NEUTRAL VEHICLE PLATFORM

Keeping the Connected Car Connected Q&A:

Innovation, Competition and Security in Data-Enabled, Digital Mobility

Neutral Vehicle Working Group

Foreword

We are excited to present the "Keeping the Connected Car Connected Q&A." The strong feedback during the initial review process has been that the "Neutral Vehicle" platform outlined in this paper is a much needed initiative that, directly or indirectly, is in the interest of all stakeholders in the transportation ecosystem. While much of the focus is on current technology and vehicles in operation, autonomous vehicles, electrification, smart cities, and new forms of transportation are becoming a bigger part of the landscape; the need for a Neutral Vehicle architecture will become even more important and urgent in this context.

An initiative like this relies on feedback in order to solidify and/or modify the initial approach, consider new questions, and stay in touch with multiple stakeholder perspectives. We are grateful for the constructive interaction with some leading experts in the field and are looking forward to keep building these relationships.

In particular, our thanks for providing initial critical review and further questions to explore go to Dr. Dan Massey, Professor at University of Colorado Boulder and former program manager in the U.S. Dept. of Homeland Security Science and Technology Directorate Cyber Security Division (including cyber security for automobiles); Derik Reiser, Assistant Vice President, IT Architecture & Innovation, Enterprise Holdings Inc.; Prof. Dr. Lothar Determann, Law Professor and Partner at Baker MacKenzie (San Francisco & Palo Alto), co-author of the article *Open Cars*, in the Berkeley Technology Law Journal; Ted Guild, Automotive Lead at World Wide Web Consortium (W3C) and Research Staff at MIT Computer Science and Artificial Intelligence Laboratory (CSAIL); and Mr. Craig Smith, Research Director of Transportation Security at Rapid7 and author of *The Car Hacker's Handbook*.

We would also like to thank the Geotab team for supporting the initiative; here our special thanks go to Neil Cawse for encouragement and technology related guidance.

Please keep the feedback coming. We value your input as we are looking to broaden our stakeholder engagement and contribute to solving some of the most critical problems of innovating and re-imagining modern transportation. For those interested in the technical architecture aspects of Neutral Vehicle, please ask for our white paper *The Neutral* Vehicle *Platform - Technical Concept*.

Dirk Schlimm
Neutral Vehicle Working Group

Keeping the Connected Car Connected Q&A

This Q&A reviews the current state of the connected car, highlights threats, and points to the neutral (connected) vehicle as a path forward to overcome challenges.

How Are Data and Digital Technology (Connected Cars) Changing the Transportation Industry?

Today, there are millions of internet-connected vehicles in operation around the globe. You can find these connected vehicles in the world's mega fleets, government service, car rental and car leasing operations, medium and small business fleets, and independent trucking. All of these organizations rely on real-time, wireless access to operational data generated by their in-motion vehicles for running an efficient and responsible business. The data and related insights can be used to:

- Promote safe driving behavior (e.g. monitor seat belt use and vehicle speed)
- Maintain vehicles (e.g. detect engine problems and monitor battery life)
- Improve efficiency and productivity (e.g. route planning and adjusting, measuring and managing fuel consumption)
- Comply with regulations (e.g. manage Hours of Service)
- Access fleet-related services competitively (e.g. used car dealerships and/or independent repair garages, competitive insurance offerings, etc)
- Integrate fleet data with other business information

While the connected car has been commonplace in the commercial transportation world for well over a decade, it is now quickly advancing into the consumer space as well.

In addition to operational and safety improvements, connected cars drive the rapid adoption of entirely new mobility models. One prominent example is car sharing, which is the ability to provide temporary digital car access via smartphone. Furthermore, as vehicles become more autonomous, new, previously unthought of opportunities for creative mobility will continue to emerge. This will have massive business and societal benefits. On the whole, today's "normal" consumer vehicle utilization is highly inefficient — according to estimates, less than 4% of actual capacity. Modern mobility schemes will help increase utilization rates, reduce resource waste, decrease traffic congestion, and will bring other radical and much needed change to how transportation is provided.

Therefore, it is no overstatement to say that modern transportation and mobility without data and digital technology has become unthinkable.

Who Has Access to Connected Vehicle Data Today and How Is Connected Data Access Provided?

