Legal Commentary

May 27, 2021

HAN KUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

BEIJING | SHANGHAI | SHENZHEN | HONG KONG

Brief Comments on Draft Automobile Data Security Provisions

Authors: Kevin DUAN | Tina WANG | Kemeng CAI[1]

On May 12, the Cyberspace Administration of China ("**CAC**") issued for public comments the *Several Provisions on Administration of Automobile Data Security (Draft for Comment)* ("**Draft Provisions**"). The Draft Provisions would be the first departmental rules dedicated to addressing data compliance requirements in the automobile industry. Unlike previous draft standards[2] proposed for connected vehicles, the Draft Provisions would apply to vehicles of all types. The key take-aways of the Draft Provisions are as follows:

- Defines the scope of important data in the automobile industry. The processing of important data would be subject to a series data protection principles and requirements such as data minimization, vehicle-end processing, data localization and export security assessment, and government filing and annual reporting.
- Emphasis on ensuring data subjects' control of personal information ("**PI**") collection and deletion.
- Strengthening of obligations to report data processing activities to regulatory authorities.
- Potential changes to industry practices. The Draft Provisions would require significant changes to current vehicle data processing designs and practices due to their requirements with respect to data minimization, vehicle-end processing, data subject control, and data localization.

Below, we analyze the key requirements for PI and important data processing provided in the Draft Provisions and offer our insights accordingly.

Applicable scope

According to Articles 2 and 3, the Draft Provisions apply to the processing of PI and important data by operators in relation to the design, manufacture, sale, operation and maintenance, and management of vehicles within China. Operators under the Draft Provisions include vehicle manufacturers, suppliers of.

[1] Intern Shimeng CAI has also contributed to the writing of this article.

[2] E.g., *Draft Information Security Technology – Connected Vehicle – Security Requirements of Data* published by the National Information Security Standardization Technology Committee on April 28.

parts and software, distributors, maintenance workshops, online ride-hailing enterprises, insurance companies, and other enterprises and institutions in the areas of vehicle design, manufacture, and services In other words, almost all entities in the automobile industry could fall into the ambit of the Draft Provisions when they process important data and PI, including of vehicle owners, drivers and passengers, and pedestrians.

Yet, it is unclear whether the Draft Provisions would apply to internal data processing activities that are unrelated to automobile management, such as the processing of employee PI. In addition, the Draft Provisions do not yet specify whether and how they would apply to vehicles that are already in the market or currently in production.

Scope of important data

Article 3 of the Draft Provisions defines the scope of important data in the automobile industry, which would include:

- Crowd and traffic data in important and sensitive areas such as military administrative zones, areas in the vicinity of science, technology, and national defense agencies and other State secret-related agencies, and areas in the vicinity of Party and government agencies above the county level;
- Surveying and mapping data, the precision of which is above maps made public by the State;
- Data on the operation of vehicle charging networks;
- Data on vehicle types and road traffic;
- Outside-vehicle audio and video data including human faces, voices, vehicle license plates, etc.;
- Other types of data that might impact national security and public interests as designated by the State cyberspace administrations and departments of the State Council.

Detailed criteria are yet to be specified as to how to draw the scope of important data in practice, such as how to calculate crowd and traffic data, how to identify important and sensitive areas, etc. Despite this, it is certain that the State attaches great attention and importance to the surrounding data collected by vehicle cameras, radars, lidars, and other sensors and such data is to be processed with great care.

Data processing purposes and principles

According to Article 4 of the Draft Provisions, purposes of PI and important data processing are to be legitimate, specific, clear, and directly related to vehicle design, manufacture, and services. Article 6 would apply to the automobile industry the general principle of data minimization set forth in the Cybersecurity Law and the Personal Information Protection Law (Second Reading Draft) and encourage operators to abide by the following principles during data processing activities: (i) in-vehicle processing, (ii) data anonymization, (iii) minimum retention period, (iv) proper precision and scope, (v) no data collection by default.

