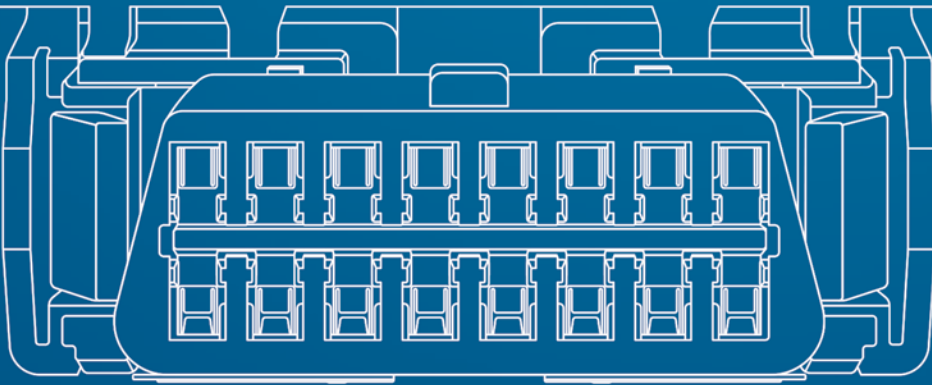Preserving Privacy And Security
In The Connected Vehicle:

THE OBD PORT
ON THE ROAD AHEAD

First Edition, 2015
White Paper

GEOTAB
management by measurement

Table of Contents

Foreword

OBD based telematics have become a key driving force in modern transportation and fleet management. Fleet owners and operators, drivers and society at large have benefited greatly from reduced accidents, reduced emissions, improved fuel efficiency and overall more productive vehicles. It would be foolish, however, to take these benefits for granted. Cyber security threats and privacy concerns have emerged as key issues for the internet based economy at large, and the transportation industry is no exception. In fact, given the leading role transportation plays in commercializing digital innovation these issues are of vital concern to the industry. Solutions to these concerns are critical to the preservation and ongoing innovation of telematics enabled commercial transportation and fleet management.

From informal exchanges with leaders in the fleet service, leasing, transportation and telecommunication industries, it has become clear that it is high time to increase awareness of the issues. There is a need to engage all stakeholders in order to ensure that a secure and open OBD port remains the centerpiece of the innovative road ahead. This white paper is meant as a starting point for discussion. It intends to place the issues into context, point out risks and opportunities, and call for concrete next steps. While the United States is the primary focus of our examples, we know from our Canadian, European, Latin American, Japanese and other worldwide partners that the issues are of no less concern to them, and we look forward to engaging in a much broader, global dialogue.

Your feedback, thoughts, and, of course, constructive criticism are most welcome.

Neil Cawse
CEO
Geotab Inc.
neilc@geotab.com

Dirk Schlimm
EVP & Advisory Board Member
Geotab Inc.
dirks@geotab.com

Introduction

The On-Board Diagnostics (OBD) port was designed to provide a simple way to test emissions data-reducing the environmental impact of vehicles and ensuring public accountability. From its early days in the 1990s, the OBD port did that and more. It has evolved into a critical tool. We now depend on the OBD port to save lives, control costs, protect the environment, increase efficiency, and provide objective data against which to measure published engine performance figures. A quarter-century after the OBD port's introduction, its ecosystem has grown to provide key, innovative technologies to support fleet owners and managers, regardless of the underlying choice of vehicle.

As manufacturers move to the "connected vehicle," regulators have voiced concerns about the security of on-board computer systems, and have raised questions about privacy protection for personal driving information.[1]

Stakeholders of the OBD ecosystem, including fleet owners, fleet managers, aftermarket suppliers, automobile industry associations, government regulators and automobile manufacturers, must ensure the ongoing availability of a robust OBD port that continues to provide critical benefits while protecting security and privacy. As with other digital technologies that have become central to contemporary life, such as the smartphone or cloud-based storage, a balance can be reached that ensures continued access to valuable OBD data without undue privacy and security costs.

