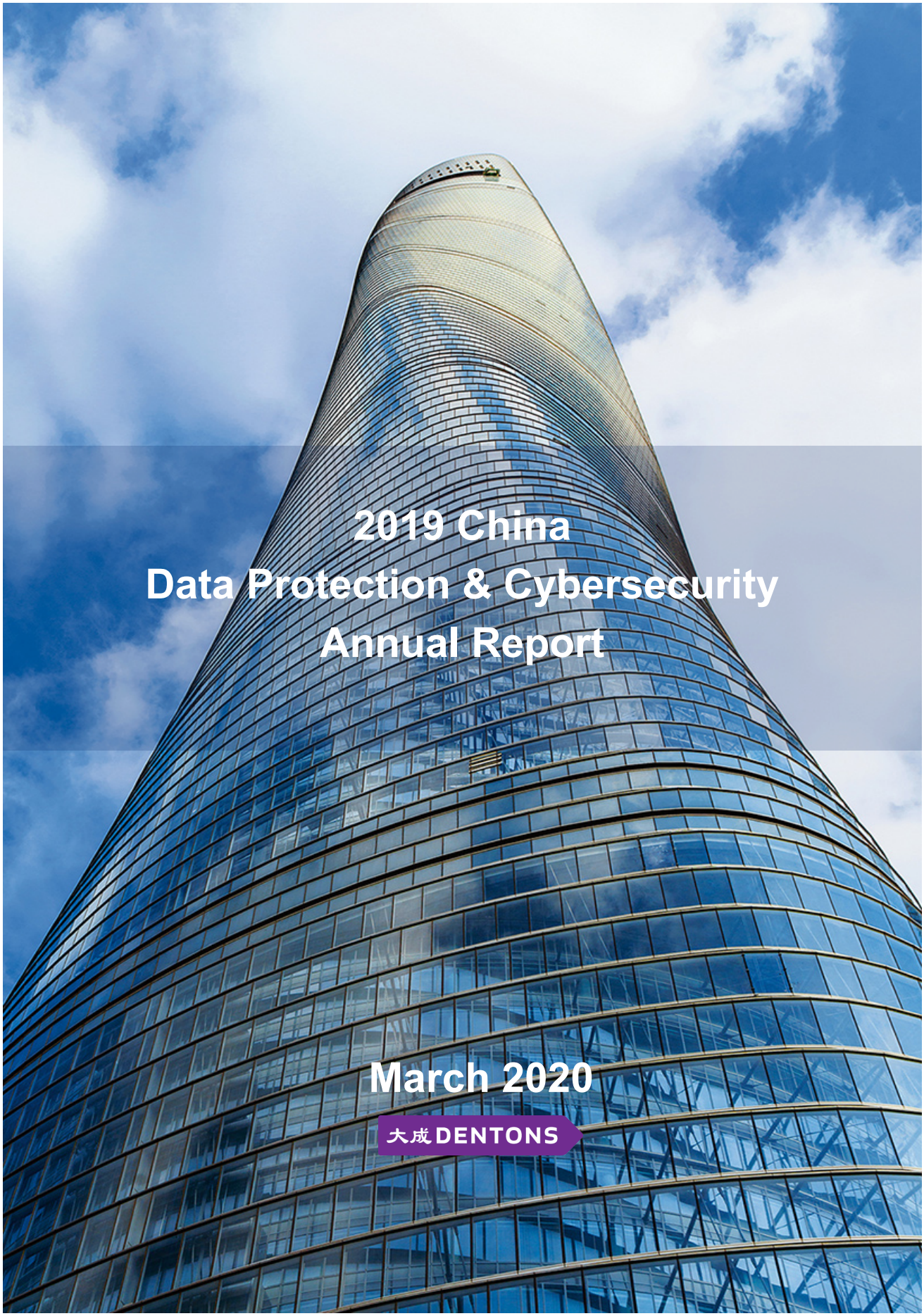

2019 China Data Protection & Cybersecurity Annual Report

March 2020

大成 DENTONS

EXECUTIVE SUMMARY

Increasingly Complex Legal Regime

Two years after the enactment of the Cybersecurity Law of China ("CSL"), various implementing regulations and standards continued to roll out throughout 2019. In the area of personal data protection, in mid 2019 a draft regulation on data localization requirement was released – the Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comments). While the CSL stipulates a general requirement of conducting security assessment for cross-border transfer of personal data collected by critical information infrastructure operators ("CIIOs"), the draft regulation provides in detail how the assessment should be carried out. It updates an older draft published in 2017 in which cross-border transfer of both personal data and important data were addressed. This draft regulation implies that personal data export will be handled separately from important data.

In the area of cybersecurity, the year 2019 marked the beginning of the so-called "Classified Protection 2.0" era. Classified Protection 2.0 refers to the cybersecurity protection baseline for network operators and a universal compliance framework under the CSL and is an upgrade of the previous information security system protection (commonly known as "Classified Protection 1.0") with broader application and further requirements on security level and compliance steps. A set of standards related to Classified 2.0 came into force in 2019.

Other important updates include a regulation specifically on children's personal data protection, or known as the Chinese version of "COPPA", that came into force on 1 October 2019; and the promulgation of the Encryption Law of China, which became effective on 1 January 2020 and will have a bearing on CIIO's use of commercial encryption.

More Active Public Enforcement

Without a single data protection authority in China, the public enforcement of data security in 2019 still presented a polycentric landscape and is great in number. Among the massive enforcement activities, quite a number of them are about personal data protection and directed at mobile Apps. The four central agencies – the Cyberspace Administration of China ("CAC"), the Ministry of Industry and Information Technology ("MIIT"), the Ministry of Public Security ("MPS"), and the State Administration for Market Regulation ("SAMR") – jointly launched a nationwide carckdown against the illicit collection and use of personal data by Apps, which lasted throughout 2019. Beyond this, each of the four agencies carried out additional enforcement activities also against personal data infringement. Most of the time, Apps that were found infringing person data would be ordered by the authorities to rectify without a penalty. In extreme circumstances, some Apps were pulled from its app store for a fixed period of time.

