NEWSLETTER

NO.5 Mar.31 2019

CYBER-SECURITY AND DATA PROTECTION COMPLIANCE

I. Domestic Legislative and Policy Development

On March 22, the Central Bank issued the "Notice on Further Strengthening the Payment and Settlement Management to Prevent the New Emerging Crimes of the Telecommunications Network", which aims to improve the emergency stop and fast freeze mechanism, strengthen the real-name management of accounts, strengthen the management of transfers, and strengthen the management of special merchants and receiving terminals.

On March 26, according to the introduction by the official from the Network Security Bureau of the Ministry of Public Security, the Standard of Network Security Protection Level 2.0 is expected to be introduced in April this year.

On March 27, the Advertising Supervision and Management Department of the State Administration for Market Regulation issued the "Notice on the In-depth Implementation of Internet Advertising Rectification", and deployed local market supervision bureaus to carry out Internet advertising rectification work in order to maintain the high pressure of rectifying false and illegal Internet advertisements and to create a good environment for the Internet advertising market.

II. Domestic Administrative Law Enforcement News

On March 20, the Market Supervision Administration Bureau of Tongjiang County, Sichuan Province imposed a fine of 250,000 yuan on the Meituan Take-out for it forced merchants to "pick one out of two". According to the investigation, the Meituan Take-out used its market advantageous position to repeatedly require the networked merchants and the newly networked merchants to sign exclusive agreements, and not to carry out same or similar business cooperation with other competitive third-party platforms. This behavior forced many networked merchants to abandon other take-out platforms and was recognized as unfair competition. 【Brief Comment: Platform companies with market advantageous position should pay special attention not to abuse market dominant position, and should be particularly cautious

about the terms of the merchant cooperation agreement, otherwise it would be easy to be considered against the Anti-Unfair Competition Law and the Anti-Monopoly Law.】

On March 24, the Beijing Police reported the phased result of "Net Cleaning 2019", which organized mobile application stores to clean up more than 20,000 illegal applications and to shut down more than 400 illegal applications.

On March 24, the Wuhan Police announced that they solved the case where a service platform of the auto financial service company was violently cracked and 300,000 pieces of user information was stolen and sold on the dark net.

On March 27, Qiaoda Technology, a recruitment data company with the largest resume database in the country, was exposed that all of its persons were taken away by the police. The company once claimed to have established multidimensional data of 800 million Chinese people by integrating up to 220 million natural persons' resumes, 1 billion address books, 10 billion ID combinations for user identification and more than 100 billion user aggregates. At present, Qiaodazhao official website and all the websites belonging to it were unable to log in. The company may be guilty of infringing citizens' personal information. 【Brief Comment: Data processing companies should pay special attention to the legality of sources of information when collecting citizen's information, and must apply pseudonymisation in data processing, otherwise it is very easy to violate the criminal law.】

III. Domestic Judicial Cases

- **The gang who collected vehicles' tracks for extortion are prosecuted.**

On March 19, the Tianxin District Court of Changsha City held a trial of a crime of infringing citizens' personal information. From November 2017 to March 2018, Li gathered several people and provided the positioning device, while others were responsible for the installation. They collected the victims' tracks through positioning devices installed on the bottom of vehicles, and planned to threaten the victims with exposing their privacy in order to extort money from them. The four people illegally collected 173 pieces of information of victims. The public prosecution agency believes that four persons including Li illegally obtained information on others' tracks with serious plot, so the criminal responsibility should be pursued for the crime of infringing on citizens' personal information. 【Brief Comment: This case is also of reference value for application software. When a merchant uses software to locate a user, it must obtain the user's express consent and must not illegally provide the user's location to a third party, otherwise it may be considered as infringing the citizen's personal information.】

- **The first outcome of the Tou vs. Teng war: Douyin was called to stop providing WeChat user authorized login service for Duoshan.**

On March 20, the Tianjin Binhai New Area Court announced the ruling of the case where Douyin and Duoshan are suspected of illegally using users' data, that Douyin was requested to immediately stop using users' avatars, nicknames from the WeChat/QQ open platform when recommending friends to Douyin users and stop providing user authorized login service of WeChat/QQ open platform for Duoshan. Meanwhile, Duoshan is requested to stop using WeChat/QQ users' avatars, nicknames obtained from Douyin by Duoshan without users' consent. Toutiao is not satisfied and alleged to file a reconsideration later. 【Brief Comment: The focus of this case lies in that whether the user's nickname and avatar data on the WeChat/QQ open platform belong to the user or Tencent. Is it a personal privacy issue? What kind of rights does Tencent enjoy as to the user's avatar? The current ruling is only a behavioral preservation ruling. We will continue to pay attention to this case.】

IV. Domestic and Foreign Important Industry News

On March 16, TechCrunch reported that China's cross-border e-commerce platform Gearbest leaked millions of users' personal information and shopping information.

On March 16, Facebook shared user data with more than 150 companies, including allowing third parties to directly access Facebook users' friends lists, contact information, etc. without the user's explicit consent. The US government is conducting criminal investigation on its data transactions. 【Brief Comment: APP operators should pay special attention to obtaining users' explicit consent and giving them the right to refuse before sharing user information with third parties.】

On March 17, TechCrunch reported that Meditab, a US health technology company, leaked a large amount of personal medical health information due to the lack of good protection of the fax server, and may face huge fines.

On March 17, Uber was sentenced to no criminal liability in the case of an Uber self-driving car crashing into a pedestrian in Arizona of the USA. The police will investigate into the driver who was responsible for safety on the car.【Brief Comment: The legitimacy and morality of the AI algorithm will be a difficult problem for human society.】

On March 20, the EU anti-monopoly regulator imposed a fine of 1.49 billion euros on Google for unfair competition on the grounds that Google abused its market dominant position and imposed some restrictive clauses in its contracts with third-party websites to prevent competitors from placing search ads on these sites.

On March 22, Finland's unconfirmed number of Nokia 7 Plus phones sent sensitive data including location, SIM card numbers and mobile phone serial numbers to Chinese servers. Finland has launched an investigation into this. The manufacturer HMD later clarified that the incident was entirely caused by human error and did not endanger the personal information of the user.

On March 22, Aqniu released the first security application guide of video surveillance to ensure that monitoring data will not be leaked or modified.

On March 27, the Shanghai Consumer Rights Protection Committee held a conference on the evaluation results of personal information protection for online shopping, travel and life services applications. In the initial evaluation, among 39 mobile apps, 14 apps have sensitive permissions corresponding to the actual functions while the remaining 25 apps excessively collects personal information of mobile phone users.

On March 29, the dark-net market Dream Market announced its website would be closed on April 30. On the same day, the Europol, the FBI and the United States Drug Enforcement Agency announced a massive strike against dark-net drug smuggling and executed dozens of arrests.

On March 30, it was reported that the Committee on Foreign Investment in the United States (CFIUS) asked Beijing Kunlun Tech Co., Ltd. to sell its previously acquired same-sex dating application Grindr on the grounds of threatening US national security. It is said that the US government is worried that the data information of this software application may be used to extort Americans. 【Brief Comment: Data compliance survey will become an important part of cross-border transactions.】

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.