



Llinks Corporate and M&A Bulletin
August 2019

上海
上海市银城中路 68 号
时代金融中心 16 楼和 19 楼
邮编: 200120
电话: +86 21 3135 8666
传真: +86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
邮编: 100005
电话: +86 10 8519 2266
传真: +86 10 8519 2929

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话: +852 2592 1978
传真: +852 2868 0883

伦敦
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com

SHANGHAI
16F/19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING
4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

HONG KONG
27F, Henley Building
5 Queen's Road Central
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

LONDON
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

master@llinkslaw.com

Privacy Protection Dilemma and Solutions in the Context of Internet of Vehicles

By David Pan | Susan Deng

The field of transportation is undergoing a major change, with its focus on "Internet of Vehicles" (IoV, also called as "Connected Vehicles"). The idea of the IoV originated from the "Internet of things" (IoT), which turns into the concept of the "Internet of things for vehicles". The IoV means a moving network made up of IoT which enables cars to interconnect with "X" (everything including vehicles, drivers, road and service platforms) through the use of modern telecommunication technology. The IoV will enhance the overall intelligent driving experience, provide users with a safe, comfortable and smart driving experience, and at the same time improve the traffic flow. ¹ Rather than merely a concept for private divers, commercial use of IoV on a large scale emerged. For example, major players like Uber and Didi announced their business plans of offering driverless car services².

Data is the key to the IoV technology application. No matter in which part of the IoV, "data/information" is the essential element to rely on. It is because of data exchange in the IoV, we could achieve "Vehicle to Cloud communication" between vehicles and the IoV services platform, "Vehicle to Vehicle communication", "Vehicle

如果您需要本出版物的中文本,
请与下列人员联系:

郭建良: +86 21 3135 8756
Publication@llinkslaw.com

For more Llinks publications,
please contact:

Roy Guo: +86 21 3135 8756
Publication@llinkslaw.com

Llinks Law Offices
www.llinkslaw.com

Privacy Protection Dilemma and Solutions in the Context of Internet of Vehicles

Road communication” between vehicles and highways facilities and “Vehicle to People communication” between the vehicle and mobile intelligent terminal, as well as the in-car communication between internal facilities and applications. If there are any interruptions in the process of data collecting, transmitting and analyzing, none of the above-mentioned functions can be properly performed.

In addition, data flow in two-way or even multi directions in the IoV structured network. For example, data may flow from the mounted terminals in vehicles to a service provider, the service provider then gives feedback and specific information to users’ vehicle; there also will be point-to-point or chain-like flow of information between service providers on the upper and lower links, or between drivers’ smartphones and service providers . It is fair to say that data is the lifeline of the IoV, without which the IoV would be non-existent. Therefore, data security equals to the security of the IoV. Despite the thriving IoV, the existing law lacks sufficient protection on data privacy of the car users and the public in the context of IoV. By analyzing two exemplified issues, the authors attempt to call attention to this problem and ultimately to jointly work out appropriate solutions.

Issue 1: Identifying Personal Information in the IoV data

The IoV involves various types of data. The authors divide the data into two main categories according to their characters: User Information and Vehicle Operation Data. The two categories can be sub-categorized in the following table:

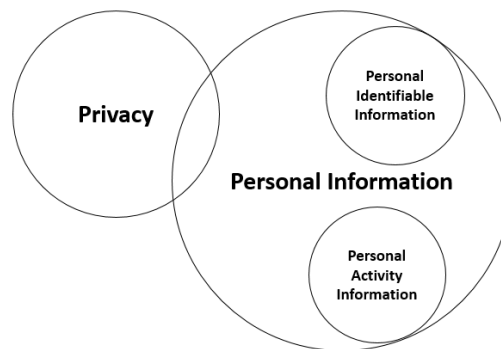
User information	Vehicle operation data
Car owner information: name, ID no., phone number, etc.	Driving route
Static vehicle information: license plate number, vehicle identification number, etc.	Operation parameter
Dynamic Vehicle information: location, movement track, etc.	Maintenance information
User's usage/driving preference	Driving habits
	Service requirements

