ISSN: 2424-8460(O)
2251-2608(P)

Original Research Article

Acquisition pathways of user data in the context of intelligent connected vehicles: Centered on the right to data portability

Ruoqing Guo, Miao Zhang
Beijing University of Technology, Beijing, 100124, China

Abstract: Intelligent connected vehicles continuously generate vast amounts of vehicle data, driving data, and user behavior data during user's operation. Although users directly contribute to the generation of this data, they are unable to actually access or utilize it due to the relative monopoly held by automakers. Cases such as the Tesla driving data dispute demonstrate that specific scenarios, including accident liability determination, vehicle repairs, and insurance claims are highly dependent on the retrieval and circulation of vehicle data. However, the current regulatory framework relies primarily on the right to know under *the Law of the People's Republic of China on the Protection of Consumer Rights and Interests* to provide case-by-case remedies, making it difficult to address users' needs for data utilization. The right to data portability stipulated in Article 20 of Regulation (EU) 2016/679 (General Data Protection Regulation, "GDPR") differs from the mere right of access. It can reshape data control relationships in the digital age by promoting data sharing, ensuring the fair distribution of data value, and strengthening the right to informational self-determination. At the institutional level, the right to data portability should not be confined to personal information in the strict sense. Instead, it should take into account the symbiotic nature of smart connected vehicle data and moderately expand its scope of application to include certain data that is directly linked to users and makes an irreplaceable contribution. Drawing on the experience of the Regulation (EU) 2023/2854 (the "EU Data Act"), which has already expanded the scope of data access and transfer for the Internet of Things (IoT) products to include non-personal data, a data portability framework for intelligent connected vehicles can be gradually established through interpretive approaches and industry pilot programs. Supporting rules should be developed to address specific issues such as data acquisition pathways, authorized transfer methods, interface standards, frequency limits, and fee mechanisms. This approach will ensure the protection of user data rights while facilitating the free flow of data.
Keywords: intelligent connected vehicles; right to data portability; data user; keep data flowing

1. Introduction

In recent years, with the rapid development of Intelligent connected vehicles and autonomous driving technologies, vehicles have gradually evolved from traditional mechanical transportation tools into terminal systems relying heavily on advanced intelligent algorithms.[1] In this context, the massive amount of data generated during vehicle operation has become key for monitoring system performance, identifying technical issues, and safeguarding data user rights.[2] Taking the Tesla "brake failure" dispute as an example, the vehicle owner requested access to the complete driving data from the 30 minutes prior to the incident for technical evaluation of the braking system and driving process. However, since the relevant

ISSN: 2424-8460(O)
2251-2608(P)

data is primarily controlled and held by the automaker, when the automaker refuses or restricts access, the vehicle owner faces the dilemma of lacking crucial evidence and being unable to substantiate claims. This highlights that complete vehicle operation data is vital for reconstructing the vehicle's status at the time of an accident and providing necessary evidence to determine whether the autonomous driving system had any defects.

The data of Intelligent connected vehicles exhibits notable "black-box" characteristics. On one hand, autonomous driving systems involve complex algorithms and decision-making mechanisms, and their operation is almost invisible to ordinary users. The only insight available is through the data recorded by various sensors and controllers. On the other hand, the data generated during vehicle operation is highly diverse, including vehicle condition data, environmental perception data, and vehicle control command data.[3] Such data is typically uploaded to the automaker through vehicle transmission modules and centrally stored and controlled by the automaker's platform. However, because the data is concentrated within the automaker, users have limited access to complete, raw vehicle operation data. This makes it difficult for them to technically verify whether anomalies exist in the Intelligent connected vehicle system, thereby undermining their ability to substantiate relevant facts and placing them at a relative disadvantage in liability determination and rights protection.

However, regarding the access to and use of intelligent vehicle data, the current legal framework still exhibits certain applicability limitations. While the Consumer Rights Protection Law provides consumers with a right to be informed, this right primarily entails an obligation for information disclosure[4]—Operators fulfill their duty by explaining or describing information, rather than providing original data that can be technically examined. *The Personal Information Protection Law* restricts data access provisions to protecting personal information and related personality rights, focusing mainly on personally identifiable information and not covering large-scale non-personal vehicle operation data and control parameters. Therefore, under the current system, consumers face difficulty in exercising feasible right to data portability or full access to balance the automaker's control over driving data.

