The Frontiers of Society, Science and Technology
ISSN 2616-7433 Vol. 4, Issue 4: 43-47, DOI: 10.25236/FSST.2022.040408

Construction of Data Access Rules for Connected Cars

Fu Xinming

School of Law School of Intellectual Property, Guilin University of Electronic Technology, Guilin, China

Abstract: *The connected car has become another Internet portal after the mobile phone, and the problem of data access of the connected car has become increasingly prominent. Vehicle data access involves issues such as data security, enterprise competition, service innovation, etc. The concept of "extended vehicle" proposed by original equipment manufacturers obtains data control rights on the grounds of security, and "factual control" of data through technical measures enables it to A situation of "exclusive control" over automotive data results in less competition, less consumer choice and less innovative services. Therefore, it is necessary to return the control of car data from "car manufacturers" to "connected car users", and the mode of data access changes from "proprietary server" to "shared server" or "in-vehicle application platform".*

Keywords: *connected car, data access, extended vehicle, exclusive control*

1. Introduction

Data is known as the "new oil" of the contemporary era. The reason is that data is very important to countries, enterprises and individuals. Data affects the security of countries, enterprises and individuals, and is related to the strategic direction of the country and the development prospects of enterprises. Connected cars are IoT devices that have digital sensors and geolocation trackers embedded in mechanical parts. Mobile communication channels facilitate external processing and use of data by various service providers. Many businesses or individuals are looking to extract and extract value from this data, including original equipment manufacturer (OEMs), connected car users, OEM-authorized and independent after-sales service providers, data marketplace operators, and analysts. Car data can be used for many types of services, including navigation, information and entertainment, maintenance and diagnostics, and insurance. Data will play an important role in driving consumers to purchase new products in automotive services. Digital services will increase price competition and drive down prices in traditional service markets.[1] Therefore, obtaining car data is also crucial for after-sales service providers and consumers alike.

2. Questions Raised

Cars are one of the main means of transportation at present. The number of connected cars can be described as huge. The data of connected cars plays a pivotal role in data security and business strategic value. According to statistics from the Ministry of Public Security of China, in 2021, the number of motor vehicles in the country will reach 395 million, of which 302 million are cars. In 2021, the Internet Society of China released the "China Internet Development Report". The report shows that in 2020 alone, the sales of intelligent networked vehicles in China will be 3.032 million, a year-on-year increase of 107%. The innovative driving force of upgrading has been mentioned at the height of national strategy.[2] This is a huge number. With so many connected cars, a large amount of car data will inevitably be generated. Over time, some users of non-intelligent connected cars are likely to become users of intelligent connected cars. By then, the amount of car data could grow exponentially. Such a huge amount of car data, which also involves national security, data protection of car users, and commercial interests of car-related companies, is enough to attract attention at the national level. For example, special legislation on car data and construction of car data access rules.

As an emerging industrial ecology with deep integration of automobiles, electronics, information and communications, etc., intelligent connected vehicles have become another Internet entrance after mobile phones. In April 2021, a car owner's claim that "Tesla brakes failed" to protect their rights aroused attention. In addition to the dispute over responsibility for the accident, this incident has also focused some of the public's attention on driving data and personal privacy, and has become a catalyst for speeding up the safety supervision of smart car data.

In 2021, the "Data Security Law" and "Personal Information Protection Law" will be promulgated and implemented successively, causing a wave of supervision in the field of intelligent networked vehicles. Then, in August 2021, the five departments jointly issued the "Several Regulations on Automobile Data Security Management (Trial)", which made more specific regulations on automobile data security. According to incomplete statistics, in 2021, nearly 20 policy documents related to ICV information security will be released or introduced at the national level. Among the intensively issued documents, the one that has a greater impact on the industry is the "Opinions on Strengthening the Access Management of Intelligent and Connected Vehicle Manufacturers and Products". It can be seen that my country attaches great importance to the security of automobile data. For the construction of the information security system of intelligent networked vehicles, it has roughly gone through a development stage from caring about the product quality of car companies to focusing on personal data protection, and then rising to the level of national security. With the further popularization of intelligent networked vehicles, its network and data security issues will be closely related to public security, and every enterprise in the ecosystem needs to cooperate to achieve real security.

At present, my country has promulgated a series of laws and regulations on the data security of connected vehicles, and a number of scholars have conducted heated discussions on this issue in the academic circles. The process of digitalization is also changing the automotive industry, and the access and use of in-vehicle data from connected cars is the main driving force behind the creation of new data protection models and innovative automotive mobility services. However, the current research on who can access the data in the car and the mode of accessing the data can be said to be lacking.

3. “Exclusive Control” of Data by Automakers: The Dual Role of Institutions and Technology

3.1 The adverse effects of “exclusive control” of car data

Automakers, i.e. original equipment manufacturers, try to achieve "exclusive control" of car data by monopolizing the data generated by connected cars through the concept of "extended vehicle".[3]This means transferring all data generated in the car directly to the OEM's proprietary server, granting them exclusive control over this data. Car manufacturers believe that the data generated during the use of connected car users is a derivative of the car itself and is a part of the car. The car data exists depending on the car itself, so car manufacturers call it "Expansion Vehicles". Automakers are directly responsible for car safety, so all data generated in the car is transmitted directly to the OEM's proprietary servers to keep car data safe and defend its "extended vehicle" concept as a reason.

