Comments for FTC Connected Cars Workshop

Geotab is a leading provider of Telematics services to commercial vehicle fleets in the USA and around the world. The FTC is charged with consumer protection and promotion of competition. In the commercial space, the connected car is already reality; businesses and governments could not operate without them. It is rapidly becoming the new normal in the consumer space as well. We believe that the following key principles and strategies will best enable competition in connected vehicles while safeguarding the privacy and other interests of vehicle owners and drivers. We have provided some comments and attached a paper for your consideration. We also recommend inviting the authors of the paper to the workshop in June.

1. Vehicle Owners Should Own Vehicle Data

First, this may already be true, in spite of the lack of full legal recognition of this fact. Second, there are two fundamental reasons that vehicle owners should own vehicle data: competition and privacy.

While data ownership is a topic of much debate, the best supported position, that is most consistent with existing legislation, is that vehicle generated data belongs to the vehicle 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 owner who desires to diligently manage, maintain, measure, and generally use their vehicle as efficiently and effectively as possible.

Current legislation on Event Data Recorders (EDRs) provides firm 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 (Passed as part of the FAST Act, H.R.22, 114th Congress, 2015). 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 (See p. 61, https://ec.europa.eu/transport/sites/transport/files/docs/study_edr_2014.pdf). Much of the EDR data collected before and after an event is very similar to the broader category of vehicle-generated data.

This is not to say that every scrap of data generated by a vehicle should automatically belong to the vehicle owner: A vehicle manufacturer may have a legitimate claim to proprietary engineering data that vehicle owners should recognize, provided that it does not interfere with gathering of operational data. This may be the legitimate purview of the manufacturer as it is used to develop and manufacture vehicles and further advance vehicle technology based on massive investment. Both vehicle owners and manufacturers are, of course, free to share operational and/or engineering data as well as data that may fall into both categories. In fact this is the key point about data: Unlike a physical object, more than one stakeholder can use data for their legitimate purposes at the same time.

Assigning ownership of the data to the vehicle owner promotes competition and personal privacy. Data can and should be shared; and the owner of the vehicle is best placed to determine with whom. This is also the best place to put ownership of vehicle data for the purpose of encouraging competition: each vehicle owner is free to share their data with whatever parties are best able to unlock its value. Regarding privacy, in the consumer setting the vehicle owner will also be the driver whose privacy is at stake while in the commercial setting employers can be held responsible for violations of driver's privacy. Accordingly, assigning ownership of vehicle data to the vehicle owner means that other parties would need to seek permission from the vehicle owner before collecting or using vehicle data, including data with privacy implications.

2. Security is the Foundation

Cyber security 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. Without security, the connected car becomes a liability rather than an asset. While leading companies set themselves apart by maintaining robust cyber security it should *not* be seen as a source of competitive advantage; i.e.weak cybersecurity at a competitor must not be welcomed. Cybersecurity is a shared responsibility, and a cybersecurity breach at a competitor can make the entire sector look irresponsible. This theory has recently become reality as cyber attacks have been carried out by commandeering large numbers of unsecured IoT devices leading Bruce Schneier to aptly coin the term cyber pollution. Thus, cyber security requires highly collaborative and proactive efforts, perhaps bolstered by legislation.

Major efforts have been made over the past years to advance telematics cyber security and the best systems operate with a "security designed in" approach. Guidelines for advanced cyber security 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. However, security should not be instrumentalized to shut off data access and create a controlled data economy or even monopoly. Rather, regularly updated industry standards are a way to enable competition for finding the best uses for the data being generated. This could be accomplished purely through private collaborations, with the aid of legislation.

3. Interoperability Enables Data Access and Competition

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. Ownership of data is not worth much, if one cannot access it or must pay an extortionate price to do so.

Interoperability is a key feature in the era of smart mobility and the digital economy as it enables access to data and competition. Open platforms that work with all brands of vehicles enable companies and consumers to choose vehicles based on suitability for the task and business need rather than compatibility with software. This enables competition around who can add the most value to the data extracted from a vehicle.

Today, 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 extracting data from vehicles. 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. The data connector of the future will probably be something different, but when considering alternative schemes, close attention should be paid as to who manages/restricts data flow and whether commercial interests may call into question independent, verifiable data and accountability. Impeding interoperability restricts competition.