According to the *China Cyber Security Law* (CSL), it is not difficult to determine that the information listed in the left column falls into the definition of “personal information”. In the right column, “Vehicle operation data” seems to include all the data automatically generated by the system during the driving process, and by drivers and passengers using the IoV applications, namely the “Machine-generated data”. Whether this kind of “Machine-generated data” belongs to personal information and thus shall be regulated by relevant laws and

Privacy Protection Dilemma and Solutions in the Context of Internet of Vehicles

regulations?

The CSL defines personal information as “all kinds of information, recorded electronically or through other means, that can determine the identity of natural persons independently or in combination with other information”. Further, according to *the Interpretation of the Supreme People’s Court and the Supreme People’s Procuratorate on Several Issues concerning the Application of Laws in Handling Criminal Cases on Citizens’ Personal Information (2017)* and the *Information security technology - Personal information security specification*, “all kinds of information reflecting the activities of specific natural persons” is categorized as personal information. The personal information here can be divided into two categories: first, information that helps to identify a specific natural person's identity; second, information that reflects a specific natural person's activities, including a personal driving record, whereabouts etc.



The meaning of “personally identifiable information” is quite self-explanatory. Nevertheless, it is hard to grasp the information when “in combination with other information” that can determine the identity of natural persons independently. For example, "in combination with other information" is a qualitative rather than quantitative requirement, so to what extent does the “personal information” need to be combined with other information to reach the legal “identifiable” standard and constitute the personal information stipulated by laws and regulations? If information A can be used to identify a specific natural person when combined with 5 other pieces of information, at the same time, information B needs to be combined with 50 other pieces of information to identify the specific natural person, whether information A and B both are deemed as personal information? If so, whether the protection level for these two pieces of information will differ in accordance with the number of information needed to be combined with?

Apparently, if a piece of information needs to be combined with more other information to identify a specific natural person, then it is less likely that it will constitute personal information, thereby the legal protection required should be weaker. As for the degree of information integration, EU’s *General Data Protection Regulation (GDPR)* requires consideration of objective factors, such as the length of time required for

Privacy Protection Dilemma and Solutions in the Context of Internet of Vehicles

identification and available technologies for data processing, etc. However, there is no similar provision in Chinese law so far. Therefore, Machine generated data might constitute personal information in certain circumstances, and network operators shall collect, process, store and safeguard such data in accordance with the certain legal requirements with regard to personal information protection.

Issue 2: Threat of the IoV technology to privacy protection

As the current hot topic, Autopilot technology plays an important role in the IoV application. Since the development of the self-driving vehicle, sensors have always been the fundamental hardware. Sensors are equivalent to the eyes of self-driving cars. According to different self-driving technology routes, sensors can be basically divided into three types: laser radar, traditional radar and camera. Sensors enable self-driving cars to identify roads, other vehicles, pedestrians or obstacles, as well as basic transportation facilities and so on. With the prevalent use of autonomous cars (either for commercial or civil use), the number of images and video information that can be captured during driving will grow exponentially. Such image capture and analysis activity is a personal information collection activity that no one can opt out of.

People can choose not to use a smartphone, go on shopping site, search in Baidu/Google, or use other any services that might collect their personal information. Nevertheless, these sensors collect data about the environment outside the vehicle, as long as a pedestrian walks on public roads, their appearance, time and geographical location information will be likely captured and recorded by sensors. There is no way that a pedestrian can choose to opt out. In such circumstance, a conflict has emerged between personal privacy invasion and the collection and processing of automobile sensor images.

