Attachment—Additional Questions for the Record

Subcommittee on Consumer Protection and Commerce
Hearing on
"Promises and Perils: The Potential of Automobile Technologies."
May 18, 2021

Mr. Jason Levine, Executive Director, Center for Auto Safety

The Honorable Janice D. Schakowsky (D-IL)

1. **During the hearing there was a lot of discussion about the potential for automated vehicle technologies to address car crash deaths and injuries, yet most of these technologies remain in the development stage. What steps could Congress take now to both accelerate the safe deployment of these lifesaving technologies and improve vehicle safety in the near future?**

This Subcommittee, as well as Congress at large, have a unique opportunity to level the playing field for motor vehicle safety today and in the future. Sooner, rather than later, Congress will take on the vital task of writing our nation's first autonomous vehicle law. When it does, for the first time, Congress can help cultivate technological innovation in a way that provides safety for everyone on the road regardless of whether they are a driver, passenger, or pedestrian and no matter their income. To begin with, it is time for the National Highway Traffic Safety Administration (NHTSA) to write performance standards for existing vehicle safety technology and it is long past time for those technologies to become mandatory equipment on new vehicles.

Advanced driver assistance systems (ADAS) - from automatic emergency braking (AEB) to lane keeping assist features, to driver monitoring systems and adaptive driving beam technology - have tremendous potential to save lives. However, until now NHTSA has done little to introduce minimum performance standards to ensure that each of these features work effectively to prevent crashes. Without minimum standards to ensure proper function of these features, and little appetite to recall faulty performers producing clearly unsafe outcomes, as we have seen in our work to recall faulty AEB systems, NHTSA continues to display minimal interest in ensuring these features work, whether through its enforcement or rulemaking authorities, which only accelerates the need for minimum performance standards.

Far too often in recent years, NHTSA has chosen to rely on its consumer information program, the New Car Assessment Program (NCAP), to incentivize manufacturers to keep up with the pack in vehicle safety. Unfortunately, if the pack is not held to a minimum standard of function, keeping up with it provides little benefit to consumers, and zero assurance that any particular ADAS system will function as intended or advertised. Congress can do more by insisting that NHTSA update the NCAP program for the first time over a decade to ensure consumers have a way to assess ADAS performance. Additionally, requiring the agency to set minimum

performance standards for ADAS technologies would provide a baseline from which NCAP can assess ADAS performance. One prominent form of ADAS, driver monitoring systems, have great potential to reduce drunk, drowsy, or distracted driving, provided that the technology works properly, as could be incentivized by NCAP ratings. Mandating that these technologies be deployed fleetwide, and not simply deployed in luxury automobiles, will ensure maximum safety gains in the future.

By some estimates, combining features such as driver monitoring systems, automatic emergency braking and lane keeping assistance systems to combat impaired driving (drunk, drugged, drowsy, and distracted) could help to dramatically mitigate 10,000, or more, crash deaths every year.

In addition to the potential to saving tens of thousands of lives, a side benefit of wide deployment of ADAS will be public comfort with the type of technology that will eventually become the foundation of driverless vehicles. Moreover, the data gathered from such vehicles, in combination with data collected from all automated test vehicles, can be used to craft reasonable regulations that set minimum thresholds for safety to better protect consumers and ensure a robust marketplace.

While any autonomous vehicle (AV) law should certainly require performance standards, expansive data collection, and a gated certification regime, it must also include cybersecurity standards, vision tests, updated occupant protection standards, and pedestrian and other vulnerable road user protection standards, while maintaining current state, local, and common law rights and authorities. It is vital that an AV law does not preempt protections provided by state and local rules of the road regarding the operation of vehicles on their streets. There is no doubt that access to courts, for innocent victims killed by an experiment for which they did not volunteer, will remain the final consumer protection backstop in a potentially lengthy unregulated environment.

