HAN KUN LAW OFFICES

Legal Commentary

CHINA PRACTICE • GLOBAL VISION

May 15, 2017

Personal Information Protection from the Perspective of Criminal Law

David TANG | Min ZHU | Will HUANG

On May 9, 2017, the Supreme People's Court and the Supreme People's Procuratorate held a press conference to release the *Interpretations of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Law in the Handling of Criminal Cases Involving Infringement of Citizens' Personal Information* (the "**Interpretations**"), which will be effective from June 1, 2017.

To protect citizens' personal information, in 2009, the crimes of "illegally selling or providing of the personal information of citizens" and "illegally acquiring the personal information of citizens" were added in *Amendment VII to the Criminal Law of the People's Republic of China*. In 2015, *Amendment IX to the Criminal Law of the People's Republic of China* combined the two crimes into one, the "infringement of citizens' personal information." The Interpretations set forth more practical conviction and sentencing criteria for the infringement of citizens' personal information and mark a milestone for the criminal protection of citizens' personal information.

Several key concepts

The Interpretations make clearer several concepts regarding the crime of "infringement of citizens' personal information" stipulated by Article 253A of the *Criminal Law of the People's Republic of China* (the "**Criminal Law**"):

a. **Citizens' personal information:** Article 1 of the Interpretations expands the scope of "citizens' personal information" from personal identification information to identification and activity information, which includes names, identity document numbers, correspondence and contact information, addresses and other identification information, account passwords, property status, whereabouts and other activity information relating to particular natural persons.

b. **Provision:** Article 3 of the Interpretations specifies that the "provision of citizens' personal information" not only includes the act of providing personal information of citizens to

particular persons, but also refers to releasing such information through the information networks or through other channels. In addition, citizens' personal information that is legally collected can still be considered the "provision of citizens' personal information" if the collector of the information provides it to others without the consent of the information subject, unless the information has been processed, the particular person cannot be identified, and the information cannot be recovered after processing.

c. **Unlawful acquisition:** Article 4 of the Interpretations specifies two standards for determining the "unlawful acquisition of citizens' personal information" stipulated by Article 253A of the Criminal Law, which refer to acquiring citizens' personal information by way of purchase, acceptance or exchange in violation of the relevant provisions of the State, or collecting such information during the process of performing duties in violation of the relevant provisions of the State.

What are "serious circumstances"?

According to Article 253A of the Criminal Law, "serious circumstances" constitutes the prerequisite for the crime of "infringement of citizens' personal information." The Interpretations specify the relevant standards for determining "serious circumstances" based on different forms of conduct. Article 5 of the Interpretations sets forth clear standards for determining the illegal acquisition, sale or provision of citizens' personal information. Article 6 sets forth standards for determining "serious circumstances" regarding "illegally buying or accepting citizens' personal information for lawful business activities." The Interpretations specify the standards for determining "serious circumstances" based on the information type and quantity, usage of information, identity of the information subjects, subjective viciousness and other aspects:

a. **Information type and quantity:** There are various types of citizens' personal information. The Interpretations set forth different standards for what constitutes "serious circumstances" based on the importance of different types of personal information as detailed below:

No.	Information Type	Determining Standard
1	Information on whereabouts, communication, credit information, property information.	More than 50 pieces
2	Accommodation information, communication records, health and physiological information, transaction information and other personal information that may affect personal and property safety.	More than 500 pieces
3	Citizens' personal information other than that described above.	More than 5,000 pieces

b. **Amount of illegal income:** People commonly sell or illegally provide citizens' personal information for profit. Therefore, the Interpretations stipulate that receiving illegal income over RMB 5,000 is a "serious circumstance."

c. **Usage of information:** Different uses of citizens' personal information that is illegally obtained, sold or provided, will result in varying degrees of harm to information subjects. Therefore, the Interpretations stipulate that the following circumstances are "serious circumstances":

   i. selling or providing information on citizens' whereabouts, which is used by others for the commission of a crime;

   ii. knowing or should have known that others are to use the personal information of citizens to commit crimes, but continuing to sell or provide such information.

