

May 6, 2019

The Honorable Joseph J. Simons
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

RE: NIXING THE FIX: A WORKSHOP ON REPAIR RESTRICTIONS

Thank you for holding a workshop on ways manufacturers may limit third-party repairs. Auto Care Association is a national trade group representing companies that manufacture, distribute, retail or install auto parts. While some of our members do manufacture products for the vehicle manufacturer, we represent the side of the business that is independent of the vehicle manufacturer. Most surveys have shown that 70 to 75 percent of consumers obtain repair for their vehicle at independent shops due mostly to trust, convenience and price. Indeed, the existence of a competitive repair industry has helped Americans keep their vehicles on the road and made vehicle ownership among the most affordable in the world.

Advances in technology, while providing significant benefits to consumers, are also being used, either intentionally or unintentionally, to provide increased control over where and how consumers obtain repairs. The impact of technology on the repair industry is further exacerbated by the fact that every day, consumers are being bombarded with messaging that warns them that obtaining repairs outside of authorized channels might jeopardize the safety and functioning of their product or, in many cases, void warranty coverage. The government needs to play a role, not only in enforcing current statutes developed to protect consumers from anti-competitive tactics, but also to examine how current and evolving technology is changing the dynamics of the repair industry and what additional action is needed to ensure competition for consumers.

Right to Repair

The value of a competitive repair industry is illustrated by the passage in 2012 of a right to repair ballot question in Massachusetts by an 86 to 14 percent margin. This measure sought to address the issues related to the computerization of late model vehicles, requiring vehicle manufacturers to share with independent repairers the same information, tools and software they provide to their franchised dealers at a fair and reasonable price. The overwhelming passage of the ballot measure was a strong indicator of the importance to consumers of a competitive repair industry and led to the signing in 2014 of a Right to Repair Memorandum of Understanding (MOU) where all of the manufacturers (except Tesla) agreed to comply with the Massachusetts right to repair law nationwide. The MOU is considered a model that is not only being attempted to be replicated by other U.S. industries, but is the model for right to repair efforts in other countries such as Australia and South Africa.

While right to repair has been a success, compliance issues continue to be a problem for some manufacturers. Under the Massachusetts law and the MOU, all of the repair software is required to be available from the manufacturer's cloud. Yet, during testing by the Auto Care Association, companies like Kia and Hyundai failed to provide any access to their repair software and others, such as Mercedes and Subaru, required that manufacturers go through the manufacturer or dealer to obtain a computer disk or thumb drive in order to obtain software capabilities. We further found that many of the sites were difficult or impossible to navigate. While Auto Care Association has had some success in moving manufacturers to correct these issues, the absence of strong compliance points to the fact that many car manufacturers fail to place resources needed to ensure the competitive repair industry demanded by customers of their vehicles.

In-Vehicle Data

Notwithstanding the right to repair laws, vehicle manufacturers are now looking at the growing use of connected technology, exempted from right to repair, to increase their control of how their vehicles are repaired. According to IHS Markit, over 87 percent of new vehicles will contain connected technology by the year 2022 and nearly every vehicle on the road will be connected by 2030. While the availability of this data could have many advantages to safety and improved availability of services for connected vehicles, there also are many competitive and privacy dangers from the connected car if the government does not step in to protect the vehicle owner.

The number one concern is the fact that the vast majority of car owners have no knowledge that their vehicle is transmitting data. According to a survey conducted for Auto Care Association by Ipsos (study attached), 3 out of 4 car owners are not aware that their vehicle is transmitting data and 71 percent of car owners think that they have control of that data. However, the truth is that all of the data transmitted by a vehicle purchased by a consumer is sent to the manufacturer who then has the opportunity to determine how that data is used. Car owners often sign agreements that permit the manufacturer to collect their data, but consumers have little to no idea about what kind of data is being captured and they definitely cannot choose to send that data to a party outside of the manufacturer's realm.

Why is this important? Clearly, with access to data, manufacturers can gain a major competitive advantage over outside competitors. Car owners receive notices from manufacturers regarding the maintenance and repair needs for their vehicle and then are directed to the repair facility that the manufacturer authorizes, not necessarily the one that is preferred by the car owner.