Finally, as it remains likely that AV companies will treat contracts involving automated technology like software or smartphone agreements, binding arbitration must be forbidden in direct-to-consumer contracts. A generation of legal precedent and consumer understandings regarding the legal relationship between a vehicle manufacturer and the end user may not have been perfect, but it has generally prevented vehicle manufacturers from attempting to bind end users into giving up their rights to seek civil justice. To do away with such a protection based on legalese buried in small print will neither engender trust in the AV industry nor will it encourage the type of transparency that is needed to keep large corporations incentivized to do the right thing.

2. **The United States pioneered the concept of sharing vehicle crash data with consumers to allow the market to drive safety decisions with the New Car Assessment Program in 1980. As I understand it, that program has not been updated in over a decade. How important is it to make sure NCAP remains up to date and what should the next version of NCAP contain to allow consumers to determine which vehicles are the best for them and their families?**

The New Car Assessment Program ("NCAP" or "5 Star Crash Rating") is arguably the greatest market-based, nonregulatory safety program in automotive history. Until NCAP, the concept of the public having access to crash information about vehicles by make and model did not exist. Today, consumers expect to have detailed information about the performance of their new vehicle when it comes to safety. NCAP proved that safety does sell. Unfortunately, because the program has not been updated in over a decade, what manufacturers are currently advertising when they claim a Five Star rating is an impression of safety, instead of the real thing.

Today, almost every single new vehicle rated by NCAP receives a top safety rating. This is not because all of the vehicles are equally safe, it is because they are all being scored on ratings that have not been updated since 2010. It is self-evident that if 98% of cars achieve superior ratings, it is impossible to distinguish between them in any significant way. Updating NCAP is essential to ensure consumers have access to relevant and useful safety information, allowing them to make informed decisions while also pushing auto manufactures to pursue innovation in safety technology. Currently, virtually every car in the NCAP system receives 4 or 5 stars, rendering NCAP ineffective for consumers who hope to make an informed decision about the safety of a vehicle.

There are many areas where NCAP can be improved, including by following some of the recommendations issued by the National Transportation Safety Board (NTSB) in 2018. The NTSB issued eight safety recommendations to NHTSA addressing the need to include performance-based standards for vehicle headlight systems, development of performance test criteria for vehicle designs that reduce pedestrian injuries, and incorporation of pedestrian safety systems into NCAP, including pedestrian collision avoidance systems and other more passive safety systems.

Specifically, pedestrian safety is a pressing issue that NHTSA must address, and NCAP must play a key role in NHTSA's consumer outreach. In 2020, despite a 13% reduction in vehicle miles travelled, pedestrian deaths on public roads hit a critical and historic figure of 6,721, which averages to one crash-related pedestrian death every 80 minutes. Additionally, an estimated 173,000 pedestrians were treated in emergency departments for non-fatal crash-related injuries in 2020. These tragedies could be dramatically reduced by incentivizing automakers to include more protective pedestrian safety features in new cars, and NCAP can be an effective means to assist in accomplishing this important task.

Currently, the US NCAP has no rankings or information available regarding emerging technology to protect vulnerable road users, whether that be pedestrian crash avoidance features or pedestrian protective designs built into hoods and bumpers on some new vehicles. However, Pedestrian Safety is factored into the rating given by The European New Car Assessment Programme ("Euro NCAP"). Euro NCAP has recognized this need and includes in its vehicle ratings both ADAS technologies and automobile design features that protect pedestrians and minimize injury and death in an accident.

In addition to the NTSB's safety recommendations, numerous ADAS safety features are not rated in NCAP and therefore information regarding their impact on a vehicles safety is not readily available to consumers. Having NCAP include information on features such as AEB, Lane Departure Warning, Forward Collision Warning, Blind Spot Detection, Cross Traffic Warning, Rear AEB, Smart Headlights, Driver Monitoring Systems, and Advanced Automatic Crash Notification will not only save lives now but is a critical part of the development of future automated vehicle systems that could work hand in glove with human drivers.