Non-negligible Criminal Enforcement

In 2019, the MPS has been cracking down on illegal sale of personal data, which led to huge amount of criminal prosecutions in this regard. Personal data infringement would give rise to criminal consequences of up to seven years' imprisonment in China. The liability could be imposed on individuals, or where an entity commits infringement, on the person in charge. On the other hand, illegal hacking was another significant aspect of criminal enforcement, usually when causing severe damages to information system or relevant database.

Private Litigation concerning Data

As in the past few years, private litigation remains a powerful weapon for big companies to gain legitimate access to customers' data, the most famous being the dispute between ByteDance and Tencent in 2019. The issue was about whether Tencent's permission to link its users accounts for one

app developed by ByteDance could be shared with another ByteDance app. The court held that ByteDance was not allowed to do so without Tencent's authorization under the Anti-Unfair Competition Law of China.

As to personal data infringement, it is still a very common type of civil disputes. Some interesting developments have been made in 2019. For example, a private action was brought by a professor who claimed that a system upgrade involving collecting facial data violated the Consumer Rights Protection Law. The civil dispute on face recognition is the first one of its kind in China. Also ByteDance was involved in another civil dispute litigating whether phone contacts are personal data, the upload of which requires informed consent.

Sectoral Regime of Data Protection & Cybersecurity

This report compiles updates of 2019 in different sectors, notably life science, finance, retail, transportation and IoT. As said, without a single data protection authority in China, sector-specific authorities and their rules are very important for players in this industry. And each sector may have very different focuses for data security. For example, following the high-profile case in 2018 of illegal export of genetic data, life science industry is exceptionally featured by the categorization of data involved, such as genetic data, healthcare big data, population data, which are all likely to be identified as important data and to entail stricter CIIO duties. On the other hand, for finance and retail industries, in 2019 the emphasis was still placed on personal data protection, though probably in different ways. For example, with the evolvement of the "new retail model", retailers pay more attention to obtaining informed consent from consumers to satisfy their marketing needs. When it comes to transportation or IoT, in 2019 cybersecurity was the central concern as indicated by various government policies.

Handling Regulatory Hurdles and Ensuring Compliance

This report also introduces typical business scenarios related to data security and corresponding compliance issues. Some scenarios are common across different sectors or different jurisdictions, such as privacy policy, employee privacy, data localization requirement, data breach incidents, but could be better tailored to China's CSL framework. Some scenarios are unique in China, for example, Classified Protection 2.0 and the use of VPN, which really requires an in-depth understanding of relevant rules

and enforcement practices. The others are often strategic business considerations but fresh new from a legal standpoint, e.g. privacy by design, data crawling, data aggregation, and intersection between big data and competition law. Similar to the rest of the world, Chinese laws are relatively lagging behind digital transformation, but we try to provide a big picture of how these issues are treated in China so far.

Road Ahead: Challenges and Opportunities

Following the implementation of the CSL on 1 June 2017, China has entered a new era for data protection, with legislators continuously rolling out laws and proposals and regulators stepping up enforcement. What is next on the horizon? The Personal Information Protection Law and the Data Security Law are in the pipeline for the moment and expected to be promulgated in the coming three years. While the Personal Information Protection Law will be close to the Chinese version of GDPR, the Data Security Law will be unprecedented in the world and pose additional security capacity challenges for MNCs. It provides a reference for the future direction of the national law – the end of lax regulation, a more comprehensive framework and heightened scrutinies. But at the same time, if data compliance could be incorporated in the organizational structure of MNCs and implemented throughout the life cycle of their products, in China MNCs can make more opportunities than they find.

Contents

I. Overview

It has been more than two years since the *Cybersecurity Law* (《网络安全法》in Chinese, "**CSL**") came into effect in 2017. Compared to the exploration and trial stage in 2018, it is regarded as the year in which the governance of cybersecurity and data compliance in China is gradually stable in 2019.

In general, with the CSL as the core, supporting relevant regulations and national and industry standards have been promulgated or published, and a supporting legislation system has been established.

From the perspective of the legislation related to protection of personal information, the national standards published in 2019 have detailed specific specifications such as consent for personal information and the need for collection, meanwhile, the legislature has begun to try to strengthen the protection of specific types of subjects, such as the protection of children's personal information, through special legislation.

From the perspective of cybersecurity, three significant national standards[1] for cybersecurity protection formally effective in 2019 mean that the era of "Classified Protection 2.0" has officially arrived, and the *Cryptography Law* (《密码法》in Chinese) also provides necessary guidance and inspiration for the use of "passwords" in cybersecurity classified protection.

[1] GB/T 22239-2019 Information Security Technology - Baseline for Classified Protection of Information System Security (《信息安全技术 信息系统安全等级保护基本要求（GB/T 22239-2019）》in Chinese); GB/T 28448-2019 Information Security Technology - Evaluation Requirement for Classified Protection of Cybersecurity (《信息安全技术 网络安全等级保护测评要求（GB/T 28448-2019）》in Chinese); GB/T 25070-2019 Information Security Technology - Technical Requirements of Security Design for Classified Protection of Cybersecurity (《信息安全技术 网络安全等级保护安全设计技术要求（GB/T 25070-2019）》in Chinese).

Meanwhile, enforcement activities become more active by four major authorities jointly or individually, in forms of day-to-day supervision and special campaigns. In addition, sectoral authorities are also active in formulating rules and exploring enforcement. In addition to continuing the special App management of personal information protection, law enforcement agencies will as well as focus their supervision on key industries such as finance, credit reporting, medical treatment, transportation, telecommunications, and the Internet.

In regard to litigation, one of the most impressive cases is the first civil dispute on facial recognition, which, to some extent, reflects people's increasing awareness of personal information protection.

All the various indications indicate that the establishment of an internal data compliance system for the enterprise has become more and more necessary, and the enterprise's data compliance work should be carried out sooner rather than later, so that the maximum value of data assets can be brought into play.

