Published on *The National Law Review* https://natlawreview.com

China Newsletter | Autumn 2019 - Privacy & Data Protection & Capital Markets

Article By:

George Qi

Dawn (Dan) Zhang

Privacy and Data Protection

Special Working Group for Rectification of Applications Releases Draft for Comments of the Methods for Identifying Unlawful Acts of Applications (Apps) to Collect and Use Personal Information App

??????????App????????????????????????

On May 5, 2019, the Special Working Group for Rectification of Applications ("App Group") released the *Methods for Identifying Unlawful Acts of Applications (Draft for Comment)* ("*Draft*"). The *Draft* lists seven major unlawful acts by apps. The App Group was established in January 2019 to promote and implement assessment of the unlawful collection and use of personal information. At that time, the Office of the Central Cyberspace Affairs Commission, Ministry of Industry and Information Technology, Ministry of Public Security, State Administration for Market Regulation released a notice that the special rectification of apps would be conducted through 2019 nationwide.

The *Draft* identifies several types of acts by apps that may be considered unlawful collection and use of personal information, and specifies what may constitute each such unlawful act, including:

- Failure to publish rules for the collection and use by apps, which among others, include: (1) no privacy policy or user agreement or relevant rules regarding collection and use of information of app exists; (2) users may need take multiple actions (i.e., more than four) to locate such rules.

- Failure to explicitly indicate the purpose, manner, and scope of collecting and using personal information, which can be reflected in multiple ways, including: (1) collecting personal information under the guise of improving user experience, where that is not the real purpose; (2) failing to list one-by-one the type of personal information collected and the frequency of collection.

- Other types of unlawful collection and use of personal information as listed in the *Draft* include: (a) collection or use of personal information without consent; (b) collection of personal information that is not related to the service provided by the app; (c) provision of the collected personal information to others without consent; (d) failure to provide the function to delete or correct personal information; (e)

collection or use of information of minors under the age of 14 without their own or their guardians' consent, in various situations.

Cyberspace Administration of China Seeks Public Comments on Draft Administrative Measures for Data Security

??????????????????????????????

On May 28, 2019, the Cyberspace Administration of China released the *Circular of the Cyberspace Administration of China on Seeking Public Comments on the Administrative Measures for Data Security* ("*Draft*"), which contains 40 articles in five sections: (1) General Provisions, (2) Data Collection, (3) Data Processing and Use, (4) Data Security Supervision and Management, and (5) Supplementary Provisions.

Aiming to facilitate implementation of the *Cyber Security Law* (in effect since June 1, 2017), the *Draft* specifies data protection obligations of network operators in several areas: (a) requirements for personal information collection and use by the network operator from various perspectives (such as readability, user consent, etc.); (b) filing with the authority if the network operator collects important data or sensitive personal information for business purposes; (c) designating the person responsible for data security; (d) protecting and processing personal information and important data according to national standards. The *Draft* mostly regulates the business operator or network operator for data protection, instead of targeting individual users.

Information Security Standardization Technical Committee Releases Version 1 of Network Security Practice Guide – Essential Information Specifications for Basic Business Functions of Mobile Internet Applications

????????????????????????—??????????????????

On June 1, 2019, the National Information Security Standardization Technical Committee released the first version of the *Essential Information Specification for Basic Business Functions of Mobile Internet Applications* ("*Specification*"). The *Specification* was based on the requirements stipulated in Article 41 of the *Cyber Security Law of PRC*, requiring that "to collect and use personal information, network operators shall follow the principles of legitimacy, rightfulness and necessity, disclose their rules of data collection and use, clearly express the purposes, means and scope of collecting and using the information, and obtain the consent of the persons whose data is gathered," and "network operators shall neither gather personal information unrelated to the services they provide," etc.

The *Specification* states the range of personal information required for normal business operations for the basic functions of 16 popular kinds of applications, i.e., map navigation, ride hailing, instant messaging and social networking, social networks of local communities, online payments, news information, short videos, online shopping, express distribution, food delivery, transport ticketing, matchmaking, jobhunting, financial loans, real estate trade, and car sales.

Highlights of the *Specification*:

- The *Specification* lists six principles for the collection of personal information by applications: (1) integration of power and responsibility, (2) definite purpose, (3) minimum necessity, (4) availability of option to agree on the authorization, (5) openness and transparency of the rules, and (6) ensuring safety via technology methods and management measures.