Based on the above analysis, this paper will focus on the issues of right to data portability and data user rights protection in the context of Intelligent connected vehicles, with an emphasis on exploring the legitimacy and necessity of granting users the right to data portability. Furthermore, by considering the technical characteristics and governance requirements of Intelligent connected vehicle data, this paper will analyze the operational mechanisms and implementation pathways of the right to data portability in practice.

2. The justification of the right to data portability for users of intelligent connected vehicles

2.1. The legitimacy of the right to data portability for users

2.1.1. From the perspective of data sharing

From the perspective of its functional role, the right to data portability serves to mitigate platform monopolies and reduce data lock-in effects. By granting individuals the right to transfer data relating

ISSN: 2424-8460(O)
2251-2608(P)

to themselves from one platform to another, data portability essentially reallocates a portion of data control from platforms back to users. In doing so, it weakens platforms' ability to lock in users through exclusive control of data, thereby fostering market competition and further enhancing consumer welfare.[5] Especially in the field of intelligent connected vehicles, automotive manufacturers are forming a closed data ecosystem by continuously accumulating data on users' driving behavior, vehicle operating status, maintenance records, and the like. In this context, if users are unable to "proactively" transfer their data, they will face high switching costs when changing service providers, accessing third-party maintenance systems, or participating in other intelligent mobility services, thereby leading to a relative monopoly over data by manufacturers.

Furthermore, data sharing itself is also an essential prerequisite for realizing the value of data. In other words, one of the key functions of the data originator's right is to provide the source for data reuse, thereby better unlocking the potential of data.[6] The EU Data Act explicitly states that its purpose is to "facilitate the switching of data processing services and enhance the interoperability of data, data-sharing mechanisms, and services within the EU" (Data Act, Recital 5). Therefore, in the context of intelligent connected vehicles, when users are able to lawfully access and transfer relevant data, other market participants can compete in areas such as after-sales services, smart services, and data analysis within the scope of user authorization, thereby promoting innovation and service diversification in the aftermarket.

2.1.2. From the perspective of data equity

From the perspective of the purpose for which the right to data portability is established, it aims to coordinate the interests between data originators and data controllers in order to achieve a fair distribution of data value. In the context of intelligent driving, the types of data are complex, encompassing both person-centered data and vehicle-centered derivative data. The latter is highly correlated with the long-term interactive processes of human driving behavior, usage behavior, and the like.[7] If automobile manufacturers were granted absolute control over relevant data solely on the basis of their actual control of such data, while disregarding users' continuous contributions to data generation, a significant imbalance would arise between the distribution of data-derived benefits and the contributions made by different parties. Accordingly, the right to data portability confers an active entitlement upon users, serving in essence as a mechanism for balancing the interests of multiple stakeholders involved in the process of data production.

Furthermore, whether a partial transfer of rights would negate the data processor's labor can also be understood in light of the purpose of the right to data portability. The right to data portability does not require data processors to unconditionally relinquish all their interests in the data, nor does it imply a denial of their technical and financial investments in data collection, cleansing, and training. Article 20 of the GDPR limits the scope of portable data to data "provided by" the user and "observed data" concerning the user's activities. This accordingly excludes environmental perception data, most categories of basic attribute data, vehicle industrial control data, vehicle control data, and application service data — Five of the six categories of data stipulated in the *Data Security Technical Requirements for Internet of Vehicles Information Services (YD/T 3751-2020)*. Taking the user's substantial contribution to data generation as

ISSN: 2424-8460(O)
2251-2608(P)

the boundary, the corresponding data originator's rights and interests may only be claimed where such contribution is both direct and irreplaceable[8].

2.1.3. From the perspective of informational self-determination

From the theoretical perspective of the right to data portability, its essence lies in granting users the right to informational self-determination. The theory of informational self-determination[9], which can be traced back to the German Federal Constitutional Court's ruling in the 1983 Census Act case, originally meant that individuals should have the right to decide on the disclosure and use of their personal information. Otherwise, in an environment characterized by highly concentrated and continuous data collection, individuals would find it difficult to maintain their free personality and autonomous life. In the context of intelligent connected vehicles, users' behavioral data and vehicle operation data are continuously collected by platforms and used for algorithm optimization. Therefore, in addition to ensuring users' right to information, it is further necessary to guarantee their right to use the data; otherwise, the former right would be reduced to a mere formality.

