

Connected Vehicles & Telematics

What you need to know and how GSA and other Federal stakeholders are taking action to protect the Federal fleet community

Agenda

- **What are Connected Vehicles Anyways?**
 - Why should I care?
 - V2V, V2I, V2X - huh?
 - Real World Examples Already Live
 - Avenues of Exploitation
- **Federal Fleet Community Best Practices & Expectations**
 - You're not alone
 - Dos and Don'ts
 - Voluntary standards
 - Upcoming changes

Agenda cont.

- **How Does Telematics Factor?**
 - Telematics is connected vehicle technology
 - GSA's Controls
 - Cyber security standards
- **Conclusion and Takeaways**
 - Do's and Don'ts
- **Q&A**

Why Care and What Are Connected Vehicles???

Why Care???

The Washington Post
Democracy Dies in Darkness

CONSUMER TECH

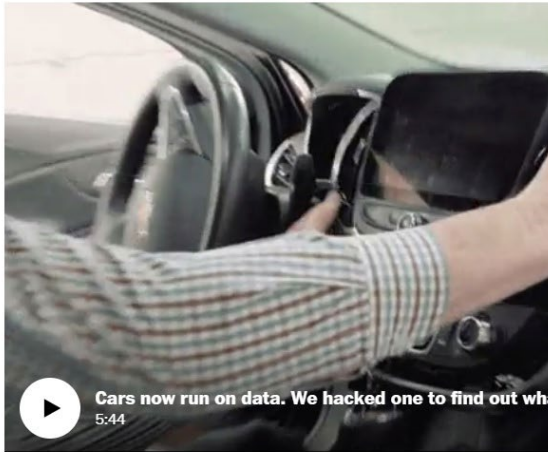
What does your car know about you?

Our privacy experiment found that automakers collect data through h connection. Driving surveillance is becoming hard to avoid.



Perspective by [Geoffrey A. Fowler](#)
Columnist | + Follow

December 17, 2019 at 7:00 a.m. EST



Cars now run on data. We hacked one to find out what
5:44

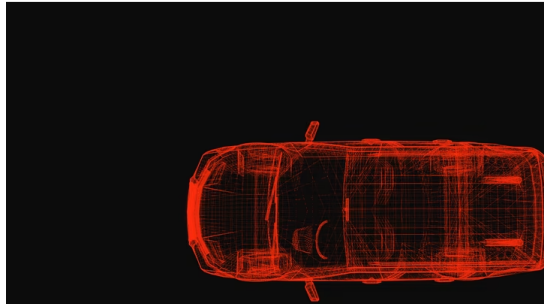
The Atlantic

TECHNOLOGY

Car Hackers Are Out for Blood

The rise of “smartphones on wheels” is ushering in cybersecurity that have never before existed on America’s roads.

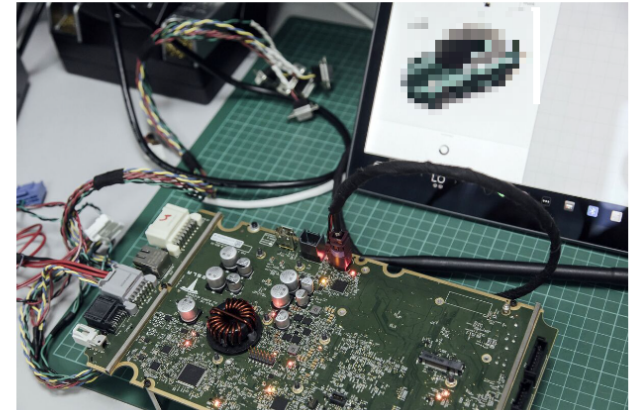
By Patrick George



Bloomberg

The Rise in Car Thefts Has Experts Searching for Weak Spots

Criminals can exploit everything from a vehicle’s Bluetooth connection to a headlight’s wiring, but white hat hackers are trying to improve security.



A motherboard in the hardware lab at Synaktiv headquarters in Paris.