At present, the car owner/fleet operator has the ability to gain real-time, direct access to their in-vehicle data by virtue of plugging a telematics device into the vehicle-standard On Board Diagnostic port (also known as OBD or data link connector) and wirelessly transmitting data to a server. The car owner/operator may also provide access to their data to other third parties (e.g. allow a garage to plug diagnostic tool into the OBD port for repair purposes). There are a variety of such telematics solutions on the market providing car owners/operators with choice as to functionality, quality and price.

Vehicle manufacturers and their service garages also have wireless access to vehicle data through embedded telematics systems, i.e. systems that are built-in by the vehicle manufacturer. Data collected by embedded systems is often used to help vehicle manufacturers offer and/or promote their services to owners/operators, such as repair services. In addition, they use stationary diagnostic tools that plug in the OBD port.

Currently, there is competition between telematics solutions offered by digital specialists/telematics experts and those offered by vehicle manufacturers. Such competition is commonplace with regard to traditional vehicle components and accessories (tires, replacement parts, etc.), and is equally commonplace with regard to digital components, such as navigations systems. As the experience with navigation systems has shown, in many digital products vehicle manufacturer's innovative capacity and core expertise is lagging behind digital native and data-centric providers even if efforts are being made to catch up. The typical vehicle manufacturer provided navigation system is perceived as cumbersome and far behind dedicated products by consumers.

Further, digital products have short life cycles, typically three years or less for a smartphone, whereas vehicles can be in operation for 10-15 years and long term vehicle owners are often stuck with the initial vehicle manufacturer-provided digital product. For example, it can be expensive or even impossible to keep vehicle manufacturer navigation systems current. With a proliferation of digital mobility products, a vehicle manufacturer simply cannot (and should not) be "all things to all people" especially since we live in a world of ever increasing specialization.

Why Do Owners/Operators Need or Want the Option of Direct Access to their Data?

It is entirely possible to purchase access to vehicle-generated data from the vehicle manufacturer using an embedded telematics or other vehicle manufacturer offering, and some vehicle owner/operators do so today. Some vehicle manufacturers have teamed up with digital technology companies to create/improve a product that is outside their traditional core expertise.

But, most often, the preference — especially for sophisticated commercial and government fleets — is to use a special purpose telematics system that is operated and controlled by the vehicle owners themselves and provides direct access to their data. There are a number of reasons for this:

- Globally leading, specialized telematics providers have a greater ability to provide real-time data at higher quality/richness, lower latency (up to true real time), and optimized efficiency for wireless transmission; it is simply a better product for what is needed (or at least considered to be such).
- Vehicle manufacturers often consider vehicle generated data as "their data" and impose licensing restrictions as to the use of data, including uses that are seen by the vehicle manufacturer as unfavorable to them or as in competition with their own services. In addition, such licenses can be temporary only or subject to unilateral withdrawal or restriction.
- The fundamental belief that innovation and the best possible and most cost effective services for businesses, governments, and consumers can only be achieved through free competition. Therefore, there must always be a competitive data offering as a matter of principle and as enshrined in anti-trust laws. A data monopoly controlled by vehicle manufacturers would be incompatible with a vibrant and dynamic mobility sector.

Therefore, in a free market, both solutions — vehicle manufacturer and specialist provided — must coexist and compete with each other.

Why Is the Current Direct Owner/Operator Access to Vehicle Data and Digital Technology Threatened?

Some vehicle manufacturers and vehicle manufacturer associations have announced plans to remove direct owner access to in-vehicle data by restricting the OBD or blocking it all together as a means of data access. They are citing a number of reasons for this:

1. The EU vehicle manufacturer association[1] maintains that vehicle manufacturers have invested in vehicle R&D and vehicle production facilities and should therefore have an exclusive right to commercialize vehicle generated data; this would include licensing vehicle generated data to vehicle owners and third parties.
2. Vehicle manufacturer controlled access to vehicle data is the only way to protect privacy and security in the connected vehicle.

There is no known legal basis for the assertion that the vehicle manufacturer "owns" the data generated by the vehicle. In fact, most legal scholars agree that data, as such, cannot be owned and that the right to use vehicle generated data lies with the vehicle owner or operator. This view is consistent with U.S. legislation that assigns ownership of data logged by in-vehicle event data recorders (EDRs or "black boxes") to car owners or lessees, not to vehicle manufacturers.