Under what automakers call an "extended vehicle" concept, other auto service providers and consumer associations are concerned that the privileged position of OEMs, which gives them exclusive control over the automotive aftermarket and related auto services, could lead to Less competition, less consumer choice and less innovation.[4] If car service providers other than OEMs can access in-vehicle data, car users can get more diversified services and more choices.

By competing with each other, providing consumers with better after-sales service and intensifying innovation by automakers and other service providers is undoubtedly good news for consumers. After purchasing a connected car from an automaker, consumers need repair and maintenance services throughout the life of the car. Because car after-sales services are so lucrative, automakers have long tried to stymie competition from other Internet service providers. With the increasing technological sophistication of automotive software and telematics, Internet service providers and accessory manufacturers can only offer their services and products if they have access to the necessary technical data. These data refer to technical specifications, diagnostic data, repair instructions, etc. A lack of access to this data could allow OEMs to exclude ISPs from their ability to provide services, hinder competition and innovation, and possibly even monopolize much of the aftermarket for connected cars. Preventing ISPs from accessing data through an exclusivity strategy can be seen as a de facto bundling strategy, where car buyers have no choice but to buy aftermarket services from OEMs and not other car service providers to offer them After-sales service.

3.2 Obtaining data control rights on the grounds of security

By extending the vehicle concept, OEMs argue that the highest standards of data security can only be ensured through OEM-owned external servers. There is no doubt that for connected car users, the data security of connected cars is very important. In the current discussion of car data access, the issue of obtaining in-car data and resources is mainly seen as a trade-off between data security on the one hand and fair competition between OEMs and other car service providers on the other. However, for the management of in-vehicle data, it is paramount that data security concerns do not justify exclusive economic control of in-vehicle data through OEMs. Even if we assume that all data must be transferred to the OEM's external servers, and that the OEM must have exclusive control over the information technology systems that go into the car for data security reasons, it doesn't justify that they need to be one of these as well. The de facto exclusive controller of the data, which in turn has the right to make commercial use of the data. With regard to connected cars, OEMs can also be seen as IT security service providers whose task is to keep the car and its data safe, while the car user still has the power to decide who should access the car's in-car data or sell this data to other car service providers. Therefore, expanding the vehicle concept requires bundling the task of providing data security services with the transfer of de facto ownership of the data to OEMs, which is unnecessary and not well justified.

3.3 “De facto control” through technical measures

OEM technical measures have de facto control over car data. Since all in-vehicle data is transmitted directly to the OEM's proprietary servers, they have achieved a monopoly over the car's data. Neither car users nor other stakeholders have access to this data without the consent of the OEM. In this regard, OEMs have acquired de facto "ownership" of the data and are therefore able to claim the economic value of the data. In addition, the extended vehicle concept can also allow automakers to create a check-in situation with other service providers; the connected car is a closed system, specifically, other service providers cannot access the connected car without the consent of the OEM Data is exchanged, nor is it possible to communicate with the driver of the car via the integrated human-machine interface. As far as OEMs have exclusive control over in-vehicle data and access to connected cars, all independent service providers wishing to provide services to car users will need the OEM's consent and contract to gain access permissions. As far as OEMs are concerned, with exclusive control, consumers can only choose between those service providers that have contracts with OEMs. Because the connected car is an expensive durable commodity, car users will be "trapped" in the closed system of OEMs. As a result, OEMs are gatekeepers to connected car data and can benefit by granting independent service providers access to connected car data.[5]

4. The Damage of “Data Monopoly” of Connected Vehicles to Innovation and Consumer Welfare

Other automotive service providers and consumers are very concerned that the exclusive control of OEMs over connected car data access will hinder competition and innovation in the aftermarket and supplementary services market in the connected driving ecosystem. Exclusive control over vehicle data gives OEMs a variety of options to increase profits through this control position. One way is to deny access to prevent other service providers from entering certain kinds of services that can be provided entirely by the OEMs themselves. Another way is to "sell" the data and the right to use the car to other car service providers looking to enter these markets.[6] It could also lead to an exclusivity agreement, that is, the right to sell data in a connected car to a service provider for a hefty fee, enabling the OEM to gain access to a specific service for a specific brand of car from such an exclusive profit from the position. However, even though OEMs allow access to some service providers, OEMs still control aftermarket and complementary services through contractual relationships with these companies. No matter which way OEMs choose to maximize profits, there is no longer a separate market for aftermarket and supplementary services, and OEMs can get all or most of the profits. Furthermore, from an innovation perspective, concerns that such market control could lead to a reduction in innovation in new services must be taken very seriously, as it enables OEMs to filter which innovative services are offered to car users. Much of the car data is unique and unreproducible, so there is a danger that subsequent monopoly prices will result in a loss of consumer welfare due to the underutilization of this data in the data economy.