Photographer:
Cyril Marcellhacy/Bloomberg

By [Jordan Robertson](#)

September 20, 2022 at 8:00 AM EDT

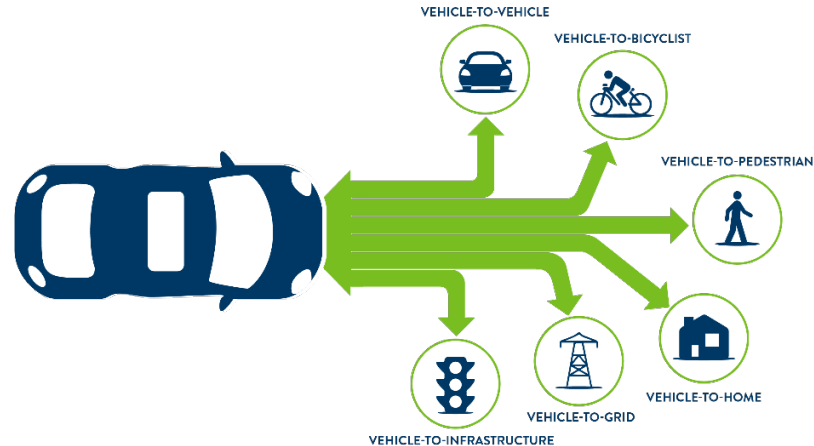


FedFleet 2024 5

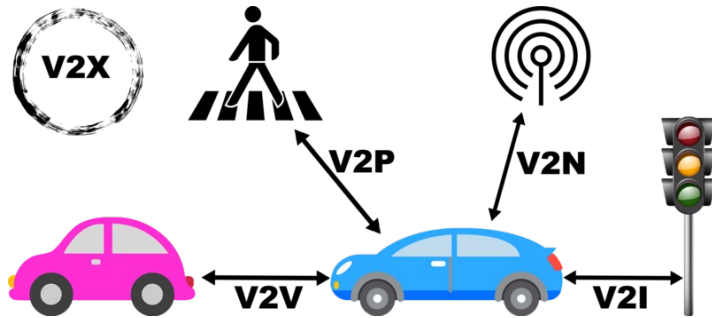
What is a Connected Vehicle

A connected vehicle is one that can communicate bidirectionally with other systems outside the vehicle

- **Vehicle-to-Everything (V2X)**
 - All categories of communication systems that transmit or receive critical information.



Connected Vehicle Communications



- **Other V2X categories**
 - **Vehicle-to-Vehicle (V2V)**
 - Real time data communication with other vehicles
 - **Vehicle-to-Infrastructure (V2I)**
 - Communication to external sensors such as connected roadways, traffic lights, lanes, etc.
 - **Vehicle-to-Grid**
 - Data exchange with electric smart grids to balance loads better
 - **Vehicle-to-Cloud**
 - Remote diagnostics, Over-the-Air Updates, Telematics
 - **Vehicle-to-Pedestrian**
 - Alert pedestrians of vehicle's presence

Connected Vehicle Capabilities and Benefits

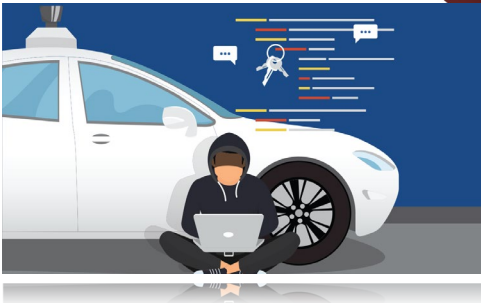
- **Over-The-Air Updates (OTA)**
 - Software updates delivered over wireless networks
 - Reduces need to bring vehicle to a dealer
 - Patches vulnerabilities
- **Advanced Driver Assistance Systems (ADAS)**
 - Systems such as crash avoidance takes human error out of driving to reduce vehicle accidents
- **Larger Datasets of Operating Information**
 - Allows fleet managers to analyze more data points in order to evaluate utilization and misuse of vehicles
- **Vehicle Feature Unbundling**

