AG/GE7315/JHU

Geneva, 12 November 2020

A global framework on the governance of transport data

IRU POSITION

- Data and digitalisation of the road transport sector has the potential to bring benefits to companies, consumers and society.
- Currently, transport operators, which are large data generators, find it difficult or at times even impossible to understand how companies receiving the data they generate handle their business/non-personal data. Data aggregators typically decide who can access data, and how the data can be used and re-used.
- This lack of transparency combined with the absence of a binding legal framework recognising the rights of the business data generators, is the root cause for transport operators hesitance to share the data they generate.
- Over 80% of transport operators carrying passengers and goods globally are small and medium sized enterprises (SMEs), with 1 to 10 vehicles per operator. Upgrading to digital tools and training the necessary staff require significant investments. Cost is a major consideration for small and medium-sized operators that should be taken into account when developing a data governance framework.

Waiting to embrace the digital transition, commercial road transport operators globally call on regulators for the following measures to be adopted when developing best practices and codes of conduct for B2B data sharing:

1. Sharing of business-generated data should always take place on a voluntary basis. At the same time, if partners do decide to share their data, they should be in a position to rely upon a binding legal framework, which will promote trust among business partners.

2. Recognise the rights of data generators regarding their access to data produced by aggregators on the basis of their raw input, as well as in connection with the use and re-use of such data by third parties.

3. Any data governance model should take into account the costs of the data economy for data generators, especially when developing global uniform standards and interoperability solutions which will be needed in order to make investments more worthwhile. Financial support and incentives for SMEs are needed to enable them to make the transition.

ANALYSIS

Currently, transport operators find it difficult or at times even impossible to understand how companies handle the data generated by their businesses. Data aggregators, which may collect data generated with or without express consent typically decide on who has access to the data and on how to use and re-use the data, often even without the knowledge, even less so consent, of the generators of such data. If practices of data aggregators are not regulated effectively, it may lead to inefficiencies in digital markets and will disrupt competition, for both data generators and data aggregators.

Transport data could be the data generated by a vehicle, i.e., vehicle performance data such as early warning for maintenance, fuel consumption, real time pollution, driver behaviour towards safety observance (seat belt) and tyre pressure or transport business data like load, route, occupation rate, rest time plan, package tracing.

Aggregator could be an online platform for example, freight exchanges or mobility as a service (MaaS) in passenger transport, vehicle manufacturer, fleet manager, a fleet maintenance company, transport service provider or a technology company. These intermediaries may collect, store, share with third parties, use or re-use raw or processed data.

Third parties could be any business entity that transport operators do not have any direct or indirect nexus and absolutely have no access or control on their business activities. In other words, the data generated could be used or re-used in any manner and the third party is neither bound to inform or take consent of the data generator nor share any benefit derived from the data used or re-used.

Steps must be taken to ensure equal opportunities for all business partners in the digital ecosystem. **IRU calls on policy makers to adopt a binding legal framework for the provision of B2B data** which should be based on the main pillars outlined below. The B2B framework data must cover any type of data flowing between businesses, irrespective of the way data is generated, including data created by transport operators and/or data automatically generated by a machine or vehicle owned by the transport operator. The pillars below should also apply in the context of business to government data flows, where authorities further open the data or otherwise share it with undertakings acting for-profit.

1. **The voluntary provision of data as the guiding principle**. Forcing the provision of business data, i.e., mandatory, would stifle innovation and could hamper the competitiveness of businesses, while further increasing the power of a few actors at the expense of the SMEs and start-ups in the market. B2B data exchange should continue to rely on **voluntary contractual agreements, in which provisions regarding the treatment of data should be clearly and explicitly stated**.

2. Responsible actors. The obligations and liability of data aggregators should be clearly defined and the rights of the data generators should be explicitly recognised, including:

a) **Access (reciprocity):** business data generators' access to the data they generate, whether in raw or processed format, should be guaranteed. It is essential to preserve data security when data is being exchanged. Access controls throughout data value chains, in adherence to strict security standards,

will be key to foster data sharing among different actors across data ecosystems.

b) **Overview:** business data generators should have the right to receive a data processing transparency report, detailing, inter alia, how the data they generated are stored and for how long, and how they are used and transferred to third parties.

c) **Consent:** an explicit consent of business data generators should be ensured for the collection of data generated by their business, for the storage, use (including further processing and aggregation) and re-use of such data over time. The language used in legal agreements to take the consent of data generators should be clear, simple and precise. The aspects of data processing should be transparent to boost trust and mitigate concerns about data misappropriation.

d) **Portability:** data generators, including transport operators, must have the right to take their data stored in one platform and transfer them to other providers. Data lock-in systems must not be allowed as they foster monopolies.

e) **Compensation:** the future framework on data must also ensure that data generators are able to ask for and receive financial remuneration in exchange for the data provided. Moreover, a mechanism should be put in place for data generators to seek compensation for damages if their rights are breached, especially, when such a breach occurs intentionally and/or due to the negligence of a party that did not perform its duties diligently.