As such, this report sorts out the legislation, law enforcement and litigation concerning data protection and cyber security in 2019, and provides legal risk analysis and compliance tips for specific industries that are relatively sensitive to data protection, like life science and finance. At the same time, this report also discusses hot issues in different business scenarios, and puts forward suggestions about best practice for reference.

II. Legislation

In the past year, a raft of regulations, standards and their exposure drafts are released for public comments, involving several hot issues that highly concerned by MNCs, like cybersecurity classified protection and cross-border transfer of data. Such intensive legislative activities reflect China's growing attention on data privacy and cybersecurity, and create regulatory challenges for enterprises at the same time.

Legislation Updates Related to Cybersecurity Protection

• New Requirements in Cybersecurity Protection

In the past, a complete set of supporting rules，such as the *Administrative Measures for the Graded Protection of Information Security* (《信息安全等级保护管理办法》in Chinese) and *GB/T 22239-2008 Information Security Technology - Baseline for Classified Protection of Information System Security* (《信息安全技术 信息系统安全等级保护基本要求（GB/T 22239-2008）》 in Chinese) in the field of Cybersecurity, especially Information Security, has been formulated and implemented for more than 10 years (commonly known as "Classified Protection 1.0"), and such rules have been updated and become more comprehensively. On December 1, 2019, the three significant national security standards represented by *GB/T 22239-2019 Information Security Technology - Baseline for Classified Protection of Information System Security* (《信息安全技术 信息系统安全等级保护基本要求（GB/T 22239-2019）》in Chinese), came into effect, which means the beginning of a new time of cybersecurity protection (commonly known as "Classified Protection 2.0").

Different from "Classified Protection 1.0", "Classified Protection 2.0" is derived from the principal provision of "cybersecurity graded protection system" in Article 21 of the CSL, therefore, its legal basis is stronger and has a stronger necessity and guiding role in enterprise's data compliance work. In addition, in order to reflect the policies and industry compatibility better, "Classified Protection 2.0" also includes applications such as cloud computing, mobile internet, the Internet of Things, industrial control systems, and big data into the protection system, and on the basis of general security requirements, expansion requirements were formulated so that relevant enterprises could maximize customization of such insurance and compliance strategies.

- **Refinement of CII Identification Standards**

Other than the cybersecurity graded protection system, another focus of the **CSL** is the protection of critical Information infrastructure ("**CII**"), and the precondition of CII protection is the identification of CII. Therefore, the Cyberspace Administration of China, together with 12 departments including the National Development and Reform Commission, the Ministry of Industry and Information Technology, the Ministry of Public Security and so on, jointly drafted the *Measures for Cybersecurity Review (Draft for Comments)* (《网络安全审查办法（征求意见稿）》in Chinese, "**Draft Measures**"), which was officially released on May 24, 2019 for soliciting opinions form the public. According to the Draft Measures, the indicators such as "whether it is concerned or affects national security, economic security, social stability, public interest" are settled to identify and measure CII.

Compared with the general scope of application provided in the existing Measures, the Draft Measures clarify that, it only applies to the procurement of network products and services by CII operators. The Draft Measures remove the process of review by third-party and expert committee, and divides the review into two stages, namely preliminary review and special review (not necessary).

- **Administrative Measures for Data Security**

On 28 May, 2019, CAC released the *Administrative Measures for Data Security (Draft for Comments)* (《数据安全管理办法（征求意见稿）》in Chinese, "**Draft AMDS**") to regulate the collection, storage, transmission, processing and use of data through internet within Mainland China, as well as the protection and supervision of data security.

Pursuant to the Draft AMDS, network operators shall make a filing with the local cyberspace administration when they collect important data[2] or sensitive personal information[3] for the purposes of business operations. Otherwise, the enterprises will be punished with administrative penalties, such as confiscation of illegal income, suspension of related businesses, suspension of business for rectification, closure of websites, cancellation of related business licenses or suspension of business licenses, etc., and even criminal responsibilities.

Besides, as the CSL requires network operators to determine the person in charge of cybersecurity and define accountabilities for cybersecurity. The Draft AMDS further provides that, the name and contact information of the principal and/or the person responsible for data security shall be listed and highlighted in the rules for collection published by the network operator.

- **Cryptography Law**

The Cryptography Law was promulgated in 2019 and has come into effect on January 1, 2020. This law is the first comprehensive law in the field of cryptography management in China, and for the first time stipulates the requirements for the use of core passwords and ordinary passwords in the form of laws. It is especially noted that Article 27 of this law stipulates that: "If CII operators should use commercial passwords for protection in accordance with relevant regulations, they must conduct commercial password application security assessments on their own or entrust commercial password testing agencies." And this provision coincides with the cybersecurity graded protection system and CII protection. According to the relevant provisions in "Classified Protection 2.0" (including drafts for comments), the cybersecurity protection grade of CII shall not be lower than grade 3 in principle, and cryptography should be used for encryption. Therefore, under "Classified Protection 2.0", CII operators are required to conduct commercial password application security assessments in accordance with this law in principle.

Meanwhile, Article 27 of this law also stipulates that if a CII operator purchases network products and services involving commercial passwords that may affect national security, it shall conduct network security review by relevant departments in accordance with relevant laws and regulations. This also means that under *the Cryptography*

[2] Important data refers to data closely related to national s ecurity, economic development, and social and public intere sts.

[3] Sensitive personal information refers to the information th at once leaked, illegally provided or abused, personal and property safety may be endangered and personal reputation, physical and mental health may be easily led to damage or discriminatory treatment.

Law, there are obvious differences in the responsibilities and obligations of different enterprises: if an enterprise is regarded as a CII operator, it should ensure that its systems are protected with commercial passwords, and security assessments of commercial password applications are conducted in accordance with laws and regulations; If the purchase of products and services involving commercial passwords which may affect national security, it is necessary to refer to the above-mentioned Draft Measures to apply for cybersecurity review.

Legislation Updates Related to Personal Information Protection

• Measures for Security Assessment for Personal Information Export

On 13 June, 2019, CAC issued the *Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comments)* (《个人信息出境安全评估办法（征求意见稿）》 in Chinese, "**2019 Draft**"), which, to a large extent, reset the regulatory framework constructed under the Measures for Security Assessment for Cross-border Transfer of Personal Information and Important Data (Draft for Comments) ("**2017 Draft**") published in 2017, and imply that the regulations on the export of personal information and important data are separated.