4. Recommendations to our Customers

The following are six recommendations we make to our customers, including fleet managers, leasing and rental car companies to ensure secure and open access to high quality, reliable data in connected vehicles, today and tomorrow.

1. **Understand the Importance of Data.** You should fully understand how your business is powered by data today and tomorrow and the implications of losing access to it.
2. **Assert Your Data Ownership.** Clearly state your expectation to own operational vehicle data. If necessary, confirm data ownership 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.
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 security of your data access platform and ensure it remains up to date. Develop your own data security program.
6. **Respect Driver Privacy.** Adopt privacy policies that protect drivers' personal data while enabling your business needs. Seek consent from drivers where necessary.

5. Determann and Perens Paper

Two Competing Visions of the car of the Future

In an upcoming article slated for publication in Berkeley Technology Law Journal two world leading experts in the field of privacy law and open source computing, Lothar Determann and Bruce Perens (Forthcoming, 32 Berkeley Tech. L.J. Issue 2 (2017)) ask a question of far reaching implications for business, consumers and governments as well as the auto and computer industries: Will the car of the future be open or closed? Determann and Perens perform a broad survey of the technological, economic, policy and legal aspects of the question which makes their piece required reading for anyone connected to the transportation and mobility industry. While the background of at least one of the authors may suggest a predisposition to openness, they are careful to evaluate both sides of the argument which makes their piece all the more compelling.

Vehicle Or Information Technology System On Wheels?

Determann and Perens define an “open car” as a vehicle, or “information technology system on wheels” that is open to constant technology upgrades, open to a wide variety of aftermarket products, open to the scrutiny of security researchers and open to competition. It has open interfaces and openly disclosed software and hardware. It will perform best in the presence of open platforms for developers. And yet, an open car does not require “open data”. Data privacy and security can be protected as well or better than the current array of proprietary automotive products do today. At the same time, the open car will enable “data accountability” which will be useful to OEMs, customers and regulators seeking to provide reassurance in light of recent high profile scandals affecting some OEMs (e.g. VW Diesel).

Open cars also do not require open source software. An open car may be regulated by government and be required to adhere to stringent standards in safety critical areas. Thus the defining feature of the open car is that owners and drivers of open cars will have maximum freedom to choose when and how to upgrade components and software (so long as they meet safety standards); the open car will enable coexistence of traditional long lasting components, such as the engine and the body of the car, and features that are rapidly changing, such as infotainment consoles and automated driving systems.

The authors explain that a “closed car” has its own merits: A “closed car” remains locked down by its original manufacturer, which is in most cases a large company with a strong brand, good safety track-record, well-capitalized, subsidized or supported by governments, and generally considered more trustworthy than many smaller companies. The OEM retains the power to choose if and when updates and upgrades are offered, with what functionality, and at what price. Owners of closed cars will have fewer choices and may have to discard an automobile if the OEM does not offer updates that are attractive, reasonably priced or necessary from a safety perspective in the rapidly evolving world of connected, autonomous cars. In that sense, a car will first and foremost remain a car rather than become a “computer on wheels”. A worthwhile thought given that the safety implications of a vehicle are much more evident and immediate than those of a laptop computer.

Nonetheless, perhaps the most compelling analogy to the debate around open cars is the rise of the PC industry in the 1990s. On PCs one could freely swap components, update software and choose which applications to install and remove while each component, update and application remained subject to its own set of quality control regimes, requirements and standards; each could communicate with the others and function together using common communication protocols. The proprietary computers of the day, however, where nearly entirely closed with almost every potential piece of hardware or software either created by the manufacturer itself or subject to its tight control.

Competing for the Future of The Car

Fundamentally, for the authors, the difference between an open car and a closed car comes down to whose choices matter most. In an open car, the choices of the vehicle owner and/or driver are paramount. In a closed car, the choices of the OEM are most important. Open cars are thus a threat to certain business models. Most notably, the “razors and blades” (or “printers and ink”) type of business model is directly threatened by open interfaces and platforms. Proprietary parts models would likewise be under threat.