I. The OBD Port: Safety, Savings, Compliance, and Choice

An OBD telematics device is a small, smart box that, depending on device capability, can be plugged into a wide range of vehicle makes and models to retrieve diagnostic information for transmittal to cloud based servers.

Aftermarket telematics devices and software offer fleet operators a range of considerable advantages including safety, reduced cost of ownership, environmental protection, and manufacturer accountability.

A. OBD Telematics Encourages Safe Fleet Drivers

A key benefit of an advanced OBD aftermarket solution is to improve fleet safety by promoting and incentivizing good driving. For example, fleet operators have the option to use OBD systems to design and manage risk and safety programs including real time driver feedback and coaching. These programs center on measurable events such as speeding, seatbelt usage, sharp cornering, or over-acceleration. The accurate analysis of these events is based largely on data collected from the OBD port and can be used to create programs that advance driver and road safety and prevent accidents. Accident reconstruction can also be used to show that drivers were not at fault.

Another important safety feature for fleet managers is Hours of Service reporting. As required by U.S., Canadian, Hours of Service regulations in other jurisdictions, drivers must record when they start driving, when they stop, and other important trip details. This safety measure combats accidents due to lack of sleep and loss of attention. Many telematics solutions reduce the overhead of this reporting; and more importantly for public safety, they provide an auditable trail to ensure compliance with the safety regulations.

Indeed, proposed new United States safety regulations, if implemented, will require electronic logging devices (ELDs) to communicate with the engine control module through the CAN bus- the network that automotive devices use to communicate. The ELDs will use the CAN bus to receive data relevant to Hours of Service monitoring, such as miles driven, and engine power status.[2] These regulations presuppose that fleet owners and managers have an easy way for their electronic device of choice to access the CAN bus.

> An important feature of the OBD Port - its universal nature - ensures that each of these safety related programs and compliance with regulations can be implemented across vehicle brand.

They do not depend on a particular manufacturer or vertical integration.

Fleet operators can choose the solution they like, knowing that data is standardized across non-homogenous fleets and compliant with applicable safety regulations in the countries where they operate.

B. Access to OBD Port Functionality Lowers Costs

The ability of fleet owners and managers to access OBD port functionality lowers their cost of ownership in at least five ways:

1. Minimizing repair and maintenance difficulties or anticipating them before they become larger,

2. Reducing fuel consumption,

3. Automating driver procedures,

4. Ensuring compliance with regulations, and

5. Analyzing trends that can be observed only when large aggregates of data are available.

The right to repair law[3] benefits fleet owners and managers by ensuring that OBD port diagnostic data available to manufacturer dealerships are made available to independent repair shops on the same terms.

With right to repair, fleet operators have competitive options for servicing their vehicles, and even have the option of servicing vehicles themselves.

The law remains hugely popular. Since it passed in one US state with over 80% of the vote, leading automakers and consumer advocates have entered into a memorandum of understanding that the law would apply nationwide. These pro-competitive benefits of the OBD port increase choice and lower costs.

Similarly, by accessing diagnostic data such as the air flow used by the vehicle, OBD-based telematics systems can provide more accurate reports on fuel usage. This enables managers to identify and correct practices that lead to fuel waste and use data for smarter fuel purchase programs.

As discussed previously, OBD port data enables fleet operators to improve driver safety. These programs not only reduce road accidents but the data can be used by fleet operators to lower fuel consumption, other costs and insurance rates.

Telematics assists fleet operators in tracking and scheduling maintenance as well. Because operators are notified of problems as they happen, maintenance can be performed on the vehicles that need it most. Indeed, a new iteration of the OBD port standard, WWH-OBD, includes codes that indicate the severity of the effect of a maintenance problem on vehicle emissions quality, further assisting managers in maintenance scheduling.[4]

Electronically ensuring compliance also lowers costs. Right now, telematics assists fleet managers to provide near-paperless Hours of Service compliance. US regulations requiring ELDs to have CAN bus access for Hours of Service compliance are currently scheduled to become mandatory in the United States in 2017.[5] Ensuring that third party aftermarket devices can use the OBD port to provide this service will be vital in ensuring that fleet operators are able to cost-effectively and uniformly ensure compliance across vehicle manufactures and types.

