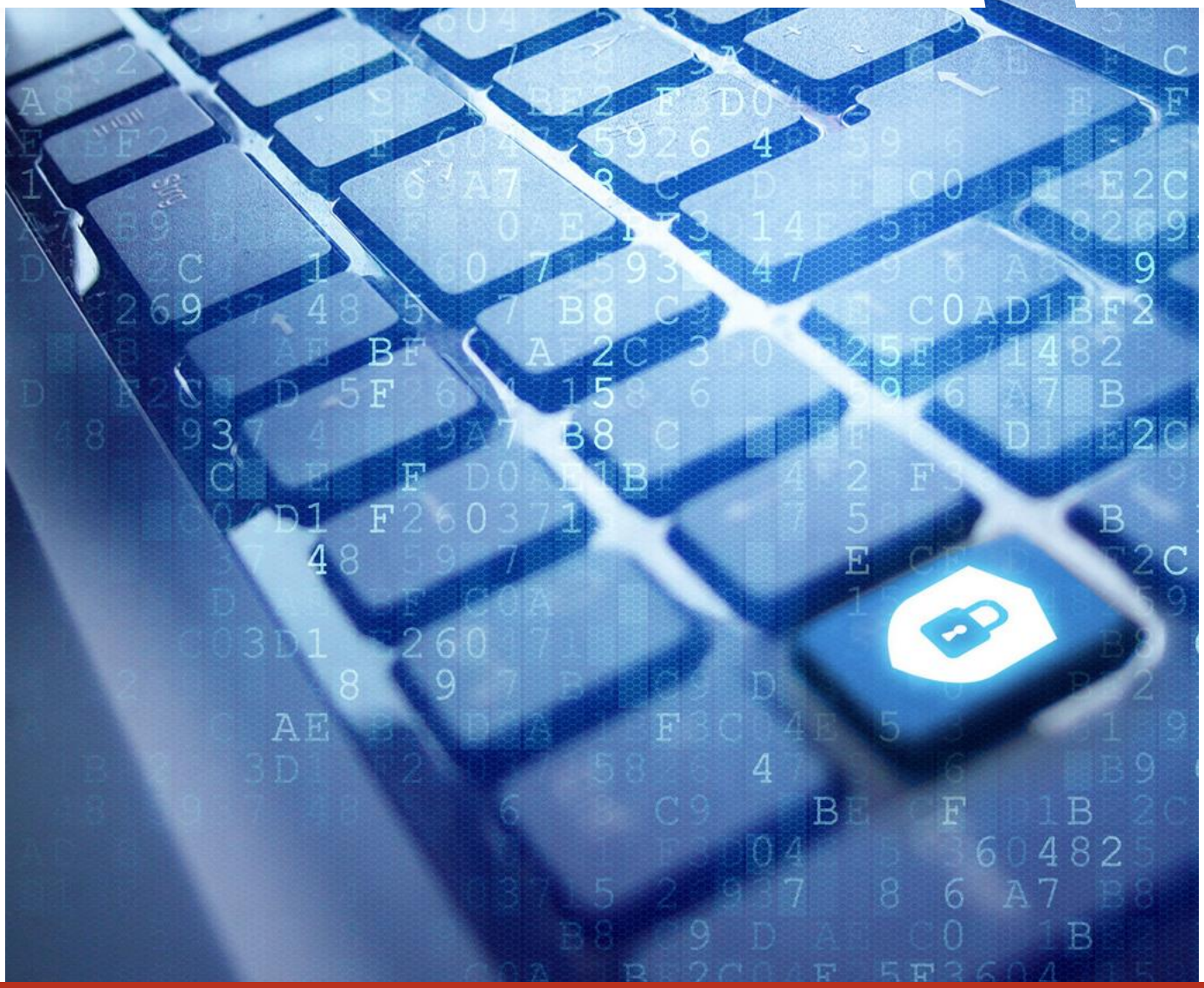
Llinks Client Alert – Cybersecurity, Data & Privacy

March 2021



Shanghai · Beijing · Shenzhen · Hong Kong · London

LINKS Law Offices
通力律师事务所

I. Legislation

On February 20, 2021, the State Administration for Market Regulation ("**SAMR**") and the Standardization Administration issued GB 40050-2021 *Security General Requirements on Critical Network Equipment* ("***Standard***"), which is expected to take effect on August 1, 2021. The *Standard* consists of two parts: security function requirements and security safeguard requirements. Security function requirements include equipment identification security, redundant backup recovery and abnormal detection, vulnerability and malicious program precaution, pre-installed software startup and update security, user identification and authentication, access control security, log audit security, telecommunication security, data security and password requirements. Security safeguard requirements are related to design and development, production and delivery, operation and maintenance stages.

