NEWSLETTER

NO.6 Apr.30 2019

CYBER-SECURITY AND DATA PROTECTION COMPLIANCE

www.changyanlawfirm.com

I. Domestic Legislative and Policy Development

1. On April 1, the Ministry of Industry and Information Technology issued the **Notice on Launching the Pilot Work of Electronic Verification of the Identity of Recorded Users of Internet Information Services**. The Ministry of Industry and Information Technology decided to carry out the pilot work of electronic verification of the identity of the ICP recorded entities from April 1, 2019 to December 31, 2019. The pilot work mainly includes the identity information collection of ICP recorded users and the submission of ICP recorded information verification form in an electronic way.

2. On April 1, 17 national standards by the National Information Security Standardization Technical Committee came into effect. These national standards include several important standards for information security technology, i.e. GB/T 36618-2018 Information Security Technology - Specification for Financial Information Service Security, GB/T 36619-2018 Information Security Technology - Naming Specification on Domain Names of Chinese Government Organs and Public Institutions, GB/T 36626-2018 Information Security Technology - Management Guide for Secure Operation and Maintenance of Information Systems.

3. On April 10, the Network Security Bureau of the Ministry of Public Security, the Beijing Network Industry Association, and the Third Institute of the Ministry of Public Security jointly issued the **Guidelines on the Protection of Internet Personal Information Security**, and formulated the management mechanism, security technical measures and business processes for personal information security protection applicable to enterprises providing services on the Internet, and organizations or individuals using private networks or non-networked environments to control and process personal information.

4. On April 15, the Ministry of Industry and Information Technology issued a **Guideline on Strengthening Industrial Internet Security (Draft)** for public comment. It is expected that by 2025, a relatively complete and reliable industrial Internet security system will be established.

5. On April 20, the draft of **Personality Right Section of Civil Code** was submitted to the Standing Committee of the National People's Congress for second review, which includes provisions on the protection of minors' personal information and the confidentiality of the privacy and personal information of the natural persons that the state organs and their staff knew during the performance of their duties. 【Brief Comments: The legislative work on personal information and privacy protection of minors has recently received more attention. In addition to this law, the Regulation on the Management of Programs for Minors implemented on the 30th of this month, also regulates the protection of minors' information privacy in radio and television programs and online audiovisual programs in many ways.】

6. On April 21, the Blue Book of Government under the Rule of Law – Development Report of Chinese Government under the Rule of Law (2018) was released. It proposes to extend the administrative remedies such as administrative compensation to personal data protection to encourage administrative agencies to strengthen the storage security and confidentiality of personal data.

7. On April 26, the State Council promulgated the Several Provisions on Online Government Services. It has 16 articles, which regulates the construction of a national integrated online government service platform, the confirmation of the effectiveness of electronic signatures, electronic seals and electronic certificates, data protection in the process of online government services, and other online government management practices.

8. On April 30, the Shanghai Municipal Government issued the **Shanghai Municipal Public Data Open Management Measures (Draft)**, which aims to provide public data open services by public management and service institutions for public data development and utilization, and clearly defines the requirement of "opening as the principle while not opening as an exception" and the principle of utilizing public data in a lawful and due process way with no harm to the legitimate rights and interests of the state, the society or third parties.

II. Domestic Administrative Law Enforcement News

1. On April 8, in order to further unblock the complaint channels for Internet information service users, the Information and Communication Administration of the Ministry of Industry and Information Technology guided the Internet Society of China to establish an Internet Information Service Complaint Platform operating online to accept complaints related to Internet information services, to determine strict time limits for handling complaints and to establish feedback

mechanism. The types of complaints accepted include service functions, personal information protection and corporate complaints mechanisms. The companies that have made access to the Platform include BAT, Jingdong, Suning, Vipshop, Meituan, Ctrip, and other leading e-commerce platform enterprises offering goods or services. 【Brief Comments: The Complaint Platform accepts complaints including personal information inquiry, correction, collection, use, deletion (account cancellation), etc., which is an important support for the provisions regarding personal information protection in laws and regulations such as the Cyber Security Law.】

2. On April 10, the General Office of the State Administration for Market Supervision issued a notice to deploy a special law-enforcement action of "Consumption Protection" and combating infringement of consumers' personal information across the whole country from April 1 to September 30, 2019 to create a safe and secure consuming environment.

