PRC Data Privacy Laws in a Nutshell

New developments in personal data protection regulations reflect a growing trend in China, in which maintaining the privacy of personal data and effecting reasonable compliance efforts to that end are becoming an important matter. Some argue such a regime reflects a new way for authorities to exert control over expression via over breadth and selective enforcement, while others maintain it is necessary to create a self regulatory climate due the expansive nature of data and its ease of transmission, portability and abuse.

BY ALEXANDER MAY
MAY 10, 2013

Data privacy is relevant to all companies and their employees operating within China. Any company in China which licenses information, gathers information, engages in market research, data management or is in media, telecommunications, retail, advertising, healthcare, provides internet content, has customer lists, customer information, patient information, among others, should be aware of the changing Chinese landscape with respect to data privacy. Chinese data regulations and guidance are replete with inconsistencies, gaps and unhelpful generalities. However, new developments reflect a growing trend in China, in which maintaining the privacy of personal data and effecting reasonable compliance efforts to that end are becoming an important matter. Some argue such a regime reflects a new way for authorities to exert control over expression via over breadth and selective enforcement, while others maintain it is necessary to create a self regulatory climate due the expansive nature of data and its ease of transmission, portability and abuse.

Notwithstanding the reasoning, companies in China have yet another amorphous compliance bugbear to obey. Given the inconsistent state of existing data privacy rules and recent dicta that position personal data at the epicenter of the data protection maelstrom, one might think it counterintuitive, if not disingenuous, that there is no legally authoritative definition of "personal data" under Chinese law.

Recent non-binding guidelines define personal data as *"computer data that may be processed by an information system, relevant to a certain natural person, and that may be used solely or along with other information to identify such natural person."* This suggests it is merely necessary to ensure that where personal data is used there must be no way the data can be connected with the individual to whom it may be attributed. This actually comports with the generally accepted definition of personal data in China, on an agglomerated basis, and is proximate to the standard definition under European Community Directives 2002/58/EC and 95/46/EC of the European Parliament with respect to data privacy.

We live in the data age and data privacy impacts every business in some way, whether it is a matter of protecting customer information, hospital records or employee information among others. Since the potential liability is not just civil but also criminal, it is necessary approach the protection of personal data with a

healthy dose of respect. Strong data privacy compliance requirements exist elsewhere in the world and in light of the lack of consistency and detail under the Chinese rules it would be prudent to comply with or seek clarity from more tightly drafted laws such as those found in the European Community Directives.

On 1 February 2013, the Information Security Technology - Guidelines for Personal Information Protection within Public and Commercial Services Information Systems (the "Data Guidelines") were issued by the Ministry of Industry and Information Technology (the "MIIT"). The Data Guidelines as they currently exist are a set of principles to be adopted on a voluntary basis.

Comprehensive, national regulations have yet to be enacted in the PRC that specifically address personal data protection. However, various layers of laws and regulations do address data protection to some extent, including: general privacy principles set forth in the PRC Constitution and broad rules under the civil law and tort liability law; industry relevant rules, such as credit reference, internet, financial, telecommunications and consumer protection; local legislation regarding personal data protection; and the PRC Criminal Law (each individually a "Data Reg" and collectively, the "Data Regs").

The Data Guidelines apply to a much broader range of businesses than the Data Regs and cover key issues such as data exports, sensitive data, subject access and correction rights. However, at this time they are still just guidelines, mere dicta with respect to the collection and handling of personal data via commercial and organizational information systems. However, that does not mean they will not be used by PRC authorities as a basis in civil and criminal data privacy cases.

Because of the fractured nature of the Data Regs, no specific national regulatory authority exists for their enforcement, which is generally dependent upon the line ministries that cover specific industries. Thus, the MIIT covers the telecommunications sector and the Ministry of Health covers the healthcare sector. Additionally, no rules currently exist that require notification or registration for the collection of personal data. However, while the Data Regs do not require the appointment of a data protection officer, the Data Guidelines recommend a personal data administrator appoint or create a data protection officer or department to protect personal data.

WHAT CONSTITUTES PERSONAL DATA?

The Data Regs define "personal data" inconsistently. However, they do quite consistently recognize that any information relating to an individual that alone or together with other information could identify such person would constitute personal data. The Data Guidelines similarly define personal data but also classify personal data into two categories: general personal data and sensitive personal data. Under the Data Guidelines, general personal data constitutes all personal data other than sensitive personal data. For the avoidance of doubt, information about a legal person (i.e., a company or organization) does not constitute personal data.

