世强律师事务所

Steptoe

STEPTOE & JOHNSON LLP

An Overview of the Data Protection and Security Regimes of the People's Republic of China

May 2017

Overview of the Data Protection and Security Regimes of the PRC

The Internet and related information technologies permit the collection of huge amounts of data, which can be processed and transmitted quickly, and stored in multiple locations. These technologies have brought convenience and opportunity to individuals, businesses and governments alike, but they have also resulted in security risks and concerns for the same stakeholders. On one hand, the Internet enables businesses and customers to interact more freely and government authorities to be more efficient in performing their functions. On the other hand, the Internet has proven to be a powerful tool supporting the perpetration of crimes and the disruption of civil society. As a result, increasingly national authorities are seeking to regulate and control the creation and transfer of data within their respective jurisdictions.

In recent years, the Chinese regulatory regime has evolved rapidly to address the opportunities, challenges and concerns posed by the Internet and new technologies. The Chinese data protection and security regimes now comprise a unified group of laws and regulations, with the *PRC Cybersecurity Law*, which will take effect on June 1, 2017, at their center.

Businesses operating in China recognize the importance of monitoring cybersecurity developments; however, navigating the Chinese data protection and security regime can be a challenging task. This overview summarizes the current status of Chinese data protection and security under existing laws and rules, data localization, security review of information technology products and services, encryption, and data privacy legal regimes and highlights how they are interlinked.

Evolution of Chinese Data Protection and Security Regime

The People's Republic of China[1] has recognized the importance of the Internet and information systems in its policies and laws for more than 15 years. At the Fifth Plenary Session of the Fifteenth Chinese Communist Party ("CPC") Central Committee in 2000, the CPC addressed informatization as a national strategy. Similarly, the Tenth Five Year Plan adopted in 2001 stated that China would promote informatization by improving China's information infrastructure and supporting the development of China's information products industry.

As well as focusing on informatization, the Chinese government has recognized the importance of data security. In 2006, China's Eleventh Five Year Plan included a section on data security, which emphasized the importance of establishing a robust information security infrastructure and promoting information security products. In the same year, the Chinese government released the 2006-2020 National Informatization Development Strategy, underscoring that establishing a national information security safeguard system is a government priority.

China has also committed to enhancing development and use of encryption technologies, improving its information security monitoring system, strengthening its ability to cope with cyber-attacks, and preventing the spread of harmful information. In the Twelfth Five Year Plan, adopted in 2011, Chinese policy-makers stated that China would develop its laws and regulations governing cybersecurity and information security and will strengthen management of the Internet. The Twelfth Five Year Plan also states that China will develop and promote "secure and controllable" hardware and software. In accordance with these policies, on January 6, 2015, the State Council issued the Opinions on Promoting Innovation and Development of Cloud Computing and Cultivating New Business Forms of the Information Industry, which instructs Chinese authorities to, among other things, strengthen rules and policies regarding personal information protection and cybersecurity in the context of cloud computing and big data, and to implement administrative measures addressing the collection, storage, transfer, and disposal of information, as well as cross-border data flows.

---

[1] In this overview, the People's Republic of China, or China, refers to mainland China, excluding the Hong Kong Special Administrative Region ("SAR"), the Macau SAR and Taiwan.

Further, the Thirteenth Five Year Plan which was adopted in 2016, states that China will build "cybersecurity review and standard" systems. More recently, on December 27, 2016, the Office of the Central Leading Group for Cyberspace Affairs issued the National Cyberspace Security Strategy, which sets out nine strategic tasks to be carried out in order to safeguard cyberspace security. Those tasks are to (i) defend China's cyberspace sovereignty; (ii) safeguard national security; (iii) protect critical information infrastructures; (iv) strengthen construction of a cyberspace culture; (v) crack down on cyber terrorism, illegality and crime; (vi) perfect a cyber governance system; (vii) reinforce the foundation for cybersecurity; (viii) improve cyberspace safeguard capability; and (ix) enhance international cooperation in cyberspace.

The Traditional Approach to Data Security: State Secrets

China has a strict set of state secrets laws, violation of which can result in CPC disciplinary actions, administrative penalties and/or imprisonment for up to ten years. If a state secret is illegally provided to a foreign party, potentially the maximum punishment is the death penalty.