According to the rule of reasonable expectation of privacy, if a person voluntarily places himself in a public place, which is a spontaneous interaction with the outside world, the person has no right to enjoy the privacy expectation. However, in practice, we need to consider it on a case-by-case basis. From the perspective of privacy protection, we should be more concerned about the practical issues that might affect data collection, such as what types of data can be collected from self-driving cars sensors and in what format? How is the information anonymized? How is the data stored, shared and protected? How long is the duration of storage? Does the personal information subject have any control right? In what way could the public assess the legality of data processing and ensure that data processors comply with rules and regulations accordingly?

Furthermore, driverless cars could provide real-time, continuous geo-location data. The third party could utilize this data to determine not only driver's current location and destination but also every place that the driver has been and the time when the driver was there. Advertisers may be able to discern the purchasing patterns of

Privacy Protection Dilemma and Solutions in the Context of Internet of Vehicles

individuals by tracking what stores they frequent. Insurers may be able to observe lifestyle of individuals by following their daily activities and dining habits, thereby helping them assess the insurance risks. All in all, data can bring benefits to the industry, convenience to consumers and better user experience, but from the privacy protection viewpoint, it could be quite intrusive.

Except for the US and EU, data protection laws in most countries have not yet specifically regulate privacy issues caused by autonomous driving technology.

On September 2017, the US House of Representatives passed the *Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution Act* (“Self Drive Act”). Unlike previously adopted “voluntary” guidelines, the Self Drive Act would become the first federal law on autonomous vehicles.³ Self Drive Act requires manufacturers of self-driving cars to develop a privacy plan on data protection and prohibit them from selling self-driving cars unless a privacy plan is in place. The privacy plan needs to include: (i) the way information is collected, used, shared, or stored; (ii) choices offered to vehicle owners or occupants regarding collection, use, sharing, and storage of such information; (iii) data minimization, de-identification, and retention of information about vehicle owners or occupants; and (iv) how privacy requirements are extended to entities that share the data. However, the manufacturer does not need to take these data protection steps if information about vehicle owners or occupants is anonymized or encrypted; or amended or combined so the information in a manner that it can no longer be linked to relevant individuals.

The GDPR, which aims to unify data protection within the EU, can be directly applicable to personal data in self-driving technology. In addition to government policy, in 2014, the *Alliance of Automobile Manufacturers* and the *Association of Global Automakers* unveiled seven privacy principles for vehicle technology and services, including Transparency, Choice, Respect for Context, Data Minimization, Data Security, Integrity and Access and Accountability. The privacy principles also stated that personal data could only be shared to third parties on the basis of contracts with consumers, with the consent of consumers or to fulfill legal requirements.

For legacy reasons, infringement of personal information in sectors like hotel, tourist and realty was rampant in China. With the advent of IoV technology, should China's legislators learn the lessons in those sectors and preemptively require manufacturers to develop privacy plans before selling self-driving cars in the market, by taking reference to US and EU law? To be specific, it is advisable for legislators to clarify the obligations of the manufacturer in collecting, processing and storing vehicle data at least as follows:

1. Ensure data security. Manufacturers should implement reasonable measures to protect collected information against loss or unauthorized access or use.

Privacy Protection Dilemma and Solutions in the Context of Internet of Vehicles

2. Consistency of data collection and use purpose. Manufacturers should use the collected data in ways that are consistent with the expressed purpose when the data was collected.
3. Data minimization. Manufactures should collect information only as needed for legitimate business purposes and not retain collected information for any longer than necessary. Distinguish between core and non-core functions when collecting personal information.
4. Ensure users' right to know and right to choose. Manufacturers should inform users the purpose of collection and obtain authorization prior to collecting personal data.

From a broader perspective, the key to safeguard personal information is to ensure the implementation of data minimization as well as data anonymization, which means the personal data is irreversibly altered in such a way that a data subject can no longer be identified, which is different from “pseudonymous” or “de-identified”)

Summary

The development of autonomous driving technology in China is flourishing. However, China's legal regime has not addressed the specific privacy issues that self-driving cars industry will soon face. At the present stage, based on the existing cyber security and data protection laws and policies, car manufacturers, fleet operators and other vendors (i.e. the IoV, mapping service providers) can start from the following aspects to meet their compliance requirements:

1. Screen and identify personal information collected, processed and generated in the process of technology application.
2. Pay attention to different types and locations of sensors, especially how each of them transmits data.
3. Whether cross-border data transmission is involved.
4. The IoV data transmission is the key concern. Pay attention to the technical measures taken in the data exchanging process, such as encryption and anonymization.
5. Various types of systems, platforms and participants are involved. The determination of responsibilities with third parties should be emphasized.

