July 10, 2018

The Honorable John Thune, Chairman
The Honorable Bill Nelson, Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate
Washington, DC 20510

Dear Chairman Thune and Ranking Member Nelson:

In preparation for tomorrow's hearing "Complex Cybersecurity Vulnerabilities: Lessons Learned from Spectre and Meltdown," we write to highlight the critical problems related to the cybersecurity of connected and autonomous vehicles (AVs). As these cars will be "computers on wheels," it is absolutely essential that strong protections be in place to safeguard against potentially catastrophic instances of vehicle hacking. We respectfully request that this letter be included in the hearing record.

Given recent high-profile cyberattacks and the tremendous threat that hacking will pose to connected and automated cars, we are very concerned that these potential risks are not being adequately addressed. In 2015, hackers demonstrated their ability to take over the controls of a sport utility vehicle (SUV) that was traveling 70 miles-per-hour on an Interstate outside of St. Louis, MO. By accessing the vehicle's entertainment system using a laptop computer, hackers located miles away from the vehicle were able to send disruptive commands to the SUV's dashboard functions, steering, brakes, and transmission. This incident is likely just a preview of the types of hacking that will be possible as vehicles become even more reliant on complex electronic systems and outside communications.

Moreover, there is a very real and dangerous possibility that instances of hacking will not only affect one individual vehicle, but could very well impact entire fleets or model lines – posing a severe risk to occupants of the hacked vehicles as well as other road users. These attacks could also clog roads, stop the movement of goods and hinder the response of emergency vehicles. Of additional concern, there are a number of tragic examples of conventional vehicles being used as weapons by terrorists. The potential for remote hacking of connected and automated vehicles by these malicious actors could have unimaginable implications for our national security. Moreover, these risks will only be exacerbated as commercial motor vehicles, specifically large trucks and buses, become more reliant on autonomous systems and are used in platoons.

Currently, Section 14 of the American Vision for Safer Transportation through Advancement of Revolutionary Technologies (AV START) Act (S. 1885), only requires manufacturers to have a cybersecurity plan in place. This is woefully inadequate and has no requirements that any protections be implemented. Instead, the legislation should be improved to direct the National Highway Traffic Safety Administration (NHTSA) to issue a minimum performance standard for all AVs (including SAE Level 2 vehicles). The agency should be required to issue this final rule within a reasonable deadline of three years after enactment. In fact, the July 6, 2018 edition of *Science Magazine* included an article penned by Joan Claybrook and Shaun Kildare which called for a cyber standard and suggested that regulators "look across industries and adapt standards from other modes and fields (banking, military, aviation, etc.) to ensure that AVs have a means

for detecting and responding to an attack appropriately and preventing a widespread threat to safety." (Please see full article attached.)

Further, we support the establishment of a method for sharing cybersecurity problems and vulnerabilities among manufacturers so that all systems can be updated accordingly. To mitigate against widespread impacts, establishing a method of quickly identifying issues and disseminating that information across all participants is critical.

The public recognizes the acute threat of cybersecurity attacks on vehicles, and for good reason. A poll conducted by Morning Consult earlier this year showed that 67 percent of adults responded that they were somewhat or very concerned about cyber threats to driverless cars. An ORC International poll from January 2018 showed that 81 percent of respondents supported the United States Department of Transportation issuing rules to protect against hacking of cars that are being operated by a computer.

We urge you to include the need for robust protections against vehicle hacking in tomorrow's timely discussion. Furthermore, the pending AV START Act should not be enacted into law without requirements that sufficiently account for the reality of cybersecurity threats, including hacking into driverless cars. Thank you for your consideration of our position. We look forward to continuing to work with you to ensure the safety of all road users.

Sincerely,

Catherine Chase, President
Advocates for Highway and Auto Safety

Joan Claybrook, President Emeritus
Public Citizen and Former NHTSA Administrator

Jason Levine, Executive Director
Center for Auto Safety

Jack Gillis, Executive Director
Consumer Federation of America

Rosemary Shahan, President
Consumers for Auto Reliability and Safety

John M. Simpson, Privacy and Technology
Project Director, Consumer Watchdog

cc: Members of the Committee on Commerce, Science, and Transportation

POLICY FORUM

TECHNOLOGY DEVELOPMENT

Autonomous vehicles: No driver...no regulation?