State secrets are defined under Chinese law as "matters that concern state security and national interests and, as determined according to statutory procedures, are known by people within a certain scope for a given period of time." State secrets not only include secret state policy decisions and secret matters relating to national defense, armed forces, state security, investigation of crimes, and foreign affairs, but also secret matters relating to the national economy, social development, science and technology, and anything that is classified by Chinese authorities specifically as a state secret. State secrets are divided into three categories based on potential harm to state security and national interests if they are divulged: top secret, highly secret, and secret.

Chinese law requires entities involved in handling state secrets to establish measures to administer state secrets compliance programs. Among other things, state secrets should be labeled as state secrets. Specifically, the law requires state secrets in writing to bear the mark "★" with the classification level on the left of the mark and the secrecy period on the right on the cover or first page of the relevant document, or if the document are is a map, drawing, or chart, after or behind the title. State secrets in other formats should indicate the classification level and secrecy period "in a way that can be easily recognized," or at "an eye-catching place." The law also requires that copies resulting from reproduction, extraction, quotation, and compilation of state secrets should be administered as originals and be subject to the same labeling requirements. Entities that administer state secrets are required to periodically report their work efforts in relation to guarding state secrets to the government, which conducts periodic inspections. On the face of the law, it seems reasonable to assume that a majority, if not all, of state secrets should carry proper labeling. However, the labeling requirement does not create a safe harbor, since information that is not labeled can still be deemed to contain state secrets by Chinese authorities. In this regard, the *Interpretations on Several Issues Concerning the Application of Law in Cases of Stealing, Spying into, Buying, and Unlawfully Providing State Secrets and Intelligence* (issued by the Supreme People's Court in January, 2001) state that "a person who knows, or should have known that an item or matter not bearing a mark of classification level relates to state security and interests, and steals, spies into, buys, or unlawfully provides such item, should be convicted and punished for the crime of stealing, spying on, buying, or unlawfully providing state secrets and intelligence in accordance with Article 111 of the Criminal Law."

Therefore, appropriate caution is required in circumstances where it is possible that state secrets may exist but are not labeled. Some industries potentially implicate state secrets more often than others. A non-exhaustive list of such industries includes national defense, meteorology, mapping, journalism, auditing, industries involving the use of geological data, and industries having access to the business and technology information systems of state-owned companies.

An Overview of the Data Protection and Security Regimes of the PRC

Data Localization

For a variety of reasons, not all sensitive data created in Mainland China is protected under the state secrets regime. For example, some information may not be of interest by itself, but could give rise to security issues when analyzed together with similar information. Data analytics have made it possible to derive information and insights that were previously unavailable from large quantities of data, so-called big data, revealing trends that a state might not deem convenient for widespread publication. This concern is underscored by reported incidents of the interception of communications and data collection, and related analysis, and the use of such data by foreign law enforcement and intelligence agencies. One approach to addressing security and privacy concerns in respect of data is to localize it.

On November 7, 2016, the Standing Committee of the National People's Congress promulgated the *Cybersecurity Law*, which became effective on June 1, 2017. Among other things, the *Cybersecurity Law* imposes a data localization requirement on personal information and important data collected and generated by the operators of "critical information infrastructures" during the course of their operations. According to the new law, all such information and data must be stored within Mainland China and a security assessment must be conducted before transmitting such information and data outside Mainland China.

The term "critical information infrastructures" awaits definition. On the basis of the limited information available, it is probably reasonable to assume that at a minimum the term refers to IT systems that process data in industry areas that are critical for China and could include critical information infrastructures in important industries and sectors such as public communications and information services, energy, communications, water resources, finance, public services and e-government affairs. Other areas where an operator is likely to be deemed an operator of a critical information infrastructure include those where damage, loss of function and data leakage could threaten Chinese national security, people's livelihoods, or the public interest. These assumptions should be revisited in the event that Chinese authorities provide a legal definition.

Prior to the promulgation of the *Cybersecurity Law*, Chinese authorities sought to protect and localize certain types of data using industry-specific rules, which prohibit the export of data outside Mainland China and are still valid. The Chinese central bank, the People's Bank of China ("PBOC") issued the *Notice of the People's Bank of China on Improving Work Related to the Protection of Personal Financial Information by Financial Institutions in the Banking Industry* in 2011, requiring banks to protect personal financial information and ensure that information collected in Mainland China is stored, processed, or analyzed within its borders. Further, generally financial institutions are prohibited from providing such information to foreign parties unless otherwise permitted under laws, regulations or PBOC rules.

