DOI: 10.24193/OJMNE.2023.43.05

ACCESS TO IN-VEHICLE DATA IN THE MAELSTROM OF PROTECTED RIGHTS AND LEGITIMATE INTERESTS AS AN URGENT CHALLENGE FOR EU LAW

Václav ŠMEJKAL, Associate Professor, Ph.D.
Škoda Auto University, Czech Republic
vaclav.smejkal@savs.cz

Abstract: *What will be the mode of the data that today's connected cars accumulate has become a critical issue for the entire automotive sector and its related supply and service industries. If quanta of highly usable data remain largely with car manufacturers, they will become gatekeepers and the entire aftermarket will either fall into complete dependence on them or lose the ability to innovate and compete. Aftermarket leaders and EU institutions are working to ensure that this data is shared from manufacturers to other supply and service providers. However, the most sensitive data is of a personal nature and its widespread sharing in the name of open competition may conflict with the right to privacy and the protection of drivers' personal data. Protecting both competition and data at the same time can be awfully expensive, with negative impacts on consumption and available mobility. This paper seeks to explain this straitjacket of three not entirely consistent requirements and to show the possibilities for emerging legislation within its framework. It shows that there are not only convincing arguments but also strong lobbies behind each of the demands, which makes finding a compromise solution even more difficult. At the end of the analysis, a solution is proposed which, taking into account all the constraints, appears to be the least detrimental to the preservation of all protected rights and legitimate interests.*

Keywords: In-vehicle data; connected cars; data sharing; competition; privacy; data protection.

1. Introduction

"Give car drivers control over their own data!", MEP Caroline Nagtegaal wrote in her question to the European Commission on 3 April 2023. She was critical of the fact that the Commission has not yet put forward sector-specific rules on access to vehicle function and resources, pointing to the urgency of the problem. The difficulty of it lies in the need to quickly ensure that all the actors around car manufacturers and their clients have access to the data generated by ever smarter vehicles, without compromising the safety, security, and privacy of those who drive them. Yet it is not easy to satisfy three groups of stakeholders who need each

other and at the same time have completely different views on what should be done with in-vehicle data. For car manufacturers, this data is an extremely valuable resource over which they have now an almost exclusive control. They also have several reasons why they would not and should not want to lose it. The entire automotive aftermarket, including garages, insurance companies, roadside assistance, and leasing companies, as well as manufacturers of navigation and traffic management apps, desperately need this data. Without it they will not break free from their dependence on car companies, and from being left behind by competitors linked to the automakers. Drivers, both individual and business owners of cars, and along with them consumer and personal data organizations, warn that the massive sharing of data that smart cars collect about themselves, their driving, and driver behaviour may put an end to the privacy, autonomy, and security that buyers have traditionally associated with the purchase of a personal.

The problem clearly has a legal dimension (even constitutional-legal, since it involves the protection of fundamental rights), economic, technical and, given its sensitivity, political, since it is directly related to affordable and safe mobility for ordinary citizens on the one hand, and at the same time to Europe's competitiveness in the global competition for technological dominance or independence on the other. Although the question "Who will have access to in-vehicle data and under what conditions?" appears at first sight to be very partial and limited in scope, it focuses on much broader and more significant conflicts and dilemmas of our time. The following analysis seeks to be aware of all these important overlaps and contexts of the question at hand, but without wanting to describe and explore them all. It aims to show what hinders the finding of an appropriate legal regime for access to in-vehicle data, to describe analytically what legal proposals are already on the table (or are at least mentioned in the literature), and finally to show what regulatory path could and should be followed by the EU, which is eagerly awaiting a legislative initiative from the Commission.

The following text, divided into four parts, will first deal with the phenomenon of data generated by car traffic. In the second part, it will be shown what accounts for the difficulty of finding an acceptable legal regime for sharing in-vehicle data, from the perspective of three different coexisting interests: i) to choose from competing offers, ii) to have affordable cars, iii) to maintain a high level of privacy and data protection. The third part will discuss the European Commission's work to date on this issue and finally the fourth part will discuss the solution that

seems most likely to be practically achievable. The focus will be on the legal aspects of the issue under examination, in particular the protection of fundamental rights, the protection of competition, the protection of consumer rights and, to a lesser extent, the protection of IPR. The main sources of data for the analysis are, on the one hand, materials published on the website of the European Commission, which has already outlined scenarios for solutions in 2022 and has long been in discussion with various stakeholders on the topic of in-vehicle data. It will also include the relevant opinions of car manufacturers, independent suppliers and service providers, data protection organisations and consumers, as well as expert comments and discussions conducted today mainly in virtual space.

The dynamics of change and the reality of the ongoing search for a legal solution to the problem at EU level mean that any conclusions drawn from the following analysis will be constantly "threatened" by further future legislative developments. Nevertheless, the author is convinced that many of the conclusions offered below have lasting validity and will represent the necessary boundaries within which future legislative solutions will have to fit, whatever their concrete form.