Driverless cars are on the road with no federal regulation, and the public is paying the price

By **Joan Claybrook**[1] *and* **Shaun Kildare**[2]

According to the latest statistics from the U.S. National Highway Traffic Safety Administration (NHTSA), 37,461 people were killed on the nation's roads in 2016 (*1*). Autonomous vehicle (AV) technology has the potential to reduce this number substantially. However, proper safeguards must be established immediately by federal regulators to govern the testing and deployment of AVs and ensure public safety. We must not undermine current safety standards for the sake of AV development. Moreover, reconsidering current requirements may be necessary to take advantage of this revolution. Nearly two-thirds (64%) of respondents in a recent CARAVAN public opinion poll expressed concern about sharing the road with driverless cars (*2*). If commonsense protections are not in place to govern AV development, and problems occur, the public will reject AVs, and the opportunity this new technology presents to improve public safety will be lost.

AV technology is still very much in development, as evidenced by the serious and fatal crashes that have occurred this year. In January of 2018, a Tesla Model S that was operating under its "Autopilot" system crashed into the rear of a stopped fire truck in California (*3*). On 18 March, an AV operated by Uber struck and killed a pedestrian crossing a road in Tempe, Arizona (*4*). Only 5 days later, a Tesla Model X was involved in a fatal crash in California, striking a safety barrier before bursting into flames (*5*). On 11 May, a Tesla crashed into the rear of another fire vehicle in Utah while operating under its Autopilot system (*6*). These crashes illustrate that sensors and algorithms of AVs are still having trouble identifying road hazards and potential obstacles reasonably expected to be in the driving path. The lack of regulation has allowed these unproven vehicles onto our roads. The crashes that have occurred were not unforeseeable and have shaken the public's trust in the technology. Commonsense requirements for the performance of AVs are necessary to protect the public and instill confidence in the technology.

Over 50 years ago, Congress passed the National Traffic and Motor Vehicle Safety Act of 1966 because of concerns about the death and injury toll on our highways. The law required the federal government to establish minimum vehicle safety performance standards to protect the public against "unreasonable risk of accidents occurring as a result of the design, construction or performance of motor vehicles" (*7*). Although motor vehicles have changed dramatically since that time and will continue to do so in the future, the underlying premise of this crucial law has not.

There are currently many regulatory gaps that need to be filled. Federal regulators should develop a list of operational scenarios and a range of conditions under which AVs must be evaluated to ensure that the public is not being placed in harm's way through the introduction of these vehicles. For example, problems associated with different weather and fouling conditions for different types of sensor need to be studied. There should be a minimum "vision test" for the AV system to make sure that it can properly identify its surroundings, including other cars, pedestrians, cyclists, road markings, and traffic signs, and respond appropriately. Moreover, manufacturers must be required to execute comprehensive testing and development before taking these vehicles onto public roads. To protect the public, strict protocols must also be established for testing of these vehicles on public roads. Recent work internationally has identified many of the same concerns with the development and deployment of AVs as noted throughout this work (*8*).

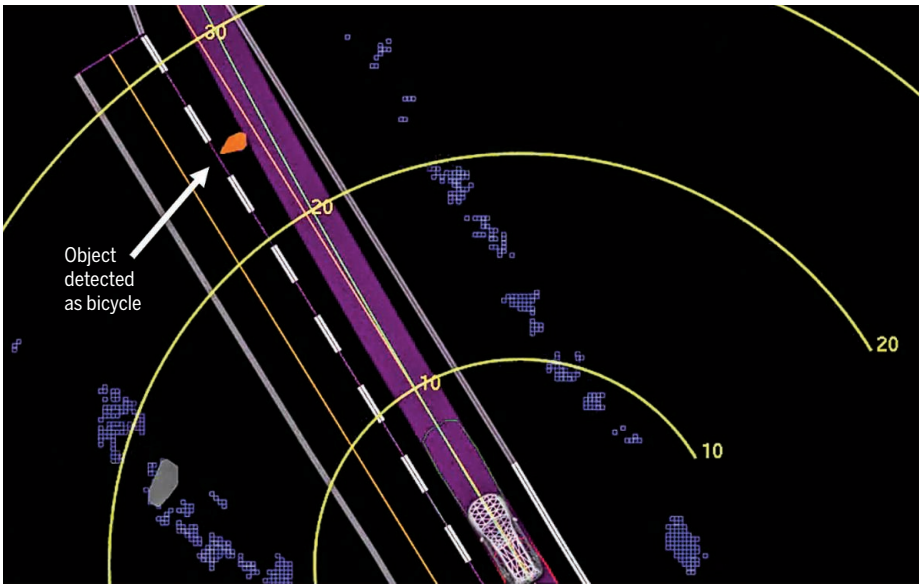
AVs that require monitoring by a human driver have been the first introduction of AV technology to the general public. However, humans are inherently bad at monitoring semi-autonomous systems and are readily distracted (*9*). Manufacturers must find a way to keep a driver engaged in the driving task, and regulators must require that engagement in a meaningful way. This is a conclusion reiterated in the findings of the National Transportation Safety Board (NTSB) investigation of a fatal Tesla crash in Florida in 2016 (*10*).

