

**Paul  
Roberts**

**Founder**

[paul@securepairs.org](mailto:paul@securepairs.org)

**SecuRepairs**

54 Cross Street

Belmont, MA 02478

617 817 0198

---

March 14, 2021

## Introduction

These comments are submitted on behalf of SecuRepairs.org (SecuRepairs) in response to a request by the National Highway Traffic Safety Administration (NHTSA) for comments on January 12, 2021, entitled “Request for Comment on Cybersecurity Best Practices for the Safety of Modern Vehicles”, Docket No. NHTSA-2020-0087.

## Statement of Interest

SecuRepairs ([securepairs.org](https://securepairs.org)) is a not for profit group of more than 200 of the country’s top information technology and information security experts. [Our membership](#) includes leading executives, academics, security researchers and information security professionals who support a digital right to repair. SecuRepairs has been closely involved in efforts to expand the right to repair automobiles and to warn about the risk of software-enforced monopolies on parts and service in the era of connected vehicles. We were vocal in support of Question 1 in Massachusetts, an expansion of that state’s automobile right to repair law that passed with overwhelming public support on November 3.

## Comments

Automobiles are on the front line of the fight to repair in the United States. We believe the draft updates to vehicle cyber security guidelines raise red flags for repair advocates and could run afoul of state right to repair laws as well as NHTSA’s own stated intention (in G.43) not to “unduly restrict access by alternative third-party repair services authorized by the vehicle owner.”

Our areas of concern are outlined below:

### Section 6.1 Vehicle Manufacturers

**[G.40]** Specifies that “any connection to a third-party device should be authenticated and provided with appropriate limited access.”

SecuRepairs applauds that guidance and the concept of “least privilege” for any third party device attached to a connected vehicle. However, we also echo the concerns of the National Motor Freight Traffic Association (NMFTA) and others that the final guidelines should make clear that delegation of trust for the authentication and subsequent authorization of the third party device should lie with the vehicle owner and long-term lessee, rather than with the OEM. Without such language, vehicle manufacturers will have de-facto “gatekeeper” roles in deciding what devices can be coupled with their vehicles, creating the risk of anti-competitive practices (see recent lawsuits targeting Apple’s

AppStore)<sup>1</sup> not to mention costly “rent seeking” and other anti competitive behaviors that will be detrimental to owners, while adding little in the way of security protection.

#### Section 8.4 Diagnostic Tools

(T.8) recommends that “vehicle and diagnostic tool manufacturers should control tools’ access to vehicle systems that can perform diagnostic operations and reprogramming by providing for appropriate authentication and access control.” That recommendation “responds to research demonstrating the ability to leverage diagnostic tools to reverse engineer and implement vulnerabilities in vehicle systems,” the guidelines explain.

We believe this language runs contrary to NHTSA’s stated position in G.43 and runs afoul of laws such as Massachusetts’ vehicle right to repair law. While access to vehicle systems should be secure and authenticated, we concur with the position of interested parties such as NMFTA that vehicle owners should control delegation of trust for authentication to the vehicle, and that any subsequent authorization must be under the control of the vehicle owner or long-term lessee, not the manufacturer. NHTSA should remove language stating that vehicle manufacturers are responsible for “providing for appropriate authentication and access control” and refrain from adopting any policy the result of which is to give manufacturers final say over access to and protection of the vehicle bus. In our opinion, such language would be used by automakers to limit access by owners and their agents for the purposes of service and repair, creating expensive, *de-facto* monopolies on aftermarket parts and service.

We agree with NMFTA, as well, that final NHTSA guidelines should clearly define a range of third-party devices that are connected to a vehicle to which the guidelines will apply while also encompassing yet-to-be developed devices that rely on logical access (wired or wireless) to vehicle data.