2. Connected cars‘ data as a legal issue

From the outset, it should be made clear that the issues raised are not the prerogative of so-called autonomous vehicles with autopilot and the problems discussed below are therefore not, for the most part, futuristic speculation. Connected cars are nowadays commonly produced cars even by non-premium brands because they are also equipped with software communicating with many sensors sensing everything possible inside and outside the car[1], usually with built-in navigation and communication plus infotainment equipment. It is reported that even the least connected cars today generate up to 25GB of data in an hour (Gooding, 2021). Ordinary users are increasingly aware that their cars are "computers on wheels" and should know that they are rather more than that, because they are technically more complex, have a longer lifetime, are

[1] Keeping an eye on seat belts, driving in lanes, hands on the steering wheel, as well as obstacles around the vehicle, is now commonplace in new cars, as is the traditional indication of mileage, average consumption, the condition of the tank or battery, oil and other fluids, tyre pressure... and days until the next technical inspection. Premium cars are of course equipped above this standard. There are about 200 data points in cars today (with at least 140 viable business uses) (Plungis, 2018).

more expensive to acquire, maintain and secure, and the risks associated with them are greater than with a regular pc or smartphone.

Much of the data that connected cars generate is not personal and sensitive. They relate to distance travelled, wear and tear on components, fluid condition, tyre pressure, temperature, etc., but in the context of other data, focused on the location of the car or driver behaviour, they, in conjunction with the VIN or registration number of the car, compose a very specific profile of the car user.[2] They are then information about how we drive, but also where we regularly go, whether alone or with someone, who we communicate with from the car, what we listen to, where we take petrol or charge the battery, what services we order via the communication system, etc.[3] This is why the European Data Protection Board (EDPB) warns in its Guidelines that "most of by vehicle generated data can be considered personal data", since the natural person is ultimately identifiable by their clever processing (EDBP, 2020, p. 3).

However, the personal nature of the data generated by connected cars (and thus their treatment under the EU e-privacy directive 2002/58/EC and in particular the regulation 2016/679 - GDPR) and the potential threats to privacy are only one of many sides of the issue. An immediately related conundrum is the question of whether such data constitutes private property at all, and who is their possible owner, or whether and when it can be protected as IPR (Amrit, 2017, Mikeš, 2019). This legally-theoretically and practically complicated problem does not have a clear and satisfactory solution yet, and also the upcoming EU legislation (the Data Act proposal being discussed by the European Parliament and the Council (Europa.eu. 2022)) addresses the regime of access right to machine-generated data and right to portability of that data, without trying to constitute ownership rights nor IP rights (Geigerat, 2022). Indeed, the EU legislator's aim is not to resolve the issue of ownership but - as the title of the Data Act suggests - to ensure fair access to and use of data. This aspect of the data accumulated by smart devices,

[2] For instance Ford US Privacy Notice categorises the data generated by the car's operation as follows Vehicle data (Information about the vehicle, its components and parts), Driving data (driving characteristics and behavior), Vehicle location (precise location and travel direction, information about the environment where the vehicle is operated), Audio/Visual (voice command and other assistance devices), Media analytics (information about what is listened to in the vehicle), Vehicle analytics (information about the usage of vehicle features, service and technology (Ford Motor Company, 2023).

[3] In-vehicle data could carry directly personal or even potentially sensitive information such as location data, heart rat, or driver fatigue etc. (Gazdag and Lestyán et al., 2023).

and in the case of connected cars mainly by their manufacturers, i.e., car companies, is an even more pressing issue.

As the economy becomes more digital, the internet of things and artificial intelligence develop, the data becomes essential new fuel without which it is difficult to do business and compete. The exclusive possession and use of this data may lead to market super-dominance by entities that we already commonly refer to as gatekeepers (Šmejkal, 2021), which, at least according to the warnings of the European left, could develop into so-called techno-feudalism, i.e., domination of more than just markets (Varoufakis, 2021). And although it is now reported that up to 80% of industrial data collected is never used and not all in-vehicle data is held by car manufacturers (ACEA, 2022, p. 5), it is nevertheless the car companies and their emerging eco-systems, made up of service providers linked to them, who are poised to become gatekeepers. The value of the in-vehicle data market is currently estimated at US$435 billion with steep growth potential (Reuters, 2023) as the transition to electric vehicles is expected to be the key driver behind sharply increased, and data generating, connectivity. Qualifying as major players in this market, on which all its other participants more or less depend, is certainly tempting.

Standardised access to the information necessary for vehicle repair and maintenance is already ensured in some respects by Regulation 2018/858/EU on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles.[4] However, according to complaints from the aftermarket, this is not a regulation providing the necessary access to data that can be extracted from today's cars and their producers do not provide open enough access to data for the rest of the industry (CLEPA, 2023). In the submission of those who are pulling the short end of the rope, there is an acute risk that the independent aftermarket will disappear in the automotive sector and a closed eco-system of car manufacturers as gatekeepers dictating to everyone else will emerge (Gill, 2022, p. 4-5). here is therefore a competition problem, because the threat of super-dominance of gatekeepers means a significant restriction of free and undistorted

[4] Regulation (EU) 2018/858 obliges, inter alia (see its Art 61), car manufacturers to provide independent repair and maintenance providers with on-board-diagnostic information, diagnostic and other equipment, tools including the complete references, and available downloads, of the applicable software and vehicle repair and maintenance information.

competition and, for the EU as a whole, a possible international competitiveness problem if the equation less competition = less innovation applies.