Car companies also have the advantage of providing more competitive services to vehicle owners. The data collected from a vehicle will permit the manufacturer to diagnose the problem, ensure that the parts, tools and information are ready when the vehicle arrives at their authorized facility, ensuring a more efficient and convenient repair experience for the car owner. Also, that data could be utilized to assist the manufacturer in predicting part failures before they occur, thus improving safety. We are not stating that the use of data for these purposes is not beneficial, but the fact that only the manufacturer can have access to this data clearly will provide the manufacturer and their authorized repair facilities with a substantial competitive advantage in fighting for the \$327 billion that consumers spend every year on repair and maintenance of their vehicles.

Further, manufacturers are the sole arbiters of where that data might be sold. While manufacturers have committed to obtain permissions to sell data, consumers have little information as to what data is being sold and the types of companies that data might be sold to. Considering the fact that consumers are almost totally unaware of the vast amounts of data available from their vehicle, they are not in a very

educated position to decide whether they are comfortable with their data being sold to third parties. Yet these decisions are being made on the dealership sales floor every day.

Assuming the huge monetization of the data available from vehicles, it is unlikely that the manufacturers will willingly give up control of the data. An April 2018 McKinsey report titled “Telematics: Poised for Strong Global Growth” concluded that the global revenue pool from car data monetization could be as high as \$750 billion by 2030. Therefore, it is critical that the government play a role in both requiring better clarity to consumers regarding their vehicle data and how that data is to be made available.

The issue of control and access to in-vehicle data is made more concerning by recent actions by Fiat Chrysler (FCA) to require authorization to obtain access to their on-board diagnostic system (OBD). Currently, when a vehicle comes to a repair facility, the first thing that occurs is that a company plugs into the vehicle, downloads any fault codes in order to determine what is wrong with the vehicle and ascertain a repair. Currently, that information is open and accessible to anyone that has the proper tooling including the car owner who might choose to do the work themselves. However, due to cyber security concerns, FCA is now requiring that the tool, shop and the technician receive authorization from FCA in order to access an owner’s vehicle. Adding insult to injury, shops wanting access must pay FCA or their contractor for access. Not only will this add to the repair costs for consumers, but FCA will have access to extensive data on the shops requesting access, including the types of vehicles they are working on, tools and parts being used and the services that the shop is providing. This competitive information will further help FCA gain a competitive edge in the very lucrative repair market.

The problem is not just FCA; other manufacturers are considering their own schemes. Should every manufacturer come up with a different system for access to repair data, it will be difficult for aftermarket tools to navigate the system and repair shops could have difficulty cost effectively providing service for their customers. While car manufacturers like FCA will claim that these actions are necessary to ensure cybersecurity, this is a fallacy. There are standards under development that will ensure cyber protections but still provide for standardized access to data needed to repair vehicles such that independent repair facilities can have direct real-time access to vehicle data with permission of the vehicle owner.

Known as the Secure Vehicle Interface (SVI), it is a collection of 20-plus industry standards that provides a firewall protecting critical vehicle systems while permitting an interface between the internal vehicle network and an external device or network—enabling secure information exchanges. The same firewall can protect wired and wireless connections, and identity and access are managed using digital certificates. Further, it is retrofit-able so that it can be used on cyber-vulnerable vehicles that are already on the road.

A major difference between the FCA system and SVI is that the latter is standardized which means that every manufacturer would implement it the same way, ensuring that scan tool companies and shops can obtain access to the data they need to repair the vehicle while also ensuring that the vehicle systems are protected from unauthorized access.

The standards needed to implement SVI are already in development and almost completed. Further, the Auto Care Association successfully demonstrated that SVI is workable during its 2018 AAPEX trade show in Las Vegas, utilizing cars and buses driven on Vegas roads. Auto Care Association has attempted to work with the vehicle manufacturers to implement a solution like SVI, and it should be no surprise considering the monetary stakes, that there has not been any willingness to come to the table to discuss this issue.

The bottom line is that the growing connected vehicle population combined with the fear of cyber intrusions threatens to make the vehicle manufacturer the gatekeeper for the in-vehicle data. For those industries that depend on data from a vehicle in order to provide services, this poses a severe risk that they will be squeezed out of the market by manufacturers seeking to capitalize on their control of data.

