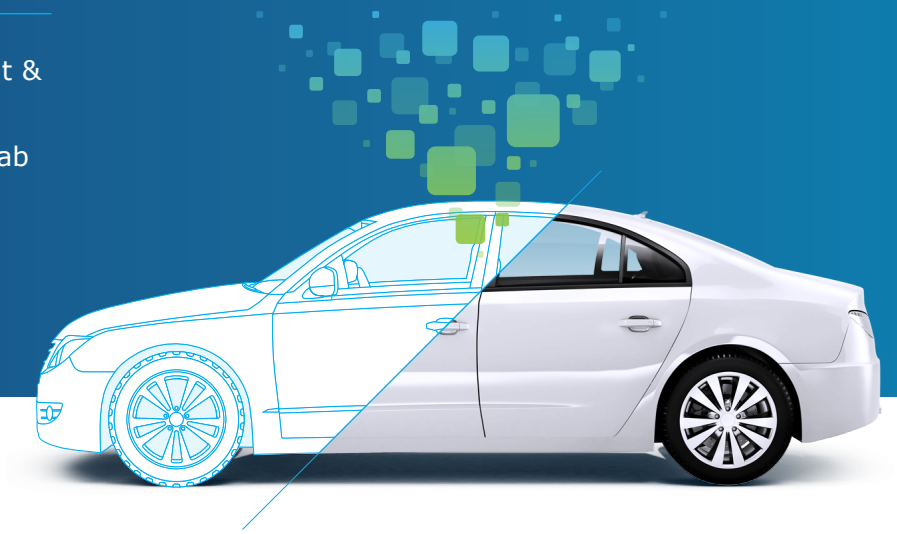
NEUTRALVEHICLE PLATFORM

Securing the Future of Connected Mobility: Six Essential Best Practices for Data-Enabled Fleet Management, Leasing and Rental Operations

Dirk Schlimm, Executive Vice President & Advisory Board Member, Geotab

Damian Kraemer, Legal Counsel, Geotab



Modern transportation and mobility without data has become unthinkable. While it may still appear as a novel concept to consumers, the "connected car" is advancing quickly.

In fact, data-enabled commercial fleet management, leasing, and car rental operations have already been widely adopted. There are millions of connected vehicles in operation around the globe including the world's mega fleets, government service vehicles, and small/medium fleets across a wide spectrum. In the commercial space, the connected car is a reality; businesses and governments could not operate without them.

Yet access to mobility data cannot and must not be taken for granted. Access faces a variety of threats ranging from cyber criminals to data restrictions serving monopolistic commercial interests. It is important that all who rely on mobility data understand the essential nature of access to their data, remain aware of the threats, and formulate their strategy to preserve data access in a connected world.

Making connected mobility work across the hyper-diverse transportation sector and beyond will require creativity, competition and collaboration. This is an essential dialogue. To be effective in a world of new competitive interests, business models and innovative opportunities having clarity of interests, purpose and strategy is vital.

As experts and partners in connected mobility we have articulated what we believe to be the bedrock principles and strategic imperatives for our customer and partner universe to ensure their competitiveness well into the future.

A. Principles

Access to Data is Essential

Access to vehicle generated data is an essential business requirement for all commercial fleets as well as fleet management, leasing and rental car companies. It enables a number of critical enterprise functions and is foundational for enabling and sustaining long-term competitiveness.

Today's well-established use case portfolio includes:

- Fleet safety
- Fleet maintenance and optimization
- Fleet productivity
- Compliance
- Access to specialized connected services

In the future, access to vehicle generated data will be even more important to ensure safety, competitiveness and innovation, including connection to a host of B2B services, financial services and smart city infrastructure as well as innovation in new mobility strategies such as car sharing.

Vehicle Owners Own Their Operational Vehicle Data

While data ownership is a topic of much debate, the best supported position, that is most consistent with existing legislation, appears to be that vehicle-generated data belongs to the vehicle operator or owner. This is especially obvious with regard to data concerning the operation, performance and maintenance of the vehicle. This data is in the legitimate purview of a vehicle operator or owner who desires to diligently manage, maintain, measure, and generally use their vehicle and fleet as efficiently as possible.

The legislation on Event Data Recorders (EDR) provides a valuable legal precedent for assigning ownership of operational data to the vehicle owner. EDRs were first introduced to monitor airbag deployment, but have gradually evolved into "black box" like devices meant to preserve information about vehicle functions around the time of a crash (an "event"). Today, EDRs are mandatory in all new vehicles sold in the United States and are used to record data like speed, acceleration, braking and seat belt status, as well as airbag information, just before and just after a crash. The US Congress has assigned ownership of this data to the owner or lessee of the vehicle in the Driver Privacy Act of 2015.[1] A report prepared for the European Commission in 2014 concurred that US EDR legislation provides the right approach and concluded that the most likely owner of EDR data in Europe is the vehicle owner.[2] Much of the EDR data collected before and after an event is very similar to the broader vehicle-generated telematics data.

This is not to say that all information pertaining to or stored on a vehicle should automatically belong to the vehicle owner: a vehicle manufacturer or producer of accessories and aftermarket parts owns trade secrets in its technology, software and business methods. Vehicle owners are permitted to engage in reverse engineering under certain circumstances such as specified in a new EU-wide trade secret law. But, any data output from cars — that is: information generated by operation of the car — belongs to the operator or owner and not to the manufacturer of the car.