> In short, OBD port functionality enables fleet operators to track, compile, and benefit from a wide range of automotive data, providing substantial cost savings.

C. Third Party Access Increases Regulatory Compliance and Public Accountability

The automotive world has been shaken by reports of alleged emissions test irregularities. According to one report, a manufacturer designed its engine control module to detect when tests were being performed and to change its emissions behavior in order to pass the test.[6] Additional recent reports indicate that diesel cars produced by certain manufacturers emit "significantly more pollution on the road" than in regulatory tests.[7]

Similarly, the EPA regulations regarding estimating miles per gallon (in the United States) require self-testing and reporting by the auto manufacturers. Questions are sometimes raised as to the accuracy of these figures.[8] In contrast, OBD-based telematics products generate measurements that draw on real life driving conditions across a wide geography, which provides a useful counter-balance to the self-testing performed by the manufacturer.

Third party data collection adds a layer of transparency that benefits fleet operators, regulators, and vehicle manufacturers. It provides fleet owners and managers with assurance that their vehicles are reaching promised efficiency benchmarks and that their drivers are complying with Hours of Service regulations. It provides regulators with independently designed tools that ensure compliance. And it provides vehicle manufacturers with a key ally to ensure transparency and enhance credibility.

In sum, OBD port functionality can help restore and solidify drivers' trust in regulatory compliance and vehicle related information, without which further regulatory interventions into vehicle operation may be inevitable. As noted above, moreover, fleet operators have come to rely on the OBD port to facilitate and automate regulatory compliance.

II. Challenges for the Connected Vehicle

The increasingly Internet-enabled automotive software infrastructure faces the same pair of risks as any Internet-connected computer system: security and privacy. As with these other systems, obscuring access, also known as "security through obscurity," will do little to harden the system against attack. Instead, it will reduce consumer choice and undermine both safety and environmental compliance. Experience from the computer industry shows that an open-design structure is what actually enhances stability and safety.

A. Security

The move to the connected car has raised security concerns over access to the CAN bus. [9] In response, the U.S. Congress has proposed legislation requiring that "[a]ll entry points" to the vehicle "be equipped with reasonable measures to protect against hacking attacks."[10]

The Alliance of Automobile Manufacturers recently published a white paper detailing how they were working to increase cyber security.[11] The Alliance argued that limiting access to what it called the "vehicle's proprietary systems" would enhance the vehicle's security.

This proposed solution, known to security experts as "security by obscurity," has been debunked. For example, the National Institute of Standards and Technology specifically advises against a closed system solution. Indeed, one of their Server Security Principles is Open Design, i.e. the principle that "System security should not depend on the secrecy of the implementation or its components."[12]

This open design principle is echoed by the United States Department of Defense. The DoD notes that open design makes it easier for third parties-analogous to owners or aftermarket manufacturers in the fleet field-to identify and fix security flaws. In contrast, a closed system relies only upon a small core development team to spot and correct issues. History has demonstrated that these core teams often cannot keep up with security threats. For this reason, according to the DoD, "'Security by Obscurity' is widely denigrated."[13]

> The road forward is clear - we need security through open design.

Designing secure systems for vehicles to join the Internet of Things will reap rewards in cost as well as safety. Economists estimate that the benefits of connection compound over time, while costs of security remain constant.[14]

For this reason, fleet owners and managers, aftermarket manufacturers, and technology companies, should work with automobile manufacturers to design a secure CAN bus that does not sacrifice the aftermarket benefits of safety, cost savings, and choice that access to the OBD port provides.

B. Data Privacy and "Data Ownership"

The collection and analysis of driving data provides many benefits previously discussed, including better safety, better transportation practice, lower operating costs, and better environmental protection. Yet it has also raised concerns that private information collected by the vehicle be adequately protected; in addition it has brought to the fore the question as to who owns the data generated or emitted by the vehicle.