d. **Principal identity:** Many information leakage cases are conducted by insiders. To crack down on such crime, the Interpretations lower the conviction criteria for information leakage from insiders. If people sell or provide others with citizens' personal information obtained in the performance of duties or the provision of services, it will be considered a "serious circumstance" if the number pieces or amount of information is greater than one half of the conviction criteria shown above.

e. **Previous convictions:** According to the Interpretations, if a person has ever received criminal punishment or has received administrative punishment within the last two years for the infringement of citizens' personal information, and again illegally acquires, sells or provides citizens' personal information, that person's conduct will be determined to be a "serious circumstance."

f. **Special provisions:** In practice, illegally purchased and accepted personal information is generally used for advertising promotions. Article 6 of the Interpretations sets forth conviction criteria under this circumstance. Under any of the following circumstances, illegally buying or accepting citizens' personal information (other than those mentioned in Items 3 and 4 of the first paragraph of Article 5 of the Interpretations) for lawful business activities shall be determined to be a "serious circumstance":

   iii. the profit from the illegally purchased or accepted personal information of citizens reaches RMB 50,000;

   iv. those involved have ever been subject to criminal punishment or have received administrative punishment within the last two years for infringement of personal information of citizens, and are again illegally purchasing, selling or providing personal information of citizens; and

   v. other serious circumstances.

What are "particularly serious circumstances"?

After defining "serious circumstances," the Interpretations set forth specific standards for "particularly serious circumstances" in both qualitative and quantitative ways:

a. **Quantity standards:** The Interpretations set forth different standards for "particularly serious circumstances" based on the importance of different types of personal information as detailed below:

No.	Information Type	Determining Standard
1	Information regarding whereabouts, communication, credit information, property information.	More than 500 pieces
2	Accommodation information, communication records, health and physiological information, transaction information and other personal information that may affect personal and property safety.	More than 5,000 pieces
3	Citizens' personal information other than that described above.	More than 50,000 pieces

b. **Serious consequences:** According to the Interpretations, acts which "cause serious consequences such as death, serious injury, mental disorder or kidnapping of the victims" or "cause significant economic losses or adverse social effects" are determined to be "particularly serious circumstances."

How is the quantity of information calculated?

In practice, a single case often involves citizens' personal information that is mixed or possibly contains many different types of information. Under this circumstance, the Interpretations specify that the quantity of information can be converted according to a corresponding ratio.

Consider the information type and quantity under the aforementioned "serious circumstances." If the quantity of information does not meet the standard of 50 pieces, 500 pieces or 5,000 pieces as shown in the table above, the quantities of information will be converted according in the ratio of 1, 10 or 100 times. The incident may be criminally investigated if the total quantity calculated according to the corresponding proportion meets the relevant standard. For example, when investigating a case, 20 pieces of type 1 information are found and 350 pieces of type 2 information are found, and the total pieces of the two types of information does not meet the respective standards of 50 pieces or 500 pieces. In this case, according to the Interpretations, the information quantity would be converted according to a ratio of 10. 350 pieces of type 2 information will be converted into 35 pieces of type 1 information and the total number will be 55 pieces, which meets the criminal standard. In other words, 20 pieces of type 1 information may also be converted into 200 pieces of type 2 information and the total

number will be 550 pieces, which will also meet the standard of 500 pieces.

Article 11 of the Interpretations stipulates that the quantity of citizens' personal information is not to be counted multiple times when the same information is first illegally acquired and then sold or provided to another party. If the same citizen's personal information is sold or provided to different entities or individuals, however, the quantity of the citizen's personal information is to be aggregated based on each such transfer. The quantity of citizens' personal information found in batches will be directly determined according to the amount of such information, unless there is evidence that the information is not true or is duplicative.

What should enterprises pay attention to?