The big online platforms, typically the so-called GAMA quartet[5], in their capacity as gatekeepers, already have their prohibited and mandated conduct in the EU dictated by the current Digital Markets Act (EU Regulation 2022/1925). A general regime for the transmission and sharing of data generated by smart devices should be established by the Data Act currently under discussion, which, according to the Commission's published proposal, seeks to empower users (Europa.eu. 2022). The users of connected devices will, in short, get the right to have access to data generated by the devices and the right to ask the car manufacturers to share "their data" with third parties, based on an B2B agreement concluded between the manufacturer and the independent service provider. However, according to independent experts, the proposal sent to the legislative process favours the users and the interests of car manufacturers rather than giving broad options to third parties[6], even if the data holder is in principle obliged to share data on FRAND terms. Contrary to the fact that consumers in their majority act emotionally rather than rationally in relation to their data, that behavioural economics has long since revealed a consumer *status quo bias* (Samuelson and Zeckhauser, 1988) that implies the majority is usually staying with a pre-set and more or less workable solution, the basic premise of the Data Act is that the individual will be willing and able to make decisions regarding the use of the rather opaque and difficult to value quantity of data generated by the machine or device he/she uses (Kerber, 2022).

In addition, from the perspective of the issues examined here, the Data Act is a general horizontal regulation for the entire Internet of Things, so it will not be specific enough to fully address the issues related to in-vehicle data. At least that is what the aftermarket thinks, and so does the Commission, which has already presented options for a follow-up sector-specific regulation for in-vehicle data in March 2022. While the Data Act already passed its first reading in the EP in spring 2023, the in-vehicle legislation promised by the Commission for Q2 2023

[5] GAMA = Google, Apple, Meta (Facebook), and Amazon are typical, but not the only gatekeepers affected by DMA regulation.

[6] The aftermarket would essentially depend on the driver taking the initiative to ask the car manufacturers to enter into an agreement with the selected independent service provider and then to provide (start providing) data to the car manufacturer on the basis of the agreement. This assumes a valued initiative and some awareness on the part of the driver and then a willingness of both professionals to come to a workable B2B agreement on FRAND terms.

had not been presented by mid-June. Before discussing the possible shape of this sector-specific regulation, it is necessary to outline the "straitjacket" into which it must fit.

3. Dilemmas, trilemmas, quadrature of the circle

The following dilemma emerges from the situation described above: volumes of data, which in the case of car drivers may be of a personal nature and should therefore be adequately protected, are to be shared with hundreds of actors across the sector to limit the market power of potential gatekeepers, preserve the openness and fairness of the downstream sector, i.e. competition with all the expected benefits for society and consumers. We therefore have two fundamental, legally protected values, competition, and privacy (personal data), which should not cannibalise each other, although their parallel provision is by no means automatically guaranteed. “Privacy must not be diluted at the altar of competition”, wrote R. Matthan in March 2021, in a note warning that the objectives of protecting fair and open competition in the marketplace may come into conflict with the protection of clients' privacy through the handling of their data (Matthan, 2021). He thus condensed into a single sentence the impending conflict that had already been highlighted by some decisions of competition authorities[7] and warnings from authors dealing with the issue (Carugati, 2021; Šmejkal, 2021; Stucke, 2022; Gorecka, 2023; Bejček, 2023).

The fact that privacy and competition protection can be pitted against each other is a reflected reality also in the automotive and in-vehicle data sector. "There is a trade-off to owning a connected car... the manufacturer can fix bugs and add new features over time, but you also lose some control over your vehicle," expressed an US Consumers Union representative (Plungis, 2018). The loss of some control is due to increased connectivity, from which cannot be separated the increased data transfer between the vehicle and the entities around it, firstly the manufacturer and secondly all others who will access the data or with whom the data will be shared under certain conditions. While some data will not be stored anywhere, and others may be anonymised and will only be used to make technical improvements to a particular component

[7] In the US, for example, this is a court case LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019), where the District court ordered LinkedIn to refrain from putting in place any legal or technical measures with the effect of blocking a third party‘s access to public profiles. In the EU, this includes warnings to Apple or the initiation of proceedings (both at EU level and in some Member States) when it tried to enhance privacy of its users by limiting third-party’s application access to its platform (Ikeda, 2021).

in the car or to make traffic management more efficient in cities, however, the really profitable services, from car maintenance planning and insurance to infotainment and all the comfort improvements that use geolocation, driving style and driver fitness, can only benefit maximally from data that allows individual targeting of a particular individual in a particular car.[8] Although the dashboard does not ask what the driver wants to do with the generated data every time the key is turned, drivers instinctively know that their car is generating data and privacy concerns are the most common reason for refusing to share it (Gooding, 2021). A solution must therefore be found that subjectively and objectively ensures sufficient data protection and privacy (i.e., effectively enforcing compliance with GDPR on all those who will process in-vehicle data) so that there would be the necessary legal titles to share data with entities outside the car manufacturer's eco-system and free competition would be maintained.

