昌言（上海）律师事务所 CHANGYAN (SHANGHAI) LAW FIRM

NEWSLETTER

NO.2 Jan 16, 2019 – Feb 15, 2019

CYBER-SECURITY AND DATA PROTECTION COMPLIANCE

I. Chinese and Foreign Legislative Developments

Domestic Legislative Developments

- *Guidelines for the Construction and Promotion of Industrial Internet Networks, Ministry of Industry and Information Technology released on January 18*

  The Ministry of Industry and Information Technology released the *Guidelines for the Construction and Promotion of Industrial Internet Networks*, clearly proposing to build an industrial Internet benchmarking network and innovative network applications, develop order and accelerate the cultivation of new technologies, new products, new models and new formats, with the goal of constructing a network infrastructure that supports the industrial full factors, the entire industry chain, and the full value chain. By 2020, a relatively complete top-level network design of the industrial Internet will be formed.

- *Notice on the Special Governance of Applications' Illegal Collection and Use of Personal Information, four departments of the Cyberspace Administration, the Ministry of Industry and Information Technology, the Ministry of Public Security and the General Administration of Market Supervision jointly issued on January 25*

  This special governance will evaluate an Application's privacy policy and the collection and use of personal information closely related to people's lives, strengthen the supervision and punishment of collecting and using personal information in violation of laws and regulations, and carry out voluntary Application personal information security certification, encourage search engines, app stores, etc. to clearly mark certification and prioritize recommending certified Applications.

- *Ministry of Industry and Information Technology announced 54 standards for communications industry on January 25*

The above industry standards include *Internet Access Log Retention Test Method Part 1: Internet Service Provider - Cable, Operation Guide on Information Security Management System of Internet Access Service, Technical Requirements of the Security of Internet Users' Account Management System, Competence Requirements of Recovering Information System Disaster*, etc.

- *Regulation on the Prohibition of Abuse of Market Dominant Position (Draft for Comments), the State Administration for Market Regulation issued on January 30*

For the first time, the Draft for Comments incorporates data monopoly into the anti-monopoly legal system, and stipulates the market dominant position of Internet operators. In addition to the consideration of market share occupied by operators, the characteristics of competition, business models, network effects, technical characteristics, market innovation, mastering relevant data in the relevant industries, and market power of operators in the relevant market should also be taken into consideration.

- *Information Security Technology - Information Identification Specification of Social Network Platform and Information Security Technology - Personal Information Security Specification (Draft for Comments), the National Information Security Standardization Technical Committee issued on February 1*

The former specification regulates the security management of information identification by the social network platform, and puts forward requirements for the management processes of generation, use, storage, transmission and destruction of information identification. The latter specification distinguishes between basic business functions and extended business functions, and raises new compliance requirements of accesses to third parties, convergence and integration of personal information, etc.

Foreign Legislative Developments

- On January 23, the **European** Commission made a decision on the adequacy of Japan. The EU-Japan Data Sharing Agreement came into effect. This means allowing personal data to flow freely between two economies on the basis of strong data protection.

- On January 24, the **European** Data Protection Supervisor (EDPS) released its Annual Management Plan 2019, calling for establishing a new culture of data protection in 2019, i.e. de-bureaucratising wherever possible, arguing against useless procedures but reinforcing meaningful safeguards for the individuals affected by personal data processing.

- On January 25, **Japan** approved a new amendment to allow government officials to invade citizens' personal devices as part of security investigation of the Internet of Things. The amendment is mainly aimed at protecting the Olympic Games to be held in Japan in 2020.

- On January 30, the **US** Congress updated the report on AI and National Security. The report pointed out that artificial intelligence (AI) has received much attention recently. No matter whether it is commercial or military, the money from government and the hot money from private investor is surging. Military trade-offs need to be done to control development. The promotion from the Congress will determine the future development of AI.

- On February 6, the **EU** recently made a decision to interlink the fragmented border security databases, so that border guards, police officers can find the personal information of entrants on a single screen. At the same time, they will also specifically create a database of biological information of non-EU citizens for identification.

- On February 11, President Trump of the **USA** signed an executive order to officially launch the American Artificial Intelligence Initiative to stimulate investment and development in the field of artificial intelligence (AI) in the USA.

- On February 13, the **EU** decided to amend the copyright law to protect original content. According to the new law, Google, Facebook and other online information platforms need to pay the media when they grab the full text of the news. In addition, content platforms such as YouTube are required to pay a higher fee to creators when providing original content.

II. Chinese and Foreign Typical Cases

Domestic Typical Cases

- *First case of the data right of comment was pronounced in China*

In April 2017, Du Chao, Qiu Xiuzhen and Zhang Meiling colluded to extort money from the Taobao store five times by means of asking for payment to delete bad comments, involving a value of RMB 20,400. The case was criminally pronounced on November 7, 2017. The court found that the three defendants were guilty of extortion. Among them, Du Chao was the principal offender and the other two were accomplices. On January 17, 2019, a civil judgment was issued. The court held that the three defendants

objectively caused the relevant data on the Taobao platform untrue, which directly affected and undermined the credit evaluation system constructed by Taobao, and damaged the legal civil rights of Taobao Company. Du, Qiu and Zhang respectively compensated Taobao for 1,000 yuan, 6,000 yuan and 4,000 yuan.