It is vital that there be standardized, mandatory data reporting. There needs to be a central repository by which all AV manufacturers and federal regulators are routinely made aware of situations identified during testing or deployment that have led to collisions or failures. Currently, there is no transparency regarding the algorithms that form the basis for AV function and thus no way to determine whether there are better approaches to solving problems that resulted in collisions or serious system malfunctions. The information required, however, is more than just that covered by an incident report but must include details on the dynamics of the collision, and more important, how the decision process of the AV may have led or contributed to the crash. Only through data collection and analysis can future regulatory needs be developed and justified. There are already examples of this type of data sharing for safety's sake, such as in commercial aviation (*11*).

Additionally, the possibility of a catastrophic cyberattack on transportation increases as the number of AVs on the road increases. Federal regulators must look across industries and adapt standards from other modes and fields (banking, military, aviation, etc.) to ensure that AVs have a means for detecting and responding to an attack appropriately and preventing a widespread threat to safety. The need for NHTSA to develop a strategy to address cybersecurity was raised more than 5 years ago in a report on the subject by the National Research Council of the National Academies (*12*); however, little progress toward meaningful regulation of this aspect of AV performance and safety has been achieved.

Despite the need for regulation, NHTSA, the federal agency responsible for keeping people safe on America's roadways through enforcement of vehicle performance standards, has issued mere voluntary guidelines that are unenforceable and place no mandates on the industry to develop and test AVs safely. In addition, the agency has failed to act to address the shortcomings of AV technology that have already been identified. For example, the NTSB determined that the driver of a Tesla Model S who had been killed in a 2016 crash in Florida had not been en-

[1]*President Emeritus, Public Citizen, Washington, DC, USA. From 1977 to 1981, she was administrator of the National Highway Traffic Safety Administration.* [2]*Director of Research, Advocates for Highway and Auto Safety, Washington, DC, USA. Email: joan@joanclaybrook.com; skildare@saferoads.org*



Uber self-driving system data playback from the fatal, 18 March 2018, crash of an Uber Technologies, Inc., test vehicle in Tempe, Arizona. Yellow lines show meters ahead of the vehicle. According to the NTSB preliminary report (https://goo.gl/2C6ZCH), although the pedestrian pushing a bicycle was first detected 6 s before the crash, she was categorized by the self-driving system as an unknown object, as a vehicle, and then as a bicycle. At 1.3 s before impact, the self-driving system determined that emergency braking was needed. However, the automatic braking system was not enabled, and no alert was provided to the driver who was supposed to be monitoring the system.

IMAGE: NTSB

gaged in the driving task, and that a probable cause was the operation design "contributing to the car driver's overreliance on the vehicle automation." Even worse, from an engineering standpoint, is that the design of the system allowed misuse. The NTSB found that these problems were not Tesla's alone but are industry-wide (*13*). Yet, NHTSA still has not initiated regulatory proceedings to address these serious safety issues. NHTSA needs to issue regulations governing the safe operation of these vehicles to ensure that development, testing, and eventual deployment into the public domain do not endanger lives.

Compounding the problem is legislation currently pending before Congress (*14*). Both a bill passed by the House of Representatives (SELF DRIVE Act, H.R. 3388) and a measure currently pending before the Senate (AV START Act, S. 1885) will allow automakers to receive broad exemptions from existing federal motor vehicle safety standards and ignore the need for NHTSA to issue minimum safety requirements. In 2015, Congress exempted test vehicles from having to comply with federal safety standards (*15*). The current legislation would allow for the potential sale of millions of AVs that can be exempt from standards that ensure occupant protection and crashworthiness. It would allow for wide-scale commercial introduction of AVs that fail to meet federal safety standards in order to increase industry profits. If this provision is not drastically altered, our nation's roads risk becoming corporate proving grounds for unverified technology, and the American public will end up being unwitting subjects in a potentially deadly experiment.