2.2. The necessity of the right to data portability for users

2.2.1. The positional conflict between data generation and data control

What distinguishes intelligent connected vehicle data from other types of data is its "symbiotic" nature. Such data is not the product of a single subject, but rather "symbiotic data" generated through the joint efforts of multiple subjects. In other words, the data originates from the collective activities of various parties. On this basis, a relationship of symbiotic interests has formed between data originators and data processors.

However, in stark contrast to users' substantial contributions to the data generation process, the actual control over intelligent connected vehicle data has long been concentrated in the hands of automotive manufacturers and platform operators. For this very reason, merely recognizing data processors' control over the data is clearly insufficient to address the imbalance of data interests in the intelligent connected vehicle context. This necessitates that data processors assume certain assistance obligations, including disclosing relevant data to originators and assisting them in exercising their rights to access, copy, and transfer data, so as to achieve a complete transfer of data control.[10] The establishment of this assistance obligation is, in essence, intended to alleviate the structural conflict between data generation and data control, and to prevent data processors from forming a relative monopoly over data resources by virtue of their technological advantages.

Furthermore, within the framework of China's current legislative system, the conflict between data generation and data control may be examined by reference to the legislative intent of the *Personal Information Protection Law of the People's Republic of China* to correct information asymmetry. The legislative logic of it is centered on protecting the personality rights and interests of natural persons in the processing of their personal information. The rights conferred in Articles 44 to 49 of this Law, which specifically address personal information rights, are essentially a response to the disparity in capacity between data originators and data controllers. Article 45, in particular, provides that individuals have the right to access and copy their personal information, and to request the transfer of their personal information where the conditions

ISSN: 2424-8460(O)
2251-2608(P)

prescribed by the cyberspace administration authorities are met. This provision, in effect, reflects a legislative tendency to break through platforms' closed control over data and to strengthen individuals' ability to have their data flow.

Therefore, the introduction of the right to data portability is precisely a means of balancing the rights structure between data originators and data processors by granting users the capacity to obtain and transfer data, thereby alleviating the increasingly prominent imbalance of data control in the field of intelligent connected vehicles.

2.2.2. The institutional mismatch between data demand and data supply

In the context of intelligent connected vehicles, users' demand for access to and utilization of vehicle data has expanded beyond the traditional realm of personal data protection to encompass a variety of practical scenarios, including accident liability determination, vehicle maintenance, insurance claims, and after-sales services. However, the corresponding data access framework remains largely confined to the conventional "notice-and-consent" model.

First, the determination of liability in accidents is highly dependent on vehicle operational data. Unlike traditional motor vehicle accidents, where liability assessments primarily rely on physical evidence at the scene and witness testimony, the attribution of responsibility in automated driving environments increasingly depends on electronic data such as vehicle operation logs and sensor-generated records. For example, in many disputes arising from automated driving accidents, key issues include whether the vehicle was under the control of the human driver or the automated driving system at the time of the accident, whether the system had issued appropriate risk warnings, and whether the driver had taken over control in a timely manner. The reconstruction and verification of these facts often require access to vehicle data.

Second, vehicle maintenance and after-sales services likewise depend heavily on data accessibility and circulation. In the era of conventional automobiles, maintenance activities were primarily based on mechanical inspections. By contrast, in this environment, fault detection, system diagnostics, software maintenance, and even remote updates all rely on operational data and derivative analytical data generated through vehicle use. In this regard, the Max Planck Institute for Innovation and Competition (MPI) has argued that categorically excluding derived data from rights of data access and use would substantially undermine the practical effectiveness of such rights. This is because a significant portion of maintenance-related information used in after-sales services consists of derivative data generated through the further processing of raw vehicle data. If independent repair providers are unable to access such data, they would be effectively prevented from offering ordinary repair and after-sales services.[11] Therefore, in the field of intelligent connected vehicles, data lock-in not only prevents users from independently utilizing vehicle data but also risks leading to a long-term monopoly of the aftermarket by original equipment manufacturers, thereby further increasing repair and switching costs.