Furthermore, NCAP must be improved to protect occupants of all sizes and ages, no matter what vehicle position they occupy. The current tests and crash dummies simply do not account for the size of Americans, nor do they allow for enhanced analysis that could provide better ratings for use by the elderly, women, and passengers of larger or smaller sizes than currently represented. Additionally, NCAP provides very little in the way of safety ratings for occupants, particularly those in rear seats. As more Americans travel by rideshare, and with an eye towards a future where many predict we will all be relegated to occupants, protection in all seating positions has clearly becomes a more pressing task. NCAP could lead the way by ensuring that consumers are able to distinguish vehicles that offer advanced protection for occupants in the rear seats, from those that do not.

3. **While Congress can pass laws regarding vehicle safety, implementation of these laws is usually delegated to the Department of Transportation and the National Highway Traffic Safety Administration (NHTSA). Unfortunately, NHTSA has fallen behind in fulfilling some Congressional mandates. How should NHTSA balance their existing requirements with future Congressional obligations? What can Congress do to assist in this task?**

Amongst the most important actions Congress can take to help NHTSA oversee advanced auto safety technologies, and improve vehicle safety overall, is to provide the agency with adequate funding. Over the last 40 years, while the number of vehicles on the road and the number of drivers have both doubled, America's only federal safety agency with rulemaking and enforcement authority has seen its vehicle safety appropriations (adjusted for inflation) drop as much as forty percent. The Rulemaking, Enforcement, and Research and Analysis departments at NHTSA, which have been directly responsible for vehicle crashworthiness and other safety standards that have saved hundreds of thousands of lives since NHTSA's founding five decades ago, remain significantly underfunded. Such chronic underfunding only encourages the cynical

and reoccurring narrative that NHTSA is incapable of overseeing the safe development of advanced vehicle technology, and ultimately the driverless vehicle industry, due to a lack of resources.

Additionally, Congress could assist NHTSA by mandating it take steps to improve vehicle safety when the agency has failed to use its existing authority. As described above, requiring an update to NCAP would benefit all consumers, and those manufacturers who want to compete to have the safest vehicle in the showroom and on the road. Also, requiring NHTSA to update its seatback safety standard (FMVSS 207), which has remained the same since 1967, would prevent the horrific deaths and life-altering injuries often caused by a parent being thrust backward over their collapsed seat at such a speed and force as to kill or paralyze their own child during a rear end collision. These incidents represent a well-known problem to both the industry and the agency that remains unresolved to this day, despite recent a NHTSA study documenting changes to FMVSS 207 that would reduce seat back dynamic rotation and prevent injury to rear passengers. Included in the data analysis was a figure that shocks the conscience: an estimated cost of less than $4.63 per automatic seat ($1.94 for manual seats) to make the adjustments that could prevent many of these life-altering injuries from taking place. It is time Congress steps in and mandates the needed safety upgrade.

Furthermore, by exercising legitimate oversight into the agency's failure to complete existing mandates, Congress could ensure that the rule of law is respected and the will of the people is heard. For example, multiple NHTSA rulemakings remain in limbo years after Congressional deadlines have passed. These include a whistleblower rule to ensure that vehicle manufacturer employees are able to come forward with defect information, a rule to provide recall notices to consumers electronically, a rule to help prevent children from being unbelted in rear seats, and a rule to establish side impact requirements to protect children in child restraints. Congress must ensure that NHTSA promptly acts on these and other items on the agency's long list of overdue rulemakings.

The Honorable Bobby L. Rush (D-IL)

1. **Mr. Levine, the Federal Trade Commission just released a report that criticized commercial practices that restricts auto repair options for consumers. For many Americans, their vehicles are the largest assets they have, and they rely on their cars to get them to work and to the supermarket. The report was approved by all 4 sitting Commissioners, Democrats and Republicans, and calls for legislation to expand repair and maintenance options for consumers. I am currently drafting such a bill. Are you familiar with the report? What is your opinion of the findings?**

The Federal Trade Commission Report, "Nixing the Fix: An FTC Report to Congress on Repair Restrictions," was issued in May 2021, in response to a Congressional directive requiring the Commission examine anticompetitive practices related to repair markets. We have reviewed the Report, focusing our attention on the areas related to auto repair. With an estimated 280 million registered passenger motor vehicles on American roads, there is plenty of repair work to go around.