Connected Vehicle Capabilities and Benefits

Connectivity & Over-the-Air (OTA) Updates	Zero Emission Vehicles (ZEVs)	Servicing Vehicles	Software Subscriptions
OTA Cybersecurity	Charging Infrastructure	Parts & Service Efficiencies	Telematics
Fixed Operations Optimization	EV Incentives	Fixed Operations Optimization	Vehicle Feature Unbundling
Warranty & Recall Solutions	EV Product & Service Offerings	Innovation in Parts & Service	Other Data Subscriptions

How are vehicles targeted?

```
1: kdb dt _PEB @peb -y KernelCallbackTable
CVE_2018_8453!_PEB
+0x058 KernelCallbackTable : 0x00007ffc`46133070 Void
1: kdb dps 0x00007ffc`46133070
00007ffc`46133070 00007ffc`460d2bd0 USER32!_fnCOPYDATA
00007ffc`46133078 00007ffc`4612ae70 USER32!_fnCOPYGLOBALDATA
00007ffc`46133080 00007ffc`ebc`f10f0 CVE_2018_8453!_fnMORDD_hook [c:\project
00007ffc`46133088 00007ffc`ebc`f1340 CVE_2018_8453!_fnMORDD_hook [c:\pro
00007ffc`46133090 00007ffc`460d96a0 USER32!_fnMORDDPTIILPMSG
00007ffc`46133098 00007ffc`4612b4a0 USER32!_fnIUIOUTDRAG
00007ffc`461330a0 00007ffc`460d5d40 USER32!_fnGETTEXTLENGTHS
00007ffc`461330a8 00007ffc`4612b220 USER32!_fnIICITOUTSTRING
00007ffc`461330b0 00007ffc`4612b750 USER32!_fnIICITOUTSTRINGULL
00007ffc`461330b8 00007ffc`460d75c0 USER32!_fnIILPCOMPAREITEMSTRUCT
00007ffc`461330c0 00007ffc`ebc`f1430 CVE_2018_8453!_fnIILPCREATESTRUCT_hook
00007ffc`461330c8 00007ffc`4612b2e0 USER32!_fnIILPDELETEITEMSTRUCT
00007ffc`461330d0 00007ffc`460db00 USER32!_fnIILPDRAWITEMSTRUCT
00007ffc`461330d8 00007ffc`4612b330 USER32!_fnIILPHELPIFOSTRUCT
00007ffc`461330e0 00007ffc`4612b330 USER32!_fnIILPHELPIFOSTRUCT
00007ffc`461330e8 00007ffc`4612b430 USER32!_fnIILPDICREATESTRUCT
```

