ALLIANCE FOR AUTOMOTIVE INNOVATION

LD 2211 - Cybersecurity Flaws and Holes

"This bi-directional, open access model could be an open invitation to cyber terrorism."

"...the current bill could create an environment ripe cyber terrorism..."

Brian Reimer, MIT Cybersecurity Researcher
Testimony to Massachusetts Legislature, 2020

"NHTSA is also concerned about the increased safety-related cybersecurity risks of a requirement for remote, real-time, bi-directional access."

"This would raise substantial safety risks for American families."

National Highway Traffic Safety Administration
Testimony to Massachusetts Legislature, 2020

"A malicious actor here or abroad could utilize such open access to remotely command vehicles to operate dangerously, including attacking multiple vehicles concurrently. Vehicle crashes, injuries, or deaths are foreseeable outcomes of such a situation."

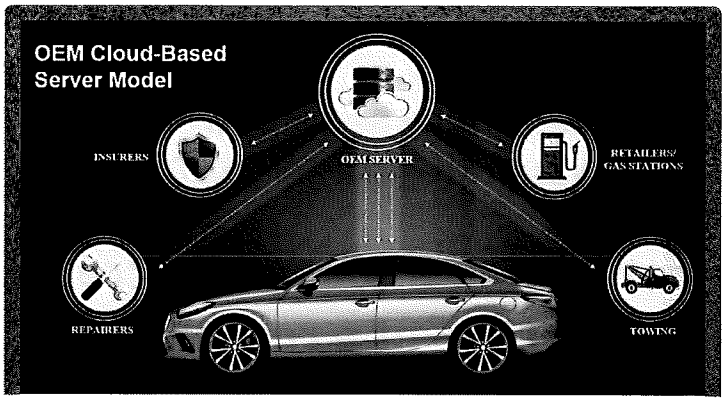
National Highway Traffic Safety Administration –
Letter to Autos, Instructing to Not Follow the Massachusetts Law, 2023

Extended Vehicle Model vs. Secure Vehicle Interface

Critically Different Cybersecurity and Privacy Controls

Cyber-Secure Data Access Model in LD 1228

- **Where is the data housed?** Secure OEM cloud-based servers. Data is constantly transmitted via a secure encrypted wireless network.
- **How does data get to authorized repairers?** Data transmitted directly from OEM server to owner-authorized entity via a secure encrypted wireless network.
- **Why is this important?** By keeping the automaker as the party responsible for delivering the data, it can be managed in a cybersecure way. This is the preferred method of federal regulators - if there is ever a problem, they want one clearly responsible party.



Cyber-Insecure Data Access Model in LD 2211

- **Where is the data housed?** Vehicle data is stored directly on the vehicle.
- **How does data get to authorized entities?** Data is transmitted directly from the car to any entity that the consumer authorizes to have the data, utilizing a cellular network connection.
- **Why is this important?** With each new connection to the vehicle that LD 2211 creates, a new pathway for hackers to also gain access to the vehicle is created. Every repair shop could be a target of hackers, as they now could be a pathway to installing ransomware on a vehicle, as their shop has a direct connection.