Article 37 of the Cybersecurity Law stipulates that, CII operators are obligated to adopt data localization, and conduct security assessment in case of cross-border transfer of personal information and important data. However, the 2019 Draft expands its application to all network operators, rather than CII operators only.

Besides, the 2019 Draft also establishes a filing system for the security assessment for personal information export, under which network operator shall submitted several materials to the competent authority for review, including the filing report, the contract between the network operator and the recipient, the risk analysis report and other materials requested by the authority.

• Provisions on Children's Online Personal Information Protection

On 23 August, 2019, CAC officially released the *Provisions on Children's Online Personal Information Protection* (《儿童个人信息网络保护规定》 in Chinese, "**PCOPIP**"), which has come into force as of 1 October 2019.

Compared with the general rules for personal information protection, the PCOPIP provides higher requirements as below to show special care for children.

- Network operators shall set up special rules and user agreements for children; and appoint special persons to protect children's privacy.

- Where a network operator transfers a child's personal information to a third party, it shall conduct security assessment by itself or a third party.

- Where a network operator ceases the operation of products or services, it shall forthwith cease the collection of children's personal information, delete that it holds, and inform the children's guardians of the cessation in a timely manner.

• Strengthened Supervision on Personal Information Collection by Apps

Since the beginning of this year, the collection and use of personal information by Apps has always been the focus of supervision in various industries. Under this background, the *Guide to the Self-Assessment of Illegal Collection and Use of Personal Information by Apps* (《App 违法违规收集使用个人信息自评估指南》in Chinese) and the *Methods for Determining the Illegal Collection and Use of Personal Information by Apps* (《App 违法违规收集使用个人信息行为认定方法》in Chinese) were issued for entities, as well as authorities to follow.

The above two regulatory documents provide detailed and specific requirements on the construction and demonstration of privacy policy in Apps, like the independence and readability of privacy policy; the key elements included in privacy policy; and the protection of users' rights to their personal information.

III. Enforcement

In 2019, data protection authorities continued to be active in enforcement activities, which can be reflected in several special campaigns launched jointly or separately by different agencies, like the "Clean Net" and "Protect Consumer" campaigns. Such tendency indicates the normalization of data protection supervision and brings compliance challenges for businesses as well.

In addition, competent authorities in certain sectors and industries like securities and finance are also paying more attention to data compliance. For example, since the second half of 2019, the China Securities Regulatory Commission has largely increased its inquiry on the data compliance situations of companies applying to be listed (especially in the SSE STAR Market). Among them, companies with main businesses involved in collecting, processing, profiling and sharing personal information have attracted much attention from the IPO authority.

A. Public Enforcement: Administrative Actions

Public enforcement still presents a polycentric landscape, since there is no single data protection agency in China. Agencies could ally with each other, or take actions on their own initiative. It also to some extent leads to the massive enforcement campaigns. Looking at the campaigns carried out, it is easy to discern that mobile App is a focus of enforcement for almost every agency. Cybersecurity， especially the implementation and filing of cybersecurity classified protection system, is an another, sometimes with sectoral emphasis. And the agencies are accumulating experiences in these cases by bringing in third-party experts in the process of actions.

• Four Ministries' Joint Campaigns Targeted at Apps

On 25 January, four ministries including the Cyberspace Administration of China ("**CAC**"), the Ministry of Industry and Information Technology ("**MIIT**"), the Ministry of Public Security ("**MPS**"), and the State Administration for Market Regulation ("**SAMR**") announced a joint nationwide campaign against the illicit collection and use of personal information for Apps from January to December. The illicit conducts include coercing users into authorizing the use of their personal information, excessive collection of personal information, collection and use of personal information without consent, illicit sale or distribution of personal information.

As a part of the campaign, the National Information Security Standardization Technical Committee ("**NISSTC**"), China Consumers' Association ("**CCA**"), Internet Society of China ("**ISC**") and Cybersecurity Association of China have been required to establish a Special App Governance Work Group regarding the illicit collection and use of personal data by Apps. As of December, 2019, the Special App Governance Work Group has received a total of 12,322 reporting, including 4,039 real-name reporting. In addition, the Group has entrusted 14 rating agencies to conduct technical evaluations of more than 1,000 commonly used Apps, including the users' agreement, users' experience, and technical testing, supervised and rectified nearly 300 Apps with serious problems, and rectified more than 800 problems. [4]Furthermore, since March 2019, SAMR and CAC has carried out a voluntary security certification scheme for Apps in which Apps operators are encouraged to apply for certification to demonstrate their Apps' compliance with the *Information Security Technology - Personal Information Security Specification* (《信息安全技术 个人信息安全规范》in Chinese, "**PISS**") in terms of collection and use of personal information. The operators of certified Apps can display the certification on websites, in offices and on relative promotional materials. The scheme not only takes technical advantages of third-party testing agencies, but also exerts significant value of search engines and applications market in supporting supervision thereby reduces the burden of regulators to a certain extent and stimulates App operators' initiative in compliance.

• Individual Campaigns on Apps Conducted by Watchdogs

CAC Launched a Special Campaign of App Chaos. From December 2018 to April 2019, the

[4] https://m.mp.oeeee.com/a/BAAFRD000020191230244167.html

CAC launched a special action against mobile Apps involving pornography information, gambling, malicious programs, and bad contents. CAC carried out full-chain governance of illegal Apps, in which 33,638 illicit apps were shut down, more than 2.34 million malicious websites were blocked, more than 24.74 million vulgar and poor information was cleaned up on social platforms, and more than 3.64 million illegal accounts were banned.[5]

MIIT Launched a Campaign against Users' Rights Infringement by Apps. On November, 2019, MIIT organized to launch a special campaign against infringement of users' right by Apps, which targeted 8 kinds of key issues, such as the illicit collection and use of personal data, unreasonable requests for user authorization, and obstructing users from canceling accounts.[6] During its campaign, MIIT asked a third-party testing agency to inspect the application stores, and urged more than 100 companies with problems to rectify. As of December 19, 2019, there were still 41 apps that had not completed rectification.[7]

MPS Carried out Massive Campaign regarding Illicit Collection and Use of Personal Information and unlawful crawlers. The MPS launched a nationwide action which is focused on combating illegal collection and use of personal information by internet companies from November, 2019, in which the police asked 27 Apps to implement rectification measures within a prescribed period, issued warnings and penalties against 63 Apps, fined 10 Apps, and commenced criminal investigation against 2 Apps.[8] Meanwhile, since September, 2019, local public security bureaus led by MPS have cracked down several fintech companies providing malicious crawler technology to collect users' personal information in financial industry, such as 51 Credit Card, Moxie Technology, and Xinyan Technology.