Of course, privacy and competition protection are not necessarily mutually exclusive. One can imagine, on the one hand, competition between manufacturers and service providers to provide a higher standard of data protection and, on the other hand, IT and organisational solutions that ensure data sharing with a reasonable level of data protection. However, in addition to the question of the political-legal-technical feasibility of such an ideal, we must immediately ask about the price that will have to be paid for combining privacy and competition. There are techno-optimists who expect not only greater security from the use of more data from connected cars, but also efficiency and savings from their operation, maintenance and servicing (Aggarwal, 2022). In doing so, they are thinking along the same lines as when they anticipate the benefits expected from ever more sophisticated robotics, automation and AI deployment in industry to enable perfect 24/7 production without inaccuracies, breaks, human failures, etc. But the “factory analogy” can only work in the case of cars if we move to random and short-term ad hoc sharing (which is perhaps, as some have claimed, the mobility model of the coming generations (Bettendorf, 2017)). However, as long as we buy or rent cars for long-term use, care for them, adapt them to our needs (not to mention the car as an accessory to personality or directly as an object of emotional relationship), the analogy of the car to the modern factory will give way to

[8] Thanks to connectivity, a growing range of car features are becoming a matter of subscription for the service provided, or an over-the-air upgrade. For the car company and downstream service providers, connected cars are thus becoming a continuous source of revenue (Wucher, 2022).

the analogy of our relationship to our personal health and fitness, or even to our own homes. With those assets that we personally care deeply about, our psychological price ceiling has no limit.

The sector already has something of an automotive data management market, whose global size was estimated at USD 2.19 billion in 2022 and is expected to hit around USD 14.29 billion by 2032 (Precedenceresearch, 2022). Even without a deeper analysis, it is clear that these are volumes estimated based on the turnover of companies, "vehicle data hubs", which monetise the services of processing (sorting, packaging), securing and transferring from source to stakeholder data for further business use. CLEPA - the European Association of Automotive Suppliers, the lobby for the aftermarket, explains in its position paper (CLEPA, 2023) the need for this kind of services by saying that each connected vehicle today delivers a distinct set of data points and there is no larger overlap of data points supported by many vehicles. Downstream services then need to be oriented towards individual brands or even model ranges without becoming cross-brand and serving the whole market. Intermediaries that provide aggregation and adaptation of such data on a commercial basis will enable just such cross-brand servicing. However, the proposed Data Act does not envisage regulating this born-in-practice intermediate for the EU (Kerber, 2022, p. 125). While this may reduce the price of shared data by the profits of intermediaries, it does not reduce the cost of the services that the use of data generated by connected cars facilitates.

These services would therefore have to be provided by car manufacturers in the absence of partial sectoral regulation, and for them CLEPA essentially calls for price regulation in the form of uniform guidance on fair, reasonable, and non-discriminatory fees and a guarantee that, in the case of SMEs, compensation for data will not exceed the costs directly related to making data available (CLEPA, 2023, p. 8). ACEA - the European Automobile Manufacturers' Association, in its policy paper on the EU Data Act (ACEA, 2022) proposal, protests against this, arguing that such data sharing obligations will require substantial investment. Increased costs are imminent for two reasons. According to ACEA, only a small part of the data generated by vehicles is currently actively stored and used. If the definition of the data that will be subject to any new regime is expanded, car manufacturers will have to invest in how they design and build cars, or what they equip them with, to be able to store and communicate such volumes of

data (ACEA, 2022, p. 5). Besides, there are those operational costs from collecting, storing, protecting, managing and disseminating via electronic means data generated by cars. Such costs may become, according to ACEA, unsustainable for individual manufactures and will severely undermine the incentives to invest (ACEA, 2022, p. 8). In short, both the car manufacturers' lobby and the aftermarket lobby, and ultimately the European Commission, understand the cost of ensuring data sharing and protection at the same time could be uncomfortably high. With a high degree of probability, it can be predicted that most of it will eventually be passed on to those who buy and rent cars, thus impacting the easy availability of car-mobility for a significant part of the population (let us disregard in this analysis the possibility that this is a development welcomed by those who aspire to a car-free future).

This puts us in a situation where the dilemma becomes a trilemma. We can imagine (and achieve) affordable data sharing at the expense of data protection and privacy. Equally, we could more easily protect the data by limiting its sharing, because GDPR compliance by a dozen large car companies and their eco-systems can be better controlled than spreading the data across markets, and it will be controlled at a still affordable price. Ultimately, we can move towards a high level of data sharing and data protection, but all indications are that it will not be cheap, and the prices of new cars and modern mobility services may be far from the average consumer's purchasing power. Of the triad of competition - privacy (personal data) - consumption (costs), only 2 out of 3 are always within our reach, and the challenge becomes achieving all three goals at once, which is what we need for a balanced functioning of not only the automotive sector but, in fact, of society. However, nothing in the proposals and discussion to be analysed in the next section suggests that a solution to this squaring of the circle is on the horizon.