However, the existing legal framework still has significant limitations in addressing these data utilization needs. First, the scope of personal information protection is inherently limited; it primarily covers the personal information of "identified or identifiable natural persons." However, in the context of smart connected vehicles, vast amounts of operational data, fault diagnosis data, and driving behavior

ISSN: 2424-8460(O)
2251-2608(P)

data often possess characteristics of both personal and non-personal data, or even fall into the category of hybrid data that is difficult to classify clearly. Consequently, relying solely on the personal information protection framework cannot fully address users' data utilization needs. Second, traditional data access rights primarily emphasize static rights such as an individual's ability to view or copy data, but they struggle to facilitate dynamic data circulation and cross-platform utilization. Particularly in the context of the platform economy, even if users can formally access certain data, they are often unable to effectively migrate that data across different platforms, and control over the data remains substantively in the hands of the platforms.[12] In this regard, compared with static rights such as data access, the right to data portability grants users dynamic rights, enabling them to independently decide on the sharing, use, and circulation of their data, thereby ameliorating the long-standing asymmetric power structure between data subjects and platforms. Finally, the consumer protection pathway is also ill-suited to address the data utilization needs specific to intelligent connected vehicles. On the one hand, the *Law on the Protection of Consumer Rights and Interests* is primarily centered on individual disputes, emphasizing business operators' information disclosure obligations or consumers' rights to damages. Its nature remains a reactive, passive model of rights protection, incapable of granting users proactive and continuous data control capabilities. On the other hand, its institutional objective is mainly to protect the individual interests of consumers, rather than to promote data circulation and sharing. Consequently, it struggles to respond to the broader user needs arising from data circulation, market competition, and aftermarket openness in the field of intelligent connected vehicles.

Therefore, in the field of intelligent connected vehicles, users' data utilization needs have gradually expanded from traditional personality protection issues to a multi-dimensional set of issues encompassing liability determination, market competition, aftermarket openness, and data circulation. However, the existing institutional framework remains largely confined to the paradigm of personal information protection and consumer rights protection, insufficient to effectively respond to the increasingly prominent needs for data access and data circulation in the context of intelligent connected vehicles. It is against this backdrop of institutional mismatch that the introduction of the right to data portability serves as a further response to users' data utilization needs.

2.3. The feasibility of the right to data portability for users

For personal data, users have a relatively clear legal basis for exercising the right to data portability. Article 20 of the GDPR explicitly grants data subjects the right to receive their personal data, which they have provided to a controller, in a structured, commonly used and machine-readable format, and to transmit that data to another controller. Similarly, Article 45 of *China's Personal Information Protection Law of the People's Republic of China* provides that "an individual has the right to request the personal information handler to transfer his or her personal information to a designated handler. If the personal information handler meets the conditions prescribed by the cyberspace administration authorities, it shall provide a means for the transfer." It is thus evident that, under both EU law and China's current legal framework, the portability of personal data has been recognized.

On this basis, with respect to non-personal data, Chapter II of the EU Data Act further establishes

ISSN: 2424-8460(O)
2251-2608(P)

a system of data access and use for data originators, beyond the existing framework for personal data protection. The Data Act does not draw a distinction based on the dichotomy between personal data and non-personal data. Instead, it adopts a definition based on usage behavior, encompassing within the scope of the rights object the data generated by users in the course of using a connected product or a related service. (Under the Data Act, a "product" is defined as a tangible movable item that obtains, generates or collects data concerning its use or environment, and that is capable of communicating such data via a publicly available electronic communications service, including products that are built into or integrated into immovable property — For example, smart watches, smart speaker systems, smart televisions, smart vehicles, industrial machinery, medical devices, and other Internet of Things devices. The "service" covered includes digital services, including software.) This means that even if the relevant data does not, in itself, satisfy the identifiability requirement under the GDPR, as long as it originates from the user's use behavior, it may become the object of data that the user can request to access, obtain, and transfer to a third party, by reference to the provisions on the right to data portability in Article 20 of the GDPR.

This institutional design suggests that the configuration of data rights may break away from the traditional dichotomy between personal data and non-personal data, and instead be based on the core criterion of behavioral participation in data generation. In comparison, although China's current law constructs a data rights system centered on personal information, it is entirely possible, at the interpretive level, to draw on the above thinking to bring such types of data within the scope of application of the right to data portability, subject to certain conditions. This would avoid the dilemma, as seen in the "Tesla rights protection case," of having to rely on other legal doctrines to address data issues.