Similar requirements exist in other industries. For example, the *Administrative Regulations on the Credit Reporting Industry* issued by the State Council on January 1, 2013 requires information collected by credit reporting agencies within the territory of China to be organized, stored and processed within China. The *Administrative Measures for Population Health Information (Trial)*, issued by the National Health and Family Planning Commission on May 5, 2014, specifically prohibits storage of population and health information collected in Mainland China on servers overseas. The *Regulations on the Administration of Online Publishing Services*, issued by the General Administration of Press and Publication, Radio, Film and Television and the Ministry of Industry and Information Technology on February 4, 2016, specify that servers and storage equipment related to the provision of web publishing services must be located within Mainland China. More recently, the *Interim Administrative Measures for the Business of Online Taxi Booking Services*, issued by the Ministry of Transport and six other departments on July 27, 2016, provide that personal information collected and business data generated by online taxi booking service platforms may not be disclosed to parties outside Mainland China.

An Overview of the Data Protection and Security Regimes of the PRC

Of particular concern for overseas securities regulators and companies listed on overseas exchanges and their professional advisors, the *Regulations on Strengthening the Protection of Secrets and Archive Management Related to the Issuance and Listing of Securities Overseas*, jointly issued by the China Securities Regulatory Commission, the State Secrecy Bureau and the State Archives Administration on October 20, 2009, requires audit work papers prepared in the course of issuing or listing securities overseas to be stored within Mainland China.

For several years before the promulgation of the *Cybersecurity Law*, China operated a voluntary national standard for personal data protection applicable to the private sector, the *Guidelines on Information Security Technology and Personal Information Protection in Information Systems for Public and Commercial Services* issued by the Ministry of Industry and Information Technology in November 2012 ("*MIIT Guidelines*"). In addition to setting forth guidance on how personal information should be protected, the *MIIT Guidelines* prohibit transfer of personal information overseas without user consent, or permission from relevant government authorities.

The voluntary standards contained in the *MIIT Guidelines* will now be superseded by the *Cybersecurity Law* and eventually by the *Measures for Security Review of Export of Personal Information and Important Data* ("*Draft Security Review Measures*"), which were issued in draft form for comments on April 1, 2017 by the Cyberspace Administration of China ("CAC"). The *Cybersecurity Law* imposes a data localization requirement on personal information and important data collected and generated by the operators of critical information infrastructures during the course of their operations in Mainland China. However, the *Draft Security Review Measures* expand data localization requirements from critical information infrastructure operators to include "network operators." The term "network operator" is yet to be defined, but appears to refer to owners and managers of IT networks and providers of network services. It is not yet clear whether a foreign company operating an Intranet system that is used by employees in China will be deemed a network operator.

The *Draft Security Review Measures* broadly define data export as "the provision of personal information and important data collected and generated by network operators in Mainland China to entities, organizations and individuals abroad." According to the *Draft Security Review Measures* "important data," a term that is used but is undefined in the *Cybersecurity Law*, is data closely related to national security, economic development or the public interest. This is a very broad definition and the measures state that the actual scope of important data is to be determined by reference to relevant national standards and identification guidelines that will be formulated later.

According to the *Draft Security Review Measures*, before exporting personal information or "important data," network operators must undertake a security assessment. The security assessment must focus on the following aspects: (i) the necessity for export of the data; (ii) details in connection with the relevant personal information, including the volume, scope, type and sensitivity of personal information and whether consent has been obtained from personal information subjects; (iii) details regarding important data such as the volume, scope, type and sensitivity of the important data; (iv) security protection measures, capabilities and "level" of the data recipient and the cyberspace security environment where the data recipient is located; (v) the risk of leakage, damage, falsification and abuse following any data export; and (vi) risks that may be posed to national security, the public interest or legitimate individual interests following the export of data or by the pooling of exported data. In addition to reviewing the data to be exported, a network operator must provide information to personal information subjects regarding the purpose, scope, contents, recipient, and country or region where the data recipient is located and relevant consents must be obtained from personal information subjects.

