Feature Article

May 2019

Legal Issues on Data Collection and Protection of Intelligent Connected Vehicles (II)

The emergence of Intelligent Connected Vehicles ("**ICVs**") will fundamentally change the ways people travel in the future. ICVs have raised many challenging legal questions, one of which is the issue of personal data protection. To authenticate authorised use and to provide more customized value-added settings to vehicle owners (for example, fingerprint identification unlocking, sound control, common destination settings, entertainment preference settings, etc.), ICVs need to collect personal information (and even sensitive personal information) of vehicle owners or drivers, such as personal identification information, personal biometric identification information, etc.

Meanwhile, through a variety of embedded connectivity systems and equipment, ICVs can collect a large amount of personal data generated during the course of driving, such as vehicle's location data, journey history, driver's driving habits and service needs, etc. These hundreds of thousands of users' raw data, after aggregation and processing, will have an enormous commercial value for secondary exploitation. According to a study released by Frost & Sullivan, vehicle data will generate USD700 to USD800 per vehicle in savings for automakers, vehicle owners, service providers and local governments, which includes perks such as lower insurance rates for motorists, lower warranty costs, more aftersales revenue for dealerships, etc[1]. It is estimated that by 2030, the market scale of global telematics system, data and service market will hit USD70 billion[2].

With the promulgation of the PRC Cyber Security Law and its associated regulations and national standards, China has been increasingly strengthening its protection of personal information. Since the beginning of this year, the Chinese regulatory authorities and the National Information Security Standardization Technical Committee have issued various notices and guidelines such as *"Announcement of Launching Special Crackdown Against Illegal Collection and Use of Personal Information by Apps"*, *"Self-assessment of the Collection and Use of Personal Information by APPs" ("**APP Self Assessment Guideline**")*, and *"Personal Information Security Specification (Revised Draft for Public Comment)" ("**Draft Revised PIS Specification**")*. These regulatory developments demonstrate strong indication of China's determination to further standardize the collection and use of personal information, and strengthen the protection of personal information security. In this article, we focus on the legal issues regarding collection and secondary exploitation of personal information regarding ICVs.

The Frequency and Method of Obtaining Individual's Consent

Under the legal framework of the Cyber Security Law and its associated regulations concerning personal information protection, consent of the data subject concerned is a prerequisite for the collection and processing of personal information. The data collection activity in the context of ICVs is also subject to the above rules. In traditional settings such as websites and mobile apps, consents can be obtained from the users through pop-up messages, click buttons and checkboxes based on the specific guidelines in Personal Information Security Specification ("**PIS Specification**"). However, in the ICV context, there are two common challenges encountered in this regard: the frequency and the method of obtaining consents from the users.

[1] "The big question: Who really owns vehicle data?", https://www.autonews.com/article/20140317/OEM06/303179999/the-big-question-who-really-owns-vehicle-data?CSAuthResp=1%3A173606114182789%3A423310%3A17%3A24%3Aapproved%3ADA1A18094864BC082F1D91C59A0CA037

[2] "Intel completes acquisition of Mobileye, what does the USD 15.3 billion buy?", https://www.iyiou.com/p/52143.html

The Frequency of Obtaining Consent

In terms of the frequency of obtaining consent, during each driving process, ICVs need to collect and process a large amount of personal information and even sensitive personal information. Different from websites or mobile apps that can identify or associate specific individuals through log into their personal accounts or identifying the commonly-used devices, in the context of ICVs, due to the possibility of misalignment between vehicle owners and drivers/passengers, it is difficult to identify whether the personal information collected during each driving process belongs to the authorizing individual. However, if requiring the ICV system operator to provide pop-ups of privacy policy and obtain consents from the driver and passenger each time when they activate the vehicles will substantially increase the cost of obtaining consent and will impose negative influence on user experience of ICVs.