3. Institutional construction of the right to data portability for intelligent connected vehicles

3.1. Overall approach

The construction of the right to data portability system for Intelligent connected vehicles should follow a gradual path: First prioritizing interpretive approaches, then promoting pilot explorations, and finally gradually improving legislation. At the current stage, it is not advisable to push for dedicated legislation immediately; instead, existing legal norms and governance practices should be fully leveraged to accumulate experience for future institutional refinement.

First, from the perspective of technological realities, Intelligent connected vehicle data is highly technical and contextually complex, and the types of data, processing entities, and utilization methods are still evolving rapidly. Establishing a unified and rigid institutional framework too early may result in regulations lagging behind technological development and even constrain industrial innovation.[13] Moreover, China has long adopted a gradual legislative model in the field of digital governance, usually establishing basic rules through principle-based laws first and then accumulating practical experience through specialized regulations and local pilot programs. Therefore, extending this approach to the governance of Intelligent connected vehicle data is pragmatically reasonable.

Second, based on existing institutional foundations, China's Personal Information Protection Law has

ISSN: 2424-8460(O)
2251-2608(P)

already established rights for personal information subjects, including access and transfer, providing a basic legal basis for cross-platform data portability. The "Data 20 Measures" opinions require establishing a classification, grading, and property rights system for data, promoting data circulation under compliance requirements, and improving rights protection mechanisms. These provisions leave interpretive space for the construction of the right to data portability for Intelligent connected vehicle data and can be further specified through industry standards or departmental regulations.

Third, from the governance practice perspective, China has in recent years adopted a "pilot first" governance approach in the field of Intelligent connected vehicles. The Pilot Implementation Opinions on the Access and Road Use of Intelligent Connected Vehicles explicitly propose accumulating management experience through pilot programs and providing support for the revision of relevant laws, regulations, and technical standards. Accordingly, the right to data portability can also be initially explored in specific regions or enterprises, gradually testing institutional costs and governance effects through the establishment of unified data interface rules, cross-platform transmission mechanisms, and user authorization standards.

Finally, from a comparative law perspective, the United States has similarly adopted a development path of experimentation first, followed by regulation, in autonomous vehicle governance. Since a unified federal law has long been absent, the U.S. primarily relies on state-level pilots to promote regulatory innovation. Represented by California and Arizona, states gradually accumulate regulatory experience for autonomous driving through road test permits, accident reporting systems, and restricted testing zones.[14] Based on practical experience, the U.S. Department of Transportation subsequently issued policy documents such as *Automated Driving Systems 2.0: A Vision for Safety and Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0*, providing guidance on data recording, safety evaluation, and corporate responsibility. This model of local experimentation followed by policy summarization and eventual unification helps prevent institutional rigidity caused by premature legislation in the early stages of immature technology and reserves space for subsequent federal-level rule coordination.

3.2. Specific design of the data transfer mechanism

3.2.1. Data transfer pathways

The realization of the right to data portability for Intelligent connected vehicles requires the establishment of clear, operable, and secure data transfer pathways. Such pathways involve not only technical means but also the protection of data user rights, compliance requirements for enterprises, and the standardization objectives of the industry.

First, direct access by the user. As provided under Article 20 of the GDPR, when exercising the right to data portability, users may directly submit a request to the data controller in order to obtain their personal data. The core objective of this pathway is to safeguard users' direct control over their own data, enabling them to independently obtain relevant vehicle data. At the same time, before providing the data, the data controller should verify the user's identity and ownership or lawful right of use of the vehicle to ensure data security and clearly define the boundaries of entitlement. Such verification serves not only as a necessary measure to prevent data misuse but also reflects the fundamental principles embodied in the Personal

ISSN: 2424-8460(O)
2251-2608(P)

Information Protection Law. Overall, the advantage of the direct access pathway lies in minimizing the risks associated with third-party involvement. However, it also requires data controllers to provide data in standardized export formats so that users can utilize the data across different platforms and tools, thereby enhancing data usability and mobility.