PERSONAL DATA PROCESSING RULES

While the Data Regs are inconsistent as to the processing of personal data, they do regulate how personal data may be processed in certain sectors. For example, in the banking sector, informed consent must be obtained from an individual about whom personal data is being processed before his/her personal data is provided to a data processor. In the telecommunications sector, an internet company must (i) obtain the prior consent of an individual about whom personal data is being processed before collecting and using that personal information; (ii) ensure the confidentiality of the collected data; and (iii) not divulge, misuse, alter or sell such data or illegally provide such data to third parties. In

the credit reference and banking sector, the specific written consent of an individual about whom personal data is being processed is required if a third party asks for the personal data of that person.

The Data Guidelines also include guidance on how organizations should process personal data, including the need for consent by an individual about whom personal data is being processed before any of their personal data is processed. However, while such consent should be express, in the case of the collection of general personal data, under the Data Guidelines, tacit consent can be deemed. Notwithstanding the foregoing, any collector of general personal data must delete all pre-collected personal data if an individual about whom personal data is being collected or processed expressly opposes such collection or processing. Prior to the collection of any data, the individual about whom personal data is being collected must be clearly informed of the purpose and method of data collection as well as the measures implemented to protect that data. Furthermore, personal data may not be disclosed to any third party if such disclosure is not relevant to the purpose of collection or otherwise without the consent of the person about whom personal data is being collected.

We live in the data age and data privacy impacts every business in some way, whether it is a matter of protecting customer information, hospital records or employee information among others. Since the potential liability is not just civil but also criminal, it is necessary approach the protection of personal data with a healthy dose of respect.

CONSENT

The Data Regs are inconsistent as to how to obtain consent from an individual about whom personal data will or may be processed. However, the Data Regs relating to the credit reference sector require written consent and in the banking sector written consent is required if a financial institution provides the personal data to a third party. Unfortunately, the Data Guidelines provide no definitive guidance on how to obtain consent. However, evidentiary prudence dictates non-electronic, written consent should ideally be obtained from an individual about whom personal data will or may be processed.

SENSITIVE PERSONAL DATA

The Data Regs do not generally distinguish between general personal data and sensitive personal data. The Data Guidelines define sensitive personal data as, "information, the disclosure or modification of which could have a negative effect on the individual about whom such personal data will or may be processed." Sensitive personal data can include identification numbers, mobile phone numbers, racial or ethnic origin, political opinions, religious beliefs, DNA and fingerprints. This definition is broader than that found in European Community Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, which we have used for reference due to the lack of comprehensive regulations and guidance in the PRC.

The Data Guidelines state the express consent of an individual about whom personal data will or may be processed should be obtained when processing sensitive personal data. Additionally, the Data Guidelines provide that data collectors or processors should refrain from directly collecting sensitive personal data from persons lacking capacity or with limited capacity to give such consent, in which case the consent of the legal guardian of such person should be obtained.

While the Data Regs contain no specific rules with respect to processing sensitive personal

data, PRC credit reference regulations do specifically prohibit credit reference agencies from collecting certain information, such as an individual's religious beliefs, DNA, fingerprints, blood type or medical history. The Data Guidelines further provide that once the purpose has been achieved for which a specific consent has been obtained to process sensitive personal data, if any such sensitive data will be further processed, then another consent must be obtained from that individual about whom personal data will or may be further processed.

Data Regs relating to the credit reference sector require a written consent from the individual about whom sensitive personal data will or may be processed. Additionally, the Data Regs relating to the banking sector require the written consent of a person about whom sensitive personal data will or may be processed if a financial institution provides that person's personal data to a third party. However, ultimately the Data Regs provide no comprehensive formalities requisite to obtaining consent to process sensitive data and the Data Guidelines provide no explicit formalities to obtain consent.

GEOGRAPHICAL SCOPE

Because no comprehensive national regulations protecting personal data privacy exist, each individual Data Reg applicable to a particular instance of data collection must be applied territorially and varies from province to province, municipality to municipality and industry to industry. Therefore, while the Data Regs generally contain no express provisions on their territorial effect, Data Regs promulgated by a provincial or municipal authority would generally only be applicable to entities that collect and use personal data covered by that authority.

APPLICABILITY OF DATA REGS

Any individual or organization that collects and uses personal data in a locale or sector must comply with the applicable Data Regs. It should be noted the Data Regs inadequately distinguish between a person who alone, or together with others, determines the purpose and means of processing personal data (a "Data Controller") and a person who processes personal data on behalf of a Data Controller (a "Data Processor").

