NEWSLETTER

NO.4 Mar.15 2019

CYBER-SECURITY AND DATA PROTECTION COMPLIANCE

I. Legislative Development and Law Enforcement

【Legislative Development】 On March 13, the State Administration for Market Regulation and the Cyberspace Administration of China issued the "Announcement on the Implementation of App Security Certification" and the "Implementation Rule of Mobile Internet Application (App) Security Certification", which encourage App operators to voluntarily pass the App security certification, and specifies the certification body, certification procedures and other details.

Comments: In response to the illegal collection and use of personal information by App, the State has carried out special governance since the beginning of this year, and issued a series of rules and regulations including the above documents. This issue also attracted great attention during the Two Sessions and the CCTV 3·15 evening party held this month. From the perspective of corporate compliance, it is foreseeable that App operators' regulation and risk control for collecting and using personal information for their products will gradually spread forward to the product development stage, and throughout the entire product development and operation.

【Legislative Development】 On March 4, Zhang Yesui, spokesman of the Second Session meeting of the 13th National People's Congress, said that the Standing Committee of the National People's Congress has included the drafting of personal information protection law into this term's legislative plan and will promote other legislation in the field of data security.

Comments: China's legal regulation of personal information protection is currently scattered in the Criminal Law, the Cyber Security Law and other laws and regulations and other normative documents. Under the legislative trend of strengthening the protection of citizen information and privacy in all countries, the "Personal Information Protection Law (Draft)" was published in 2017, and the legal profession raised some concerns over the classification of personal information, the balance between the protection of personal information and the development needs of the big data industry, and the relationship between this law and the previously issued low-level legal documents in various fields. In addition, in the past two years, European and American countries have more and more practical experience in the implementation of personal privacy protection and social effects thereof, which may have an impact on the formulation of provisions of this Law.

【Policy News】 On March 5, in the Government Work Report, Premier Li Keqiang repeatedly mentioned network, data, AI and other aspects related to cyber security and data compliance. The Report made it clear that the government's work tasks in 2019 include persistence in innovation to lead development, fostering and growing new growth drivers, promoting transformation and upgrading of traditional industries through Internet information technologies and other means, promoting the accelerated development of emerging industries such as big data and AI, improving the support of science and technology and encouraging innovation. Li affirmed the achievements of introducing "Internet +" in the fields of industrial upgrading and reform and reform of government service, and made it one of the 2019 missions to introduce "Internet +" in market regulation, emerging industry development, education, medical and health fields, spiritual civilization construction, and party conduct and clean government construction.

【Law Enforcement News】 On March 7, the Ministry of Public Security held a press conference in Beijing to inform the public the result of "Clean Net 2018" special action conducted by security organs of the whole country. During the special action, a total of 57,519 cybercrime cases were detected, and 83,668 suspects were arrested. For websites and high-risk application services with outstanding harmful information, the security organs organized 144,000 times of safety supervision and inspections, found and rectified 1.346 million safety risks and management problems, and investigated and handled more than 34,000 Internet companies. In response to the law violations of APPs, more than 35,000 APPs with malicious programs and malicious acts were cleaned up according to laws. For key areas such as online games, webcasts, short web videos, and online media, 104 related companies were investigated and handled according to laws. In view of the current situation of the wide spread of illegal and criminal information, more than 4.29 million illegal information were found and cleared, more than 20,000 illegal websites (columns) were closed, and 365 illegal websites with outstanding illegal information were listed for rectification.

【Law Enforcement News】 On March 12, the Ministry of Education issued the "Key Points of Education Informationization and Network Security Work in 2019", mentioning that the Ministry of Education will conduct joint operations with the network department to govern the chaos of campus APPs, to regulate the introduction of third-party campus APPs and the independent development of campus APPs, to explore the establishment of a long-term mechanism to regulate the management of campus APPs, and to promote the orderly and healthy development of mobile Internet.

【Law Enforcement News】 On March 15, the CCTV 3·15 evening party exposed a series of illegal activities or real risks involving network security, data compliance and privacy protection, including 1) probe box, by discovering user's mobile phone Wi-Fi signal, to identify a user's mobile phone number and collect a user's personal big data information, plus the use of harassing calls to make profits, 2) bank card with "flash payment" function may be stolen, and 3) 714 online loan APPs displayed by the financial search platform, etc. After the evening party was broadcast, it caused great influence. The Ministry of Industry and Information Technology immediately deployed, ordered the relevant enterprises to stop violations of laws and regulations and to conduct verification, required the application store

to remove the APPs involved in the cases, organized the inspection and rectification of similar products.