Second, user-authorized transfer. In practice, users may need to transfer vehicle data to third parties, such as insurance companies, after-sales service providers, or research institutions. Under the user-authorized transfer pathway, users provide explicit authorization, and data controllers transfer data in accordance with established identity verification and transmission procedures. Authorization may be completed through the signing of an electronic authorization form or by clicking a consent button, ensuring that each transfer occurs with the user's knowledge and consent. The rationale for this design is to balance convenience and security: It allows data to flow when necessary while preventing unauthorized sharing. At the same time, to reduce the risk of data leakage, data should be anonymized or de-identified before transmission by removing unnecessary personal identifiers. This mechanism is not only consistent with personal information protection principles but also provides an operable security standard for industry governance.

Third, standardized interfaces. Given the multi-stakeholder and multi-platform data interaction demands within the ecosystem of Intelligent connected vehicles, the establishment of a unified standardized interface is of great significance. Standardized interfaces should be made available to both data controllers and all legitimate requestors, enabling data access through unified APIs or data exchange protocols. The rationale for this pathway is threefold. First, it balances efficiency and security by avoiding reliance on individualized approval procedures for every request. Second, standardized protocols can clearly define access procedures, authentication methods, and data formats, thereby improving interoperability and reducing technical costs for enterprises and third parties. Third, standardized interfaces facilitate regulatory oversight, enabling authorities to monitor compliance and promptly identify abnormal access activities. To achieve these objectives, automakers or relevant industry regulators should formulate unified standards governing registration, identity verification, authorization review, data access, and incident response procedures, while adopting common data formats such as JSON and XML to ensure cross-platform compatibility.

3.2.2. Limitations on the number of requests

To safeguard users' right to data portability while also taking into account the reasonable operational costs and technical capacities of enterprises, free access to basic data should not be entirely unlimited. Unrestricted requests may increase data transfer costs and technical burdens for enterprises, hinder the development of small and medium-sized enterprises, and ultimately shift these costs onto consumers. To balance information rights and data processing costs, reasonable limitations on the number of free portability requests may be introduced by drawing upon the approach adopted in the California Consumer Privacy Act[15].

At the same time, requests involving personal safety or data accuracy should not be subject to quantitative limitations. For example, in the event of traffic accidents, vehicle emergencies, or data errors,

ISSN: 2424-8460(O)
2251-2608(P)

access to relevant data should be prioritized to ensure that restrictions on request frequency do not impede the flow of critical information. Allowing unrestricted access under specific circumstances facilitates timely rescue efforts, the correction of erroneous decisions, and improvements in data quality, thereby reducing overall social costs.

3.2.3. Charging mechanism

The implementation of the right to data portability for Intelligent connected vehicles should follow a model under which basic data is provided free of charge, while value-added services may be subject to reasonable fees. On the one hand, the fundamental purpose of the right to data portability is to ensure users' ability to control and utilize their own data. If enterprises were generally permitted to charge for access to basic data, the practical threshold for exercising the right would be significantly increased, thereby undermining the effectiveness of the system. On the other hand, data storage, processing, and transmission require technological and operational investments, and a completely free model may weaken enterprises' incentives to provide data services. Therefore, it is necessary to establish a balanced charging mechanism that protects data user rights while also safeguarding the legitimate interests of enterprises.

With respect to basic data closely related to users themselves, such as driving trajectory data and traffic accident records, the principle of free access should be maintained. Such data not only concerns personal information interests but is also essential for accident determination, product liability claims, vehicle maintenance, and other practical needs. *China's Personal Information Protection Law* grants individuals the rights to access, copy, and transfer their personal information, with the institutional objective of ensuring continuous individual control over such information. From a comparative law perspective, the EU Data Act likewise requires that users be able to access data generated by connected products free of charge. Accordingly, no additional charging barriers should be imposed on data that satisfies users' basic informational and rights-protection needs.

However, the principle of free access does not mean that enterprises must provide data without compensation under all circumstances. Where users frequently submit requests exceeding a reasonable scope, or authorize third parties to conduct continuous and high-frequency data access activities, enterprises may incur additional costs associated with data processing, system maintenance, and security protection. In particular, where standardized API interfaces are made available, enterprises must invest in server resources, network bandwidth, and cybersecurity measures to maintain stable system operations. In such circumstances, permitting enterprises to charge reasonable fees based on actual costs is consistent with the principle of cost allocation and may also help prevent the abuse of data access rights.