With regard to privacy, it can hardly be seen how data control by the owner (most often being the driver) would not be the best privacy protection, as any potential personal data would relate to them. This concept equally holds true in commercial settings where the vehicle owner is the driver's employer and would be able to use vehicle data for legitimate business purposes subject to applicable privacy laws. Therefore, if and to the extent the vehicle manufacturer were to use vehicle data that is classified as personal information protected by privacy laws they — all the more — would need owner/driver consent.

Security, on the other hand, is a serious argument. In fact, cybersecurity is *the* issue in the fast growing Internet of Things (IoT), ranging from mobile phones, to personal computers, smart TVs, smart medical devices, and connected cars. As in the rest of the IoT world, cybersecurity is a threat to the connected car to the extent that there are weak security practices. Such weak practices can exist both in third party telematics devices and in vehicle manufacturer embedded data connections. The fact that there are low quality/low security telematics devices is, however, not a reason to block the OBD port as a data link. Rather, the answer is to increase the security of telematics devices and, for that matter, the security of vehicle manufacturer embedded connections. In that regard, leading practices have now been developed (see below) and will need to be upgraded continuously. The goal must be secure *and* effective data access.

Is Cybersecurity a Reason to Close Down the OBD Port and Eliminate/Restrict Direct Owner Access to Vehicle Data?

Cybersecurity for connected vehicles is a serious concern. The attack surface of a modern vehicle contains 20-30 wireless entry points. These entry points vary both in terms how easily they are subject to unauthorized access (i.e. can be hacked) and what damage can be done by a malicious actor (hacker).

It is true that there are commercially available, substandard/inadequate third party devices - as there are weak vehicle manufacturer embedded telematics solutions - and both must be avoided. At the same time,

[1] European Automobile Manufacturers' Association - ACEA. (2016, Apr.). *ACEA Strategy Paper on Connectivity.* [Online] Available: http://www.acea.be/publications/article/strategy-paper-on-connectivity

reputable and globally leading telematics providers have implemented technical solutions that secure data access through the OBD port (more on this below) just as leading vehicle manufacturers have implemented solutions to secure their embedded telematics systems.

It is very important that vehicle owners/operators who control the physical access to the OBD port and have the ability to choose telematics providers become security aware; they must only use high quality devices and/or purchase vehicles that provide adequate telematics security, including the ability for easy updates to address newly identified security vulnerabilities (cybersecurity is and always will be dynamic).

Therefore, while security is undoubtedly a challenge to be taken seriously, closing the OBD port to all third party, owner controlled devices (including those with sophisticated security features) is not the solution as it would take away data access and choice from owners. Instead, the mobility industry must take on the challenge of providing data access systems that are both open to competition and provide the needed security.

How Do Vehicle Owners Know Whether a Direct Data Connection (such as an OBD Based Telematics Solution) to Their *Current* Vehicles/Fleet Is Secure?

Direct access telematics solutions have been available for many years and commercial-grade applications have driven the connected car revolution. Given the known risks of cyber-attacks, large commercial fleet operators, governments (especially the U.S. government), and globally leading providers of specialized telematics solutions have completed their own investigations into the required cybersecurity practices for fleet telematics platforms.

As a result, there are a number of best practices and recommendations that have gained recognition in the expert community, including guidance provided by the IEEE Center for Secure Design,[2] the U.S. Department of Transportation (John A. Volpe Center) Telematics Cybersecurity Primer for Agencies (prepared for The Department of Homeland Security),[3] the GEOTAB, 15 Security Recommendations for Building a Telematics Platform Resilient to Cyber Threats,[4] and the Society of Automotive Engineers OBD interface security guideline SAE WIP J -3005-2 (draft).

The nature of cybersecurity is such that this work must continue at all times as the threat landscape and potential for new vulnerabilities remains ever changing; i/n addition, cybersecurity cannot succeed in isolation but must include all stakeholders in the connected car ecosystem. Geotab is actively engaged in advancing this work.

What Are the Efforts to Achieve Cybersecurity for Direct Data Connections in New Vehicle Design?

---

[2] IEEE. (2017, Aug. 23). "Design Flaws and Security Considerations for Telematics and Infotainment Systems" [Online]. *IEEE Cybersecurity*. Available: https://cybersecurity.ieee.org/blog/2017/05/30/design-flaws-and-security-considerations-for-telematics-and-infotainment-systems/

[3] J. Clark and D. Chin. (2017, May 18). *Telematics Cybersecurity Primer for Agencies*, U.S. Department of Homeland Security.