The Method of Obtaining Consent

In terms of the method of obtaining consent, there is no established practice in the industry. Recommended methods include signing "Privacy Authorization Agreement" with the vehicle owner at the point of sale, affixing QR codes of privacy policy on vehicle devices, or pre-installing privacy policy or video tutorials on the vehicle screen. However, not all of these methods are perfect in the context of ICVs. For example, if notice is provided and written consent is obtained only at the point of sale, withdrawal of such consent becomes very troublesome, and it is difficult for a subsequent purchaser of a second hand ICV to establish a direct contractual relationship with the ICV manufacturer. The methods of affixing QR codes, pre-installing privacy policy or video tutorials have the problem of ensuring whether the relevant individuals have fully given their consent for the collection and processing of their personal information.

Our View

On the above issues, we believe that it is neither reasonable nor necessary to frequently send privacy policies and obtain consents from the ICV users. According to PIS Specification, when the cost of delivering privacy policy to each individual is too high or it is obviously too difficult to do so, the private policy can be delivered by way of public announcement[3]. We have noticed that in practice most smartphone manufacturers display the privacy policy to users and obtain their consents to such policy during the initial setup or activation of the smartphones. In the subsequent use process, normally there will not be automatic pop-ups of the private policy, but the users can still search and view the private policy in the settings interface of the smartphones or on the smartphone manufacturers' official websites.

As a future large intelligent mobile terminal device, ICV manufactuers can refer to the common practice of smart phone manufacturers on this issue – to obtain consent of the vehicle owners through the signing of hard copy privacy authorisation agreements at the point of sale or pop-ups of privacy policy at the initial activation of the ICV system. There is no need for the ICV system operator to repeatedly push the privacy policy to drivers and passengers during each time of driving for obtaining their consent.

In terms of fingerprints, voiceprints and other sensitive personal information that require the initiative action of individuals for the collection, besides the acceptance of the privacy policy, system operators shall use pop-ups or other explicit methods to explain which sensitive personal information is collected for which kind of extended business function, and ensure obtaining the individuals' express consent for such collection.

In addition, ICV system operators need to ensure that the vehicle users can easily access and view the privacy policy from the vehicles, e.g., through affixing QR code of privacy policy or pre-installing privacy policy or video tutorials on vehicle screen. In the meantime, if the main content of the privacy policy changes (for example, there are changes concerning the basic situation of the personal information controller, the purpose to collect and use personal information, the business functions for which such personal information is used, or the collection methods, frequency and scope), ICV system operators need to update the private policy in a timely manner and notify the vehicle owners in an effective way.

[3] Clause 5.6 (e) of PIS Specification.

Guidance of the APP Self-Assessment Guideline on the Preparation of Privacy Policy

In early 2019, National Information Security Standardization Technical Committee, China Consumers Association, Internet Society of China and Cybersecurity Association of China formed a special working group on illegal collection and use of personal information by apps. In March 2019, the working group issued the APP Self-Assessment Guideline which provided more practical guidance for companies to prepare privacy policies on the basis of the PIS Specification. If the ICV system operator shows its privacy policy to ICV users and interacts with the users through the vehicle screen or mobile app, the operator must follow the App Self-Assessment Guideline to prepare the privacy policy and design the product. Major highlights are as follows:

(1) Independence and readability of privacy policy: the PIS Specification requires that privacy policy shall be publicly available and easy to access. The APP Self-Assessment Guideline further provides that the privacy policy shall be a separate document and, after entering the main function interface of the app, users can access the privacy policy with no more than four clicks;

(2) Clear description of business functions and the types of personal information collected: the privacy policy shall set out each business function of the app that collects personal information and shall not use words such as "etc., for example". There should be a one-to-one correspondence between the business functions and the types of personal information collected by each such function. The privacy policy needs to highlight the type of sensitive personal information collected;

(3) The purpose, method and scope of personal information collection shall be explicitly indicated: when users install, register or open the app for the first time, the app operator must remind the users to read the privacy policy. If the app collects sensitive personal information or transfers personal information to a third-party server by embedded third-party code or plug-ins, the app operator must clearly inform the users through pop-up windows or other apparent ways;

(4) The collection and use of personal information shall be subject to the user's voluntary consent, and no compulsory binding authorization is allowed: before collecting personal information, the app shall provide the users with the option of agreeing or disagreeing at their own discretion, and shall not package multiple business functions and force users to give one packaged authorisation to these functions.