II. Chinese and Foreign Typical Cases

Domestic Typical Cases

- **Shanghai Office of Cyberspace Administration made an administrative punishment on "Wall Street News".**

On March 4, the official WeChat Account of Shanghai Office of Cyberspace Administration issued a message saying that an administrative punishment was imposed on "Wall Street News". The "Wall Street News" website (https://wallstreetcn.com/) and APP operated by Shanghai A Niu Information Technology Co., Ltd., in the absence of Internet news information service qualifications, illegally posted news information, and the content orientation was biased, disrupting the order of network information dissemination. The Shanghai Office of Cyberspace Administration decided to impose a fine on Shanghai A Niu Information Technology Co., Ltd.

Comments: Every online media and WeChat official account must pay special attention to the accuracy of the content when posting (especially reposting) news. It should not be taken out of context or misleading. Otherwise, it is easy to be considered as disrupting the order of network information dissemination. If news is to be published first and independently, special attention should be paid to qualification certificates.

- **"Big data killing" exposed in ticket price, Ctrip said it was caused by a system bug.**

A Weibo user exposed that tickets were sold out when re-searching on Ctrip. He re-selected the ticket, but found the total price was nearly RMB1,500 higher. However, he found that the airline's official website showed tickets were still on sale. The phenomenon of big data killing was suspected to appear on Ctrip again. On the morning of March 11, Ctrip issued an apology statement on this matter, saying that the second payment showing no ticket was caused by the system bug, and there was no big data killing. Ctrip said that after the preliminary statistics, the bug will only affect a small number of users when the ticket volume is tight, affecting about 1,300 users with about 100 successful orders. Ctrip will take the initiative to contact the customer one by one to bear the users' losses caused by it.

Comments: The illegality of "big data killing" (i.e. big data analysis brings price cheat on long-term customers) caused hot discussions in the past two years. It is suspected of violating the Consumer Rights Protection Law, Price Law, Telecommunications and Internet Users' Personal Information Protection Regulations, and other laws and regulations. Finally, the first paragraph of Article 18 of the Electronic Commerce Law has the corresponding provision: *When providing the results of search for commodities or services for a consumer based on the hobby, consumption habit, or any other traits thereof,* ***the e-commerce business shall provide the consumer with options not targeting his/her identifiable traits and respect and equally protect the lawful rights and interests of consumers***. Once this provision is violated, the business shall be ordered to

correct within a time limit, and the illegal income shall be confiscated. Fine can be imposed between RMB 50,000 and RMB 500,000 according to the circumstances. Therefore, operators should take full account of the compliance of their final results when making algorithm settings.

Foreign Typical Cases

- **Facebook filed lawsuits against four Chinese sellers selling fake accounts and good comments**

On March 1, Facebook announced that it and Instagram had filed lawsuits against four Chinese companies and three individuals in the federal court, alleging that the defendant sold fake accounts and likes and buying followers, and infringed their trademark rights on the website, as well as squatting Facebook domain names. Facebook accused the defendants of selling a fake account in violation of its terms of service, using its trademark to squat domain names and conduct fake account promotion in violation of the US Lanham (Trademark) Act and Anti-cybersquatting Consumer Protection Act, requiring the defendants to pay $100,000 and stop the infringement.

- **US prosecutors conduct criminal investigations on data transactions between Facebook and other technology companies**

On March 13, it was reported that a grand jury in New York, USA, had launched an investigation and summoned at least two large companies engaged in smartphone manufacturing. More than 150 Facebook partners are said to have access to millions of Facebook users' personal information, including Amazon, Apple, Microsoft and other large technology companies. Facebook entered into deals with these companies to help them build Facebook apps on their phones and tablets and integrate Facebook functionality into their operating systems. For example, users can share photos directly with Facebook friends without having to directly access Facebook apps or websites. In order to make these integration functions work, Facebook need to give these companies user data permissions through a so-called private API. These companies could have direct access to user data, including a list of friends and contact information without the user's consent.

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.