PUBLICATION

A Look Under the Hood: Massachusetts Updates Its Vehicle Right to Repair Law

November 13, 2020

On November 3, 2020, Massachusetts voters overwhelmingly voted "yes" on Question 1 of the State Election Ballot, thereby approving the Initiative Law to Enhance, Update and Protect the 2013 Motor Vehicle Right to Repair Law (the "Initiative") as an amendment to the Massachusetts Motor Vehicle Right to Repair Act (the "Act"). The Initiative requires that vehicle manufacturers provide motor vehicle owners and independent car repair facilities with expanded access to telematic (wireless) mechanical data related to vehicle diagnostics, maintenance and repair. While the Act has been in place in Massachusetts since 2013, the Act only regulated diagnostic information obtained from a "non-proprietary vehicle interface device" (e.g. a port) and did not contemplate telematic data. Automobile manufacturers, dealers, vehicle owners and independent repair shops need to consider key provisions from the Initiative in light of the new requirements.

Key Provisions

Beginning with 2022 models, the Initiative requires that all vehicle manufacturers selling new telematics-equipped motor vehicles into Massachusetts (including passenger and heavy duty vehicles) design their systems in such a way that vehicle owners and independent third-party repair shops have access to the vehicles' systems through an interoperable, standardized and open access telematics system.

System Specifications

The Initiative requires that:

- The telematics system must be accessible through a mobile-based application.
- The system must be "secure".
- The vehicle owner must have direct access to the telematics system through the mobile-based connection.
- Access to the telematic system must include read/write capabilities, including the ability to read mechanical data and to send commands to in-vehicle components (e.g. braking, acceleration, steering controls) for the "purposes of maintenance, diagnostics and repair".
- Upon authorization by the vehicle owner, all mechanical data must be accessible to an independent automobile repair facility for such time as is necessary to complete a repair or for such time as agreed to with the vehicle owner for the purposes of vehicle maintenance, diagnostics and repair.
- The manufacturer may not require, whether directly or indirectly, that access to the telematic system require any type of authorization, unless the system for accessing vehicle networks and their on-board diagnostic systems is made standard across all makes and models sold into Massachusetts and is administered by an entity that is independent of the manufacturer.

When selling a vehicle that contains a telematic system, a car dealership must provide a notice (to be developed by the Massachusetts Attorney General) to the prospective buyer, obtain his/her signature and provide him/her with a copy of the signed notice. Failure to provide this notice can be grounds for sanctions by the dealership's licensing authority, up to and including revocation of the dealership's relevant licenses.

If an owner of a vehicle or independent repair facility covered by the Act is denied access to the mechanical data, the owner or the facility may bring a civil action against the manufacturer for any remedies available under the law, and each denial of access is subject to treble damages or $10,000, whichever is greater.

Potential Cybersecurity Concerns

In a July 20, 2020 letter to Massachusetts State Representative Chan and Massachusetts State Senator Feeney, the National Highway Traffic Safety Administration raised various cybersecurity concerns regarding the Initiative, including the following:

- Due to the accelerated timeline, manufacturers may have to remove existing cybersecurity protections to meet the new access requirements, thereby leaving systems at an increased risk of cyber-attacks, which would increase the risk to public safety.

- The implementation of universal and standardized access requirements may increase the risk of a cyber-attack being successful. The requirement that systems be "secure" is vague and undefined and does not reflect best practices.

- The Initiative may prohibit manufacturers from complying with federal motor vehicle safety protocols.

Whether these concerns are well founded remains to be seen.

Key Takeaways

With the 2022 deadline for implementation of the Initiative rapidly approaching, vehicle manufacturers must begin working towards compliance now. Failing to do so can lead to substantial consequences.

If you have questions, or would like to learn more about the Initiative, any related laws, or any aspect of your data privacy and cybersecurity practices, please contact any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.