New Requirements for Personalized Display and Exit

As mentioned above, the personal information collected by ICVs has very high commercial value for secondary exploitation. For example, by analyzing the consumption information, vehicle movement track and behavior pattern of the vehicle owners through particular algorithms, these vehicle owners will be labelled with different charateristics, which will provide rich data sources for business promotion, user profiling, precision marketing, etc. On the basis of these information, ICV companies can push personalized contents to vehicle owners and potential customers through mobile phone or vehicle terminals.

Due to the privacy concern of personalised display, the Draft Revised PIS Specification adds specific rules concerning this topic, which provides that when pushing personalised contents to the data subjects, the data controller is required to clearly mark the words "personalized display" or "tailor-made push" and provide the data subjects with a simple and straightforward option to exit from the personalized display model, or guarantee the ability of the data subjects to adjust and control the degree of personalized display.

It is worth noting that, according to the Draft Revised PIS Specification, “personalized display” means "activities of presenting information, providing search results of goods or services to a data subject based on the web browsing history, interests and hobbies, consumption records and habits of such specific data subject". In other words, personalized display refers to a process of displaying specific contents to a "specific individual" based on the personal information of such "specific individual", which requires the source of personal information and the recipient of such personalised display to be the same. As a result, it does not constitute personalised display if you push contents to a group of individuals based on the labelled information of such group.

To give an example, an individual uses an information app in relation to the auto industry. Through analysing the individual's browsing history of the app, the app operator identifies that the individual is a fan of a certain brand of car, so the app operator often pushes the advertisements and promotion information of that brand of car to the individual. This activity constitutes a personalized display. On the contrary, if the information app operator pushes the advertisements and promotion information of that brand of car to a particular group who are potential customers based on the characteristic information of such group (e.g. gender, age, income range and other labels), this does not constitute a personalized display.

Conclusion

As the biggest commercial application scenario of artificial intelligence, development of ICVs has attracted great attention from governments around the world which are issuing new rules to encourage the testing and driving of ICVs on their streets. In order to avoid the risk of product recall from a data privacy perspective, ICV manufacturers are advised to (1) take into account privacy and data protection issues of ICVs as part of the product design and development process; (2) ensure the design and development of ICVs to be carried out within both international and local sales country's data protection regime; and (3) carry out privacy or security risk assessment and test their security measures before launching the product. China currently does not have personal information protection laws specifically applicable to the ICV industry. Laws and regulations concerning personal information protection in China are developing and evolving very fast. Under this background, external counsel shall work closely with relevant stakeholder's in-house counsel and technology teams to come up with forward looking and creative legal solutions, so as to create value for the development of ICV and telematics businesses in China in a legally compliant way.

Contact us:

For a deeper discussion on how the issues discussed in the article may impact your business, please contact us:

Catherine Shen

Commerce & Finance Law Offices

Partner

+86 (10) 6569 3471

shenxiaolin@tongshang.com

Andrew Zhang

Commerce & Finance Law Offices

Partner

+86 (10) 6569 3399

zhangxinyang@tongshang.com

About Commerce & Finance Law Offices:

Commerce & Finance Law Offices is one of the leading full service law firms in China. The firm focuses on providing the best legal solutions for Chinese and multinational clients with regard to their various kinds of complicated cross-border and domestic transactions. Commerce & Finance Law Offices is particularly well-known for its practice in the fields of Capital Markets, Merger and Acquisition, Private Equity, Dispute Resolution, TMT, Healthcare, Education, Banking & Finance, Investment Fund and Intellectual Property.