4. Commission’s initiative and responses to it

The European Commission has already launched a public consultation in March 2022 on a proposal for sector-specific legislation that would provide an appropriate solution for in-vehicle data sharing (European Commission, 2022). It has proposed 4 scenarios (Options 0-3) to the interested public, varying in increasing regulatory intensity. Briefly, these are:

- Option 0: Only the Data Act applies, there is no specific sectoral act. Such a solution represents a lesser regulatory burden but also highly likely does not ensure sufficient

data sharing. The specific needs of aftermarket and mobility services are not taken into account. Apart from the fact that regulation will not hinder spontaneous developments in the sector, such a solution will have all foreseeable negative consequences.

- Option 1: Specific sectoral act mandates equal and non-discriminatory and transparent access to data. However, the regulatory intervention is reduced to the minimum necessary: just a public list of data generated by each car model. To this and to downstream functions (e.g., the possibility of remotely unlocking the vehicle door for a shared mobility service) and resources (charging / discharging of batteries) equal access for all parties will be ensured. No new risks for safety and security will arise, new ongoing costs and obligations for manufacturers and the public sector should still be acceptable.
- Option 2: Beyond what Option 1 would require a standardized minimum list of data, functions, resources to must be made available. Permanent and secure access to on-board diagnostics and to bi-directional communication with the driver will be provided. This will require additional measures at the level of cybersecurity and privacy. It will therefore be a more elaborated, ready-made solution increasing accessibility and efficient use of generated data. However, costs become higher, administrative surveillance more complicated.
- Option 3: Beyond what is required by Options 1 and 2, it will be defined in what ways and modes data access will be provided and how this will be controlled. These detailed and constantly updated governance rules on access to data look like the best solution for competition, innovation, consumer choice, privacy, and data protection. However, the Commission acknowledges that compliance costs will be higher overall, for all car manufacturers and third parties, public budget, legislators, enforcers.

The ratio of pros and cons of the different options is logical and clear: from a free safari that is relatively easy to supervise and maintain (Option 0) to a costly but clear and safe zoo (Option 3). The individual options are difficult to evaluate from an external perspective, as we do not even know the final form and practical implications of the Data Act yet, so the functionality of upgrades to the standard required by it can only be speculated. Moreover, the proposals are not sufficiently specified to the extent that it is clear which data is already being

shared and only the standards for such sharing will possibly change, and which data will be affected by the new obligation and standard for the first time, which of the data will be purely technical or anonymised and which will instead require a strict privacy regime.

The external observer's appreciation is not helped by the subsequent discussion of the proposal, which is also available on the Commission's website (European Commission, 2022). It shows that, at least in the first reactions, none of the influential lobbies stands in the middle, none of them advocates "something between" Options 1 and 2. The car manufacturers, represented by the aforementioned ACEA, the American Automotive Policy Council (AAPC) or the Autonomous Vehicle Industry Associations (AVIA), would prefer the Commission to follow the baseline scenario approach, i.e. if possible Option 0 would prevail. Conversely, virtually everyone outside the circle of car manufacturers, be it the aforementioned CLEPA, the Council for Motor Trades and Repairs (CECRA) or the European consumer organisation BEUC, prefers Option 3. Individuals, often expressing themselves anonymously, would probably agree on the slogan "my car, my data!", as they demand the fullest possible control over all data generated by cars, i.e. no automatic transfer of data outside the car and free decision-making on whether data is deleted, anonymised or, subject to individual informed consent, used and shared. Given what has been written on the subject above, this is a division of positions that is to be expected and justified by the priority interests of each of the groups concerned.

However, viewed through the prism of the described trilemma "competition - privacy (personal data) - consumption (costs)", both extreme options (i.e., 0 and 3) are not a satisfactory solution. Leaving in-vehicle data in the Data Act regime, i.e., option 0, overlooks the difference in how the car market works with all its traditional and emerging aftermarket and other services, compared to e.g., smart fridges or phones. It is hard to imagine that a robust and thriving aftermarket could expand just by accessing all the necessary in-vehicle data on the basis of requests from individual users of these cars, or by making do with the basic technical data already provided today under Regulation 2018/858/EU on the approval and market surveillance of motor vehicles. This is supported by empirical data on the use of Article 20 of the 2016/679 GDPR on data portability, which is based on a similar principle. This has shown that without the addition of the necessary "functioning infrastructure for direct data portability between multiple providers", its potential remains untapped (Symoudis and Mager, et al., 2021). Similarly, the

potential for competition and innovation would remain untapped if most valuable data remained with car manufacturers.

In contrast, the overregulation that Option 3 seems to promote is not only costly but potentially bureaucratic, and therefore usually a brake on competition and innovation (Bejček, 2023, p. 25). Option 3 looks on paper like a solution combining high protection of competition and privacy, but the Commission itself recognises its cost to all stakeholders and the ongoing need to continuously update regulation to avoid slowing down innovation, which could run up against rapidly outdated rules on what data, how categorised and processed, with what security and under what FRAND conditions, should be made available. This already shows the extraordinary intellectual, organisational and, ultimately, financial costs that the effective operation of such a system would require.