SAMR Cracked down on Consumer Personal Data Infringement. SAMR launched a nationwide campaign against consumers' personal information infringement named "Protect Consumer" from 1 April to 30 September, which focused on key industries and areas that are deemed vulnerable to personal information infringement such as real estate, small loan finance, education, insurance, beauty and fitness, decoration, travel, transportation, telemarketing, and website or application operation.[9] It is said that, during the operation, SAMR investigated and dealt with a total of

[5] http://www.cac.gov.cn/2019-04/12/c_1124357539.htm
[6] ： http://www.cac.gov.cn/2019-11/04/c_1574399754695177.htm
[7] http://www.gov.cn/fuwu/2019-12/20/content_5462577.htm
[8] https://mp.weixin.qq.com/s/smT4RbHsA_x0vIZjEKV_yg
[9] http://www.samr.gov.cn/xw/zj/201904/t20190410_292685.html

1,474 cases of consumer information infringement, seized more than 3.692 million pieces of information, collected fines of more than 19.64 million yuan, transferred 154 cases to public security organs, organized 4,225 law enforcement collaboration, 3,536 administrative interviews and 10,653 promotional activities.[10]

- **The Supervision of the Cybersecurity Law Enforcement**

In 2019, the MPS continuously intensified the supervision of cybersecurity law enforcement. From May to September, the MPS deployed cybersecurity law enforcement inspections which focus on national critical information infrastructure, important information systems, big data and other related application systems.

For example, according to the report released by the Guangzhou PSB on 4 December[11], since this year, the Guangzhou PSB organized a large-scale cybersecurity inspection operation, and imposed administrative penalties on 266 illegal subjects who failed to fulfill their network responsibilities, failed to implement cybersecurity technical measures, and collected personal information of citizens out of their scope. A total of more than 56,000 malicious apps were pulled off shelves.

- **Special Action for Improving Capabilities to Protect Network Data Security in Telecommunications and Internet Industries**

Since July, 2019, MIIT has carried out the Special Action Plan for Improving Capabilities to Protect Network Data Security in Telecommunications and Internet Industries to address data security issues such as excessive data collection and abuse, illegal transactions and user data leakage, and to establish an integrated network data security system for the industries. [12] By the end of October, MIIT completed data security inspections of all basic telecommunication companies, 50 key internet firms, and 200 mainstream Apps.

As reported, as of November 20, MITT organized several supporting units to conduct a rolling assessment of data security risks for 140 APPs that fell into 14 categories with a large number of users and frequent downloads.[13]

[10] http://www.gov.cn/xinwen/2019-11/19/content_5453362.htm
[11] http://m.xinhuanet.com/gd/2019-12/05/c_1125313595.htm
[12] http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757016/c7021335/content.html
[13] https://www.secrss.com/articles/15326

B. Public Enforcement: Criminal Prosecutions

Since January 2019, the MPS has deployed national public security organs to carry out special actions on the "Clean Net 2019" to crack down on network criminal activities such as hacking and infringement of citizens' personal information. Subsequently, the "Clean Net Operation" on the localities swept the country, with a number of typical cases emerged in various industries and departments throughout the criminal lifecycle. For example, in Guangdong Province alone, more than 2960 cases were detected, and more than 10,420 suspects were detained. [14] Below are the typical cases happened in 2019 in this regard, sorted by the crimes committed, so as to shed a light on the future landscape of criminal prosecutions in data and privacy protection.

• Infringement of Citizens' Personal Information

"Private Detective" Infringed Citizen's Personal Information in Wuxi. On 9 August 2019, Wuxi Xinwu Court released the judgment of Wuxi's first case of private detective infringing personal information. The two defendants who tracked the victims and illegally provided the whereabouts information to other people were separately sentenced to three years and three months in prison, one year sentence with probation of one and half years, and fined 20,000 yuan and 8,000 yuan.[15]

China Telecom's Employee Sold Personal Information of as Many as 200 Million Users. On 19 September 2019, the Intermediate People's Court of Taizhou City, Zhejiang Province upheld the first-instance ruling on the sale of 200 million pieces of personal information of China Telecom users by employees of China Telecom 's wholly-owned subsidiary. Four appellants were found constituted infringement against citizens' personal information.[16]

Public Interest Litigation of Consumer Personal Information Infringement Is Elected as Typical Case. On 10 October 2019, Zhuji City 's real estate and decoration industry's infringement of consumer personal information

[14] "广东警方'净网 2019'专项行动：破案 2960 余起，缴获公民个人信息 98 亿条"， https://mp.weixin.qq.com/s/XXYS_socYVhDafIz_lspoA?scene=25#wechat_redirect

[15] "无锡首例"私家侦探"侵犯公民个人信息案宣判，两被告人获刑"，https://www.thepaper.cn/newsDetail_forward_4224974

[16] (2019) Zhejiang Ruling No. 692 Criminal Ruling, http://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=95ffdf1815f24479aee9ab2e0114cd48, and (2018) Zhejiang 1081 Criminal Judgment No. 1339，http://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=2750f21b4eab4c079299aa7f00a1be81

case was selected as a typical public interest litigation case of the Supreme People 's Procuratorate. At the end of 2018, Chen, Yang, Luo and others were sentenced to three years in prison, suspended for four years, and fined 10,000 yuan for infringing citizens' personal information; however, the real estate company involved did not receive the corresponding administrative penalty in a timely manner. Zhuji People's Procuratorate thus issued procuratorial suggestions and work letters to Zhuji Administration for Market Regulation and the Industry Association respectively. In the end, the decoration company involved was fined 30,000 yuan, and the real estate company involved was fined 100,000 yuan.[17]