Privacy laws differ, sometimes substantially, around the world. Germany, for example, has some of the most restrictive privacy laws in the world. These restrictions have even raised concerns whether the country will be left behind in the development of Industry 4.0, showing that data exchange is an essential part of the modern economy and key to future innovation. In the United States, traditionally more liberal, a new legislative proposal is calling to limit the collection of any data from a vehicle to instances in which the owner has given express consent.[15] In this context, especially to the extent that it involves personal data (again the definition depends on the respective jurisdiction), communication of the benefits of telematics enabled fleet management will be crucial; the clearer these benefits are articulated the stronger the fleet industry's position to advocate credibly for a fair and practical balance between privacy and data enabled fleet management.

It is important for fleet operators, employees, and regulators to reach this right safety/privacy balance when it comes to the management of entire fleets. Safety, efficiency, and consumer protection may require the fleet company to have data about its drivers' use of company vehicles.

Privacy concerns can be addressed through appropriate regulation or employee policies setting out how the data may be used. As with smartphone data and even healthcare records, a reasoned approach would seek to balance the most useful availability of data to those who need it with appropriate measures to ensure its proper use and adherence to good privacy practice.

When it comes to data ownership, it is important to note that in many jurisdictions personal data is not subject to property rights in the traditional sense. For example, while an individual may (rightfully) think they own their social insurance or passport number, it could not be bought and sold. Further confusion is created by not differentiating between different kinds of data (such as personal, vehicle related, fleet related and aggregated) or overlooking different contexts (consumer vs. commercial, for example). In a broader sense, however, the question of data ownership is often the wrong question.

> Asking "who owns the data" unnecessarily sets up an all or nothing paradigm which shuts out the opportunity for constructive win-win solutions.

GEOTAB
management by measurement

Vehicle Data

The fact is this: The same data can be legitimately used by different parties for different appropriate purposes.

A primary example is the fact that fleet data is routinely used, and required to be used, by fleets, fleet service providers, and telematics companies to create the benefits that have been highlighted. Therefore, rather than asking who owns the data, industry participants should seek to understand who needs the data, for what purpose and how it is used to add value. And again, the more compelling the value proposition the more credible and compelling the case for related use of data.

The flexibility of the OBD ecosystem provides fleet managers with an important tool to address the above concerns. Unlike built-in systems, OBD aftermarket products enable fleet operators to switch to a competing product without overhauling their entire inventory. In other words, with the OBD port and aftermarket products, fleet operators can choose or switch to products that provide the information they want on terms that strike the right balance between the benefits of data collection and analysis on the one hand, and privacy as well as data use on the other.

There is no question that some of these issues are complex and that a balanced approach will depend highly on different jurisdictions and sensitivities around the world. But the principle remains the same. Shutting off or restricting data availability through the OBD in the name of privacy or claims of exclusive data ownership would result in the loss of tremendous benefits for all involved the same way that indiscriminate data use would enable all manner of abuse.

III. The Road Ahead

To ensure that the OBD port continues to save lives, reduce costs, protect the environment, increase efficiency, and ensure public accountability, solutions are needed that address legitimate concerns without putting at risk the availability of key data. Fleet owners and managers, fleet service providers, the aftermarket industry, and vehicle manufacturers need to work together to address security and privacy concerns through open, multi-platform structures that provide transparency and do not impose rigid regulatory or data-access restrictions.

There are five actions we can undertake together now to accomplish this goal.

1. First, fleet owners, industry associations and managers can work together with telematics providers to educate regulators and vehicle manufacturers about the benefits of aftermarket telematics OBD port data-both to preserve current benefits and to promote future innovation.

2. Second, standards on OBD port safety and compatibility are continually evolving in SAE and ISO committees. Geotab is currently participating in the standards-setting process to ensure that sensible security standards are implemented that preserve access to OBD port data. This work could be enhanced by involving fleet managers and service providers.

3. Third, as the recent Hours of Services regulations show, the legislative process is an important mechanism to protect safety and privacy in the connected car, without sacrificing the gains provided by OBD port functionality. Fleet management associations and other industry groups could work with aftermarket providers to engage in the legislative process and ensure that aftermarket telematics benefits are not sacrificed in the name of security or privacy.