The Center for Auto Safety was founded in 1970 to stand as an advocate for consumer safety and consumer protection when it comes to motor vehicle related issues. Vehicle safety is often dependent upon vehicle maintenance and repair. Historically speaking, competition for consumer business in the vehicle repair field has led to a greater consumer choice and better prices. Moreover, it has long been the Center's position that such competition is an excellent incentive to ensure the quality of repairs at both independent and manufacturer licensed repair shops.

Therefore, assuring consumers have access to reliable mechanics and the opportunity to choose which mechanics will service their vehicle is an important element of vehicle safety. Historically speaking, competition for consumer business in the vehicle repair field has led to a greater consumer choice and better prices. Moreover, it has long been the Center's position that such competition is an excellent incentive to ensure the quality of repairs at both independent and manufacturer licensed repair shops.

As a general matter, we agree with the Commission's unanimous conclusion that repair restrictions are rarely adequately justified and believe that consumer choice is beneficial to the safety of every driver, passenger, and pedestrian on the road. More specifically:

With respect to telematics: Automakers exert unreasonable control over telematic information collected from vehicles – this includes performance and status information necessary to perform proper repairs and maintenance. As vehicles continue to require more software (and software updates) and possess more computer systems the average vehicle has 50+ electronic control units, each with its own processor, access to this data is critical for independent repair shops in order to effectively repair the vehicle. Most relevant repair data is available on the open-source CAN bus, but this access is not guaranteed, and OEMs are

currently free to use proprietary protocols that would completely lock out access to everyone except those included under their proprietary umbrella. Even when ECU status is available, OEMs may restrict access to critical ECUs, main processors, or software to drive business to their own licensed repair centers. While the CAN bus protocol for ECU communication and programming is widely used, it is not universal. OEM use of proprietary data bus architectures that are not readily accessible by independents and individuals erects yet another barrier to economical repairs.

Currently, OEMs are free to use proprietary network protocols in their vehicles and engage in what amounts to a monopolistic practice in order to prevent independents from even diagnosing problems. Only the open-source CAN bus data is ordinarily available to independent repair shops. Deviation from the CAN bus without providing alternative data access to independents and owners is another expensive barrier to repairs, again disenfranchising owners, independents, and people of limited means who are often uniquely dependent on their vehicles for employment, child care, and the necessities of life. OEMs that do not use a CAN bus should provide alternative low-cost access to individuals and independent businesses to encourage maintenance visibility and proper repairs. These barriers, limited access to data and restricted access to software/hardware components needed to diagnose and repair vehicles, may put independent shops in the untenable position of attempting to diagnose vehicle problems, or perform maintenance, without a full set of vehicle data on which to base their conclusions, putting both motorists and independent businesses at risk. It also places an extra burden on component suppliers who would lose the ability to sell their products to independent repair shops, unfairly restricting consumer choice as well.

At the Center, we have frequently seen the tragic results of unrepaired or improperly repaired vehicles, and believe that the negative safety impacts of limiting independent repair access to needed vehicle data and components must be part of the conversation, in addition to the economic benefit of ensuring that consumers are free to choose their place of repair.

With respect to Parts - Original Equipment Manufacturers (OEMs) have long held a virtual monopoly in the area of repair parts that has served to restrict consumer choice and increase prices for repair. Not only does current law allow OEMs to restrict access to and availability of repair parts, but a perhaps more pressing issue is that in the context of modern cars, OEMs possess an unreasonable level of control over an increasingly more important part of the vehicle – software and data systems – and who may access them.

In order to properly perform repairs and maintenance on consumer vehicles, independent repair shops (and consumers) must have the ability to access manufacturer service and diagnostic software, hardware, official service information or other tools necessary for an OEM repair. OEMs are continually issuing service bulletins and other updates to their dealer repair facilities to ensure that safe and proper repairs are made to consumer vehicles, and

access to these bulletins has historically also been limited, to the detriment of consumers seeking honest repairs.