II. Law Enforcement

On February 5, 2021, the Ministry of Industry and Information Technology ("**MIIT**") issued the *Notification on Apps' Illegal Access to Microphones, Contacts, Albums and other Authorities to Infringe User Rights and Interests*. The MIIT engaged a third-party inspection agency to inspect mobile Apps, but 26 Apps have not yet finished rectification based on inspection results as of the report date. For Apps that have not been rectified within the specified time, the MIIT will consider imposing administrative penalties in accordance with laws and regulations.

Recently, Shanghai Communications Administration punished a number of Apps that infringed on user rights and interests and collected personal information in violation of laws and regulations. Among them, a travel social media App, an office App and an educational App were imposed administrative penalties for frequently asking users for system permissions, sharing users' personal information with third-party SDKs without consent, and failing to disclose personal information collection and use rules and failing to provide functions of deleting or correcting personal information in accordance with laws respectively. In addition, certain Apps were ordered to rectify because of adopting default consent, failing to promptly respond to users on account cancellation and other reasons.

Llinks Comments: With regard to App violations, in 2020, more than 520,000 Apps with a high usage rate have been technically tested, more than 1,500 Apps have been required to rectify wrongful activities, and 120 Apps have been removed from the App store. The MIIT, the Ministry of Public Security and the App Governance Working Group are mainly responsible for the rectification ordering on App violations. In 2021, the App supervision and rectification work will continue to be carried out in an orderly manner, and the law enforcement focus has clearly gone deeper into issues such as acquiring system permissions and third-party SDK violations. Personal information protection and data compliance should be the top compliance concerns for App operators.

III. Foreign Trends

On February 17, 2021, a social media giant was fined seven million euros by an Italian antitrust watchdog for failure to promptly correct improper commercial practices in relation to user data processing. In 2018, the antitrust body ordered the company to publish an amended statement on the homepage of its website for Italy, its App and the personal page of each registered Italian user because the company had not informed users properly of its data collection and utilization rules. However, the recent investigation proved that the company did not abide by the order.

It was reported that a social media giant agreed to pay 92 million dollars to settle a class action lawsuit over alleged privacy violations, which included claims that the App collected “highly sensitive personal data” to track users and target ads at them to make profits. The settlement agreement still waits for court approval.

About Llinks' Cyber Security and Data Compliance Services

Llinks' partners have been representing clients in data and cyber security related legal matters, such as offshore server, log records storage and filing, personal data collection and use, data integrity, centralized data process, differentiation between trade secrets and state secrets, etc. After 2010, Llinks' partners started to represent domestic and foreign enterprises in forming whole-process compliance solutions for the collection, use, transfer and destruction of customer personal information in digital marketing environment. In the course of handling these cases, Llinks' team has built up its solid capacity in tracing the logical chain which underlies all the data privacy laws and regulations. On that basis, our team can provide clients with practical and economical solutions which meet the requirements of the regulatory authorities.

Our team also includes some experienced lawyers who previously have served as law enforcement officials in cyber security administration. Their insights contribute to a better understanding on the regulatory authorities' key concerns and priorities in law enforcement, which is critically important for us to work out a practical solution for clients.

We have been working closely with relevant government consultancy departments and academic research institutions on the trend of legislation and implementation of the CSL regime. Our team has published special reports and analytical articles in this field. In September 2018, LexisNexis published a special issue written by our team, on *Companies' Compliance in the Context of China*, which contains six articles on practical issues concerning cyber security and data compliance. In September 2018, we drafted a series of concise bilingual articles titled *30 Practical Questions about the CSL*, which were later exclusively published online by Wolters Kluwer. In September 2019, as regulations and practice evolved, we updated the *30 Practical Questions about the CSL* and renamed the combined articles as *2019 The Blue Book of PRC Cybersecurity and Data Compliance (Bilingual)*. In November 2020, based on the latest cases and typical scenarios, we updated again and presented the *2020 Blue Book of PRC Cybersecurity and Data Protection Compliance (Bilingual)*. From 2018 to 2020, we published several Chinese and English professional articles, such as *Three Major Problems of China's Internet Security Data Law, China-US Game of Data Regulation*, in the national and foreign journals such as Insights, The American Lawyer, China Business Law Journal and the Legal System Daily.

For more information, please contact:

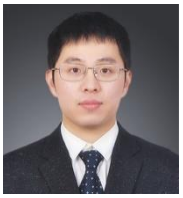
David Pan Lawyer
Mob: +86 136 2172 0830
Tel: +86 21 3135 8701
david.pan@llinkslaw.com

Kenneth Kong Lawyer
Mob: +86 185 1210 5880
Tel: +86 21 3135 8777
kenneth.kong@llinkslaw.com

Xun Yang
Mob: +86 152 2182 2373
Tel: +86 21 3135 8799
xun.yang@llinkslaw.com

Patrick Gu Lawyer
Mob: +86 188 1746 8818
Tel: +86 21 3135 8722
patrick.gu@llinkslaw.com

Nigel Zhu Lawyer



Jianqi Yang Lawyer

Susan Deng