- *Bug appeared on Pinduoduo platform with tens of millions of coupons stolen*

  In the early morning of January 20, a black-and-grey gang stole coupons worth of tens of million yuan from the Pinduoduo platform through a bug of expired coupons and made unjustified profits. In response to this behavior, Pinduoduo fixed the bug immediately, traced the source of orders involved in this case, and also reported it to the public security.

- *Nanjing cracked the first domestic case of infringement of personal information through technical positioning*

  Wu cracked a location information protection system of a mobile chat program, developed a new positioning software, and sold it through online channels. The amount of money involved in this positioning software case is more than 400,000 yuan in two years. Many domestic black gangs and evil gangs are also using this positioning software to carry out illegal criminal activities such as illegal detention and intentional injury.

  According to media reports on January 25, Wu was transferred for examination before prosecution for being suspected of providing procedure or instrument dedicated to invade computer information system. The other two were transferred for examination before prosecution for being suspected of infringement of citizen's personal information due to frequently illegal use of this software to locate other people.

- *On January 26, Ningbo cracked the case of infringement of citizens' personal information that 8 persons sold tens of thousands of information of vehicles.*

Foreign Typical Cases

- On January 21, the French data regulator issued the first GDPR ticket, which imposed a fine of 50 million euros (or about 366 million yuan) on the US search giant Google.

- On January 22, according to media reports, the New Jersey prosecutor sued 26-year-old Oleksandr Ieremenko and 27-year-old Artem Radchenko. The two were accused of sneaking the transaction information from the EDGAR filing system of the US Securities and Exchange Commission (SEC), illegally profiting more than $250,000 US dollars. They were accused of security fraud, telecommunications fraud and computer fraud and complicity.

- On January 28, US courts said banks and individuals affected by the 2017 Equifax information disclosure could start suing Equifax, while small enterprises may need

to suspend prosecution unless they can prove that the information disclosure had a direct negative impact on themselves.

- On January 30, the governor of the Bangladesh central bank said that the country will file a lawsuit against a Philippine bank, Rizal Commercial Banking Corp (RCBC), in New York, because the bank participated in a historically largest online robbery.

- On January 31, the US media NBC reported that the FBI recently arrested a Chinese Apple engineer, Jizhong Chen. Thousands of Apple's business secret documents were found in his computer.

- On February 3, the German antitrust agency (Bundeskartellamt) ruled that Facebook abused its market dominant position and collected users' information without the users' knowledge or consent. On February 7, it ordered a crackdown on Facebook's data collection.

- On February 5, the European Commission recently announced the recall of a German-made children's watch: ENOX Safe-Kid-One. The watch was complained by Icelandic users that it was able to secretly monitor children in violation of Icelandic customer protection regulations.

- On February 15, the US Federal Trade Commission (FTC) and Facebook were negotiating a multi-billion dollar fine because the company failed to protect users' data. If the negotiation is successful, the agency's investigation into Facebook's privacy infringement will come to an end.

III. Industry Information

- In mid-January 2019, the venture capital investment company Strategic Cyber Ventures (SCV) released a report 2018 Cybersecurity Venture Capital Investment on the financing of venture capitals in the security industry in 2018. The results of the survey show that the financing has exceeded 5 billion US dollars in 2018, but this momentum is not sustainable in 2019.

- On January 16, a 3TB data leakage happened to the Oklahoma Securities Commission of the United States, including millions of materials of surveys conducted by FBI on some enterprises over several years. The reason for the leak was that the server storing the information lacked password protection.

- On January 16, the Wales government, the Air France and the security company Thales Group of France will spend £20 million to establish a national digital

center in South Wales.

- On January 18, the largest data leak in history broke out. The cloud storage server MEGA had nearly 773 million unique e-mail addresses and more than 21.22 million unique passwords leaked. The span of leaked data is between 2008 and 2018.
- On January 22, Florence Parly, the Minister of the Armed Forces of France, declared that the cyber war had begun. She claimed that the European countries' military would use cyber weapons and set up a military bug bounty program.
- On January 24, the Cyberspace Administration of China cleaned up 7873 malicious mobile applications.
- On January 28, the blockchain information services' filing and managing system was put into operation. The Regulation on the Management of Blockchain Information Services was officially implemented on February 15, 2019.
- On February 2, the database of Rubrik, an IT security and cloud data management giant, leaked. The database stored tens of gigabytes of data, including the name and contact details of each client.
- On February 7, Carbonite, a cloud-based data backup provider, announced a plan to acquire the network security company Webroot for $618.5 million in cash.
- On February 13, GBG, an expert in identity data intelligence with its headquarter based in the UK, agreed to acquire IDology, an authentication and fraud prevention service provider based in Atlanta, for $300 million in cash.
- On February 13, it is exposed that 2.56 million people's personal data was leaked by SenseNets Technology Co., Ltd.
- On February 15, data packages of 617 million online account information of 16 websites were sold on the dark network recently. The publisher asked the buyer to pay in bitcoin, and the total selling price was about 20,000 US dollars.
- On February 16, a netizen released a video saying that the application of Jingdong Finance obtained users' sensitive images and uploaded them.

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 is very experienced in cross-border M&A, compliance (cyber-security law, data protection, anti-bribery etc.), government investigations, intellectual property rights protection, start-up company financing, real estate transactions and labor law.

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 working as an in-house counsel for two years at China Merchants Bank, Wuxi Branch. She mainly conducted legal and compliance review of banking businesses modes, contracts and internal regulations, and participated in demonstration of the legality of innovative products and major projects. She also had a legal internship in Hong Kong.