Further, extending the current restrictive model to the modern context where vehicle repairs are as likely to be a software update as a physical part creates an environment where consumers have only one place to go – the dealer service facility – to continue operating their vehicle safely and efficiently both during and after the warranty period.

For example, most vehicle designs rely on the CAN bus for communication among the multiple electronic control units and main computer in a vehicle. The CAN bus in its native form is intrinsically insecure. No regulations exist that require OEMs to either develop or avail themselves of available technology to harden the CAN bus. This is a much graver cybersecurity exposure than presented by independent repairs which rely on the same suppliers as the OEM for replacement parts. What is most important when it comes to maintaining the cybersecurity of vehicles is for manufacturers to harden their attack surfaces, including such seemingly benign components as wireless tire pressure sensors, and isolating their vehicle control systems from infotainment and data gathering systems, to enable any qualified individual who wishes to repair the vehicle (including consumers) to do so in a way that minimizes the risks of cyber tampering and quarantines any actual instance of a breach. NHTSA must write cybersecurity standards for new vehicles that require both defensive strategies and offensive test and verification considerations when it comes to external threats. After all cybersecurity threats do not start at the repair shop and do not stop at the dealership door.

Finally, the Center recognizes the value of repairs being undertaken by experienced and qualified mechanics in the automobile field. However, we have yet to see objective data demonstrating that such experience and qualified repairs can justifiably be limited to OEM franchised dealership repair facilities instead of allowing consumers to benefit from competition.

2. **Mr. Levine, the FTC's report states that "the burden of repair restrictions may fall more heavily on communities of color and lower-income communities. Many Black-owned small businesses are in the repair and maintenance industries, and difficulties facing small businesses can disproportionately affect small businesses owned by people of color." My bill will allow independent repair shops to repair and maintain cars in their own communities. Do you have any thoughts on this aspect of the FTC report?**

As you note in the question above, for many Americans, their personal motor vehicle is the most expensive purchase they will ever make. Therefore, keeping their vehicle in good service, for both utilitarian and financial reasons, is extraordinarily important. Having access to a local repair shop not only provides convenience (and thus a greater likelihood of vehicles being regularly serviced) it can help to encourage regular repairs based on a relationship of

trust with a local, independently owned, merchant. As the FTC Report details, restricting repairs exclusively to larger, manufacturer licensed facilities can have a deleterious effect on small businesses which can have a significant impact on smaller communities. Presuming the accuracy of the FTC's data, such restrictions could have a disparate impact on communities of color and lower income communities which historically have relied upon small, locally owned businesses. Keeping vehicles in safe condition, and fully repaired, is vital to the safety of everyone on the road. With over 100 Americans being killed every day by vehicle crashes any steps that can be taken to ensure that vehicles are being repaired is important for safety. The right to repair will mean little without convenient access to vendors who can provide such service based on a relationship of quality and trust.

The Honorable Lori Trahan (D-MA)

1. **I represent Massachusetts, the first state to pass automobile right to repair in 2012. As we move towards a world with more connected vehicles, the importance of data protection and cybersecurity increases. And while this is true, we have seen large companies use privacy and cybersecurity as an excuse to increase repair restrictions. Fortunately, the FTC recently released a comprehensive report examining repair markets.**

   The report found that, "[t]he record contains no empirical evidence to suggest that independent repair shops are more or less likely than authorized repair shops to compromise or misuse customer data. Furthermore, although access to certain embedded software could introduce new security risks, repair advocates note that they only seek diagnostics and firmware patches." Do you agree with these conclusions? Why is ensuring that independent repair shops can maintain vehicles important for public safety?

As a general matter, we agree with the Commission's unanimous conclusion that repair restrictions are rarely adequately justified and believe that consumer choice is beneficial to the safety of every driver, passenger, and pedestrian on the road.