The *Draft Security Review Measures* provide that security assessments are to be conducted and recorded by network operators themselves, unless conditions that mandate a government assessment exist. Network operators are legally responsible for their assessment results. A network operator must request the relevant government department to conduct the security assessment if the

data to be exported: (i) contains information regarding more than 500,000 individuals in any single transmission, or in several aggregated transmissions; (ii) is more than 1,000 gigabytes in volume; (iii) contains data in connection with nuclear facilities, chemical biology, national defense, population and health, large-scale engineering activities, marine environment or sensitive geographical information; (iv) contains cybersecurity information, such as information regarding system vulnerabilities and the safety of critical information infrastructures; or (v) concerns information and data provided by critical information infrastructure operators. Conducting cyber security self-assessments is likely to be challenging for foreign companies in China until the legal regime is clarified and some experience of operating the new regime is gained by regulators. Similar concerns apply to making determinations regarding whether to refer a matter for assessment by a competent government authority.

The *Draft Security Review Measures* provide that security assessments should be conducted at least once a year, and that assessment results should be reported to relevant regulatory or supervisory agencies in a timely fashion. Security assessments must be redone if (i) there are changes to data recipients, (ii) there is a major change in the purpose, scope, volume and type of data to be exported, or, (iii) if there is a major security incident involving the data recipient or data that has been exported.

The *Draft Security Review Measures* specifically forbid export of data in the following circumstances:

- If a personal information subject has not given prior consent to the export of his/her personal information, or if the export of personal information could jeopardize individual interests;
- If the export of data could give rise to risks regarding Chinese national politics, the economy, science, national defense, or could impact national security or harm the public interest; or
- If the cyberspace administration authority, public security bureau or national security authority determines that certain data should not be exported.

Security Review of Information Technology Products and Services

Since the Edward Snowden incident, the terms "de-IOE" and "safe and controllable information technologies" have become increasingly used in the cybersecurity area in China. In September 2014, the China Banking Regulatory Commission ("CBRC") issued the *Guidance Opinions on the Use of Secure and Controllable Technology to Strengthen the Internet Security and Information Construction of Banking Industry* ("*CBRC Secure and Controllable Technology Opinion*"), which is aimed at promoting the use of secure and controllable information technologies in the banking industry. Such technologies are described as, "information technologies that are able to satisfy the need for information security of the banking industry and of which the technical risks, outsourcing risks, and supply chain risks are controllable." The *CBRC Secure and Controllable Technology Opinion* instructs banks to implement a preference for technologies and solutions that are open, transparent, and widely applicable and to award contracts to contractors who are willing to cooperate in sharing key technology and expertise. Accordingly, the CBRC has required all banks, including foreign banks, to increase the percentage of secure and controllable information technologies in their operations every year, with the goal of having such technologies make up 75% of banks' overall technology by 2019. On 26 December 2014, the CBRC issued *Guidelines on Promoting the Use of Secure and Controllable Technology in Banking Industry (2014-2015)* ("*CBRC Guidelines*"). The *CBRC Guidelines* contain detailed requirements for secure and controllable technology for IT products divided into 10 categories and more than 60 sub-categories. Some notable requirements include the requirement for filing the source code of certain products with the CBRC, which raises concerns with foreign IT providers regarding intellectual property protection The CBRC was reported to have suspended the implementation of the *CBRC Guidelines* on April 13, 2015 due to various concerns from the banking and IT sectors, but the targets set forth in the *CBRC Secure and Controllable Technology Opinion* are not reported as having been suspended.

An Overview of the Data Protection and Security Regimes of the PRC

As discussed above, the *Cybersecurity Law* regulates the security of all network products and services used by critical information infrastructure operators and states that network products and services must comply with the requirements of relevant national standards. Additionally, key network equipment and network security products must achieve certification before entering the Chinese market. Specifically, network products and services used by critical information infrastructure operators that impact national security must pass a national security review conducted by the CAC and other relevant government agencies.

On February 4, 2017, the CAC released the draft *Measures for Security Review of Cyber Products and Services* ("*Draft Cyber Security Products Review Measures*"). The *Draft Cyber Security Products Review Measures* are intended to "raise the level of security and controllability of cyber products and services and guard against supply chain security risks" and provide that, "important network products and services that are used by information systems that have a bearing on national security and public interests shall pass cybersecurity review." The draft provides that cybersecurity reviews should address:

- Risks that the products and services may be subject to illegal control, interruption and shutdowns;
- Risks existing in the development, transfer and technical support in connection with products and their key components;
- Risks that products and service providers illegally collect, save, process and utilize relevant information of the users by means of the products and services that they are providing; and
- Risks that products and services-providers engage in unfair competition or activities detrimental to the interests of users by taking advantage of users' reliance on products and services.