Another concern, for those cars that can be driven either autonomously or by a human driver, is that the Senate bill dangerously departs from well-settled federal law by allowing manufacturers to disconnect steering wheels, brakes, and other safety systems, when such a vehicle is operated in an autonomous mode, without any government review and approval. Furthermore, neither bill encompasses all AVs, including those that depend on a human driver to monitor their operation. These vehicles are already on the road, have been involved in multiple deadly crashes, and will comprise a sizable portion of the AV fleet for years to come. Neither bill being considered by Congress requires NHTSA to deal with the regulatory issues that we describe and develop critical standards that will be essential to assuring the proper development and operation of AVs. In addition to all of these concerns, Congress has not provided NHTSA with sufficient funds to deal with the expanded duties it will have in response to the advent of AVs. AVs are already being tested in states and cities across the country. Some state and local governments have started to put in place the first requirements to preserve public safety in the absence of any substantive action by the federal government. Unfortunately, both bills before Congress will preempt these regulations, despite NHTSA having yet to issue any federal standard for AVs. This unprecedented attack on the historic state responsibility to protect their residents will create a regulatory vacuum that will needlessly put the public at risk. Until NHTSA issues safety standards and regulations for AVs, state and local governments have every right, and in fact a duty, to protect their citizens. Traditionally, states are allowed to act where the federal government has not taken specific action; however, the issue of preemption may have to be resolved by the courts. NHTSA has failed to respond meaningfully to the development of AV technology. Although the technology has the ability to save lives once developed, at the same time it can risk lives (and has already claimed several) if it is not executed properly. A federal framework developed around ensuring safety, not just supporting corporate development, is necessary. Congress must end the deregulatory efforts and focus on balancing productive competition while maintaining the levels of safety required by established law and practice. A failure to put proper safeguards in place will result in the continued erosion of the public confidence in this potentially lifesaving and game-changing technology. ■

REFERENCES

1. National Center for Statistics and Analysis, *2016 Fatal Motor Vehicle Crashes: Overview*. Traffic Safety Facts Research Note. Report no. DOT HS 812 456 (National Highway Traffic Safety Administration, Washington, DC, October 2017).
2. ORC International, CARAVAN Public Opinion Poll: Driverless Cars (12 January 2018).
3. P. Valdes-Dapena, "Tesla in Autopilot mode crashes into fire truck," *CNN Tech*, 24 January 2018.
4. E. Rosenfield, "Tempe police release video of deadly Uber accident," *CNBC*, 21 March 2018.
5. D. Shephardson, "U.S. opens probe into fatal Tesla crash, fire in California," *Reuters*, 27 March 2018.
6. K. Allen, "Tesla Model S was in Autopilot mode during Utah crash, driver says," *ABC News*, 15 May 2018.
7. Public Law 89–563.
8. International Transport Forum, Safer Roads with Automated Vehicles? (ITF, 2018).
9. http://acrs.org.au/files/papers/arsc/2015/CunninghamM%20033%20Autonomous%20vehicles.pdf
10. National Transportation Safety Board, Collision between a Car Operating with Automated Vehicle Control Systems and a Tractor-Semitrailer Truck Near Williston, Florida, May 7, 2016, Accident Report NTSB/HAR-17/02, PB2017-102600 (12 September 2017).
11. www.faa.gov/news/fact_sheets/news_story.cfm?newsId=18195
12. *Transportation Research Board Special Report*, vol. 308, *The Safety Challenge and Promise of Automotive Electronics: Insights from Unintended Acceleration* (Transportation Research Board, Washington, DC, 2012); www.nap.edu/catalog.php?record_id=13342
13. Collision Between a Car Operating with Automated Vehicle Control Systems and a Tractor-Semitrailer Truck Near Williston, Florida, May 7, 2016; NTSB, Accident Report NYST/HAR-17/-2.
14. S. 1885, American Vision for Safer Transportation through Advancement of Revolutionary Technologies (AV START) Act, 115th Congress, 1st Session (2017); H.R. 3388, Safely Ensuring Lives Future Development and Research in Vehicle Evolution (SELF DRIVE) Act, 115th Congress, 1st Session (2017).
15. Fixing America's Surface Transportation Act, Sec. 24404, Public Law 114-94 (2015).

10.1126/science.aau2715

Autonomous vehicles: No driver…no regulation?

Joan Claybrook and Shaun Kildare

Science **361** (6397), 36-37.
DOI: 10.1126/science.aau2715