JUNHE BULLETIN

May 27, 2017

Protection of Personal Information

Supreme Court and Supreme Procuratorate Interpretation Raises New Challenge for Data Protection Compliance

Currently although there is no omnibus personal information protection law in China, relevant provisions are scattered throughout several laws, administrative regulations and department rules, a violation of which may lead to relevant civil and administrative liabilities. In regard to criminal liabilities, Amendment (VII) to the Criminal Law, effective since 28 February 2009, has added Article 253 (A) to establish the "crime of selling or illegally providing personal information of citizens" and the "crime of illegally obtaining personal information of citizens". Amendment (IX) to the Criminal Law in 2015 has combined these two crimes into the "crime of infringing on citizens' personal information" and also expanded the scope of application of this offense from specific industries and areas such as employees of financial institutions, telecommunication companies, education or medical institutions, to all individuals and entities and increased the maximum penalty that could be imposed on violation[1]. However, in practice, elements which this criminal offence require are not entirely clear. Specifically, in this digitalized age, practices of enterprises utilizing data in various industries are developing rapidly and in many aspects experimental and whether those practices may cross the line and raise criminal liabilities is still very much in a grey area.

Recently, the Supreme People's Court and the Supreme People's Procuratorate promulgated the *Interpretation by the Supreme People's Court and*

[1] http://www.junhe.com/law-reviews/192

the Supreme People's Procuratorate on Issues Concerning the Application of Law in Handling Criminal Cases of Infringing on Citizens' Personal Information (hereinafter the **"Interpretation"**) [2]and relevant typical cases[3], and the Interpretation will become effective at the same time as the *Cybersecurity Law*. The Interpretation provides more specific conditions for "the crime of infringing on citizens' personal information" for the first time, which has important meanings to define and decide the scope of criminal liabilities. We will analyze certain provisions that we consider may have significant influences on the personal information compliance practice for enterprises.

I. Clarifying the Scope of "Violation of the Relevant State Provisions"

The criminal behavior of "the crime of infringing on citizens' personal information" includes "selling or providing citizens' personal information to third parties in violation of the relevant state provisions" or "stealing or illegally obtaining citizens' personal information by other methods". With respect to the former, "violation of the relevant state provisions" is the precondition for such a crime. Currently, personal information protection regulations are scattered throughout several laws, administrative regulations, departmental rules and normative documents. As a result, the scope of "the relevant state provisions" would substantially impact whether or not a violation can be considered a crime.

Article 96 of the Criminal Law provides, "'violation of State Provisions' as mentioned in this Law refers to violation of the laws enacted or decisions made by the National People's Congress or its Standing Committee and the administrative regulations and rules formulated, the administrative measures adopted and the decisions or orders promulgated by the State Council." The scope of the "state provisions" in Article 96 of the Criminal Law does not include local regulations and departmental rules, while the Article 2 of the Interpretation clearly provides that "violation of the relevant state provisions" refers to "violation of the laws, administrative regulations and departmental rules in relation to the personal information protection", which includes departmental rules that contain broad legal protection requirements for different industries and types of personal information. Such interpretation would be critical for practice of enterprises to consider when setting up the internal compliance rules and policies and judicial practice in this aspect is also worthy constantly monitored to keep alerted to elements to constitute the crime.

II. Clearly Stipulating that Providing Citizen's Personal Information without Consent Commits a Crime

Before the promulgation of the Interpretation, Section 1 of Article 253A of the Criminal Law was construed in practice mainly as illegal selling. For

[2] http://www.chinacourt.org/law/detail/2017/05/id/149396.shtml
[3] http://www.chinacourt.org/article/detail/2017/05/id/2852365.shtml

example, seven typical criminal cases regarding infringement on citizens' personal information, published at the same time with the Interpretation, are all relevant to situations of illegally selling or purchasing citizens' personal information. It was unclear whether enterprises' providing or transferring personal information which was legally obtained through normal business activities to a third party for free or by cooperation will raise criminal liabilities.

Article 3 of the Interpretation explicitly provides that "providing citizens' personal information which was legally collected to others without consent of the citizens" will also constitute "the crime of providing any citizen's personal information" under Article 253A of the Criminal Law. In practice, the content and form of the consent raises many disputes and debates due to lack of clear requirements under law. In addition, the Interpretation adopts a provision in the Cybersecurity Law that when providing personal information to others, if "the information has been processed in a manner that it is impossible to identify a specific person and it cannot be restored", it will not be subject to the consent requirement for transfer. In practice, where it is difficult for enterprises to obtain consent from the subjects of the personal information or it is hard to prove that prior consent of the subjects has been obtained, anonymization is an approach to mitigate potential legal risks. However, standards for anonymization are still ambiguous at this stage.

III. Concept of "Illegally Obtaining Citizen's Personal Information by Other Methods" Expands

In previous cases of crimes of infringing on citizens' personal information, illegally obtaining is mostly construed as illegal purchasing personal information. Article 4 of the Interpretation provides a clearer definition, which clearly provides that without consent from subjects of the information, receiving, exchanging and collecting personal information during the performance of duties or providing services are all regarded as illegally obtaining personal information.

IV. Our Observation

The Interpretation will become effective on June 1, 2017 together with the Cybersecurity Law. The Cybersecurity Law is for the first time introduced cybersecurity and information protection requirements on the level of law, while the Interpretation has further clarified the boundaries of legal responsibilities in relation to personal information protection. However, the Interpretation provides certain broad interpretations of Article 253A of the Criminal Law which will result in certain ambiguities between crime and non-crime. For example, the specific requirement of "consent" before collecting information is not clear; how to determine the "whereabouts tracks" of personal information is not clear, and the specific implementation and measurement of sentencing is subject to practical judicial decisions.

We understand that the effectiveness of the Interpretation and Cybersecurity Law will largely

enhance the compliance duties of enterprises in relation to data protection and cybersecurity protection. It is necessary for enterprises to enhance internal management, improve compliance awareness of their staff and remain on alert for further developments regarding the data protection laws and regulations and their implementation.

Marissa DONG	Partner	Tel: 86 10 8519 1718	Email:dongx@junhe.com
Lena YUAN	Associate	Tel: 86 10 8553 7663	Email:yuanq@junhe.com
Mengyao Zhou	Intern	Tel: 86 10 8553 7892	Email: zhoumy@junhe.com

YIN Xiao (associate) also has contribution to this Article.