4. Conclusions

The development of intelligent connected vehicles is transforming traditional automobiles into mobile intelligent terminals that continuously generate, process, and circulate data. Consequently, the interest structures, control relationships, and rights configurations surrounding vehicle data are also undergoing significant changes. Although users are deeply involved in data generation, they have long remained in a disadvantaged position of "contributing data without being able to control it." The traditional regulatory

ISSN: 2424-8460(O)
2251-2608(P)

path based on consumers' right to information can address certain data access needs on a case-by-case basis, but it largely operates at the level of dispute remediation. It struggles to genuinely respond to data governance challenges arising from data circulation, platform lock-in, and information asymmetry. The introduction of the right to data portability, in essence, reaffirms users' subject position in data relationships within the digital society. By granting users the ability to transfer and reuse their data, this right mitigates the structural imbalance caused by the excessive concentration of data control.

At the same time, data generated by intelligent connected vehicles is not purely personal information. Its generation process involves multiple factors, including user contributions, device operation, and platform governance. Therefore, the construction of relevant institutional frameworks cannot simply replicate the logic of traditional personal data protection. Instead, it should establish a more finely calibrated balance of interests among data sharing, industrial incentives, and individual rights. By expanding existing regulations at the interpretive level and conducting incremental regulatory pilots tailored to the characteristics of the autonomous driving and connected vehicle industries, we can not only help alleviate practical challenges such as the burden of proof for users, reliance on repair services, and platform lock-in, but also provide replicable regulatory insights for the allocation of data rights in future fields such as the Internet of Things and artificial intelligence.

Fundings

Beijing University of Technology "National College Students Innovation and Entrepreneurship Training Program Support Project" (GJDC-2026-01-78).

About the author

Ruoqing Guo (2005-), a female, from Jiaocheng, Shanxi Province, is currently majoring in law at Beijing University of Technology.

References

[1] Industrial Information Security Development Research Center of China. (2020). *White paper on data security of autonomous driving (2020)* [Report]. Beijing, China: Industrial Information Security Development Research Center of China.

[2] Wang, Y. F., Chen, M. J., & Zhou, L. W. (2022). Vehicle motion model and analysis of "Tesla brake failure" incident. *Mechanics and Practice*, 44(4), 852–856.

[3] Yong, C. (2023). Research on data governance framework of intelligent driving. *Jinan Journal (Philosophy & Social Sciences)*, 45(4), 62–72.

[4] Wan, F. (2017). Legal application of operators' disclosure obligations in China's *Consumer Rights and Interests Protection Law. Politics and Law*, (5), 151–160.

[5] Ye, M. (2023). The significance and realization of the right to personal information portability in the field of data anti-monopoly. *Guizhou Social Sciences*, (12), 66–75.

[6] Ding, X. D. (2023). On the rights of data originators. *Journal of Comparative Law*, (3), 14–25.

[7] Xu, Z. M. (2022). Legal regulation of data processing of intelligent connected vehicles: Reality, challenges and approaches. *Journal of Lanzhou University (Social Sciences)*, 50(02), 100–111.

[8] Wang, N. (2025). The right of data originators and its realization—From the perspective of data symbiosis.

ISSN: 2424-8460(O)
2251-2608(P)

Finance and Law, (5), 131–146.

[9] Qin, Z. (2025). Restatement of the right basis for personal information protection in the pan-AI era—Centered on the right to self-determination of personal information. *Gansu Social Sciences*, (4), 136–145.

[10] Shen, W. X. (2025). On the relationship of rights and obligations between data originators and data processors. *Global Law Review*, 47(4), 37–52.

[11] Wang, N. (2025). The right of data originators and its realization—From the perspective of data symbiosis. *Finance and Law*, (5), 131–146.

[12] Song, G. (2024). Research on interpretation and implementation path of the right to data portability. *Journal of Dalian University of Technology (Social Sciences)*, 45(2), 85–92.

[13] Fu, X. H. (2025). Hasty unified legislation on artificial intelligence is inadvisable. *Oriental Law*, (3), 17–30.

[14] Zhang, Y. J. (2018). Research on administrative law regulation of driverless vehicles. *Administrative Law Review*, (1), 68–77.

[15] Xiang, D. Y., & Sun, H. N. (2025). Legislative review and structural improvement of the right to data portability of personal data in China. *Price: Theory & Practice*, (06), 180–186.