[4] A. Sukhov. (2016, Sep. 14). "15 Security Recommendations for Building a Telematics Platform Resilient to Cyber Threats" [Online]. *Geotab Blog*. Available: https://www.geotab.com/blog/telematics-cybersecurity-recommendations/

With regard to future vehicle design, there are a number of proposals to "harden" the OBD port (the data link connector) via a gateway and thus make it less susceptible to threats posed by substandard devices.

While these efforts are valuable and welcomed, they must ensure that they achieve both: (1) restricted data access via low standard, insecure devices, and (2) continued data access via advanced, high functioning, secure devices including direct, real-time access to relevant data and functionality required for advanced mobility (such as digital door lock/unlock).

Vehicle owner and operators must continue to educate and create awareness of the essential nature of direct data access and digital functionality to their business models and work creatively, constructively and collaboratively to achieve the twin goals of high data functionality and robust security.

What Is the "Extended Vehicle"? To What Extent Does It Contribute to Secure, Data-Enabled Mobility?

The Extended Vehicle (ExVeh) is a scheme proposed by mainly European vehicle manufacturers. While on the surface it is touted as a data access program for owners and third parties, it builds on the above mentioned push to bring access to vehicle generated data under the control of the vehicle manufacturer and put vehicle/fleet owners into a position where they must buy/license data from the vehicle manufacturer or, as the case may be, from a consortium of vehicle manufacturers. The (current) ExVeh includes proposals to:

1. Remove real-time, direct data access functionality from new vehicles across vehicle makes and models;
2. Allow for vehicle manufacturer controlled data collection only and transfer such vehicle manufacturer collected/controlled telematics data to a cloud server;
3. Combine the telematics data collected by multiple (participating) vehicle manufacturers into one single cloud platform; and
4. Make a subset of pre-processed data available to customers for a fee and subject to license terms.

A central feature of the ExVeh scheme is to create a cloud server for data collected from vehicles across multiple vehicle manufacturers, dubbed the neutral server. Access to the ExVeh data would have to be negotiated.

While addressing vehicle security at some level (similar to above: weak devices could no longer access data through the OBD port, but neither could secure devices and vehicle manufacturer related vulnerability would remain as well) and providing the potential benefit of a large data depository (big vehicle data) with opportunities for the facilitation of connected car and related services the ExVeh puts control over data exclusively into the hands of the participating vehicle manufacturers.

Thus many industry stakeholders have expressed the concern that the ExVeh would restrict/monopolize in-vehicle data access by individual owners (commercial and consumer vehicle owners would only have one source to buy data) and would potentially monopolize the big data application ecosystem (service providers and customers would only have one source for data analytics). What is more, the current proposals around ExVeh contain a measure of data pre-processing which would remove owners further from the "actual" or "real" data so that quality and competitiveness of ExVeh data would even be further from the "direct" data that fleet owners want and need (for reasons outlined above); in the same vein further undue restrictions could easily be applied in the licensing regime. The current regime of direct, real-time data access and dynamic development of digital technology would be all but eliminated.

This is why the ExVeh scheme has been criticized by policy makers and has been judged to be incompatible with fair competition and competition laws in an expert report prepared at the request of the European Commission (DG Move).[5]

What Is the "Neutral Vehicle"? To What Extent Does It Contribute to Secure, Data-Enabled Mobility?

In response to the ExVeh scheme, a number of concerned stakeholders in the mobility ecosystem have asked for an alternative model that would preserve the freedom to innovate, compete, and create value while advancing cybersecurity. The central tenets of such a model should be security, being "open" to innovation and competition, and access to vehicle data that is placed on a "neutral" data exchange server. It is in response to these requests that the Neutral Vehicle Working Group has been formed.

A key component of the Neutral Vehicle would be a neutral data exchange that becomes a depository of vehicle generated data. Such data would, among other options, be **collected by participating, owner-authorized telematics providers and embedded telematics systems.** In order to achieve cybersecurity, only those data collection devices/technologies that meet an established, supervised security standard (see above) would be permitted to participate.

The Neutral Vehicle data exchange would include functionality to normalize data and data definitions so that data originating from various vehicle makes and models would be easier to manage and integrate with mobility applications and services. Mobility products, applications and services would connect to the Neutral Vehicle Server via Application Program Interface (API) offering both products based on anonymized data analytics and products for specific owners/consumers based on their consent to work with their data. The products, applications, and services would cover the current spectrum of garage services (vehicle manufacturer dealer and independent), fleet management, insurance, accident notification, ridesharing and the like and leave the opportunity open for innovative future products based on additional types of data, but all would be subject to vehicle owner consent, data privacy control and choice.