Shanghai's First Case of Setting Website for Selling Citizens' Personal Information. On 21 November 2019, the People's Procuratorate of Jiading District in Shanghai filed a public prosecution against the 4 defendants for infringing citizens' personal information through the establishment of a website for paid consulting. It is reported that, at the beginning of 2017, Zhang, one of the defendants, acquired more than 8.2 million pieces of real estate owners' information in various districts of Shanghai from others, and another criminal suspect Shu inputted the aforementioned information into a database, set up a website and conduct daily server maintenance.[18]

• Illegal Obtainment of Computer Information System Data

Dongguan "hackers" Illegally Hacked 2,400 Servers. In September 2019, the Dongguan Police arrested a criminal suspect who wrote a script Trojan to invade and control the computer server. Investigation revealed that more than 2,400 servers nationwide using a software system developed by a technology company in Dongguan were illegally invaded and controlled. The criminal suspect illegally hacked into 20 online loan website platforms and illegally obtained about 700,000 pieces of personal information, from which he profited 12,000 yuan.[19]

• Damage on Computer Information System

Hospital Registration System Is Maliciously Obstructed to Prevent Patients' Visits. On 10

[17] "浙江省诸暨市房地产、装修行业侵犯消费者个人信息公益诉讼案入选最高检公益诉讼典型案例" https://mp.weixin.qq.com/s/bKl4W1Ij5nIXJ3TYhhHB8w

[18] "上海首例！4 人建立网站售卖公民个人信息被提起公诉", http://sh.people.com.cn/n2/2019/1121/c134768-33561994.html

[19] "东莞黑客非法入侵 2400 多台服务器，已被逮捕！", https://k.sina.com.cn/article_5999804563_1659dc09300100m6iu.html

January 2019, the police arrested four major suspects in Beijing, Henan, Shanxi and Yunnan who were suspected of damaging computer information systems by using malicious software to bypass normal verification mechanisms to preempt hospital registration numbers. On 15 April 2019, the police arrested four criminal suspects, all of whom were detained for damaging computer information systems.[20]

- **Unlawful Use of Information Network**

Zhang Jingyuan and Others Infringed Personal Information through Developing Software and Creating Group Chat. On 14 October 2019, the Jinhua Intermediate People's Court of Zhejiang Province upheld the first-instance judgment on a case of infringing personal information. One of the defendants, Liang Yi, was convicted of unlawful use of information network for he developed several software that can automatically register accounts on websites and created a chat group that sells personal information of citizens.[21]

- **Assistance of Criminal Activities Committed through Information Network**

Sogou Promotion Agent Assisted Criminal Activities Committed through Information Network. On 14 November 2019, the People's Court of Dingtao District, Heze City, Shandong Province found the defendant Zhao Sheng guilty of assisting criminal activities committed through information network and was sentenced to one year and one month, suspended for two years, and fined 30,000 yuan. From the end of 2015 to June 2017, the defendant Zhao Shenggang assisted customers that collect personal information of citizens to commit crimes on the Sogou search platform.[22]

C. Private Enforcement

As in the past few years, private litigation remains a powerful weapon for big companies to gain legitimate access to customers' data. Users' consent may or may not be the concern of these companies, while the competition for data assets become the crux. Meanwhile, due to the increasingly awareness of the importance of citizens' personal information protection, civil litigation is no longer a privilege of a few tech giants, but a new battlefield for citizen privacy protection. Individuals are coming forward to

[20] "公安部举行'净网 2019'专项行动典型案例发布会", https://www.scio.gov.cn/xwfbh/gbwxwfbh/xwfbh/gab/Document/1657073/1657073.htm

[21] (2019) Zhejiang 07 Criminal Judgment No.751, http://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=d7da7c69c5ba4b699ce1aaf800bb714f; and Criminal Judgment No. (2018) Zhejiang 0782 Criminal Beginning No. 2095, http://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=1804a62545764b3c94fcaa9b00a54f48

[22] (2019) Lu 1703 Criminal Judgment No. 361, http://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=f65e0b87658343e59f5dab1b017f1efa

bring cases to the courts, making the mission of data compliance more imminent than ever before.

- **Unfair Competition**

TikTok and Duoshan Illegally Shared WeChat Users' Information. On 10 May 2019, the Third Intermediate People's Court of Tianjin upheld the Tianjin Binhai New District People's Court ruling, which requested TikTok to discontinue providing Duoshan with the log-in services through authorized WeChat or QQ accounts from the open platforms. Duoshan was also banned from using WeChat/QQ users' profile and nicknames obtained from TikTok.[23]

A Tech Company in Hangzhou Crawled and Appended Dealer's Database of Women Apparel Customers. On 31 October 2019, the Hangzhou Internet Court found that a tech company that illegally obtained and used the account and password on the "Women 's Clothing Network" to obtain the dealer database information constituted unfair competition.[24]

- **Infringement of Personal Privacy**

Toutiao Uploading Address Book Information without Users' Consent Infringed Personal Privacy. On 20 June 2019, Beijing Haidian People's Court heard the case of Toutiao uploading address book information without users' consent in infringement of personal privacy. The three main disputes between the claimant and the defendant were: (1) whether the address book was personal privacy or not; (2) whether Toutiao had fulfilled the full disclosure obligation before reading and uploading the user's address book information; and (3) whether Toutiao should delete and overwrite the original address book when users prohibited Toutiao from reading and stopped re-authorizing Toutiao from collecting address book information. This case involved the coordination of the development of the Internet industry and the protection of personal privacy. It was of great significance to address the heated issues of intelligent algorithms, personal information protection, and smart application industry development. [25]

The First Civil Dispute on Facial Recognition Was Brought by a Professor in China. On 1