5. Construction of data access rules for connected cars: Strengthening the autonomy of connected car users and breaking “exclusive control”

5.1 The return of car data control: from “automaker” to “connected car user”

Connected car data is data that is closely related to individuals generated by connected car users in the process of using the car, so it can be said that connected car data is part of personal data. Personal data has the attribute of property rights, and connected car data also has The attribute of property rights should return the control of connected car data from the current control of car manufacturers to the hands of connected car users. Car data is formed by personal network behavior, and the data code collected and processed by the car enterprise platform. Car data is essentially a data code, and the data code contains personal information, so the car data is a valuable data code; because of its certain value attributes, these data codes can have realistic property attributes. Ownership is a property right, the right of the owner to possess, use, benefit and dispose of property according to law.[7] Car data is the property of car users and should be owned by car users. Car users have the right to possess, use, benefit and dispose of car data in accordance with the law. Therefore, there is no legal basis for the exclusive control of car data by OEMs. The control of car data should be returned to the connected car users, instead of being exclusively controlled by OEMs and using users' car data for transactions. profit from it.

5.2 Technical solutions for secure data access: from “proprietary server” to “shared server” or “vehicle application platform”

Since OEMs apply the concept of "extended vehicle" in connected cars, which means that the OEM's "shared server" has exclusive technical control over access to in-vehicle data, other Auto service providers cannot offer this innovative service directly to connected car users. OEMs will always have immediate access to all in-vehicle data, while other automotive service providers will only have access to OEM-processed or aggregated data.

A short-term proposal for the OEM's control of connected car data is the concept of a "shared server", where external servers are not under the OEM's exclusive control, but in a separate server from the OEM. under the control of the server. The concept would remove the OEM's privileged position by replacing a "proprietary server" with a neutral server that could then provide non-discriminatory access. But this "shared server" doesn't solve the problem of directly accessing connected cars to access data in real-time or to perform remote diagnostics and repair services directly in the car, so it only solves part of the competition. In the long term, the preferred technology architecture for connected car service providers will be an open, interoperable telematics system, the "vehicle application platform". The system will technically enable users to directly decide who has access to in-vehicle data and the car's information technology systems.[8] It will be an open connected driving ecosystem in which car users can freely choose between a variety of service providers. The basic idea of both solutions is to remove the OEM's exclusive control over access to in-vehicle data and resources. Without this control, OEMs would have significantly less choice in the aftermarket and supplementary service markets, and both solutions would lead to more competition, innovation and consumer choice than the "extended vehicle" concept.

Both in-vehicle application platforms and proprietary server solutions can address data security issues, and proprietary servers may have cost advantages. However, closed proprietary systems are not necessarily more secure than well-designed open systems; instead, often multi-layered, interoperable open systems architectures may even provide better protection against cybersecurity attacks. An open and interoperable in-vehicle application platform needs to implement a complex safety and cybersecurity system. The solution is to separate the functions and data that are sensitive to safety and security from the vast amount of other data not relevant to safety. This is particularly important, however, to strictly control whether independent service providers wanting to serve car users must meet certain security standards and the security of their services; therefore, addressing data security issues for interoperable telematics platforms , which is one of the important tasks in constructing data access rules for connected vehicles.

6. Conclusions

Car data access involves important issues such as data security, enterprise competition, and service innovation. Through the concept of "extended vehicle", OEMs have formed a situation of "exclusive control" over car data, and have an impact on both service innovation and consumer welfare. cause some damage. This paper solves the problem of network connection by returning the control of car data from "car manufacturers" to "connected car users", and changing the data access mode from "proprietary server" to "shared server" or "in-vehicle application platform". I hope that the problem of exclusive control of car data and the lack of car data access rules will help.

Acknowledgements

The work was financially Innovation Project of GUET Graduate Education and Project supported by the Research on Legal Supervision of Face Recognition Application from the Perspective of Data Security.

References

[1] Bertin, M., & Frank, M. (2018). Access to Digital Car Data and Competition in Aftersales Services. Available at SSRN: https://ssrn.com/abstract=3262807 or http://dx.doi.org/10.2139/ssrn.3262807
[2] See NetEase. (2022, April 22). The Internet of Vehicles Is Emerging, Is Data Security Pressured? https://www.163.com/dy/article/H5NKDH2M0552UI69.html
[3] See Kerber, wolfgang, & Frank, jonas. (2017). Data Governance Regimes in the Digital Economy: The Example of Connected Cars. Available at SSRN: https://ssrn.com/abstract=3064794
[4] See Kerber, wolfgang. (2017). Rights on Data: The EU Communication 'Building a European Data Economy' From an Economic Perspective. Available at SSRN: https://ssrn.com/abstract=3033002
[5] See Zech. (2016). A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data. Journal of Intellectual Property Law & Practice, 460–470.
[6] See Shapiro. (1995). Aftermarkets and Consumer Welfare: Making Sense of Kodak. Antitrust Law Journal, 483–511.
[7] Shi yuhang. (2016). Legal Regulation of Personal Data Transactions. Theory and Exploration, 05.
[8] Kerber, wolfgang, & Daniel gill. (2019). Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation. Tech. & Elec., 244.