However, the Data Guidelines do distinguish between administrators of personal data ("Data Administrators") and receivers of personal data ("Data Receivers"). Data Administrators are those that determine the purposes and means of personal data processing and who control and process personal data. Data Receivers are those that receive personal data from an information system and process it per the consent of the individual about whom such data will or may be processed. A Data Administrator under the Data Guidelines is akin to a Data Controller under the Data Regs. Please note that both hard copy and electronic records are subject to the Data Regs, but the Data Guidelines only apply to personal data processed via information systems.

PERSONAL DATA SECURITY

The Data Regs impose no consistent or detailed security requirements. However, some sector-specific regulations, particularly the credit reference, banking and Internet sectors, impose general obligations to securely maintain personal data. The Data Guidelines only state that organizations should have necessary and sufficient administrative and technical measures to ensure the safety of personal data.

Although no uniform rules on the processing of personal data by Data Processors exist, the Data Regs relating to the banking sector require banks and financial institutions to conduct due diligence investigations on third party service providers to ensure they adequately protect personal data that may be disclosed to them by such a bank or financial institution.

While the Data Regs do not require entities to notify a particular agency or person in the

instance of a privacy breach, in the banking sector, the People's Bank of China must be promptly informed of the improper disclosure of personal financial data contra banking regulations. Internet service providers must notify the MIIT of improper disclosures of personal data where serious consequences are or may be caused by such a disclosure. PRC law regulates those who engage in "the service activity of providing information to internet users through the internet." These parties are considered "internet service providers" under PRC law even though they are actually content providers. It is hard to imagine how an internet service provider can effectively predict every serious consequence that may be caused by the disclosure of personal data, which seems to open an internet service provider to the caprice of governmental hindsight or abuse. This could be viewed as another lever of self censorship imposed on internet content providers in China.

RESTRICTIONS ON CROSS-BORDER TRANSFERS

The Data Regs do not uniformly address cross-border transfers of personal data. However, related banking sector and credit reference sector rules require that personal data collected in the PRC must be processed in the PRC and offshore entities may not be provided with such information unless explicitly permitted by law.

Under the Data Guidelines, Data Administrators can transfer personal data to individuals or organizations outside the PRC only if: express consent is obtained from the individual about whom the personal data relates or a government body with the authority to give such consent; or a specific law permits such a transfer.

CONSEQUENCES OF VIOLATIONS

Penalties for violating the Data Regs depend on which Data Reg has been breached and the nature of the breach. Punishments may include censure, fines, disgorgement of profits and suspension or revocation of key licenses or approvals. Aggrieved parties can also seek civil compensation in some cases. Under Article 253 of the PRC Criminal Law, employees of state-owned enterprises and financial, telecommunications, transport, education and medical organizations can be imprisoned for up to three (3) years for selling or illegally providing personal data obtained in the course of their employment to third parties. However, one need not be an employee of a state-owned entity to be criminally culpable, as is evidenced by the recent case against Peter Humphrey, of China Whys (a foreign-owned business risk advisory firm in China) who was recently charged with serious criminal personal data violations arising from his investigative business and illegally obtaining personal data.

The Data Regs fall under no one body's jurisdiction and are enforced by the courts, the public security bureau, the administration for industry and commerce and other regulators, particularly with respect to their supervisory powers over the credit reference, banking, telecommunications and internet sectors.

Data privacy in China is still evolving. In the absence of comprehensive, binding rules on how to treat data privacy issues in the PRC, we recommend prudence as the primary guideline. Pamir Law Group has experience in dealing with tricky data issues, including the collection, sale and analysis of various kinds of data and how such data should be treated to either be compliant or mitigate future liabilities due to clients' current activities.

The Author

ALEXANDER MAY
Special Counsel
amay@pamirlaw.com
(T) +86-21-5256-9933
(F) +86-21-5256-9936

Taipei

7F, No. 214, Dunhua North Road,
Song Shan District
Taipei 10546, Taiwan
(P) +886-2-5588-1799
(F) +886-2-5588-1790

Shanghai

Suite 1801, Xingye Tower 168
Jiangning Rd. Jingan District
Shanghai 200041, China
(P) +86-21-5256-9933
(F) +86-21-5256-9930

Beijing

65 Xiaojingchang Hutong, Gulou
Dong Ave, Dongcheng District
Beijing 100009, China
(P) +86-10-6515-7574
(F) +86-10-6515-7574