[23] "法院正式裁定：抖音多闪立即停止共享微信用户信息等违规行为"，https://view.inews.qq.com/a/TEC2019032000603200?openid=o04IBABEwjeAOWN8JWfyp7TwaFLI&key=&version=17000329&devicetype=iOS12.1.4&wuid=oDdoCt2nVnxSTnnP0WiHFL2ervI8&sharer=o04IBABEwjeAOWN8JWfyp7TwaFLI&uid=&shareto=，and"北京拍拍看看科技有限公司、深圳市腾讯计算机系统有限公司商业贿赂不正当竞争纠纷二审民事裁定书"，http://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=7f71b394c3574897b94caa7b012f348e

[24] "女装网遭'撞库'被告构成不正当竞争被判赔偿 35 万元"，http://www.rmfz.org.cn/contents/2/245660.html?from=groupmessage

[25] "今日头条"擅自上传通讯录侵犯个人隐私案庭审实录"，https://m.gelonghui.com/p/281016

November, the People's Court of Fuyang District of Hangzhou officially accepted the first case of facial recognition in China. In this case, Guo Bing, a distinguished vice professor in Zhejiang Sci-Tech University, sued Hangzhou Safari Park, claiming that the Park has violated the Consumer Rights Protection Law by upgrading the annual card system to force the collection of personal facial features.[26]

[26] "中国人脸识别第一案：动物园因启用人脸识别技术被诉至法院", http://news.ifeng.com/c/7rHNBE5VpuA

IV. Sectoral Regime

The CSL and its supporting documents are generally applicable to all walks of life. However, different industries may have different degrees of emphasis according to their respective industry characteristics. This chapter selects five representative industries that are sensitive to data and privacy protection, including traditional sectors like life science, finance and retail in the context of the new digital era, as well as emerging industries such as autonomous driving and the Internet of things.

A. Life Science

On Dec 30th, 2019, the Shenzhen Nanshan District People's Court sentenced a Chinese scientist, who created the world's first genetically edited twins, to three years in prison for carrying out "illegal medical practices". The gene-edited baby scandal not only catalyzed the promulgation of the *Regulations on the Management of Human Genetic Resources,* but also raised increasing public attention to data protection in the healthcare industry.

• Types of Data

Rules pertaining to data protection in the healthcare industry are scattered in various laws and regulations with different focus. For entities in the healthcare industry, categorization of data is a prerequisite for effective data compliance.

a) Healthcare Big Data

Legislation: *The Administrative Measures on Standards, Security and Services of National Healthcare Big Data (For Trial Implementation)*

Focus: Localization; security assessment[27] for cross border transfer

b) Human Genetic Resources

Legislation: *The Regulations on the Management of Human Genetic Resources*

Focus: International scientific research activities using China's human genetic resources shall be carried out in cooperation with Chinese entities; collection and preservation of human genetic resources; Prior approval for cross border transfer

c) Population Health Information

Legislation: *The Measures for the Management of Population Health Information (For Trial Implementation)*

Focus: Localization[28]; graded storage

d) Pharmaceutical Data

Legislation: *The Pharmaceutical Data Management Specification (Draft for Comments)*

Focus: Full life-cycle application[29]

e) Medical Device Data

Legislation: *The Guidelines for Technical Review of Network Security Registration for Medical Devices*

Focus: Not compulsory; applicable to the registration and declaration of Class II and III medical device products with network connection function for electronic data exchange or remote control

f) Scientific Data

Legislation: *The Measures for the Management of Scientific Data*

Focus: Restriction on the sharing of data involving state secret, state security, social public interests, commercial secret and personal information

g) Medical Record

Legislation: *The Regulations for Medical Institutions on Medical Records Management (2013)*

Focus: Medical record keeping

[27] Rules on cross-border transfer varies depending on the data type, some require prior approval, some assessment before transportation, others are proscribed from transportation of any kind. *The Administrative Measures on Standards, Security and Services of National Healthcare Big Data (For Trial Implementation)* allows cross border transfer of "healthcare big data" when the security assessment has been conducted.

[28] The *Measures for the Management of Population Health Information (For Trial Implementation)* proscribes any storage of "population health information" outside the Chinese territory.

[29] Full life cycle refers to the entire process of data generation, recording, processing, auditing, analysis, reporting, transfer, storage, restoration, recovery and destruction.

It is worth noting that according to *the Information Security Technology Personal Information Security Specification*, healthcare data may be identified as "important data" closely related to national security, economic development, and social and public interests, which entails strict compliance obligations on localization and cross-border transfer if the entity involved has been identified as an operator of critical information infrastructure ("CII Operator"). Additionally, the *Draft Information Security Technology Guideline of Security Assessment of the Cross-border Transfer of Data* has also included the healthcare and pharmacy industry in Appendix B: instruction for identification and classification of important data, which just epitomizes the importance of healthcare data.

- **Prone to be Identified as CII Operator**

According to the CSL, as long as an entity has been identified as a CII Operator, it is obliged to follow the localization rules and conduct security assessment before the cross-border transfer of personal information and important data collected and generated in China. *The Draft Regulations for the Security Protection of Critical Information Infrastructure*, on the other hand, stipulates that entities in the healthcare industry shall be included in the scope of critical information infrastructure as its damage, dysfunction or data leakage may severely jeopardize national security, people's livelihood and public interest. Therefore, it is highly possible that entities in the healthcare industry will be considered as CII operators and shall assume relevant responsibilities.

- **Best Practice**

Considering the special attribute of healthcare data and the tendency for entities in the healthcare industry to be identifies as CII Operators, closer attention shall be paid by relevant parties to the following rules.

– Categorize the healthcare data circulated within the entity, which may include but is not limited to personal information, healthcare big data, human genetic resources, population health information, pharmaceutical data, medical device data, scientific data, and medical record. Upon the categorization, develop data protection policies and strategies in compliance with the relevant laws and regulations.

– Move servers storing healthcare data and personal information into the territory of China. Prepare early for assessment or prior approval procedures if cross-border transfer becomes necessary.