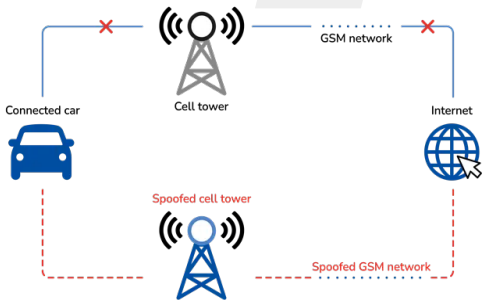


1 0-Day Exploit

2 PII Scrapping

3 Man-in-the-Middle Attack

4 Worst case scenario: Vehicle takeover



Potential for Exploitation

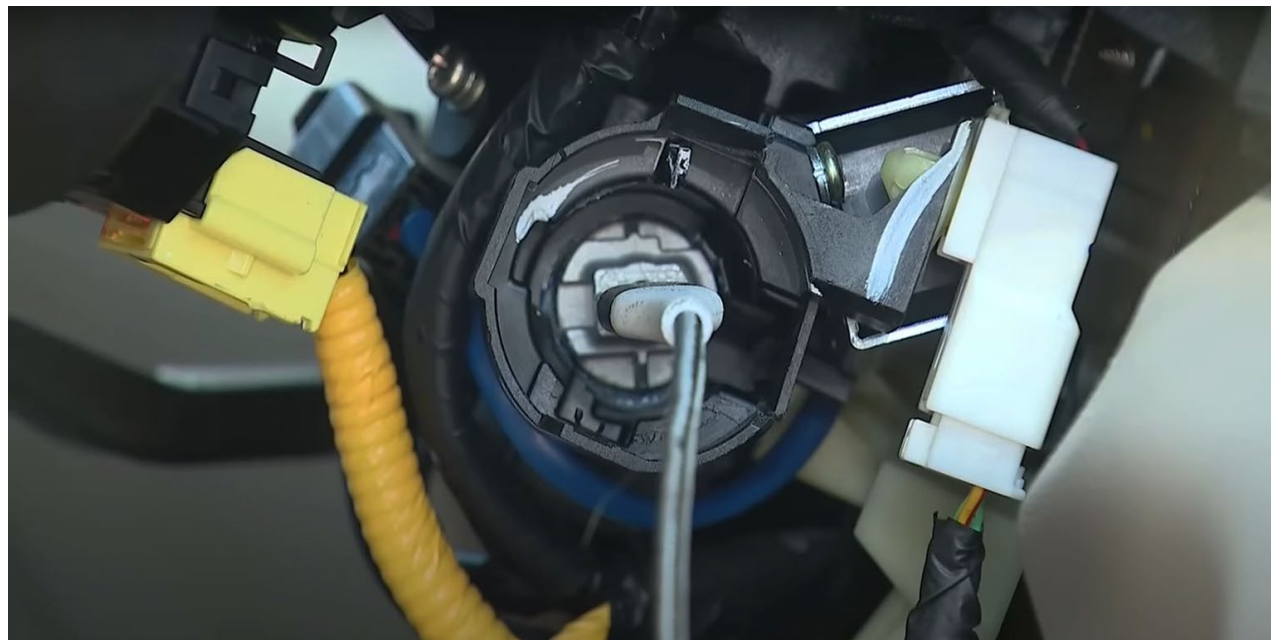
- Previous scenarios are complex attacks
- **Most “hacks” attack the path of least resistance**
- Example: Luxury car stolen with repeater signal from key fob



- Easy to buy cheap parts to build repeater
- Grabbed signal from the key fob in less than 1 minute
- Relay antennae used to strengthen signal from the fob inside the victim’s house

Potential for Exploitation

- Even simpler “hack”
- Example: OEM vulnerable to theft via USB cable



How easy was it?*

1. Rip plastic cover off
2. Force USB-A plug into ignition
3. Turn ignition

*OEM conducting software patches now

Again, why care?

Federal Fleet Community Best Practices & Expectations

Connected Vehicle Fleet Community

You are not alone in cybersecurity, there are many involved in securing our infrastructure and assets

- Automotive- Information Sharing and Analysis Center (Auto-ISAC)

- Large group of automotive industry members focussed on mutual information sharing
- Automotive Cybersecurity Training (ACT)
 - Comprehensive training program for vehicle cybersecurity to improve safety & security.
- Federal agencies welcomed to join as Community Partners



Connected Vehicle Fleet Community

You are not alone in cybersecurity, there are many involved in securing our infrastructure and assets

- **Other Government Agencies**

- DOT Volpe Center
- FBI Automotive Sector Specific Working Group (SSWG)
- National Highway Traffic Safety Administration
- National Institute of Standards and Technology
- Department of Energy
- Joint Office of Energy and Transportation

Connected Vehicle Fleet Community

Any agency that operates a connected vehicle is part of the CV Community and has a responsibility to protect their assets and users

- **Everyone is responsible for CV cybersecurity**
 - Understand capabilities of new vehicles
 - See Something Say Something
 - Develop a game plan for a possible future cyber attack
 - Follow published guidance and best practices on cybersecurity and protecting your users and vehicles
 - Stay updated on emerging threats against connected vehicles