These principles are not provided as mandatory obligations. Yet, we reasonably foresee the regulatory

authorities issuing future implementing rules that take these principles into account. Among other principles, operators would be encouraged to incorporate the principles of "in-vehicle processing"[3] and "no data collection by default"[4] into the technical planning at an earlier vehicle design and development stages.

Rules on PI processing

According to Article 9 of the Draft Provisions, operators shall obtain data subjects' consent unless laws and regulations otherwise stipulate. When processing PI, operators shall inform data subjects of the items enumerated under Article 7[5], such as the contact information of the person in charge of handling matters related to users' rights and interests, when the data collection will be initiated and how to stop it, and how to delete the collected data. Where it is not practically feasible to obtain data subjects' consent (e.g., when collecting PI outside of the vehicle), consent is not needed for anonymized or de-sensitized data, e.g., by deleting images that can be used to identify an individual or blurring the human faces in such images.

The Draft Provisions respond to the longstanding dilemma on how to lawfully handle pedestrians' PI. According to Article 9, data anonymization and de-sensitization relieve operators from the onerous and nearly impossible burden of obtaining pedestrians' consent. However, there are still two open points that require clarification: (i) whether the term "de-sensitization" has the same meaning as "anonymization" or instead refers to "de-identification"; (ii) whether only vehicle-end data anonymization and de-sensitization would serve to exempt the consent requirement or server-end anonymization and de-sensitization would also suffice. If only vehicle-end data anonymization and de-sensitization would serve to exempt the consent obligation, then operators would have to ensure strong in-vehicle processing capacities. Otherwise, operators would have to rely on legal bases other than authorization and consent for processing PI, which are to be established by the forthcoming Personal Information Protection Law.

Enhanced protection of sensitive PI

Article 8 of the Draft Provisions set forth enhanced requirements for the processing of sensitive PI. The Draft Provisions do not define sensitive PI in the automobile industry but only name three examples, which are vehicle location, audio and video of the drivers or passengers, and data that could be used to determine illegal driving behaviors. When processing sensitive PI, operators would also need to pay attention to the following requirements in addition to those mentioned above:

[3] Article 6.1 of the Draft Provisions: Principle of in-vehicle processing: there shall be no outward data transmission unless it is in fact necessary.

[4] Article 6.5 of the Draft Provisions: Principle of no data collection by default: unless it is indeed necessary, the default setting of each drive shall be no data collection. The consent by the driver to data collection shall only be valid to the specific drive.

[5] According to Article 7 of the Draft Provisions, items that shall be informed to the data subjects include: (i) contact information of the person in charge of handling matters related to users' rights and interests, (ii) types of the data being collected, (iii) when the data collection will be initiated and the way to stop it, (iv) the purpose and use case of each type of data, (v) the retention location and period of the data, or the rules on determining the same, (vi) how to delete the data stored within the vehicle and the data already transmitted outwards.

- **Purpose**: The purpose of processing sensitive PI shall be limited to direct services to **drivers or passengers**, e.g., improving driving safety, driving assistance, navigation, entertainment, etc.
- **Informed consent**: No sensitive PI is to be collected by default. **Each instance** of collection shall be subject to the **drivers'** consent and such consent shall **no longer be valid** at the end of each drive (e.g., when the driver leaves the driver's seat). Drivers and passengers shall be informed of the ongoing collection of sensitive PI via HMI or voice prompt.
- **Control by individuals**: **Drivers** shall be able to stop the collection at any time in a convenient manner. The **vehicle owners** shall be given access to the collected sensitive PI in a convenient and structured manner. Operators shall delete the data within two weeks upon the **drivers'** requests.

The requirements for sensitive PI processing provided in the Draft Provisions are stricter and more detailed than existing regulations, such as the shorter data deletion period. Some of the aforementioned requirements, such as obtaining consent for each drive, could significantly change existing vehicle settings as well as people's driving behavior. Furthermore, Article 8 could be interpreted such that consent is the only legal basis for processing sensitive PI. This may be problematic if the processing of vehicle locations is required to fulfil operators' legal obligations or to protect drivers' safety in emergencies.