- The *Specification* lists the necessary information to be collected for the basic functions of 16 kinds of applications. For map navigation, location information including pinpointing and track progress may be required. For online payment, cell phone number, account number and password, identity (name, identity card category, identity card number, term of validity, photocopy); bank account information (bank name, card number, term of validity, bank reserved mobile number); transaction information (payment instruction, transaction amount, trading object, commodity, transaction time, transaction channel, transaction type, currency), transaction authentication information.

Seeking Public Comment, Cyberspace Administration of China Publishes Draft Measures for Security Assessment for Cross-Border Transfer of Personal Information

??????????????????????????????????

On June 13, 2019, the Cyberspace Administration of China published the *Measures for Security Assessment for Cross-Border Transfer of Personal Information (Draft for Comment)* ("*Draft*") and collected public comment. The *Draft* establishes a security evaluation system for when a network operator exports overseas personal information collected during its business operations within PRC. Such system would facilitate the functioning of the *Cyber Security Law*, in effect since June 2017, and specifically regulate the outbound transfer of personal information.

Highlights of the *Draft*:

- Before personal information is exported, the network operator shall conduct the security assessment and report such cross-border transfer of personal information to the local-level cyberspace department every two years or whenever the purpose or type of personal information is changed.

- The materials for the report prepared by the network operator shall include: (a) the report form, (b) the contract signed by and between the network operator and the recipient, (c) the analysis report for security risks of the cross-border transfer of personal information and security guarantee measures, etc.

- The network operator shall keep records of the cross-border transfer of personal information, and retain such records for at least five years. The following information shall be included in the records: (a) date and time of cross-border transfer of personal information, (b) identity of the recipient, such as name, address, and contact information, (c) type, quantity, and degree of sensitivity of the personal information involved in the cross-border transfer, etc.

- The network operator shall on an annual basis before Dec. 31, report its cross-border transfer of personal information, contract performance, and other information for the current year, to the local-level cyberspace departments.

Seeking Public Comment, Ministry of Industry and Information Technology Releases Draft Administrative Provisions on Network Security Vulnerabilities

??????????????????????????

On June 18, 2019, the Ministry of Industry and Information Technology released the *Administrative Provisions on Network Security Vulnerabilities (Draft for Comment)* ("*Draft*") and collected public comments. The *Draft* targets network security vulnerabilities, and intends to ensure that vulnerabilities of network products, services, and systems are repaired in a timely manner. The *Draft* is relatively short, containing 12 clauses, and aims to regulate the providers of network products and services, network operators, and third-party organizations or individuals.

Highlights of the *Draft*:

- Upon discovery or having knowledge of vulnerabilities in their products, services, or systems, providers of network products or services and network providers shall (a) immediately verify the vulnerabilities, and take vulnerability repair or preventive measures for the relevant network products within 90 days and for the relevant network services or systems within 10 days, (b) if the vulnerability repair or preventive measures need to be taken by users or relevant technical partners, inform the affected users and relevant technical partners of the vulnerability risk and relevant required repair or measures via public notice or customer service, and report the relevant vulnerabilities to the Information Sharing Platform of Cybersecurity Threat of the Ministry of Industry and Information Technology.

- Third party organizations or individuals shall follow the principles of necessity, authenticity, and objectivity when releasing the information about the vulnerability to the public, and shall not: (a) release the relevant information about vulnerability before the providers of network products and services or the network operators; (b) intentionally exaggerate the hazards and risks of vulnerabilities; (c) release or provide the methods, procedures, and tools specifically designed to engage in activities endangering network security by making use of vulnerabilities of network products, services, and systems.

Capital Markets

Science and Technology Innovation Board Rules Announced by CSRC

??????????

On March 1, 2019, the China Securities Regulatory Commission (CSRC) formally announced the rules and documents for the establishment of the Science and Technology Innovation Board (STIB), including, among others, *Administrative Measures for the Registration of Initial Public Offerings on the Science and Technology Innovation Board (for Trial Implementation)* (the "*STIB Registration Measures*") and *Measures for Follow-up Regulation of Companies Listed on the Science and Technology Innovation Board (for Trial Implementation)* (the "*STIB Follow-up Regulation Measures*").