This brief assessment shows that the first positions formulated in relation to the Commission's proposal are rather negotiating positions and that both poles of opinion are aware of and may gradually accept the necessity of a compromise that will better address the trilemma of competition-privacy-consumption. The EU can afford to sacrifice neither fundamental rights, which are privacy and personal data protection (Articles 7 and 8 of its Charter of Fundamental Rights (CFREU)), nor free and undistorted competition, which is part of its priority objective of the functioning of the internal market (Article 3(3) TEU and Protocol 27). Needless to stress that the provisions protecting competition are among the EU's public policy norms (European Court of Justice, 1999) and they are also directly related to safeguarding the economic rights of the European consumer (Article 169 TFEU and Article 38 CFREU). The most that can be considered is the intensity and priorities of the enforcement of EU instruments for the protection of privacy (personal data) and competition and weighing them against the costs that different options for setting their relationship will bring to the burden of stakeholders and, ultimately, consumers.

5. Probable and possible solution(s)

In view of the above, realistic expectations can only be linked to Options 1 and 2 of the European Commission's proposal, or combinations thereof, as well as to variations on the measures they propose.

The starting point for the search for a solution was undoubtedly indicated by the numerous responses to the four European Commission options, which called for a more precise definition of the distinct categories of data involved. For example, ACEA, representing car manufacturers, argues that only a very small portion of the in-vehicle data is of interest to service providers as most of vehicle-generated data are primarily of a technical nature. This mainly performance data than helps to ensure safe operation of the vehicle, exist only temporarily, are used locally within vehicle systems, and are never stored (CarDataFacts.eu). Logically, we are talking here about the quantity of data, not its value for further use, let alone its value in case of monetisation. In any case, however, it is good to remember that the demanding management of sharing would only concern a minority of the data generated by cars.

Among these further usable data are those that can be separated from the VIN and the vehicle registration number without losing their usefulness (for urban traffic management, for troubleshooting a given vehicle type, etc.). The challenge then remains, in particular, to define and establish a regime for sharing and permitted use of that category of data which is of high value for further use. Inevitably, this value depends on being able to personalise offers of goods and services based on the personal data processed (insurance or leasing terms and conditions, assistance services, infotainment and, of course, other supplies and services that can effectively arise from the evolution of individual drivers' needs).

The regime for handling this potentially sensitive category of data should of course be primarily based on the GDPR (i.e., in the case of sharing such data between data processors only based on a legal requirement, or prior consent of the data subject). However, already defining and separating this data from the rest is a challenge, and it is followed by another one in the form of categorizing, processing, packaging… simply making the data suitable for further use, as most third parties will not be able to use simple access to a part of the server (whether under the control of a car manufacturer or a neutral trustee) and the raw data stored in it. CLEPA, representing the aftermarket, therefore asks that sectoral regulation should ensure, inter alia, the definition of a pre-set standardised minimum dataset; provision of a common automotive application programming interface to ensure data flow from the sensor to the service; a governance body or structured forum to set a framework to assign respective roles, rights, authorisations, and liabilities... (CLEPA, 2023, p. 3).

While the legal obligation to prepare the data in this way beforehand would be a justification for processing it under the GDPR, such processing requires an intellectual and financial investment. In addition to the issue of cost, and thus the cost of further provision of such prepared data, there is also - as car manufacturers in ACEA point out - the issue of trade secrets, of protection of original databases, of copyright, etc. The very act of sharing or transferring large volumes of such data may, of course, raise additional issues of transferring responsibility for its security and, consequently, liability for data breaches, loss, misuse, which is alluded to by the requirement to define the interface for its transfer and the distribution of the burden represented by the operation of the whole rather complicated system.

A regulation that would adjusts all that, if it wants to satisfactorily address the trilemma described above, faces a different dilemma: between generality and detail, between under- and over-regulation. From the problems outlined, it should be as specific as possible and the regime for sharing the sensitive part of in-vehicle data, roles and responsibilities of all parties should be defined and standardised as much as possible. It is beyond the scope of this analysis and its author to determine whether this is possible without regulation hindering innovation and the dynamic development of the sector. However, if setting up a data sharing regime is the main task of sectoral regulation, it should try to be extremely specific on the one hand and flexible and open to change on the other.

Under the pressure of these rather contradictory requirements, it seems most realistic to seek some regulation not for the actual form and content of multi-sharing between car manufacturers and amount of third parties of the aftermarket (and millions of drivers), but rather for the data management market regime. The solution seems to be to bring independent data aggregators and dealers into the game, i.e., data professionals, who will relieve automakers, but more importantly the independent downstream providers of goods and services (and ultimately individual drivers), from having each to become higher-level data professionals. Car manufacturers will not be the main data custodians, nor will it lead to the combinations of DigiTech companies with car manufacturers. All car-generated data would go to a neutral trustee who would secure and distribute them in some standardized way. It would make car manufacturers, downstream service providers and possibly even drivers, mere clients of a few strictly licensed and regulated (even in terms of operating costs and margins) data companies

that would ensure that the necessary level of protected data is available in usable form at an affordable price (something along the lines of health insurance companies in the post-Bismarck model of health insurance system (Wallace, 2013)). This is the most interesting solution discussed in the literature (Kerber, 2022), but not yet reflected by the Commission, while it is becoming increasingly clear that this solution could bring security, transparency, and possibly also cheaper operation of the whole complex data sharing system.