The *Draft Cyber Security Products Review Measures* further provide that the CPC and relevant government agencies and key state-owned enterprises must procure network products and services that have passed security review as a matter of priority, and may not purchase network products and services that have failed security review. Key industries are stated to include finance, telecommunications and energy. It is possible that other industries could be deemed to be key industries going forward. All network products and services procured by critical information infrastructure operators that could impact national security must pass a cybersecurity review. The issue of whether network products and services will affect national security falls to be determined by government agencies responsible for protection of critical information infrastructures.

The Cybersecurity Review Office ("CRO"), which has been established under the CAC, will assume responsibility for conducting cybersecurity reviews. The CRO has the authority to initiate a cybersecurity review based on requests from government agencies, suggestions from national industry associations, market feedback or applications made by companies themselves. According to the *Draft Cyber Security Products Review Measures*, a cyber security review expert committee will be established and third party agencies recognized by the State will be engaged to conduct cybersecurity reviews. Specifically, third party agencies will undertake security assessments, and the cyber security review expert committee will conduct a comprehensive evaluation of the security integrity of cyber products and services, and their providers based on the assessments of the third party agencies. The *Draft Cyber Security Products Review Measures* address concerns about the security of proprietary information disclosed for the purposes of cybersecurity reviews by requiring entities and personnel engaged in cybersecurity review work to keep confidential all information obtained during the course of a cybersecurity review. It remains to be seen, however, how and whether such confidentiality requirements will be implemented and what rights foreign companies in China have to challenge any breaches impacting their intellectual property rights.

An Overview of the Data Protection and Security Regimes of the PRC

Encryption

Encryption products and technologies help prevent and mitigate threats to data security and personal information. Chinese law regulates the import and export, manufacture, sale, and the general use of commercial encryption technologies and products. The central government agency charged with enforcing the Chinese encryption regime is the State Encryption Management Bureau ("SEMB"). The import or export of commercial encryption products requires approval by the SEMB, who also license the sale of commercial encryption products in Mainland China. Import and export of commercial encryption products is also under the jurisdiction of the General Administration of Customs ("GAC").

Generally, Chinese law prohibits any person based in Mainland China from selling commercial encryption products that are not "made in China." However, foreign-invested companies and foreign representative offices are allowed to use foreign-made encryption products in Mainland China, provided that a permit for using foreign-made encryption products has been obtained from the SEMB. Encryption products made in Mainland China must be approved by the SEMB. Only entities designated by the SEMB are allowed to develop and manufacture encryption products in Mainland China, and encryption technologies developed by designated entities are protected as state secrets. Users of encryption products are not permitted by law to transfer encryption products to other entities or individuals. Violation of encryption regulations can result in warnings, confiscation of encryption products, fines, and potentially other administrative or criminal penalties, if state security is jeopardized.

In April 2017, the SEMB released a draft *Encryption Law* ("*Draft Encryption Law*"), which, if enacted in its current form, will tighten controls over the import and export of encryption products. The *Draft Encryption Law* defines encryption as items or technologies that apply specific transformations to data for purposes of encrypted protection or security certification and classifies encryption into three categories: core encryption, normal encryption and commercial encryption. Core encryption and normal encryption are used to protect state secrets, whereas commercial encryption is used to protect information that does not constitute state secrets. Under the *Draft Encryption Law,* the export of core encryption and normal encryption is prohibited and import or export of commercial encryption is subject to licensing. The PRC Ministry of Commerce ("MOFCOM") and the SEMB are tasked with relevant licensing work. In addition, the *Draft Encryption Law* provides that MOFCOM, SEMB and the GAC will jointly issue a commercial encryption import and export control list.

Data Privacy Laws

Privacy laws address concerns about privacy or personal information. Historically, personal data privacy has been protected in Mainland China in a variety of different provisions scattered across a number of laws, regulations and guidance, and data protection has been inconsistent. This situation is set to change with the promulgation of the *Cybersecurity Law,* which together with the *Draft Security Review Measures*, for the first time provides for a unified personal data protection regime.