#### Section 8.5 Vehicle Internal Communications

(T.10) requires that “critical safety messages, particularly those passed across non-segmented communication buses, should employ a message authentication method to limit the possibility of message spoofing.” SecuRepairs supports the use of message authentication to prevent spoofing. However, any guidelines should be written so as to provide vehicle owners and lessees or their agents to be able to authenticate to the vehicle bus. Allowing vehicle OEMs (rather than vehicle owners) to be the authentication authority will violate G.43 as well as state vehicle right to repair laws and lay the groundwork for OEMs to exclude owners and their agents from any repair requiring access to the vehicle network.

---

<sup>1</sup> <https://edition.cnn.com/2020/08/13/tech/fortnite-apple-store-removed/index.html>

## Section 8.8 Software Updates/Modification

(T.22) recommends automakers “Maintain the integrity of OTA updates, update servers, the transmission mechanism and the updating process in general.”

We oppose this language as written, as we believe it would violate G.43. Looked at together with (T.21), which recommends that auto manufacturers employ state-of-the-art techniques for limiting the ability to modify firmware to authorized and appropriately authenticated parties” this language lays the policy groundwork for exclusive manufacturer control over the critical software update process.

Among the questions that NHTSA’s final guidelines should clarify are:

1. Who or what counts as “authorized” parties? NHTSA guidelines should clarify that vehicle owners or lessees and their agents (independent repair shops) shall be considered authorized parties. Absent such clarifying language, vehicle OEMs would be free to constrain access to licensed dealerships and repair providers contravening G.43 and specific guidelines in Massachusetts’ right to repair law.
2. NHTSA’s guidelines should specifically define what the agency means by “modifying firmware.” Doing so will prevent overly restrictive policies that will counteract G.43 and state right to repair laws. Specifically, NHTSA should clarify that merely downloading and applying an update of vehicle firmware to a vehicle does not count as “modification.” Absent clarifying language, SecuRepairs worries that NHTSA guidance will be read as implying that only OEMs and their authorized service providers should have the exclusive right to apply software updates to cars. Such a restriction would constrain owner and independent repair (per G.43) and be burdensome especially in areas of the United States in which visiting an authorized dealership may involve a multi-hour drive by the vehicle owner. Nothing in NHTSA’s guidelines should prohibit a vehicle owner from downloading or obtaining a software update and applying it themselves.
3. NHTSA’s guidelines should make clear that vehicle owners and their agents be given access to OEMs OTA updates and servers using a standardized interface, access to which is provided at a reasonable fee. Laws like Massachusetts 2013 vehicle right to repair law specifically prohibit OEMs from creating proprietary interfaces for maintenance that lock out independent repair and owners. NHTSA’s guidelines should be mindful of these laws and strive not to contravene them.

## Conclusion

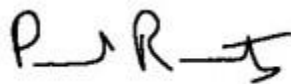
As security experts, we firmly believe in the concept that there is no “security in obscurity.” In other words: limiting access to or knowledge of the workings of connected cars does not protect them from attacks or harm. That is because cyber criminals are both determined and resourceful.

Rather, we believe that the best path to a future, secure ecosystem of connected vehicles requires greater transparency about the workings of vehicle software, hardware and communications, as well as a vibrant ecosystem of owners, independent security researchers and independent repair professionals. Encouraging automakers to open their vehicle platforms to scrutiny by outside experts (including through bounty programs) will help keep the cybersecurity of vehicle fleets strong.

And, as automakers look to leverage apps and driver data to supplement declining car sales revenues, NHTSA should look out for the interest of vehicle owners and lessees: giving them - rather than automakers - ultimate control over authentication and authorization decisions for their vehicle...their property.

Whatever their accomplishments, the updated NHTSA guidelines must prevent, at all cost, a situation in which consumers face maximum pain (a costly manufacturer monopoly on aftermarket parts, repair and service) for minimum cyber security and safety gain in the form of a “black box” system that confuses obscurity with security. We urge you to take our suggestions into account as you move forward with these guidelines.

Sincerely,

A handwritten signature in black ink, appearing to read "P. Roberts". The signature is stylized with a horizontal line under the "P" and a long horizontal stroke extending from the "t".

**Paul Roberts | [paul@securepairs.org](mailto:paul@securepairs.org)**