Privacy Protection Dilemma and Solutions in the Context of Internet of Vehicles

Contact Details

If you would like to know more information about the subjects covered in this publication, please feel free to contact the following people or your usual Llinks contact.

Author	
David Pan Tel: +86 21 3135 8701 david.pan@llinkslaw.com	
Shanghai	
David Yu Tel: +86 21 3135 8686 david.yu@llinkslaw.com	Bernie Liu Tel: +86 21 3135 8678 bernie.liu@llinkslaw.com
Selena She Tel: +86 21 3135 8770 selena.she@llinkslaw.com	Nicholas Lou Tel: +86 21 3135 8783 nicholas.lou@llinkslaw.com
Dali Qian Tel: +86 21 3135 8676 dali.qian@llinkslaw.com	Kenneth Kong Tel: +86 21 3135 8777 kenneth.kong@llinkslaw.com
David Wu Tel: +86 21 6043 3711 david.wu@llinkslaw.com	David Pan Tel: +86 21 3135 8701 david.pan@llinkslaw.com
Elyn Jiang Tel: +86 21 6043 3710 elyn.jiang@llinkslaw.com	
Beijing	
David Yu Tel: +86 10 8519 2266 david.yu@llinkslaw.com	Bernie Liu Tel: +86 10 8519 2266 bernie.liu@llinkslaw.com
Yuhua Yang Tel: +86 10 8519 1606 yuhua.yang@llinkslaw.com	
Hong Kong(in Association with Dennis Fong & Co., Solicitors)	
David Yu Tel: +86 21 3135 8686 david.yu@llinkslaw.com	Sandra Lu Tel: +86 21 3135 8776 sandra.lu@llinkslaw.com
London	
Yuhua Yang Tel: +44 (0)20 3283 4337 yuhua.yang@llinkslaw.com	

Privacy Protection Dilemma and Solutions in the Context of Internet of Vehicles

¹ Xiao Jing, Brief analysis of the Internet of Vehicles technology and application [J], Shanghai Automotive, 2019, (4) : 9-12.

² Yipeng Zhang, Travel Company's Automatic Driving Ambition, Active Exposure or a Forced Choice? See https://mp.weixin.qq.com/s?__biz=MjM5OTQzOTE0MA==&mid=2651469828&idx=1&sn=0a1d3c93305dce59a3f88b29770181eb&chksm=bcc5e64f8bb26f592920848a0f46e875c225b1c12d7400644cd43cc074665505c9c8739bf9af&mpshare=1&scene=1&srcid=0811br4obLXqTHyIRrgAAhLL&sharer_sharetime=1565538039715&sharer_shareid=0f98598f0c9ca8fba0963cf9080a14f7&key=ae82afc765e556e13c68071ee609eb3eef7982dda37302a0b853f962d182692ea2ea2dc59462b816e5f46efca7af20c6f2259881af75d6d7b01e194f23c4848d46e49d41fea8a0706ccf9442c50b7933&ascene=1&uin=MTAxNTI2MTQ0MA%3D%3D&devicetype=Windows+10&version=62060834&lang=zh_CN&pass_ticket=ePRveXoAoQaA58Jgs%2F2gb2MG8f4GfS3W5skxjTmYzF4zjOCZC4uNdYXRPgQzRbTL.

³ Late to the Scene, the “Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution Act” (“SELF DRIVE Act”) Seeks to Set Course for Future Development, <https://www.jdsupra.com/legalnews/late-to-the-scene-the-safely-ensuring-12636/>