Time will tell whether this, undoubtedly demanding solution will be implemented, and before that happens, perhaps a series of follow-up analyses will bring it closer. In any case, the broader context, which was only mentioned in the Introduction, but was not included in this analysis, also works in favour of the proposed solution. Turbulent developments in all socially sensitive markets, from finance to energy, to pharmaceuticals and health care or housing, are leading in the EU to stricter regulation, to a higher share of the state or straight to a mixed economy. It would be surprising and especially counterproductive if the market with the essential oil for Industry 4.0, i.e. with data, was left with only the existing regulation preventing the abuse of market power and the abuse of personal data. We are gradually becoming as dependent on data as we are on the access to capital or electricity. If the EU does not want to become lagging behind or even dependent in relation to other great powers in this respect, it cannot afford to leave in-vehicle data without sophisticated regulation.

6. Conclusion

An attempt to polemically present what all the legislative solution to a certain ripe problem, complicated by the clash of conflicting interests, but also not always compatible fundamental rights and freedoms of EU law, must deal with, can hardly lead to a clear and satisfactory conclusion.

As has perhaps been shown convincingly enough, only unsatisfactory solutions are easily achievable. The easiest to achieve is poor data sharing and therefore poor competition in the sector, but at least with privacy protection at the level we have so far. Alternatively, the sharing of data can be expanded while its protection is reduced, which will become the price for more open competition and higher efficiency in downstream supplies and services. Or - if the authorities promoting competition and data protection are up to the task of effectively enforcing

compliance with the regulations - we can expect better data sharing with their strict protection, but at a significantly higher price for all involved, which will ultimately burden the buyer and the taxpayer. Better than these solutions is the technically, economically and legally demanding search for a form of regulation that avoids both extremes (leave unregulated vs. regulate as much as possible) and focuses primarily on the regime of those data that are the most sensitive from the point of view of privacy protection and at the same time the most valuable in terms of further commercial use. A specifically regulated market should be created for in-vehicle data, at the centre of which will be the specialized subjects of licensed and closely supervised data companies.

1. References

2. ACEA (2022) *ACEA Position paper – proposal for a Data Act*. Available at: https://www.acea.auto/publication/position-paper-proposal-for-a-data-act/ (Accessed: 09 June 2023).
3. Aggarwal, D. (2022) *Connected vehicle data is driving the future of Auto Industry*, *Telematics Wire*. Available at: https://telematicswire.net/connected-vehicle-data-is-driving-the-future-of-auto-industry (Accessed: 09 June 2023).
4. Bejček, J. (2023). Sustainability of 'Traditional Antitrust' under the Challenge of 'Sustainability' and Digitization. *Acta Universitatis Carolinae - Iuridica*, 69(2), pp.9–31. doi:https://doi.org/10.14712/23366478.2023.12.
5. Bettendorf, N. (2017) *Generation Z may not want to own cars. can automakers woo them in other ways?*, *NPR*. Available at:
6. https://www.npr.org/2017/12/08/568362029/generation-z-may-not-want-to-own-cars-can-automakers-woo-them-in-other-ways (Accessed: 09 June 2023).
7. CarDataFacts.eu. (n.d.). *CarDataFacts.eu - Safe and secure access to vehicle data.* [online] Available at: https://www.cardatafacts.eu/ (Accessed 09 June 2023).
8. Carugati, C. (2021) *The antitrust privacy dilemma*, *SSRN*. Available at: https://ssrn.com/abstract=3968829 (Accessed: 09 June 2023).

9. CLEPA (2023) *Position paper on access to in-vehicle data - CLEPA – European Association of Automotive Suppliers*. Available at: https://clepa.eu/mediaroom/clepa-position-paper-on-access-to-in-vehicle-data-2/ (Accessed: 09 June 2023).
10. EDBP (2020). *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications* | European Data Protection Board. [online] Available at: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-12020-processing-personal-data_en (Accessed: 09 June 2023).
11. Europa.eu. (2021). Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC|*EUR-Lex - 32018R0858 - EN - EUR-Lex.* [online] Available at:
12. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0858 (Accessed: 09 June 2023).
13. Europa.eu. (2022). Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)|*EUR-Lex - 52022PC0068 - EN - EUR-Lex.* [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN (Accessed: 09 June 2023).
14. European Commission (2022) *European Commission - Have your say*. Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Access-to-vehicle-data-functions-and-resources/feedback_en?p_id=29298097 (Accessed: 09 June 2023).
15. European Court of Justice (1999) Judgment of the Court of 1 June 1999. *Eco Swiss China Time Ltd v Benetton International NV*, C-126/97, EU:C:1999:269.
16. Ford Motor Company (2023). *Ford Privacy policy*. Available at: https://www.ford.com/help/privacy/#USprivacypolicy (Accessed: 09 June 2023).
17. Gazdag, A., Lestyán, S., Remeli, M., Ács, G., Holczer, T. and Biczók, G. (2023). Privacy pitfalls of releasing in-vehicle network data. *Vehicular Communications*,

[online] 39, p.100565. doi:https://doi.org/10.1016/j.vehcom.2022.100565 (Accessed: 09 June 2023).