As we said above, cyber security can go hand in hand with competition and the FTC can play a role in ensuring that competition in the aftermarket is preserved. Failure to take action on a timely basis will mean a loss of transparency, access to competitive repair markets, and it will inhibit the development of innovative services that might improve the car owning and driving experience.

Magnuson Moss Warranty Act

Adding to the issues facing the independent aftermarket is the growing use of scare tactics to move car owners away from using parts and service that are outside of the control of the manufacturer. Auto Care Association has been alerting the Federal Trade Commission to some of the most egregious practices for nearly a decade and we have included copies of the multiple letters we have sent the FTC. These letters span the gamut of issues from Honda's bulletin disparaging the use of non-original equipment (OE) parts, to a particularly troublesome bulletin from Kia that could have endangered the car owner. Specifically, Auto Care Association and other aftermarket groups filed complaints with the FTC back in 2012 regarding a bulletin issued by Kia that warned against the use of an aftermarket oil filter. Without providing any details, Kia sent a bulletin to their dealerships that they should remove any aftermarket oil filters from vehicles taken into their shops and replace with an OE oil filter at a charge to the customer. This bulletin was actually the subject of an article in Consumer Reports that recommended for Kia owners to go to the dealer for oil changes in order to not jeopardize warranties.

Auto Care Association and others in the aftermarket sent a follow-up letter to the agency in 2016 with an update that provided evidence of the reason behind the Kia OE filter requirements. Specifically, testing demonstrated that the engine on Kia vehicles had abnormal oil pressure, causing the oil filters to burst and resulted in extensive engine rebuild costs to consumers. Kia could have put a bulletin out that warned of the safety issues, but instead chose to cover it up and blame the issue on the use of aftermarket filters. While the problem with Kia has now resulted in NHTSA action, this illustrates some of control that the vehicle manufacturer is able to exert absent any oversight by the FTC.

The problem related to Magnuson Moss has two sides: One--there is little enforcement of the law at both the manufacturer and the authorized dealer level and two--most car owners are unaware of Magnuson Moss.

I have included the results of two surveys that were conducted in Florida and Maryland that illustrate this point. Both surveys show that about a quarter of consumers who purchase new cars are told by the dealer that they must have the vehicle serviced at the dealership in order to maintain the warranty. The survey further states that a vast majority of consumers think they should not have their vehicle warranty voided if they have work performed outside of the warranty and most owners further think that they should be informed in writing regarding their warranty rights.

The survey results strongly indicate that more education is needed. The FTC has placed information on their website that is very helpful regarding Magnuson Moss, but we believe additional and more pinpointed education programs are necessary. The State of Connecticut requires that new car dealers provide a notice when a vehicle is purchased regarding the consumer's rights under the new car warranty.

There have been attempts in other states, but these have been strongly opposed by the vehicle manufacturers and the new car dealers. We believe that educating the consumer regarding warranties might help contradict issues that occur every day in the dealership regarding misleading information on warranties. Such notices should also be given when a warranty is rejected by a dealership since many dealerships might not be aware of the law.

In summary, the Auto Care Association urges the Commissions to play a major, proactive role in promoting competition in the repair industry. Simply having laws like Magnuson Moss are not enough; there must be strong, vigorous enforcement and aggressive education of consumers. However, the FTC also must look at the emerging technologies that are coming on vehicles and recognize that while they could have beneficial impacts, the government has a role in making sure they are not used to eliminate competition for the repair of the products.

We hope this current effort will result in a further examination and action by the FTC that will increase competition in the repair industry and ensure that consumers are able to take advantage of new technologies and the innovation and services that will be available from their implementation. While companies need to be provided protection for their innovations, those protections should not go beyond the intellectual property used to design and build those products to include how they are serviced and what services might be available for the owners while the cars are in use.

There are also issues related to parts availability from manufacturers and issues related to the servicing of vehicles equipped with Advance Driver Assist Systems which are outlined in submissions from LKQ. We echo these concerns and believe they should be considered by the FTC as part of this effort.

Thank you again for the chance to comment and we look forward to participating in the July workshop. Please feel free to reach out to me should you have any questions or comments regarding this submission.

Sincerely,

A handwritten signature in black ink that reads "Aaron Lowe". The signature is fluid and cursive, with the first name "Aaron" being larger and more prominent than the last name "Lowe".

Aaron M. Lowe
Senior Vice President
Regulatory and Government Affairs