Thus the Neutral Vehicle would ensure cybersecurity, consumer choice, and innovation well into the future.

What Is the Current Status of the Neutral Vehicle?

Several proposals currently exist for neutral vehicle type schemes that are on the continuum from ExVeh to true Neutral Vehicle. It should be made clear that offering a high functioning Neutral Vehicle, that meets the current needs of fleets and consumers, enables access to a wide spectrum of mobility service providers and enables competition and innovation well into the future, requires a deep expertise in telematics cybersecurity, data diagnostics, data normalization, large scale data management, system reliability and expandability plus the ability and willingness to collaborate and integrate stakeholder needs.

As an expert in large scale, open and secure telematics, Geotab is currently collaborating with key industry stakeholders to put forward and further refine a Neutral Vehicle architecture and functionality that meets the stringent requirements of the real world, is carefully considered and rigorously planned,

[5] M. McCarthy, M. Seidl, S. Mohan, J. Hopkin, A. Stevens, F. Ognissanto. (2017 May). *Access to In-vehicle Data and Resources*, European Commission [Online]. Available: https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf

and follows a governance model that keeps the Neutral Vehicle truly neutral.

What are some of the key features of the Neutral Vehicle?

As the concept of the Neutral Vehicle gains shape it is critical that the foundational building blocks that ensure the key goals of security, competition, and innovation remain in clear view. They include:

1. Robust and continuously evolving security standards for both data access points and backend that are underpinned by industry best practices and supervised/enforced by a competent authority with intimate knowledge of the Neutral Vehicle.
2. High degree of interoperability and standardization (APIs) for easy connectivity for both Neutral Vehicle users (fleets, fleet managers and consumers), service providers, vehicle manufacturers and other customers (e.g. smart cities).
3. Infrastructure and architecture (cloud server capability) to support a super large system with room to expand and high levels of system reliability.
4. Extensive experience with mixed fleet telematics (normalizing data across a wide range of make/models) and ongoing work to normalize and optimize data measurement parameters to expand Neutral Vehicle functionality and user friendliness. **Note**: it would appear that harmonizing make/models would be a major challenge for ExVeh given single brand/platform mindset of vehicle manufacturers.
5. Built-in commitment to neutrality, innovation, and industry-wide perspective and declared goal to keep forward looking users, service providers and vehicle manufacturers at the forefront of a dynamic mobility ecosystem, value creation and societal benefit.
6. Governance model that ensures the Neutral Vehicle remains neutral and is not subject to special interests.
7. Smart design, architecture and functionality that support compliance with data privacy legislation dependent on and appropriate for a wide spectrum of uses cases (commercial, consumer, government) with varying privacy impacts and considerations.
8. Commercial infrastructure that appropriately balances compensation for service development, management, and governance and industry nature of the Neutral Vehicle.

As competing models of the Neutral Vehicle emerge, all of these principles should be "stress tested" in detail. This is especially required to ensure that a monopolistic ExVeh scheme, less than a "neutral" Neutral Vehicle model, or a not yet functioning Neutral Vehicle is prematurely introduced as an alternative to the current direct data access regime available to vehicle owners and service providers.

Connected Car and Neutral Vehicle: Where Do We Go From Here?

The connected car is a contested space where established industry participants and new entrants are staking out their positions and are working to create facts on the ground. Such is the nature of a technology revolution that brings both unprecedented innovation and disruption. The advance of highly autonomous vehicles (HAVs) and electric vehicles (EVs) will only add to the need for new thinking as it will bring new challenges such as the demand for additional and new communication, power, and connectivity infrastructure.

In such an environment, every stakeholder must realize the critical importance that reliable, high quality data plays for the ability to shape their future; and they must assert with determination and passion their interest and right to access, use and compete with data.

Direct owner access to data and the Neutral Vehicle are on the side of innovation, competition, and

consumer choice which, in a free market society, is the right side. Security, critical as it is, must enable these values rather than become an argument for a closed, static digital economy that, in the worst case, serves one interest group only and insulates them from competition.

This is no time to sit back and wait. It is a time to develop and put forward viable solutions, test their mettle to make sure they are the real thing, and keep innovating and wrestling with problems until the job is done.

Comments, questions and any other feedback on this white paper can be emailed to:
info@neutralvehicle.com