CV Best Practices

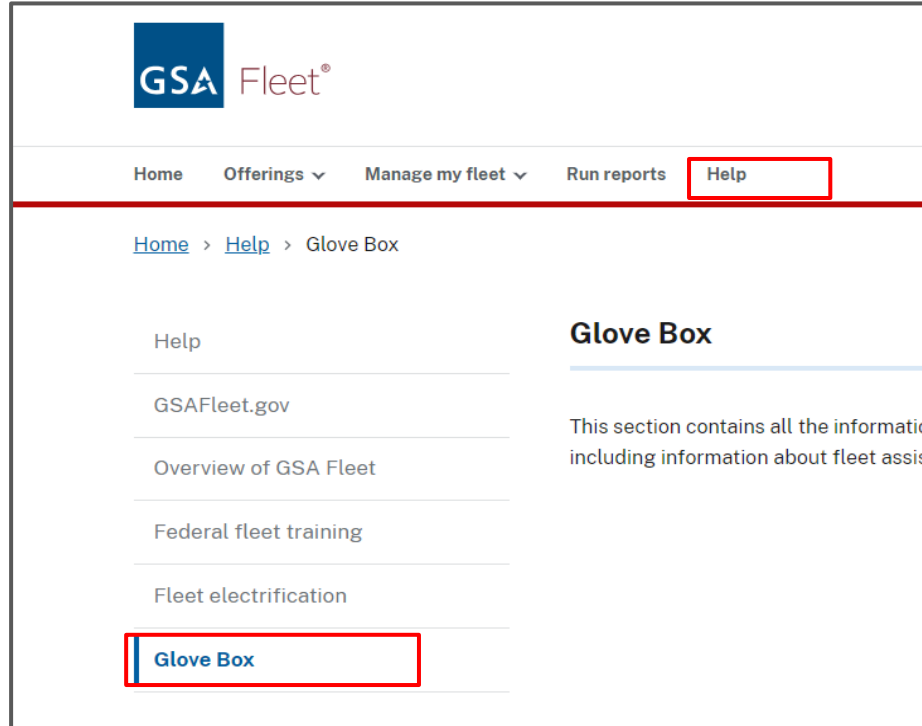
Operators and Fleet Managers Have a Role in Cybersecurity Hygiene and Safety

- **Do's**
 - Restore/reset vehicle to factory settings
 - Disable any hotspots the vehicle may have
 - Delete any bluetooth connections
 - Ensure vehicle software/firmware updates are current
 - Regularly change passwords to vehicle related apps
- **Don'ts**
 - Connect your phone to vehicle through USB or bluetooth
 - Ignore problems or glitches in the vehicle
 - Don't ignore service alerts / OTAs

GSA Fleet Cybersecurity Materials

- **Connected Electric Vehicle (EV) Report**
 - Based on market research on connected vehicles and included recommendations on data management, cybersecurity, charging infrastructure and roles & responsibilities.
- **PII Clearing Guide**
 - Provides step-by-step instructions for clearing personal information from vehicle infotainment systems.
- **GSA Fleet Cybersecurity Brochure**
 - Contains a list of best practices to maintain vehicle cybersecurity hygiene.

GSAFleet.gov Resources



The screenshot displays the GSA Fleet website interface. At the top left is the GSA Fleet logo. A horizontal navigation bar contains the following items: Home, Offerings (with a dropdown arrow), Manage my fleet (with a dropdown arrow), Run reports, and Help (highlighted with a red box). Below the navigation bar is a breadcrumb trail: Home > Help > Glove Box. On the left side, there is a vertical list of menu items: Help, GSAFleet.gov, Overview of GSA Fleet, Federal fleet training, and Fleet electrification. The 'Glove Box' item is highlighted with a red box. On the right side, the 'Glove Box' section is titled, followed by a blue horizontal line and a paragraph of text: 'This section contains all the information including information about fleet assist'.

GSAFleet.gov Resources cont.

Glove Box

This section contains all the information you as a driver need for your GSA vehicle, including information about fleet assistance and electric vehicle charging.

Fleet service card

GSA Fleet leased vehicles card for fuel, maintenance, and repair services. Call **1 (866) 400-0411** for support or contact your Fleet Service Representative (FSR).