4. Fourth, in order to address privacy concerns, aftermarket telematics stakeholders should develop a clear view of appropriate and acceptable uses of OBD data, as well as being proactive in taking steps necessary to protect the security of that data. Healthy and proactive self-regulation plays an important role in protecting privacy, building credibility and avoiding overreaching intervention by regulators or other stakeholders.

5. Fifth, rather than claiming mutually exclusive ownership of data industry participants should seek approaches that allow use of data that create the greatest common benefit and are compatible with privacy rights and the underlying commercial value proposition that are being provided.

We have work to do. Geotab looks forward to working with fleet customers, automobile manufacturers, standards organizations, and government regulators to ensure safety and privacy on the road ahead.

GEOTAB
management by measurement

References

[1] *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*, Sen. Ed Markey, (Feb. 2015), http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.

[2] Electronic Logging Devices and Hours of Service Supporting Documents, 79 Fed. Reg. 17655 (proposed 3/28/2014).

[3] M.G.L. 93K §§ 2(c)(i), 2(d)(i); Automotive Aftermarket Industry Association, Coalition for Auto Repair Equality, Alliance of Automobile Manufacturers, and Associate of Global Automakers Memorandum of Understanding § 2(c)(i) (January 15, 2014).

[4] WWH-*OBD - made simple!* (Sept. 2012), https://vector.com/portal/medien/cmc/press/PDG/WWH_OBD_AEL_201208_PressArticle_EN.pdf

[5] Overdrive, *ELD mandate poised to begin two-year countdown* (Aug. 19, 2015), http://www.overdriveonline.com/eld-mandate-poised-to-begin-two-year-countdown/

[6] New York Times, *How Volkswagen Got Away With Diesel Deception* (Oct. 8, 2015), http://www.nytimes.com/interactive/2015/business/international/vw-diesel-emissions-scandal-explained.html.

[7] The Guardian, *Four more carmakers join diesel emissions row* (Oct. 9, 2015), http://www.theguardian.com/environment/2015/oct/09/mercedes-honda-mazda-mitsubishi-diesel-emissions-row.

[8] Edmunds, *Here's Why Real-World MPG Doesn't Match EPA Ratings* (Nov. 20, 2015), http://www.edmunds.com/fuel-economy/heres-why-real-world-mpg-doesnt-match-epa-ratings.html.

[9] 60 Minutes, *Preview: DARPA* Dan, (Feb. 6, 2015), https://youtu.be/7E1WsdODxu0

[10] SPY Car Act of 2015, S. 1806, 114th Cong. § 2 (2015).

[11] Alliance of Automobile Manufacturers, *Auto Cyber-Security: Continual Testing, Checks and Balances* (July 2015), http://www.autoalliance.org/auto-innovation/cyber-security.

[12] United States National Institute of Standards and Technology, *Guide to General Server Security* p. 2-4 (July 2008), http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

[13] DoD *Open Source Software (OSS) FAQ*, http://dodcio.defense.gov/OpenSourceSoftwareFAQ.aspx (last accessed Oct. 9, 2015).

[14] Atlantic Council Center on International Security, *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures*, p.15 (Sept. 2015), http://www.atlanticcouncil.org/cyberrisks/risk-nexus-september-2015-overcome-by-cyber-risks.pdf/.

[15] SPY Car Act of 2015, S. 1806, 114th Cong. § 4.

About Geotab

For over a decade, Geotab has been a proven industry leader in the area of fleet management and vehicle tracking technology, also known as telematics.

Geotab's advanced telematics is used to manage fleet productivity and significantly reduce accidents. Geotab helps manage the maintenance, inventorying and fuel management of the company's fleet vehicles. Geotab data is open and is easily integrated into your IT systems to automate. Since Geotab provides end-to-end hardware and software solutions that are entirely scalable, both enterprise organizations and small-to-medium sized firms are active users. Geotab is the inventor and manufacturer of the products. These products are represented and sold worldwide through hundreds of partners. With over 450,000 devices deployed in the field, and with software that processes over 600 million data points daily, Geotab has established itself as a world leader in helping businesses move forward.