In general, the Interpretations set forth clearer conviction and sentencing criteria for the crime of infringement of citizens' personal information, which aims to strike at such crime by lowering the relevant criteria to some degree. We would therefore recommend that enterprises pay attention to the following issues:

a. Expansion of legal sources regarding protection for personal information

In accordance with Article 2 of the Interpretations, "violating relevant national provisions" mentioned in Article 253A of the Criminal Law means the violation of laws, administrative regulations, and departmental rules on the protection for personal information of citizens. What needs to be focused on is that the legal sources cited here are an extension of the laws and administrative regulations, which were common in previous legislative practice for departmental rules. In this manner, the Interpretations greatly expand the amount of applicable regulatory documents that cover personal information protection. In practice, the ministries and commissions of the State Council and their authorized agencies may issue departmental rules regarding the protection of personal information. Such authorities generally include: National Health and Family Planning Commission of the PRC, Ministry of Human Resources and Social Security of the PRC, Ministry of Industry and Information Technology of the PRC, Ministry of Science and Technology of the PRC, the People's Bank of China, China Banking Regulatory Commission, China Securities Regulatory Commission, China Insurance Regulatory Commission, State Ministry for Industry & Commerce of the PRC, China Food and Drug Administration, Cyberspace Administration of China, and so on.

b. Enterprise management to face increased risk of criminal liability

In accordance with Article 7 of the Interpretations, entities that commit crimes specified in Article 253A of the Criminal Law will be subject to the conviction and sentencing criteria for natural persons in accordance with the Interpretations. Officers directly in charge and other persons directly responsible will be punished, and the entities will also be fined. As stated above, the Interpretations lower the conviction and sentencing criteria for the infringement of

citizens' personal information. In addition, a noteworthy trend in current the departmental rulemaking by some authorities is that natural persons must be punished for their own illegal acts or the illegal acts of entities which they oversee or are responsible for. Therefore, it is no exaggeration that enterprise management personnel now face higher risks of criminal liability in relation to personal information and big data services.

c. Defense of lawful business activities

The Interpretations clearly stipulate that it is a "serious circumstance" potentially subject to criminal liability when a person illegally buys or accepts citizens' personal information for lawful business activities, and obtains profits of more than RMB 50,000 by virtue of such information (other than those specified in Items 3 and 4 of the first paragraph of Article 5 of the Interpretations). Therefore, as an enterprise whose business involves personal information, "lawful business activities" obviously cannot be a defense against criminal liability. Considering this, such enterprises should establish or improve their internal processes and controls regarding collecting personal information, while also reviewing contractual provisions regarding personal information in services agreement between themselves and their customers, thereby legally collecting and using personal information necessary for business.

d. Desensitizing personal information

In coordinating with provisions of the Cyberspace Law, the Interpretations stipulate that it shall be determined as an illegal act to provide others with lawfully collected personal information of citizens without the consent of those whose information is collected, unless such information has been processed to the degree where the particular person cannot be identified and such identifying information cannot be recovered. However, a large quantity of desensitized information and data can actually be recovered to some degree by virtue of technology. Therefore, it is a technological challenge to relevant enterprises to achieve true desensitization, to reach the degree where a particular person cannot be identified and such identifying information cannot be recovered. Failing to achieve desensitization will no longer merely result in civil or administrative liability.

e. Information leakage from insiders

Information leakage from insiders is an existing problem in industries with respect to the protection of personal information and big data. Considering this, the Interpretations lower the conviction criteria for information leakage from insiders. If people sell or provide others with citizens' personal information obtained in the performance of duties or provision of services, and the number or amount of which has reached more than half of the conviction criteria mentioned above, the case will be determined a "serious circumstance." We would therefore recommend that relevant enterprises to improve employee management by

i. making specific guidance regarding how to legally obtain, use and protect personal information of citizens when performing their duties or providing services;

ii. improving internal control policies and compliance training, thereby protecting enterprises from harmful consequences caused by the acts of their employees.

Han Kun Cybersecurity and Data Compliance Series:

I : Big Data Policy and Legal Issues in the Healthcare Industry

II : Comments on the Network Security Law

III: Comments on the Measures on Security Assessments for Personal Information and Important Data to be Transmitted Abroad (for Public Comment)

IV: The Unveiling of Cybersecurity Reviews

● 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.

Should you have any questions regarding this publication, please contact **Mr. David TANG （+8621-6080 0905; david.tang@hankunlaw.com ）, Mr. Min ZHU （ +8621-6080 0955; min.zhu@hankunlaw.com ）** or **Mr. Will HUANG (+8621-6080 0967; will.huang@hankunlaw.com).**