Determan and Perens are advocates of a free market system. In such a system, companies (such as OEMs) are generally free to design their products at their discretion which could include a closed concept.Yet, a free market would equally as strongly argue for consumer choice and the presence of a rich aftermarket, long a key component of a vibrant transportation sector. Of course some OEMs may opt for a proprietary model while others prefer an open model.The authors predict that an open car will outshine its closed competition on issues of technology, competitiveness, sustainability and environmental policy. Open cars would be able to be upgraded to use the latest and best technology in hardware and software. There would be open competition for who was best able to provide the upgrades based on capability and price while still meeting safety and emissions standards. Upgrading a vehicle’s computer systems is less costly and more environmentally friendly than replacing the entire car and open disclosure of software and hardware would allow experts from around the world to audit an open car’s safety and environmental performance.

The authors carefully consider the role of government. Open cars, they argue, will live and die by the standards that govern them. Governments can be most helpful by encouraging broad based, fair standards that address the interests of as many stakeholders as possible: vehicle owners, drivers, OEMs, pedestrians, other drivers, fleet managers, and others.

Different OEM Approaches

Determann and Perens do note that at least some traditional automakers seem to be considering more open business models, involving open platforms and standards. These OEMs have been carefully observing business models that information technology companies have successfully introduced with respect to smartphones and other devices. Traditional car manufacturers rightfully perceive information technology companies as their biggest challengers in the years ahead. Some have started to build increasingly connected cars in reliance on robust, open developer communities. At least a few will no doubt attempt to replicate the successes of Apple and Google by providing an open platform that others can build upon; and they may well succeed. In the process, they will likely discover for themselves what technology companies learned long ago: interoperability is valuable to consumers.

Other OEMs, however, are pursuing a strategy of closing off the car, even going so far as to assert ownership over the data produced by vehicles they manufacture. According to Determann and Perens, opposition to open cars is motivated by three factors: economics, policy and ignorance. The economic motivation is most easily understood. One can realistically expect that the most vociferous opposition to open car standards will come from companies most invested in business models that are directly threatened. The policy motivation is often misunderstood insofar as it is not usually opposition to open cars *per se*, but willingness to sacrifice openness for other considerations thought to be more important; often security, safety or privacy. Here policy motivations shade into ignorance, especially when policy makers do not understand that perceived trade-offs may not be necessary. For example, openness and security often come together, in spite of intuitions to the contrary.

Open Cars and Cyber Security

Advocates for closed cars cite concerns over cybersecurity, safety and data privacy; but upon closer review, Determann and Perens suggests that risks in these areas do not truly justify roadblocks for open cars but should be better understood to support increased openness. Cyber security in closed systems is generally illusory. Security through obscurity is well-known to be among the least effective ways to secure electronic systems. Well designed code can be entirely public and still provide the best security available. Safety standards can just as easily apply to aftermarket suppliers as to OEMs and open cars do not imply open data. Controls on the data generated by cars can be made independent of the openness of the car's various sub-systems.

Open Cars and the Law

After reviewing current laws in a variety of fields, Determann and Perens conclude that current laws are not holding the open car back. Right-to-repair statutes that require OEMs to provide the same tools and information to independent mechanics as they do to their dealers help. Competition laws preventing tying, monopoly and unfair warranty practices also provide a strong tailwind pushing for the adoption of open car standards. Intellectual property laws, although leaning the other direction, do not present any insurmountable obstacles to open cars. Automotive product and safety rules have not yet dictated a preference for open or closed; and onboard diagnostic ports - originally required to monitor emissions by the California government - have become a gateway to openness and transparency.

However, there are dangers. Product liability concerns and the exaggerated cybersecurity concerns create hurdles. If manufacturers of open cars are held responsible for risks created by third party software or parts this could also slow the development of open car platforms. Automakers may be (or become) reluctant to open their products further. They may even decide to lock products down if they are indiscriminately held responsible for cyberattacks and the like. The sheer burden of litigation may be enough, especially in the US. Sector-specific legislation and regulation may be required if courts take a wrong turn in this respect. Proper allocation of liability and burden of proof may dictate how some OEMs respond. Shared liability models and insurance can play a role here.

Now Is the Time to Enter the Discussion

Determann and Perens have kicked off an important debate. It is now important that all stakeholders in transportation and mobility, especially those on the consumer and business customer side, make their desires and preferences known. And it will be up to OEMs, automotive aftermarket companies, technology providers and regulatory agencies to rise to the challenge. In addition to functionality, quality, innovation, and price, the challenge will include safety and security - the new frontier in the connected economy well beyond the auto sector.