3. On April 16, the Cyberspace Administration of China issued a notice that with regard to the industry chaos including disseminating illegal information, anonymous registration, fraudulent deception, providing platform services for offline illegal activities through instant communication tools, a special rectification action is launched recently on instant communication tools. The first 9 illegal apps such as "inbilin", "liaoliao" and "Metalk" were shut down. On the 28th, "tantan" app was removed from several Android application platforms.

4. On April 18, it was reported that since the Office of the Central Cyberspace Affairs Commission, the Ministry of Industry and Information Technology, the Ministry of Public Security, and the State Administration for Market Supervision guided to set up a special working group for rectifying illegal collection and use of personal information, more than 3,480 pieces of report information were received involving 1,300 apps by April 16. For 30 apps with large users and serious problems, the working group sent a rectification notice to their operators, requiring App operators to seriously rectify problems and report the rectification result to the working group within one month. If rectification is overdue, the working group will advise the relevant departments to expose the app publicly. If the circumstance is serious, the app will be removed from the platform and its service will be stopped. 【Brief Comments: The collection and use of user's personal information should follow the principles of legality, due process and necessity, and should meet the requirements of obtaining users' consent, informing the user of the scope of information collected or used and the aim thereof, and the withdrawal mechanism.】

5. On April 22, it was reported that the Wuhan Branch of the People's Bank of China announced the administrative penalty for the Bank of Communications International Trust Co., Ltd., which was fined RMB 290,000 for "inquiring personal information and corporate credit information without consent". 【Brief

Comments: According to Article 40 of the Regulation on the Administration of Credit Investigation Industry, the institution that provides or inquires information to the financial credit information basic database which inquiries about personal information or credit information of the enterprise without consent, illegally provides or sells information, discloses information due to negligence etc., will be fined ranging from 50,000 yuan to 500,000 yuan, and its responsible person may be subject to civil and criminal liability.】

6. On April 24, the national cyberspace administration system interviewed 685 websites, warned 248 websites, suspended the update of 125 websites, canceled the illegal websites' permission or filing with the telecommunications authorities, closed 2,087 illegal websites, and transferred 286 pieces of clues of relevant cases to judicial organs. The relevant websites closed more than 89,000 illegal account groups in accordance with their user service agreements.

7. On April 26, the National Copyright Administration, the Cyberspace Administration of China, the Ministry of Industry and Information Technology, and the Ministry of Public Security jointly launched the "Sword 2019" special campaign against Internet infringement and piracy.

III. Domestic Judicial Cases

- **The former official of the Industry and Commerce Bureau was arrested for taking advantage of position to obtain citizens' personal information and selling them.**

On April 7, the Jingshan Municipal Procuratorate of Jingmen approved the arrest of the criminal suspect Zhang for allegedly infringing citizens' personal information. As an official working at an Industry and Commerce Bureau, Zhang took advantage of position to download a large amount of personal information and sold them through the Internet. Through forensic examination entrusted by the public security organ, it is confirmed that since April 2017, Zhang has extracted and downloaded more than 50,000 pieces of personal information and obtained illegal benefits of more than 230,000 yuan.

- **Tai'an court tried a case involving 63 persons suspect of infringing citizens' personal information.**

On April 10, the case of infringing citizens' personal information by 63 people including Yu was publicly heard in the first instance court of Feicheng Court in the city of Tai'an. This case involved the most persons among this type of criminal cases in this court in recent years. From 2017 to 2018, the defendant Yu and other 62 defendants used WeChat and other online platforms to buy and sell various kinds of citizens' personal information such as household registration information, credit information, and owner information of phone numbers, and illegally profited more

than RMB 400 million. The case is currently under trial.

- **A former employee of 58 Tongcheng illegally obtained resumes and was sentenced for infringing citizens' personal information.**

On April 10, it was reported that Sun, a former 58 Tongcheng employee, worked for the companies Ganji and then 58 Tongcheng since December 2014. During this period, Sun took advantage of work to illegally obtain more than 646,000 resumes of job seekers through various means, and provided, sold them to many people. When the case was exposed, Sun gained illegal profits more than RMB 20,000. The Shanghai Xuhui Court finally found Sun guilty of the crime of infringing citizens' personal information and sentenced him to four years and six months in prison with a fine of RMB 10,000.