Localization of PI and important data

Article 12 of the Draft Provisions provides that operators shall, **by following applicable laws**, store PI and important data within the territory of China and apply for government security assessment for outbound transfers of such data. This ambiguity on localization of PI could be interpreted in two ways. On one hand, the Draft Provision could *per se* mandate all types of automobile PI be stored within China, considering the high sensitivity of data in the automobile industry. On the other hand, it could also be interpreted that the Draft Provisions would not impose additional data localization obligations other than those proposed in the Personal Information Protection Law (Second Reading Draft), pursuant to which automobile operators would be obligated to store PI in China only if they are deemed operators of critical information infrastructure or PI handlers who process PI exceeding certain volume threshold. As for important data, it is more likely the Draft Provision would *per se* mandate local storage of all important data in the automobile industry, considering that the Data Security Law (Second Reading Draft) would empower CAC to stipulate localization rules for important data together with other State Council departments.

Data access and utilization by third parties

In the event that partners of scientific research and commercial operations need to access or utilize PI and important data stored with China, Article 16 would require operators to (i) take effective measures to ensure data security and prevent data leakage, and (ii) strictly restrict the access and utilization of important data and sensitive PI.

Based on textual interpretation, Article 16 would apply to the "access and utilization" of data by third parties rather than "cross-border transfers of data". Considering the common practice of remote data access and emerging technologies such as privacy computing, it is worth exploring whether the aforementioned

requirements and restrictions would apply to cooperations between operators and both domestic and overseas partners.

Obligations to report data processing activities

The Draft Provisions would strengthen obligations for reporting data processing activities in the following situations:

- **Advance reporting of important data processing**: Article 11 would require that, prior to processing important data, operators report to the State cyberspace administrations at provincial levels and competent departments regarding the data types, volume, scope, retention location and period, use cases, and whether the same is to be provided to third parties. Unlike the filing requirement proposed under Article 15 of *Measures for Administration of Data Security (Draft for Comment)*[6], the Draft Provisions would require operators to predict important data processing activities and report the same in advance.

- **Display the types and scope of data in readable plaintext during random inspections**: According to Article 15 of the Draft Provisions, the State cyberspace administrations, along with relevant departments of the State Council, will conduct random inspections of cross-border transfers of PI and important data. Operators would be required to display the types, scope, and other information in readable plaintext.

- **Annual reporting on data security management**: Operators who process PI relating to **more than 100,000 data subjects** and/or important data would be required to report to the State cyberspace administrations at the provincial level and relevant departments by December 15 of each year regarding their data processing activities[7]. Should there be cross-border data transfers, the operators would also be required to report the circumstances surrounding cross-border data transfers[8], including, *inter alia*, data subjects' complaints and handling of the same.

[6] Article 15 of the Measures for Administration of Data Security (Draft for Comment): A cyberspace operator shall file certain information with the local cyberspace administration with respect to the collection of important data or personal sensitive information for business, and the filing information shall include collection and use rules, purpose, scale, method, scope, type and duration, while excluding data content per se.

[7] According to Article 17 of the Draft Provisions, the following matters shall be included in the annual report: (i) name and contact information of the person in charge of data security and the person in charge of handling the person in charge of handling matters related to users' rights and interests, (ii) types, volume, purpose and necessity of the processed data, (iii) data security protection and management measures including data retention location and period, (iv) situations regarding data sharing with third-parties within China, (v) facts and handling of data security incidents, (vi) user complaints regarding PI and data, and handling of the same, (vii) other data security situations designated by the State cyberspace administrations.

[8] According to Article 18 of the Draft Provisions, the following matters on cross-border data transfer shall be included in the annual report: (i) name and contact information of the data recipient, (ii) types, volume and purposes of the transferred data, (iii) the data retention location abroad, scope and method of data use, (iv) data subjects' complaints concerning cross-border data transfer and handling of the same, (v) other situations concerning cross-border data transfer designated by the State cyberspace administrations.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

Kevin DUAN

Tel: +86 10 8516 4123
Email: kevin.duan@hankunlaw.com