[Call 1 \(866\) 400-0411](#)

[Contact Fleet Service Representative \(FSR\)](#)

Guide to your GSA Fleet leased vehicle

Everything you need to know about the benefits and operations of your GSA Fleet vehicle.

[View user guide](#)

Charge at public stations

Learn how to charge your GSA Fleet electric vehicle at public charging stations.

[View user guide](#)

Assistance card

Access the numbers for GSA Fleet's contact center in order to get on the road after an accident or find the nearest maintenance location.

[View user guide](#)

Accident reporting kit

Access all the forms necessary to report your accident.

[Learn more](#)

Tesla guides

Find all the information you need to operate your GSA Fleet leased Tesla.

[View GSA Tesla quick guide](#)

[View GSA Tesla guide](#)

PI/Data clearing guide

Learn what personal information might be stored in your vehicle and how to remove it.

[View user guide](#)

CV Standards and Regulations

Implementation of these standards and regulations are currently voluntary for U.S. manufacturers; some may still adhere to them.

- United Nations Economic Commission for Europe (UNECE) R-155 & R-156
- ISO/SAE 21434:2021 Road Vehicles - Cybersecurity Engineering
- ISO 26262-1:2018: Road Vehicles - Functional Safety
- ISO/FDIS 24089: Road Vehicles Software Update Engineering
- [NHTSA Best Practices for the Safety of Modern Vehicles](#)
- Other future standards always being developed
 - Vehicle industry is already heavily regulated as is

Other Cybersecurity Developments

- NIST SP 800-161 C-SCRM Practices for Systems and Organizations
 - GSA taking steps to ensure vendors are implementing these standards
- Pending rule changes to the Federal Acquisition Regulation
- 2023 FedRAMP Authorization Act
 - “Authoritative standardized approach to security assessment and authorization for cloud computing products for federal systems”
 - Modernizing and improving processes for vendors seeking FedRAMP certification

How Does Telematics Factor?

Telematics

- **Telematics is combination of telecommunications and informatics**
 - By its nature, telematics is part of the CV infrastructure
- **Mandated by Executive Order 14057**
- **GSA's Telematic Service**
 - Geotab physical device
 - Network interfaces use authentication, encryption, and message integrity verification
 - Utilizes vehicle's existing OBDII port for installation
- **Activation of Embedded OEM Telematics Modem**
 - Utilizes existing eligible vehicles factory telematics systems
 - Provides same level of service as physical device
 - OEM data feed brought into vendor's FedRAMP environment

Telematics

- **Controls**
 - Federal Risk and Authorization Management Program (FedRAMP)
 - Process to approve and adopt cloud computing by implementing standards and security authorizations on government-wide scale.
 - FedRAMP Authorization Act was signed as part of the FY23 National Defense Authorization Act (NDAA).
 - Update aligns with NIST Special Publication 800-53
 - Cyber and Supply Chain Risk Management (C-SCRM)
 - C-SCRM Plan & Vendor Risk Assessment

Telematics Cybersecurity

- **Cybersecurity Protections**

- AES 256 Data-at-Rest (DaR) and Data-in-Transit (DiT) Encryption
- Yearly penetration testing conducted by FedRAMP approved 3rd Party-Approved Organization (3PAO)
- FIPS 140-2
- HERP/HERO/HERF Certification
- Certifications and authorizations
 - GSA FedRAMP Authority to Operate (ATO) granted 4/24/20
 - FedRAMP Moderate - 325 Baseline Controls (NIST 800-53) met
 - DHS Cybersecurity Review, approval granted July 2018 by Volpe Center

Conclusion!

Threats are real, but complex attacks are less likely than low effort attacks.

Connected vehicle technology benefits drivers and fleets but requires threat mitigation like any technology.

DO implement cyber hygiene into your fleet operations.
DON'T operate vehicles with out-of-date updates.

Multiple federal agencies and industry are tackling this issue but it takes all of us to take it serious.

See something, say something!