The *STIB Registration Measures* specify the fundamental rules for registration of initial public offering at STIB, including (a) setting out the general principles of STIB registration, confirming that STIB

adopts a registration-based IPO system; (b) with the focus on information disclosure, streamlining and optimizing the current stock issuance conditions, highlighting the principle of materiality with an emphasis on risk-control measures; (c) systemizing the arrangement and process for IPO on STIB with key stages accessible to the public; (d) strengthening the requirements for information disclosure; (e) stipulating that price of newly offered shares shall be determined by quotation from qualified investors; (f) establishing a whole-process regulatory framework.

At the same time, the *STIB Follow-up Regulation Measures* contain rules for post-registration regulation for public companies, including (a) specifying that other CSRC regulatory rules for public companies shall also apply to STIB-registered companies, unless otherwise provided in the *STIB Follow-up Regulation Measures*; (b) setting out the corporate governance rules for STIB registered companies, *inter alia*, with respect to companies with special voting arrangements; (c) establishing a reinforced information disclosure system with increased requirements on industrial and business risk disclosure; (d) optimizing the arrangements for shareholding reduction, material asset restructuring, share incentive plans, etc.; and (e) establishing a strict delisting process.

CSRC Publishes Answers to Several Questions About Initial Public Offerings

??????????????

On March 25, 2019, CSRC published the *Circular on Issuing Answers to Several Questions About Initial Public Offerings* (the "*CSRC Answers*"), aiming to provide detailed guidance on IPO rules and their application in certain frequently encountered scenarios. The *CSRC Answers* mostly focus on commonly seen legal and financial issues, including valuation adjustment mechanism, special types of shareholders, financial internal control, decline in performance, etc.

Highlights of the *CSRC Answers*:

- Valuation adjustment mechanism. The *CSRC Answers* specify that any valuation adjustment mechanism (VAM) shall be terminated prior to application for an IPO unless it can meet the following standards: (a) the issuer is not a party to such VAM; (b) the VAM will not result in change of control; (c) the VAM is not related to the market value of the company; and (d) the VAM will not cause material adverse effect to the issuer's capacity of continuous operation or otherwise cause material adverse effect to investor interest.

- Foreign controlling structure. Where the controlling shareholder resides outside of China and controls the issuer through complicated shareholding structure, CSRC requires the sponsor and issuer's counsel to (a) review the reasons for such structure, the legality and reasonableness, the authenticity of shareholding status, whether there is nominee shareholding or shareholding through trust, whether there is any arrangement affecting controlling power, and the source of funding made by the shareholder, and (b) describe and opine on whether there is clear shareholding ownership by the controlling shareholder and the actual controlling person, and how the issuer could ensure the effectiveness of its corporate governance and internal control measures.

- IPO of company delisted or spin-off from overseas stock exchange. If the issuer was previously listed on an overseas stock exchange, it shall describe and disclose the legality and compliance records with respect to the information disclosure, stock exchange, and the board and shareholder's meeting resolutions during its past IPO and listing period, the legality of its delisting process, and whether it has ever received any penalty; if any sale of assets by an overseas delisted or listed company is involved, the issuer shall also disclose whether it has complied with foreign exchange rules. The

sponsor and the issuer's counsel shall review and opine on the abovementioned matters. Any new shareholder acquiring over 5% shares of the company through trading on the exchange should also be disclosed and reviewed.

CSRC and UK FCA Jointly Announce Launch of Shanghai-London Stock Connect

??????????????????????

On June 17, 2019, CSRC and the UK Financial Conduct Authority made *The Shanghai-London Stock Connect-Joint Announcement by the China Securities Regulatory Commission and the UK Financial Conduct Authority* (the "*Joint Announcement*"), signaling official approval of the proposed Shanghai-London Stock Connect.

According to the *Joint Announcement*, the Shanghai-London Stock Connect contemplates a reciprocal depository receipts arrangement between the Shanghai Stock Exchange (SSE) and the London Stock Exchange (LSE), whereby SSE-listed companies may apply to be admitted to trading on the newly formed Shanghai Segment of LSE (i.e., the westbound limb), and LSE-listed companies will also be able to apply for admission to the Main Board of SSE (i.e., the eastbound limb). In the initial stage, qualified securities institutions in each of the two markets may conduct cross-border conversion business in relation to the depository receipts. Initially, capital flow under the Shanghai-London Stock Connect will be subject to a maximum cross-border quota, with the eastbound aggregate quota being RMB250 billion and the westbound aggregate quota being RMB300 billion.

National Law Review, Volume IX, Number 302