detection problem that autonomous vehicle systems face," says Steven Shladover from UC Berkeley.[19] In March 2018, a 49-year-old woman walking a bicycle was hit and killed by an autonomous vehicle.[20] Without surprise, there are many comments from members of the League of American Bicyclists on this Advanced Notice of Proposed Rulemaking.[21]

Bicyclists are not the only group of individuals at an increased risk. Engineers and researchers must also keep in mind not to push the limits on "target" discrimination if they seek to remain within Section 30102(a)(9)'s "protect[] the public against *unreasonable* risk of accidents" phrase.[22] A 2014 Google patent allowed autonomous vehicles to be programmed to hit the "smaller" of two pedestrians, should no other option be available to avoid a collision with a human being.[23] The average female and child are typically "smaller" than the average male. This may be discrimination that results in a violation of Section 30102(a)(9) – actively creating an unreasonable risk of accidents to women and children.[24]

---

[14] *Id.*
[15] *See id.*
[16] Jeremy A. Carp, *Autonomous Vehicles: Problems and Principles for Future Regulation*, 4 U. PA. J. L. & PUB. AFF. 81, 95 (2018) (citing National Traffic and Motor Vehicle Safety Act).
[17] 49 U.S.C. § 30102(a)(9)-(10).
[18] *See id.*
[19] Peter Fairley, *Self-Driving Cars Have a Bicycle Problem*, IEEE SPECTRUM (Feb. 24, 2017), https://spectrum.ieee.org/transportation/self-driving/selfdriving-cars-have-a-bicycle-problem.
[20] Matt Bevilacqua, *Uber Was Warned Before Self-Driving Car Crash that Killed Woman Walking Bicycle*, BICYCLING (Dec. 18, 2018), https://www.bicycling.com/news/a25616551/uber-self-driving-car-crash-cyclist.
[21] 85 Fed. Reg. 78058 (comments section).
[22] 49 U.S.C. § 30102(a)(9) (emphasis added).
[23] Laura Emmons, *The Reasonable Robot Standard: How the Federal Government Needs to Regulate Ethical Decision Programming in Highly Autonomous Vehicles*, 33 J. CIV. RTS. & ECON. DEV. 293, 321 (2020); *see also* Todd Spangler, *Self-Driving Cars Programmed to Decide Who Dies in a Crash*, USA TODAY (Nov. 23, 2017), https://www.usatoday.com/story/money/cars/2017/11/23/self-driving-cars-programmed-decide-who-dies-crash/891493001.
[24] *See* 49 U.S.C. § 30102(a)(9).

Is this within the NHTSA's legal obligation to "protect[] the public against *unreasonable* risk of accidents?"[25] This is a controversial topic and opinion. Answer? No, shifting the risk of accident from "large" target to "small" target is not within the NHTSA's legal obligation to "protect[] the public against *unreasonable* risk of accidents."[26] Aiming for the "smaller" target actively creates an unreasonable risk of accidents to women and children in comparison to men.[27] Then, what should the NHTSA do to "protect[] the public against *unreasonable* risk of accidents?"[28]

Let's imagine the classic trolley scenario: let the trolley kill five people tied to railroad tracks, or pull a switch diverting the trolley to instead intentionally kill one person tied to railroad tracks?[29] This is synonymous with someone programming an autonomous vehicle to avoid hitting a large group of people, but in exchange intentionally hitting and potentially killing a small group of people. Is this within the NHTSA's legal obligation to "protect[] the public against *unreasonable* risk of accidents?"[30] Answer? Yes, minimizing the overall damage and death will "protect[] the public against *unreasonable* risk of accidents"[31]

This is a controversial topic and opinion; however, it is important not to confuse the difference between NHTSA's *ethical* obligations with their *legal* obligations. Section 30101 of Title 49 of the United States Code imposes that the NHTSA's purpose is to "reduce traffic accidents and deaths and injuries resulting from traffic accidents."[32] This is aligned with requiring *someone* to program autonomous vehicles to intentionally hit and potentially kill a human being if it means saving the lives of multiple others.

CONCLUSION

I appreciate the opportunity to submit the foregoing comment in the hopes that it will help the NHTSA in (1) improving the reliability of Autonomous Driving Systems, to include redundant systems and safety-related cybersecurity measures; and (2) implementing standards-based regulations that align with the NHTSA's legal obligations.

Sincerely,

Ken Kajihiro

Ken T. Kajihiro
Student, University of Richmond School of Law

[25] *See id.* (emphasis added).
[26] *See id.* (emphasis added).
[27] *See id.*
[28] *See id.* (emphasis added).
[29] Emmons, *supra* note 22, at 294.
[30] *See* 49 U.S.C. § 30102(a)(9) (emphasis added).
[31] *See id.* (emphasis added).
[32] 49 U.S.C. § 30101.