3. **Financial support targeting SMEs**: the costs for the industry of transitioning to a digital economy should not be underestimated. Operators will have to develop their digital infrastructure, such as a software for data exchange, enabling interoperability with other operators and digital service providers, such as eCMR based platforms for goods transport and Mobility as a Service vendors for passenger transport services. In addition, support for technology innovation should be underpinned by a strong focus on skills. Workers need to be upskilled, particularly in the transport sector, to take full advantage of the opportunities offered by data-based business models in critical areas such as artificial intelligence (AI), machine learning (ML) or cloud computing. In addition, to meet the challenges of the digital economy, the transport sector needs data experts. Information campaigns on general data literacy in the workforce should be implemented at national level.

4. **Standardisation and interoperability**: an absence of uniform standards, for example APIs/data formats, makes interoperability between platforms difficult. It increases the risk of lock-in with one platform for data generators as the cost of investing in software that can respond to the diverse data format requirements of various platforms is discouraging for businesses. In the transport sector, transport operators need simple, uniform and accessible APIs/data formats.

Data has become an asset to companies[1] and in the transport sector the trend to collect, store, share, use/re-use of the data generated, especially by businesses, will continue at an increasing pace with the development of the internet of things (IoT), ML, AI and automation.[2] Innovative solutions, such as connected vehicles, smart cities and digital platforms will lead to an increase in data generation.

The same players in the transport and mobility space can have different roles in different data relevant circumstances. For example, a company can act as a data

[1] Estimates suggest that the world will generate about 90 zettabytes (approximately a billion terabytes) of data in 2020. By 2025, worldwide data is expected to grow to 175 zettabytes, with much of the data residing in the cloud.

[2] It is estimated that the global AI-derived business value in 2020 is likely to be about USD 2.65 trillion. Between 2018 and 2019, the percentage of organisations using AI technologies increased from 4% to 14%.

generator when the data it generates is collected by an aggregator in the upstream of the data value chain. The same company can act as a data aggregator if, in the course of its business, it also collects data of other companies in the downstream of the data chain. For the purpose of this position paper and of further data regulation, the notion of data generator and data aggregator must be assessed on a case-by-case basis, depending on the respective role of the company and its relevant position in the data value chain. For example, companies acting as fleet managers or transport service providers aggregate data from individual vehicles or operators but can be considered data generator vis-à-vis a third party which is in the upstream of the data value chain.

Governments across the globe recognise the value of data and are taking steps to create a data market that drives competitiveness in the global data economy[3]. So far, the emphasis has been on the protection of personal data (individuals).

In the context of sharing non-personal data (businesses), a number of challenges need to be tackled, such as:

1. **B2B data governance**. The lack of clarity on data generators' access to data stored and/or further processed by data aggregators on the basis of their raw input, as well as in connection with the use and re-use of such data by third parties.

2. **Transparency and trust**. The lack of trust by transport operators that the data they generate will be used in line with or even without contractual agreements, given the often unequal bargaining power between the parties and the lack of transparency.

3. **Financial**. The lack of economic incentives, including the fear of losing a competitive edge and/or the fear of no economic return, together with the lack of clarity on total cost for data generators to develop data driven systems.

4. **Data misappropriation**. The risk of misappropriation of the data (as single or aggregate data) by third parties.

Explanation 2:

In-vehicle data is directly transferred to the manufacturer or a data aggregator who in turn will process it further. The data generated by vehicles is already and will increasingly be key for the after-market services. In principle, the raw data belongs to the generator of that data, but as this data is instantly transmitted, the data generator may not even have access to their raw data. Similarly, manufacturers will always be in a better position to provide services or even to completely exclude other service providers from entering into the market creating captive markets[4] at the detriment of free market competition. This lack of transparency on part of the data aggregators in processing data and the risk of misuse of the data by third parties led to a situation where transport operators do not trust in data sharing practices. Manufacturers or data aggregators in general can be considered as data generator vis-à-vis a third party which is in the upstream of the data value chain.

a) Current legal framework does not support B2B data sharing practices

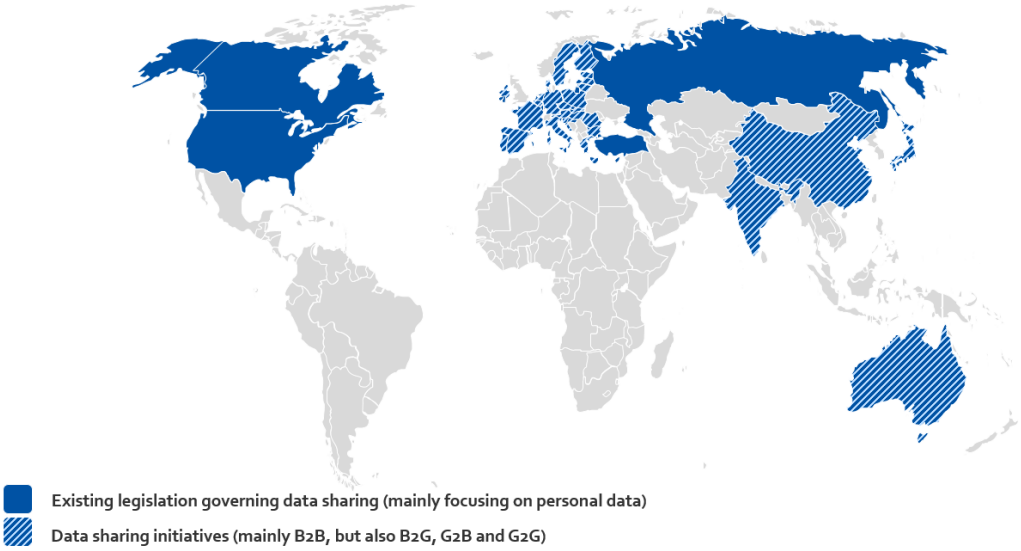
Laws in most countries provide general rules which could have an impact on data handling from different perspectives, as well as sectoral legislation with a focus on specific types of data flow[5]. The scope of intervention through general rules, such as