18. Gill, D. (2022). The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources. *SSRN Electronic Journal*. doi:https://doi.org/10.2139/ssrn.4115443 (Accessed: 09 June 2023).
19. Geiregat, S. (2022). The Data Act: Start of a New Era for Data Ownership? *SSRN Electronic Journal*. doi:https://doi.org/10.2139/ssrn.4214704 (Accessed: 09 June 2023).
20. Gooding, M. (2021) *Data from your connected car could be sold to the highest bidder*, *Tech Monitor*. Available at: https://techmonitor.ai/policy/privacy-and-data-protection/connected-vehicle-data-apply-carplay (Accessed: 09 June 2023).
21. Gorecka, A. (2023). *Competition law and privacy: extensive data acquisition as the 'eye' of the problem.* [online] Network Law Review. Available at: https://www.networklawreview.org/phd-privacy/ (Accessed: 09 June 2023).
22. Amrit, S. (2017). *Who owns the Machine Generated Data in IoT – Men or Machine?* [online] IIoT World. Available at: https://www.iiot-world.com/industrial-iot/digital-disruption/who-owns-the-machine-generated-data-in-iot-men-or-machine/ (Accessed 9 Jun. 2023).
23. Ikeda, S. (2021) *EU Tech chief shoots down one of Apple's strongest arguments: 'privacy and security' cannot be used as defenses against antitrust charges*, *CPO Magazine*. Available at: https://www.cpomagazine.com/data-privacy/eu-tech-chief-shoots-down-one-of-apples-strongest-arguments-privacy-and-security-cannot-be-used-as-defenses-against-antitrust-charges/ (Accessed: 09 June 2023).
24. Court of Justice of the European Union (1999) Judgment of the Court of 1 June 1999. *Eco Swiss China Time Ltd v Benetton International NV*, C-126/97, EU:C:1999:269.
25. Keegan, J. and Ng, A. (n.d.). *Who Is Collecting Data from Your Car? – The Markup*. [online] themarkup.org. Available at:
26. https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car (Accessed: 09 June 2023).

27. Kerber, W. (2022). Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives. *GRUR International*. doi:https://doi.org/10.1093/grurint/ikac107 (Accessed: 09 June 2023).
28. Matthan, R. (2021). *Privacy must not be diluted at the altar of competition*. [online] mint. Available at: https://www.livemint.com/opinion/columns/privacy-must-not-be-diluted-at-the-altar-of-competition-11617119152799.html (Accessed 9 Jun. 2023).
29. Mikeš, S. (2019). *Co je nového v právu.* 1st ed. Praha: Nová Beseda.
30. Plungis, J. (2018). *Who owns the data your car collects?*, *Consumer Reports*. Available at: https://consumerreports.org/automotive-technology/who-owns-the-data-your-car-collects (Accessed: 09 June 2023).
31. Precedenceresearch (2022). *Automotive Data Management Market Size, Report 2023-2032*. [online] Available at: https://www.precedenceresearch.com/automotive-data-management-market (Accessed: 09 June 2023).
32. Reuters (2023). EU plans rules for fair access to connected car data. [online] *Automotive News Europe*. Available at: https://europe.autonews.com/automakers/eu-rules-connected-car-data-remain-limbo (Accessed 09 June 2023).
33. Samuelson, W. and Zeckhauser, R. (1988). Status quo bias in decision making. *Journal of Risk and Uncertainty*, [online] 1(1), pp.7–59. doi:https://doi.org/10.1007/bf00055564.
34. Stucke, M. (2022). *Data Competition Won't Protect Your Privacy*. [online] Institute for New Economic Thinking. Available at:
35. https://www.ineteconomics.org/perspectives/blog/data-competition-wont-protect-your-privacy (Accessed 09 June 2023).
36. Syrmoudis, E., Mager, S., Kuebler-Wachendorff, S., Pizzinini, P., Grossklags, J. and Kranz, J. (2021). Data Portability between Online Services: An Empirical Analysis on the Effectiveness of GDPR Art. 20. *Proceedings on Privacy Enhancing Technologies*, [online] 2021(3), pp.351–372. doi:https://doi.org/10.2478/popets-2021-0051 (Accessed: 09 June 2023).

37. Šmejkal, V. (2021). Three Challenges Of Artificial Intelligence For Antitrust Policy And Law. *InterEULawEast : journal for the international and european law, economics and market integrations*, 8(2), pp.97–118. doi:https://doi.org/10.22598/iele.2021.8.2.5.
38. Varoufakis, Y. (2021). Techno-Feudalism Is Taking Over | by Yanis Varoufakis. [online] *Project Syndicate*. Available at:
39. https://www.project-syndicate.org/commentary/techno-feudalism-replacing-market-capitalism-by-yanis-varoufakis-2021-06 (Accessed: 09 June 2023).
40. Wallace, L.S. (2013) *A view of health care around the world*, *Annals of family medicine*. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3596027/ (Accessed: 09 June 2023).
41. Wucher, O. (2022) *Continuous source of revenue for oems*. [online] Q_PERIOR AG Available at: https://www.q-perior.com/en/fokusthema/pricing-of-digital-services-and-vehicle-data-continuous-source-of-revenue-for-the-automotive-industry/ (Accessed: 09 June 2023).