- **Insulting traffic policeman through live webcast, the suspect was arrested.**

On April 11, the Cyberspace Administration of Shouyang County together with the Cybersecurity Brigade of the Public Security Bureau and the Chaoyang Police Station jointly investigated the case of publicly insulting traffic policeman on the Internet and arrested one suspect. The criminal suspect publicly released the speech and video insulting traffic policeman three times in the live webcast. The video spread rapidly through the Internet, causing many Internet users' attention, with a bad social impact. Li was criminally detained by the Public Security Bureau for suspicion of the crime of creating disturbances.

- **Baidu sued Toutiao for stealing a large amount of search contents, claiming a compensation of RMB 90 million and requesting an apology for 30 days.**

On April 26, Baidu officially claimed that it sued Toutiao (Beijing Byte Dance Technology Co., Ltd.) for unfair competition to Beijing Haidian District People's Court because Toutiao stole a large number of Baidu "TOP1" product searching results including the TOP1 searching results which most match user's demands through Baidu's advanced algorithms and historical data mining, and the TOP1 searching results which cost Baidu a lot to operate with eco-partners. Baidu requested Toutiao to immediate stop infringement and make compensation for Baidu's economic losses and reasonable expenses in total of RMB 90 million, and to apologize on its APP and website homepage for 30 consecutive days.

- **Former employee of Dji leaked company's code and was investigated for criminal responsibility.**

On April 28, it was reported that a Shenzhen court made a first-instance judgment on the Dji source code disclosure case. According to the investigation, Dji's former employee uploaded the code under the company's confidentiality measures to the "public warehouse" of GitHub through a computer instruction, causing the disclosure of source code and triggering serious loopholes. The disclosed source code caused

economic losses of RMB 1.164 million to the company. The employee was sentenced to six months in prison for infringing trade secrets and was fined RMB 200,000.

【Brief Comments: Source code is often one of the most important trade secrets of high-tech enterprises, with high commercial value. Improving the trade secret protection system and strengthening the training of employees' confidentiality awareness are important measures for modern enterprises to protect their own rights and interests and improve their market competitiveness.】

- **Baidu's former employee hopping to the competing company was arrested by the police, suspected of stealing trade secrets.**

On April 28, it was reported that a former Baidu employee who had breached the non-competition agreement and hopped to the competing company was under compulsory measure taken by the police for suspicion of criminal offence. Rumor has it that after breaching the agreement and working for the competing company, the employee concealed the truth and continued to defraud Baidu of compensation for non-competition by means of colluding with the new company. This person was arrested for defrauding Baidu of compensation for non-competition and stealing trade secrets.

IV. Domestic and Foreign Important Industry News

1. On April 3, US cybersecurity company UpGuard found that hundreds of millions of Facebook users' information records were stored on the Amazon AWS cloud computing server, which could be easily and publicly accessed by anyone. The Facebook spokesperson acknowledged to the mainstream media that the users' multiple sets of personal data were stored in the Amazon AWS database. Once notified of this issue, the company deleted the problematic database with Amazon.
   【Brief Comments: The development of virtual machines and cloud services has greatly reduced the operating cost of network companies and improved operational efficiency, but the information security issues shall not be underestimated. Cloud operators and users are paying more and more attention to technical protection and legal compliance of cloud security.】

2. On April 8, the British government issued the Online Harm White Paper, proposing legislation to strengthen self-regulation of online platforms such as social media to protect users from harmful content, including child abuse images, cyberbullying, extreme thoughts and terrorist attacks. The new legislation will apply to any platform that allows users to share content and communicate online with others. If the company running the platform fails to do so, it may be subject to fines and the senior executive will assume personal responsibility.

