U.S. Department of Transportation
National Highway Traffic Safety Administration

NHTSA

August 22, 2023

Eric A. Haskell
Assistant Attorney General
Office of the Attorney General
Commonwealth of Massachusetts
One Ashburton Place
Boston, MA 02108

Dear Mr. Haskell:

Thank you for your engagement with the United States Department of Transportation, National Highway Traffic Safety Administration (NHTSA), and our other Federal government partners to advance our mutual interest in ensuring safe consumer choice for automotive repair and maintenance. NHTSA strongly supports the right to repair. We are pleased to have worked with you to identify a way that the Massachusetts Data Access Law may be successfully implemented—promoting consumers' ability to choose independent or do-it-yourself repairs—without compromising safety. We write to confirm our mutual understanding of that path forward.

As you are aware, NHTSA's concerns regarding the Massachusetts Data Access Law arise from the risk associated with the ability to, at scale, remotely access and send commands that affect a vehicle's critical safety systems.

Based on our further conversations, NHTSA understands that, according to the Massachusetts Attorney General, one way that vehicle manufacturers can comply with the Data Access Law is by providing independent repair facilities wireless access to a vehicle from within close physical proximity to the vehicle, without providing long-range remote access. For instance, NHTSA understands that, according to the Attorney General, vehicle manufacturers could comply with the Data Access Law by using short-range wireless protocols, such as via Bluetooth, to allow the vehicle owner or an independent repair facility authorized by the owner to access all "mechanical data," as defined by the Law, for that individual vehicle. In NHTSA's view, a solution like this one, if implemented with appropriate care, would significantly reduce the cybersecurity risks—and therefore the safety risks—associated with remote access. Limiting the geographical range of access would significantly reduce the risk that malicious actors could exploit vulnerabilities at scale to access multiple vehicles, including, importantly, when vehicles are driven on a roadway. Such a short-range wireless compliance approach, implemented appropriately, therefore would not be preempted.

NHTSA requests your confirmation that a solution allowing wireless access when in close physical proximity to the vehicle would be compliant with the Massachusetts Data Access Law.

Based on our discussions to-date, it appears that the Massachusetts Attorney General and NHTSA also share a common understanding that implementing this compliance option with the secure "open access platform," as required in the Law, is not immediately available, and that vehicle manufacturers may require a reasonable period of time to securely develop, test, and implement this technology. We welcome the opportunity to work with you and other stakeholders on the safe and timely implementation of this option.

Two additional points bear emphasis. First, NHTSA wishes to reiterate the point made in its June 13 letter that some vehicle telematics functions—when and if appropriately secured—can advance vehicle safety. Disabling vehicle telematic functions as an attempt to comply with the Data Access Law would harm vehicle owners, first responders, and other telematics users. For example, vehicle telematics can be life-saving technology, communicating essential data about a vehicle's location to emergency services in the event of a crash. Safety investigators, including police, NHTSA, and other governmental authorities, increasingly rely on access to vehicle data about crashes and other safety issues collected via telematics. NHTSA would have substantial concerns about the detriment to safety if vehicle telematics functionality were disabled, and believes such a result would disserve vehicle owner safety without advancing the right to repair.

Second, NHTSA wishes to emphasize that its concerns regarding risk associated with the broad ability to remotely access and send commands that control a vehicle's critical safety systems do not arise from a belief that any particular entity or person seeking to repair a vehicle—whether a vehicle manufacturer or manufacturer-affiliated dealer, an independent repair facility, or a do-it-yourself vehicle owner—necessarily poses a greater cybersecurity concern than another. Whenever access to write or execute command functionality remotely is contemplated, it is important to be vigilant to minimize risks. NHTSA works to minimize this risk at any level of access—whether by an original equipment manufacturer, dealer, or independent repair facility—and is continually overseeing existing systems for cybersecurity vulnerabilities. NHTSA supports technological developments that can enhance vehicle safety and consumer choice. NHTSA will continue to evaluate safety programs and protocols as technology in this area evolves, which may also enable additional safe compliance pathways under the Massachusetts Data Access Law.

NHTSA values the dialogue with the Massachusetts Attorney General toward achieving the dual goals of consumer choice in repair facilities and vehicle safety, and looks forward to continued dialogue to help ensure that vehicle manufacturers safely and expeditiously comply with their obligations under the Data Access Law and the Federal Vehicle Safety Act.

Sincerely,

KERRY ELIZABETH KOLODZIEJ

Digitally signed by KERRY ELIZABETH KOLODZIEJ
Date: 2023.08.22 12:23:02 -04'00'

Kerry Kolodziej
Assistant Chief Counsel
for Litigation and Enforcement