Up until the promulgation of the *Cybersecurity Law*, the *Decision on Strengthening Network Information Protection*, issued by the Standing Committee of the National People's Congress of China in December 2012 ("*NPC Decision*") and related regulations and guidance provided the practical regime for protection of personal data. The *NPC Decision* addresses "electronic information that can be used to identify the identity of individual citizens" and "electronic information concerning the privacy of citizens." According to the *NPC Decision*, the guiding principle for collecting and using electronic personal information is that the reasons are "legal, righteous, and necessary." The *NPC Decision* requires any entities that collect or use electronic personal information to specify the purpose, method, and scope of the collection or use, and obtain consent from the person(s) whose electronic personal information is collected or used. In addition, entities must make public their rules regarding the collection or use of electronic personal information. Violation of the *NPC Decision* can result in warnings, fines, revocation of licenses, bans on responsible individuals from engaging in the provision of Internet services, and suspension of business. A violation could also give rise to liability under

other Chinese laws. For example, the *PRC Criminal Law* prohibits selling and illegally providing personal information and violations can result in imprisonment for up to seven years for individuals and fines for entities, while persons in charge and any other persons who are directly responsible for crimes may also be punished under the law. The new *Cybersecurity Law* specifically forbids theft and the illegal collection, sale and provision to others of personal information.

In addition to the *NPC Decisions*, the *Guidelines on Information Security Technology and Personal Information Protection in Information Systems for Public and Commercial Services* (referenced above as the *MIIT Guidelines*) provide guidance on personal information protection in Mainland China. The *MIIT Guidelines* provide for a voluntary national standard, which defines personal information as "computer data that can be processed by information systems, is related to certain individuals, and can be used to identify certain natural persons independently or in combination with other information." The *MIIT Guidelines* categorize personal information into general personal information and sensitive personal information. Collecting sensitive personal information requires explicit consent, while consent for general personal information can be implicit. Examples of sensitive personal information provided by the *MIIT Guidelines* include national identification numbers, mobile phone numbers, information regarding race, political views and religion, the gene data, and fingerprints. The importance of the *MIIT Guidelines* with regard to protection of personal information is likely to diminish with the implementation of the new cybersecurity regime.

Chapter Four of the *Cybersecurity Law* addresses protection of personal information, which is defined as "information that can be used separately, or in combination with other information, to identify a natural person." The basic principles for collecting, using and storing personal information set forth in the *Cybersecurity Law* are consistent with most existing regulations (including various industry-specific rules) and the Guidelines, but generally the new law imposes more stringent requirements. Under the *Cybersecurity Law*, network operators must publicize their rules regarding data collection and clearly indicate the purposes, methods and scope of information collection and use. Network operators must also obtain the consent of data subjects when collecting or using personal information and they are prohibited from collecting personal information that is not relevant to the services they provide.

Further, the *Cybersecurity Law* requires critical infrastructure operators to keep personal information strictly confidential, and not to leak, falsify, or damage such information. Without the consent of data subjects, network operators must not provide personal information to other parties, except for information that has been processed and can no longer be recovered and through which no particular individual can be identified. Currently, no guidance is available regarding the form or contents of user consents. Additionally, network operators must take measures to prevent disclosure of, damage to, or loss of personal information. When any disclosure, damage or loss of personal information occurs or could occur, network operators must take remedial measures immediately, including informing users who may be affected and reporting to competent government agencies.

As discussed above, the *Cybersecurity Law* and the *Draft Security Review Measures* require that personal information collected and generated by critical information infrastructure operators or network operators be stored within Mainland China. Under the *Draft Security Review Measures* consent must be obtained from data subjects and a security review must be conducted before personal information may be exported outside Mainland China. The *Draft Security Review Measures* also require non-network operators to perform a security review before exporting personal information, although currently very little guidance is available regarding how such security reviews must be conducted.

Foreign companies operating in Mainland China should pay close attention to the final version of the *Draft Security Review Measures* in order to determine the scope of any new compliance requirements, which potentially could be very onerous.

An Overview of the Data Protection and Security Regimes of the PRC

****

Chinese laws and policies in the area of data privacy are expected to become more complicated as the regulatory environment evolves to address concerns arising from emerging technologies. Steptoe advises companies across a broad range of industries on data protection and privacy laws. In addition, we regularly help companies formulate or revise privacy policies to comply with new laws or take account of new technologies or changes in business operations. As one of the first US law firms to begin practicing in the area of cybersecurity, Steptoe is a recognized pioneer in the field. Our China data privacy practice draws upon our experience in other jurisdictions and provides strategic counseling on opportunities and challenges facing businesses in China.

Susan Munro
Partner
Steptoe & Johnson LLP
Beijing
smunro@steptoe.com

Bo Yue
Associate
Steptoe & Johnson LLP
Washington DC
byue@steptoe.com

Edward Lin
Senior Legal Consultant
Steptoe & Johnson LLP
Beijing
xlin@Steptoe.com