[3] See the recent publication by the European Commission of its Strategy for Data.
[4] Captive markets could for instance be vehicle maintenance information only available to authorised repair-shops, fleet economy data only available if entire fleet is of same vehicle supplier.
[5] See IRU overview of the existing governance framework for data.

competition law, is limited and procedures are excessively lengthy. Regarding specific legislation on data, a concrete recognition of the rights of data generators only exists in the context of business to consumer data flow (i.e., personal data).

In jurisdictions in countries such as Australia, China, India, Japan and the United States of America, the existing legislation is also insufficient to protect the interests of the parties involved when it comes to sharing of non-personal data. If any, legislative efforts are being considered to establish appropriate data sharing mechanisms in few countries (See diagram below).

Worldwide, the legal framework governing B2B data sharing is non-existent or too vague and the position of data generators, including transport operators, is not adequately taken into account.



Source: IRU

b) Online platforms and competition

Data represents a major economic asset,[6] since the use of data underpins the business models of all online platforms. The massive increase in collection, processing and storage capacities has increased concerns about the concentration of information. Online platforms bring enormous benefits and the COVID-19 crisis has made the many advantages of online platforms even more apparent. However, a small number of large online platforms[7] are in a position that allow them to act as gatekeepers, with adverse effects for innovation and competition. This could lead to:

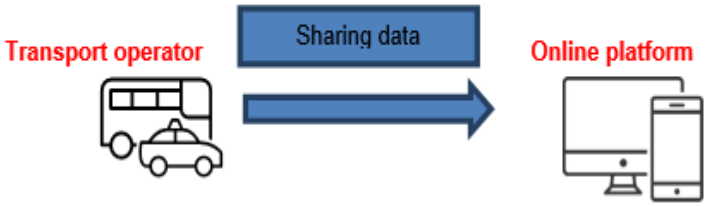
1. Data generators being in an asymmetric/unequal bargaining position vis-à-vis online platforms. The online platform might act as a private regulator, which limits data generators' ability to freely and efficiently make decisions; and

2. Data generators not having access to the data necessary to compete, and even access to their own data produced on the basis of the raw input and managed by a single online platform, is often cumbersome. Innovative start-ups and SMEs might face hurdles to enter the market or compete on merit, ultimately leading to a few players controlling the market.

[6] For example, the total value of European consumers' personal data in 2011 was estimated at EUR 315 billion. In 2020, big data in the European Union should become a market worth USD 1,000 billion (Report by Boston Consulting Group).
[7] In a list of the worlds' 70 largest online platforms with respect to market capitalisation – America has 73%, China has 18% and Europe has 4% of the platforms (Economist, 2020).

For example, in the case of Mobility as a Service (MaaS), [8] as with many other digital markets, once stabilised, these markets may naturally shift to favour one provider. Loss of customer control by the transport operator, which is a characteristic of this type of intermediation markets, will amplify the dependence on MaaS vendors, especially, if combined with data lock-in imposed by some vendors. To address this challenge, a legal framework on data governance should confer to transport operators' rights such as data reciprocity and portability (the possibility for a platform user to retrieve its data and/or move it to other platforms).

Explanation 3:



For example, when transport operators share their data with online platforms, there are no rules offering any guarantees or transparency on the re-use of this business data. The transport operators may lose control of commercially sensitive information of their business without any legal protection, for instance, the price or volumes or capacity on a certain route. Once the online markets stabilise, they will naturally tip to a monopoly where one player is dominant. The more important the online market become in terms of securing a substantial customer base, the stronger leverage online platforms will have over transport operators and other intermediaries. This may result in unfair terms and conditions for transport operators and intermediaries, including but not limited to high commission fees.

Therefore, it is crucial to ensure that all service providers, including, transport operators, are able to access and control their own data, and emphasise the need to adopt policies that are oriented to ensure transparency, openness, competition and fairness in the (digital) value chain.

* * * * *

[8] See IRU Position on Mobility as a Service and "Towards a European strategy on business-to-government data sharing for the public interest" - Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing (European Commission, 2020).