

On November 3rd here in Massachusetts there will be a question on the ballot about updating our Right to Repair Law. A yes vote on Question 1 would update the current law and grant access to telematic and wirelessly transmitted data to the vehicle owner and independent repairers.

I run a small family-owned shop in Lawrence, MA where we specialize in hybrid and electric cars. I am also the Vice President of the New England Service Station and Automotive Repair Association (NESSARA), an advocacy and training group for the automotive industry headquartered in Massachusetts.

When campaigning for this measure, supporters often state the old argument that independent repair shops like mine lack the tooling and information necessary to effectively repair vehicles. The Massachusetts Right to Repair Coalition (R2R Coalition) started its “Yes on 1” campaign repeating this old argument from the last Right to Repair fight in 2013. The argument is false and potentially damaging to independent repairers. For example: I work on a lot of Toyota Prius. Using my Techstream subscription coupled with my VSP credentials, I can do anything that a Toyota dealer can, provided I invest in the right tools. When I first heard this initial argument repeated by the R2R Coalition, I was against Question 1 on principle, and viewed it as an attempt by the R2R Coalition to rally their old troops.

As time went on, the R2R Coalition presented new arguments, one of which was featured in a WBUR article as the following scenario:

“Let's say you're driving along, and your starter's going to go out. So the manufacturer pings the car and says, 'Hey, go to a dealership right now. Your starter's about to go out.'”

You say, 'Well, I have a trusted, independent repairer. I've been using him for 15 years. He's a local guy.' I go down to the independent repair shop, he plugs into the [on-board diagnostic] port, and no code comes up for the starter. So, he says, 'Nothing wrong with your car.'”

You leave. Ten miles out, your starter goes out. What then? You've lost faith in your independent repairer. You're broken down. It's too late because you didn't go to the dealership. And, so you're being forced to the dealership on something that your independent repairer should be able to fix.”

Technical inaccuracies aside, statements like this make me think about things like brake pad wear sensors and Mode 6 data. We know that the manufactures are already using telematics to push maintenance and repair work back to the dealers. Manufacturers are emailing drivers when maintenance reminders pop up, advertising the local dealer, and even using the vehicle’s navigation screens to locate the nearest dealer. Independent repair shops are at an obvious disadvantage.

The main financial backer of the R2R Coalition is the Auto Care Association (ACA), an advocacy group comprised of parts manufacturers and distributors. Their leadership consists of representatives from companies such as AutoZone, Advance Auto Parts, Federated Auto Parts, NAPA, Dorman Products, Standard Motor Products, Bosch and many more companies in the aftermarket automotive repair supply chain. ACA members are currently cut out of the data stream that modern telematic cars emit and they want to change that.

A key part of the new Right to Repair amendment that is not getting much publicity is Section 3 which states that starting in model year 2022, any vehicle sold in Massachusetts *“shall be required to equip such vehicles with an inter-operable, standardized and open access platform across all of the manufacturer’s makes and models. Such platform shall be capable of securely communicating all mechanical data emanating directly from the motor vehicle via direct data connection to the platform.”* What is being described is a standardized gateway module that will lock down the car’s computer network from communicating via the DLC. The section goes on to say that the *“platform shall be directly accessible by the owner of the vehicle through a mobile-based application.”* This part of the bill raised many questions for me, most of which have not been answered. The R2R Coalition has described this to me as a process by which the vehicle owner will use a mobile app to “grant access” to the service provider they choose, either the dealer or an independent repair shop. What if the customer does not use a smart phone? What happens during an OBD state emissions test? Many manufacturers build in desirable features like remote starting and infotainment into their telematic systems. Will customers be required to grant dealers exclusive access to keep those features (effectively excluding independent shops from diagnosing and repairing vehicles)? How is the access transferred if the vehicle is sold, especially if the sale is private? What if someone other than the owner, such as an adolescent, bring the car in for service?

The ACA has conveniently developed a vehicle-side interface and driver-side mobile app that meet the definition of an *“inter-operable, standardized and open access platform”* required by the amendment, called the Secure Vehicle Interface (SVI). I have not seen SVI in action but it was debuted at the 2018 APPEX conference. If SVI is adopted, imagine this scenario: Your check engine light turns on while driving. In your center display, a message pops up saying your vehicle set a trouble code for an oxygen sensor along with a map directing you to the closest O’Reilly Auto Parts or Bosch Service Center. Do you install customer-supplied parts? Is your shop a Bosch Service Center? How would SVI affect how we connect to the vehicle?

The opponents of the bill are the Coalition for Safe and Secure Data, which is financially backed by the Alliance for Automotive Innovation (Auto Innovators), whose members are essentially every automaker selling cars in the US and the technology companies they partner with to develop vehicles. The Auto Innovators are currently waging a fear mongering campaign, claiming that bad actors will hack connected cars if the bill passes. Their example is that a stalker or sexual predator could use call logs and GPS data to track and monitor their victims.

There is merit to the argument that connected cars are at risk. I have heard the following hypothetical: An aftermarket scan tool company’s servers are hacked and the hacker uploads malware to every scan tool that connects to the server for an update. The malware is then uploaded to every car the scan tool connects to. The malware would then disable every infected vehicle at the same time on the same date or cause the throttle to go wide open causing rampant accidents. I do not like the idea of my wife driving around with my son in a world where that is possible.

Currently, telematic data is not strictly necessary to fix a car. The future is where I think the bill becomes powerful. The bill defines *“Telematics systems”* as *“any system in a motor vehicle that collects information generated by the operation of the vehicle and transmits such information ... utilizing wireless communications to a remote receiving point where it is stored.”* Today, I plug my scan tool into an EPA mandated Data Link Connector and get everything I need. What happens when the DLC goes away

entirely? The example is Tesla. When the EPA certified the Model 3, it stated in its report, under OBD Deficiencies Comments, "*Battery Electric Vehicle - No OBD requirements.*" Teslas do not have DLCs other than the early Model S, which reportedly only had vehicle power and ground populated, and did not connect to the vehicle's computer network. This lack of connection, coupled with the fact Tesla will not release their diagnostic software to the aftermarket or even sell us parts, is in direct violation of the original 2013 law. I know the "lack of dealerships" and "Tesla is a technology company, not a car company" claims and don't buy it. All software updates on Teslas are done wirelessly. A Tesla certified body shop can connect to a vehicle using Telsa Toolbox via an ethernet cable but my understanding is the functions are limited compared to a Tesla Service Center. I am starting to see Teslas in my bays for simple services. What am I going to do when one is towed in with a major issue?

Teslas are a small percentage of the cars on the road but what if the big manufactures adopt their model? The EPA has set the precedent that no emissions means no DLC. The big manufacturers leave the DLC in so their legacy scan tools and dealer techs can work on their EVs. What if GM decides to make their Buick line all-electric and sell their cars from boutique storefronts?

The industry is also speculating that the scan tool as we know it is going away. Rather than physically plugging in an interface, coupled with a laptop and software, the scan tools will be built into the cars. A technician will log in to the cloud and do what he or she needs to do on the vehicle. Most updates will be done wirelessly on the go, like Tesla. How many of you make money performing calibration updates?

In summary, the fight is over big data. On principle, I'm opposed to the arguments and campaign tactics being presented by each side; however, the bill will hopefully secure me the access I need to fix the car of the future. The issue is bigger than Massachusetts – it is global. If the new Right to Repair passes it could easily end up in the Supreme Court. Each person needs to decide for themselves how to vote. Personally, I am voting YES on Question 1. We can't let the Perfect be the enemy of the Good.