3. On April 9, Facebook agreed to change its misleading terms of service required by the European Union and consumer protection agencies in some countries. In

the disclosed promise, Facebook clarifies to the users how the platform uses the user's personal information for targeted advertisement to make money, and clarifies that if "without proper professional investigation", it may be responsible for abusing these data. In addition, Facebook revised the rules on liability restrictions, unilaterally changing terms, and temporarily retaining contents deleted by consumers. On the 18th, Facebook admitted that the passwords of millions of Instagram users were stored in the internal server log in clear text and were closely watched. On the 24th, Facebook announced the financial report for the first quarter of 2019. The company estimates in the financial report that the US Federal Trade Commission (FTC) may impose a fine of $3 billion to $5 billion on Facebook for processing users' data. 【Brief Comments: The supervision and punishment that Facebook faced in Europe and the United States have sent a warning signal. China's Internet and technology-based enterprises must pay attention to local regulations and requirements related to information protection, data compliance and cybersecurity in the process of "going out".】

4. On April 10, Yahoo paid for the previous data breach accident and accepted a settlement of up to $117.5 million to reach settlements with millions of victims in this case. This case affected approximately 3 billion accounts between 2013 and 2016, with $117.5 million being the largest compensation ever in data breaches. 【Brief Comments: The cost of violation of data information protection is huge, and the establishment of an internal compliance system helps to control this legal risk from both the root cause and the result (recognition of responsibility and judgment of penalty amount).】

5. On April 14, a series of activities regarding 5G demonstration zone were held in Guangzhou, Guangdong Province. The China Academy of Information and Communications Technology, the Guangzhou Development Zone Management Committee and Huawei jointly signed the "Cooperation Agreement on Joint Construction of 5G Demonstration Zone".

6. On April 22, the US Federal Bureau of Investigation's Internet Crime Complaint Center released the 2018 Internet Crime Report, which showed that the number of complaints about Internet crimes increased by 14.3% in 2018, resulting in losses of more than 2.7 billion US dollars, which is nearly twice of that in 2017.

Bo XIAO

Changyan Shanghai Office
Executive Director

E-mail: xiaobo@changyanfirm.com

Dr. Bo Xiao earned his Ph.D. degree in Law from Fudan University, his LL.B. and LL.M. degrees from the People's Public Security University of China, and has worked as a judge in the People's Court of Pudong District, Shanghai for more than 13 years. He has tried over 1,000 cases. Dr. Xiao later joined Zhong Lun Law Firm as a Partner, and accumulated rich experience in defending criminal cases and handling corporate crisis. Dr. Xiao's practice area includes criminal defense, regulatory and anti-bribery, crisis-management, white-collar crime, dispute resolution, especially in the financial industry, capital market and TMT industry. Dr. Xiao published numerous articles in criminal defense field.

Justin CAI

Changyan Shanghai Office
Vice Executive Director
and Senior Partner

E-mail: justincai@changyanfirm.com

Mr. Justin Cai earned his LL.M. degrees respectively from Duke University and Fudan University. Mr. Cai has over 16 years' work experience in leading international/Chinese law firms such as King and Wood, Zhong Lun, Weil Gotshal and MWE China (McDermott Will & Emery), and has provided legal services to numerous Fortune 500 companies. Mr. Cai's practice areas include cross-border investment, compliance (cyber-security law, data protection, anti-bribery, FCPA etc.), intellectual property rights protection, start-up company financing and real estate transactions.

Guo RONG

Changyan Shanghai Office
Associate

E-mail: rongguo@changyanfirm.com

Ms. Guo Rong earned her LLM degree and LLB degree respectively from Sun Yat-sen University and Nankai University. Ms. Rong has over 5 years' work experience in law. Before joining Changyan Shanghai Office, Ms. Rong had been working as in-house counsel in Netease., Inc and KWG Group. Ms. Rong's practice area includes TMT industry, logistics of E-commerce, real estate and dispute resolution.

Serene HUANG

Changyan Shanghai Office
Associate

E-mail: serenehuang@changyanfirm.com

Ms. Huang earned her LLM and LLB degrees respectively from the Chinese University of Hong Kong and the Southwest University of Political Science and Law. She had been an exchange student at Ghent University for nearly half a year. Before joining Changyan, she had been an in-house counsel for two years at China Merchants Bank, Wuxi Branch and has experience in compliance review.