1 Passed as part of the FAST Act, H.R.22, 114th Congress, 2015.

2 At p. 61, https://ec.europa.eu/transport/sites/transport/files/docs/study_edr_2014.pdf

A car manufacturer should have access to proprietary engineering data that enable the manufacturer to spot and address safety risks and make its products better. Vehicle owners and operators should recognize such legitimate needs of manufacturers and service providers to receive access to certain data to provide services or other value-adds. But, vehicle owners and operators — not manufacturers or service providers — should be in control of whether they want such services and associated data sharing or not and from/with whom. The original car manufacturer should not be in control in this respect, just like a PC or smartphone manufacturer is not permitted to access data on PCs or smartphones sold to consumers, except at their request or with their express permission.

Vehicle owners and operators can of course contractually and with make & model selection relinquish control over access to vehicle data to vehicle manufacturers. If they do, they lose the ability to select services, parts and accessory products from third parties and become dependent on safety updates, upgrades, service and parts form the vehicle manufacturer. Perhaps some vehicle manufacturers will at some point offer vehicles free of charge or at a highly discounted price in return for control over vehicle data and guaranteed revenue from updates, upgrades and services (razor / razorblade model). But, vehicle owners and operators should seek compensation for such a loss of control and choices and not relinquish such control without careful consideration of all implications and consequences.

Interoperability Enables Data Access

Interoperability is a key feature in the era of smart mobility and the digital economy. Open platforms that work with all brands of vehicles enable companies to choose vehicles based on suitability for the task and business need rather than compatibility with software.

Today, telematics data interoperability is provided by the OBD port. Originally mandated for measuring emissions data, the OBD port has developed as the data connector of choice for high performance fleets following best transportation practice. Use of the OBD for fleet relevant data connections, including engine diagnostic and a host of in-vehicle data is standard practice and is covered by several international automotive and industry standards ensuring safety and reliability. In fact, the OBD port as a data link has become an expected vehicle feature in commercial, government and leased vehicles and the basis for government mandated road safety compliance programs such as "Hours of Service." OBD data accuracy has also been certified for government tax programs.

While there are calls to limit and even eliminate the OBD as a data connector it is important to bear in mind that there is currently no viable alternative for independent, high quality and unrestricted data access. When considering alternative schemes, close attention should be paid as to who manages/restricts data flow and whether commercial interests are compatible with independent, verifiable data and accountability.

Security is the Foundation of Data Access and Connected Mobility

Cybersecurity is a key requirement for all access to vehicle data and the future of the connected car. Government authorities have rightly warned of the dangers of vehicle hacking or data breaches. There can be no data-enabled mobility without security.

Major efforts have been made over the past years to advance telematics cybersecurity and the best systems operate with a "security by design" approach. Guidelines for advanced cybersecurity for open telematics platforms are now available and work on their ongoing improvements continues in automotive and industry standards bodies around the world (SAE, ISO, ASAM, IEEE and others).

Security is the most critical enabler of reliable data access and the dialogue around security remain important. Security should, however, not be instrumentalized to shut off data access and create a controlled data economy or even monopoly. Just as with computers, security features of OEMs have not always proven the most reliable and car operators and owners should reserve the right and ability to opt for third party security features, parts, accessories and services as they determine most beneficial.

Mobility Solutions Should Consider Driver Privacy

Irrespective of who owns vehicle and fleet data, the privacy of drivers should be considered in all use cases of data. While in a consumer setting the driver will most often be the vehicle owner or lessee, in a commercial or government setting the vehicle owner is the driver's employer and the vehicle is driven for business purposes; private use of a business vehicle is of course possible as well. Commercial and government owners must develop privacy policies that conform to local laws and good privacy practice. Being proactive in privacy matters and following reasonable and responsible approaches beyond the legal minimum will help deployment in the long run as telematics data systems do benefit drivers due to reduced accidents and fatalities.

When selecting a telematics solution fleet managers should determine whether and to what extent the solution offers privacy features such as (1) granular access privilege settings, (2) allowing vehicle owners to control whether dealers and manufacturers have access to data, (3) enable administrators to identify vehicles without reference to driver names, and (4) transparent, complete and comprehensive published technical and organizational security measures (TOMs).

B. Best Practices

Based on the above principles, the following are best practices for fleets as well as fleet management, leasing and rental car companies to ensure secure and open access to high quality, reliable data today and tomorrow:

1. Understand the Importance of Data.

Your business is powered by data today and will be more so tomorrow. It may suffer considerably if you lose access to vehicle data or the ability to process data across brands and platform with telematics solutions of your choice.

2. Assert Your Data Ownership.

Clearly state your expectation to own and control operational vehicle data. If necessary, confirm data ownership and control contractually with the vehicle manufacturer.

3. Procure Open OBD Vehicles.

Only procure vehicles that provide for independent, open data access through the OBD port. Do not procure vehicles that shut down or choke off data access ports, because this can lock you into single brand systems that are not interoperable across your fleet or put you at the mercy of OEMs to update or upgrade outdated systems at their time and price.

4. Choose a Quality Platform.

Select your data access platform so that it meets your needs for data quality, variety, and availability. Express a clear preference for platforms that enable mixed fleets.

5. Do Not Compromise Security.

Exercise due diligence to ascertain the security of your data access platform and ensure it remains up to date. Develop your own data security program and select 'best of breed' security solutions for vehicles, telematics, services and parts.

6. Consider Driver Privacy.

Adopt privacy policies that minimize and consider drivers' personal data while enabling your business needs.