



Published on *Search Autoparts* (<https://www.searchautoparts.com>)

[Search Autoparts](#) > [Print](#) > > The aftermarket telematics debate between data security and access

The aftermarket telematics debate between data security and access

By *badams*

Created 03/08/2018 - 15:59

Submitted by badams on Thu, 03/08/2018 - 15:59

As telematics systems become part of, and evolve into, a “connected car” ecosystem in new automobiles, consumer privacy and technology security advocates have begun ringing alarm bells about the new vulnerabilities these systems represent.

A mix of telematics and other types of connectivity solutions have emerged – dongle-based third-party systems, usage-based insurance (UBI) solutions, smartphone-connected systems, and increasingly advanced (and proprietary) OEM systems. If not properly secured, these systems could be used by hackers to gain access to drivers’ personal information or payment data, or (in a worst-case scenario) gain control of systems within the vehicle itself.

“This isn’t just security on a phone connected to a vehicle, but the security of the over-the-air updates the manufacturer issues, or security of the data being collected when the car transmits to the cloud,” says Christina Segal, vice president and general manager of connected vehicle systems at Honeywell. Honeywell recently partnered with LG Electronics to develop a cybersecurity solution for connected vehicles. The solution could detect anomalies that indicate an intentional hack of a vehicle while protecting in-vehicle network traffic.

Automotive OEMs are increasingly using security concerns as a justification for further lock down of their own telematics systems and access to vehicle data via OBDII ports. In the “Cybersecurity for Modern Vehicles” guidance that the National Highway Traffic Safety Administration (NHTSA) issued recently, limiting third-party device access to vehicle systems was listed as a best practice.

That type of limitation is a threat to aftermarket companies that want continued access to vehicle data, and worry that OEM telematics systems will increasingly be used to control vehicle data and drive more repair business to dealerships.

The Auto Care Association and other industry organizations are working together to develop alternatives that would ensure aftermarket access to vehicle data.

For example, the industry successfully lobbied to have language supporting open access inserted into the AV START Act, a bill targeted at promoting safe development of self-driving cars. Senator James Inhofe (R-Okla.) added an amendment to the bill that requires the Department of Transportation to convene a federal advisory committee to provide recommendations on “with respect to the ownership of, control of, or access to, information or data that vehicles collect, generate, record, or store in an electronic form that is retrieved from a highly automated vehicle or automated driving system.”

"We're hoping that the bill can go out without objection," says Aaron Lowe, senior vice president of government affairs for the Auto Care Association. "The Inhofe amendment is not in the House version of the bill, though. What the amendment does is begins the discussion of how consumers can control access to data."

The Auto Care Association always has held that vehicle data belongs to the vehicle owner, a position shared by large fleet owners and rental car companies. Optimally, the consumer would be the gatekeeper as to where the data goes, not the OEM.

"We view that as important, because if the owners can decide where the data goes, they will likely direct the data to the independent service industry," Lowe says. "It's a big fight, and we need the independent aftermarket to contact their legislators to support this."

However, the bill has stalled in Senate in part because of concerns around privacy and cybersecurity.

Last year, the Auto Care Association also rolled out its Secure Vehicle Interface (SVI) model at the AAPEX show, and met with a positive response from the industry.

The organization is working with the Society of Automotive Engineers (SAE), International Society for Standardization (ISO), and other standards bodies to gain industry wide support for the SVI.

"We are taking a two-pronged approach," says Joe Register, vice president of emerging technologies at the Auto Care Association. "We are working through the standards bodies because they have access over new car architectures. We are also working to make sure the interests of the aftermarket are served and the standards are equally applicable to retrofit devices."

OEMs, on the other hand, support what is known as the Extended Vehicle (ExVe) methodology, which gives the automakers full control of vehicle data access via proprietary, cloud-based servers. SVI would provide access for both the aftermarket and automakers using shared servers.

"The SVI model is a way to make sure that all the information that comes in and out of the vehicle uses the same standard specifications," Register says. "So if an automaker wants a particular piece of information, they can get it, but in the same way everybody else gets it. Requests can be throttled based on priority. It's a different philosophy [than ExVe]."

The SVI model provides protection via a gateway to the vehicle systems, whether access is through wired or wireless systems. "Right now the manufacturers spend the bulk of their energy trying to protect the OBD port, but that's not the only part of the vehicle that is vulnerable," Lowe says.

There has been resistance to the SVI model within ISO and SAE, however, which could potentially put vehicle data access at risk. "The problem is really getting the standards groups to move this along so the car companies can adopt it," Lowe says.

"We want to make sure we have the same access to the data that the car companies have," Lowe says. "If repairers have to go through the manufacturer's servers to get the data, that's not good for the independent aftermarket."

"We think the information that comes from the operation of the vehicle is the customer's information," Register says. "Everything we do is from the standpoint of being able to make sure the customer retains their ability to get the data and control their choice of where it's being repaired."

Subscribe to Aftermarket Business World and receive articles like this every month....absolutely free. [Click here.](#)

[Aaron Lowe](#) [Auto Care Association](#) [Automotive Aftermarket Technology](#) [Distribution News](#) [Honeywell](#) [Market Trends & Analysis](#) [National Highway Traffic Safety Administration](#) [NHTSA](#) [telematics](#) [News: Distribution](#)

[Aaron Lowe](#) [Auto Care Association](#) [Automotive Aftermarket Technology](#) [Distribution News](#) [Honeywell](#) [Market Trends & Analysis](#) [National Highway Traffic Safety Administration](#) [NHTSA](#) [telematics](#) [News: Distribution](#)

[Motor Age](#) [ABRN](#) [Aftermarket Business](#) [Nace Automechanika](#) [Training Courses](#)



[Privacy Policy](#) [Terms of Service](#) [Legal Entities](#)

©2018 UBM. All rights reserved. [A UBM Company.](#)

Source URL: <https://www.searchautoparts.com/aftermarket-business/automotive-aftermarket-technology/aftermarket-telematics-debate-between-data-se>