The Center for Auto Safety was founded in 1970 to stand as an advocate for consumer safety and consumer protection when it comes to motor vehicle related issues. Vehicle safety is often dependent upon vehicle maintenance and repair. Therefore, assuring consumers have access to reliable mechanics and the opportunity to choose which mechanics will service their vehicle is an important element of vehicle safety. Historically speaking, competition for consumer business in the vehicle repair field has led to a greater consumer choice and better prices. Moreover, it has long been the Center's position that such competition is an excellent incentive to ensure the quality of repairs at both independent and manufacturer licensed repair shops. At the Center, we have frequently seen the tragic results of unrepaired or improperly repaired vehicles, and there can be negative safety impacts of limiting

independent repair access to needed vehicle data and components, to say nothing of the economic benefit of ensuring that consumers are free to choose their place of repair.

2. **Additionally, the report found that, "replacing a part on a device with an identical OEM part or functionally equivalent aftermarket part is unlikely to create a cybersecurity risk…. the record supports arguments that consumers and independent repair shops would be equally capable of minimizing cybersecurity risks, as are authorized repairers." As technology changes, do you think we can achieve the goals of safety and cybersecurity, while maintaining competition in repair markets?**

As a threshold matter, the Center takes the position that NHTSA should, either of their own accord or because the agency is required by statute, provide minimum cybersecurity performance requirements for automakers and suppliers to enable validation of design approaches that assure long-term cybersecurity effectiveness and vehicle safety throughout a connected vehicle's life cycle.

It may never be possible to implement 100% effective prophylactic cybersecurity measures, thus NHTSA should endeavor to promote full life cycle vehicle cybersecurity. In order to assure sufficient information for post-incident forensic analysis and the ability to share lessons learned with the entire connected vehicle community, including the public, a robust data set will be required. NHTSA should mandate that vehicle software, logic-bearing devices, sensors, and data processing equipment configuration are embedded in vehicle data records in the event of a successful attack causing a life-threatening or deadly incident.

NHTSA should be determining the needed scope and means of cyber testing to enhance public safety and enabling the auto industry to realistically validate their cybersecurity designs, ensure that capabilities have been validated, and make certain that validation results are available to the public. The results of cybersecurity testing and validation should be incorporated into the information available to consumers to assist their evaluation of various modern vehicle offerings.

The argument that such NHTSA capabilities do not currently exist does not absolve NHTSA of its legal duty to act in the face of clear threats to vehicular safety. The need to address connected vehicle cybersecurity is new and NHTSA's response to that need must also be entirely new.

Yet, as the FTC noted, "the record contains no empirical evidence to suggest that independent repair shops are more or less likely than authorized repair shops to compromise or misuse customer data." And, as the question notes, the FTC concludes "[w]ith appropriate parts and repair information, the record supports arguments that consumers and independent repair shops would be equally capable of minimizing cybersecurity risks as are authorized

repairers." The reverse is also true of course, authorized repairers and independent repair shops are equally capable of creating a cybersecurity risk.

Until such standards and steps are taken by NHTSA, however, without much evidence it is often posited that restricting the right to repair will somehow improve cybersecurity for consumers in passenger vehicles. For example, most vehicle designs rely on the CAN bus for communication among the multiple electronic control units and main computer in a vehicle. The CAN bus in its native form is intrinsically insecure. No regulations exist that require OEMs to either develop or avail themselves of available technology to harden the CAN bus. This is a much graver cybersecurity exposure than presented by independent repairs which rely on the same suppliers as the OEM for replacement parts. What is most important when it comes to maintaining the cybersecurity of vehicles is for manufacturers to harden their attack surfaces, including such seemingly benign components as wireless tire pressure sensors, and isolating their vehicle control systems from infotainment and data gathering systems, to enable any qualified individual who wishes to repair the vehicle (including consumers) to do so in a way that minimizes the risks of cyber tampering and quarantines any actual instance of a breach. NHTSA must write cybersecurity standards for new vehicles that require both defensive strategies and offensive test and verification considerations when it comes to external threats. After all cybersecurity threats do not start at the repair shop and do not stop at the dealership door.