Position paper

Call for a regulatory framework on access to vehicle data

Brussels, 31st May 2021

Executive summary

ETRMA calls for the Commission to come forward this year with a clear legal framework for fair access to in-vehicle data. This is an important milestone in the effort to make connected and automated mobility a reality. The framework must ensure a level playing field. Only clear rules and fair access to data will unlock the innovation and creativity needed for new and secure mobility services. This will be essential to ensure that Europe keeps pace with technological evolution and the development of the platform market.

Introduction

ETRMA represents 14 world-leading tyre companies employing directly about 370.000 people. The global sales of ETRMA's tyre corporate members represent 70% of total global sales and 7 out of 10 world leaders in the global tyre sector are ETRMA Members[1]. ETRMA members have strong manufacturing, as well as Research & Development presence within the EU and candidate countries, with 86 tyre-producing plants and 16 R&D centres.

Data-driven applications are being developed for use in a wider Tyres-as-a-Service (TaaS) value proposition, with direct tangible benefits for road safety and transport environmental performance. This encompasses several use cases, for example:

- Tyre pressure monitoring is already key for CO_2 emission reduction.
- Endurance and tyre wear predictions may provide information to users to avoid premature dismissal.
- Tyre wear predictions combined with weather and tyre pressure information can allow braking distance to be optimized in real-time in automated vehicles development.
- Tyre wear predictions can provide road operators with information on infrastructure quality.

The European Commission's target for a regulation to 'open up access to car data to mobility services'[2] – announced less than six months ago – and to 'review the current EU type-approval legislation for motor vehicles'[3] as set out in the February 2020 data strategy are significant commitments in line with the level of ambition needed to allow access to in-vehicle data and fair competition for all actors in the transport ecosystem.

Risks and issues related to vehicle data access

What is at stake is fair access to in-vehicle data, enabling the continuity of offers and the deployment of new business models, which will contribute to the deployment of greener and safer mobility in Europe.

---

[1] *ETRMA's membership include the following tyre manufacturers: APOLLO VREDESTEIN, BRIDGESTONE EUROPE, BRISA, COOPER TIRES, CONTINENTAL, GOODYEAR, HANKOOK, MARANGONI, MICHELIN, NOKIAN TYRES, PIRELLI, PROMETEON, SUMITOMO RUBBER INDUSTRIES AND TRELLEBORG WHEEL SYSTEMS. Furthermore, members include Associations in the following countries: Finland, France, Germany, Hungary, Italy, the Netherlands, Poland, Spain and the UK.*

[2] https://ec.europa.eu/transport/themes/mobilitystrategy_en

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN

Vehicles on the market in the next five years are being designed now. It is increasingly uncertain that all the necessary vehicle data will be made available on new models. Indeed, we are currently observing that On-Board Diagnostics (OBD) ports, the only entry point currently accessible by third parties in vehicles, are gradually being closed. This uncertainty is further compounded by layered obligations to meet cybersecurity requirements[4]; comply with the high-risk Artificial Intelligence principles[5] and ensure the protection of users' personal data[6][7].

Some stakeholders suggest indirect means of accessing in-vehicle data, such as cloud-based solutions, as the way to preserve vehicle's cybersecurity. **ETRMA believes that indirect in-vehicle data access alone restricts TaaS with the effect of stifling all present and potential innovation**. The restrictions of indirect access are notably the following:

- Limited data set available, with access mostly controlled and monitored by the vehicle maker;
- No sufficient real-time or high-frequency data access;
- No direct bi-directional communication with the driver.

On the issue of cybersecurity, so far we have no evidence that a cloud based solution would be more secure than an in-vehicle local access. European standards such as Secure Vehicle Interface[8] would secure the in-vehicle access for certified and authorized parties in the context of an independent cybersecurity governance. However, in the absence of an EU framework, there is the risk of fragmented approaches to the issue, with the effect of delaying the deployment of connected and automated driving across the European Union as a whole.

ETRMA's Recommendations

- Establish robust EU legal framework to access in-vehicle data, allowing enhanced mobility services to be developed and deployed;
- Resolve any ambiguities resulting from the absence of legislation or from horizontal rules across sectors;
- Allow fair competition for all actors in the mobility ecosystem with a clear requirement of separation of duties for the role of OEM as vehicle manufacturer and mobility service provider;
- Help the industry to plan its next steps by clarifying the definition and remit of digital services as they apply to "native" connected vehicles;
- The future governance of vehicle data access must place users at its heart, in line and with the same ambition of the fundamental principles of separation of duties, data sharing and privacy protection.

[4] https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security
[5] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0043&rid=8
[7] https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf
[8] https://www.svi-for-mobility.org/