B. Financial Services

It is no news that the rapid development of information technology has dramatically changed the modern finance industry; technology becomes part of the foundation as the supporting pillar of this industry. An emerging sub-industry, "Fintech" (as a shortened version of financial technology), is an indicator of such revolution. Data protection and cybersecurity plays an important role in the strategies and management of financial institutions. Given the significant status of finance, it has always been one of the regulators and enforcers' priorities.

• Latest Regulations

With mobile banking and online banking being commonplace, the People's Bank of China ("**PBOC**") took actions on assessing the security management of financial apps. In September 2019, the PBOC issued a *Notice on Issuing Financial Industry Standards and Strengthening the Security Management of Mobile Financial Apps User End*, to improve security protection capabilities, enhance personal financial information protection, improve risk monitoring ability and complaints management, and strengthen industry self-discipline. An updated *Specification on Mobile Payment* is provided at the same time. The explicit consent of the user is required before the collection of personal financial information and collection of personal financial information irrelevant to the service provided is prohibited.

Shortly after that in October 2019, the People's Bank of China circulated the draft *Trial Measures on the Protection of Personal Financial Information and Data* ("**Trial Measures**"), intending to regulate the collection, process, use, sharing and transfer of personal financial data by financial institutions. It requires the thorough assessment of third-party data providers; cooperation shall be terminated where the legal provision of relevant financial information cannot be guaranteed. The *Trial Measures* is expected to be released in 2020, according to the latest work plan of the PBOC.

In December 2019, the PBOC further released *Implementation Measures for Protecting Financial Consumers' Rights and Interests* to solicit public opinions. A whole chapter of which focuses on the protection of consumer financial information protection. Together with fragmented rules regarding personal financial information protection among *People's Bank of China Law*, *Commercial Banks Law*, *Securities Law*, *Insurance Law*, etc., it is foreseeable the supervision of personal financial information protection will be further strengthened.

• Enforcement Activities

A Personal Information Protection Working Group on Apps, established in January 2019, aims at the collection and use of personal information by apps in violation of laws and regulations. In its over-a-year campaign, the Working Group has evaluated thousands of apps and a significant amount of the Apps in issues are financial Apps. The types of apps involved include online banking, mobile payment, insurance, wealth management, online loans, etc. Therefore, starting from September 2019, the PBOC coordinated the China Banking and Insurance Regulatory Commission ("**CBIRC"**) and the Cyberspace Administration of China ("**CAC**") as well as other departments jointly launched a rectification action against internet financial industry to crack down the personal information infringement, especially where the cooperation with illegal crawler technology companies involved.

Along with the rectification movements, the PBOC and other competent departments have also launched the pilot project of financial application registration work. With the above-mentioned efforts, orderly competition and sound government of the financial app can be achieved under the strict administration.

• Best Practice

Considering cybersecurity and financial information risks have become one of the main risks financial instrument face nowadays. We recommend stakeholders to take into accounts information protection and cybersecurity when constructing financial security protection system and to include the relevant subjects in its strategic development plan.

Ensure the sound performance of security facilities and completeness of trusted network and examine common vulnerabilities & exposures and deploy attack detection and defense network mechanism to satisfy Classified Protection II.

Evaluate and assess the legality, legitimacy and necessity of the purpose, method, and scope of the collection and use of financial information. Adopt technical and strategic measures such as data encryption, access control, secure transmission, and signature authentication to prevent personal financial information from being illegally stolen, leaked, or tampered with during transmission, storage, and use. Violation of relevant laws and regulations, as well as user agreements, shall be avoided; refrain from disclosing, illegally selling or providing personal financial information to others.

C. Retail, Luxury and Fashion

Retail is a sector where customer data is like oil, with efficient mining of it fueling new personalized communication strategies, targeted marketing and one-to-one engagement.

And for all we know, the use of innovation technology in retail is transforming the relationship between retailers and customers, such as face recognition technology. For a retailer's perspective, technology creates new opportunities to sell products, communicate with customers and analyze the shopping preferences of customers, for example, push precise marketing and location-based offers. Currently, with the development and use of new technologies, retailers must pay attention to data protection of online and offline retail, including but not limited to consumer consent, the use of cookies, precise advertising.

Otherwise, the retailers always cooperate with other companies in handling with raw data for analyzing the predilection of customers. Therefore, a proper due diligence of your vendor relationships must be conducted before cooperation.

- **Mass and A Wide Variety of Data**

All retailers are likely to hold and use a wide variety of personal data, relating to employees, customers and potential customers (for example, for consumer research and marketing purposes). These records are a hugely important and valuable resource for retailers which can be used in excavating the need of customers.

- **Informed Consent**

Obtaining customers' consent to marketing is an important factor for retailers. Generally, retailers should pay particular attention to how they obtain consent in a clear, specific and free given way under PRC law.

According to PISS and the *Information Security Technology- Guidelines for Personal Information Notices and Consent (draft for comment)*, retailers must ensure that an individual consent to the processing of his/her personal data by affirmative action in some scenarios where pre-ticked boxes are not sufficient. For example, sharing personal data with third-party service providers for providing services not pertaining to the core business need prior affirmative consent from the customers.

Furthermore, with wide use of the face recognition technology in shopping malls and brand stores, retailers which use the face recognition technology in their shops shall display notices prominently at camera installation, shopping guides and payment

counters, and clearly inform the nature and purpose of the information collection equipment and obtain the consent of data subjects or their legal guardian except for the scenario where the collected face information is only used to compare with the face information stored locally on the device or only processed locally without sending to the remote server.

- **Recording Keeping**

According to the E-commerce Law, an e-commerce platform business shall record and retain the information on the commodities and services and transaction information released in the platform and ensure the integrity, confidentiality and availability of the information. The information on commodities, services, and transactions shall be retained for at least three years from the day of completion of the transaction. For those which sell products in e-commerce platform, keeping relative records more than three years is necessary.

- **Enhanced Data Protection Rights for Individuals**

For retailers, precise marketing is a significant way to promote these products by sending e-mail, SMS and making a phone call. Except for the right to discontinue receiving such advertisements required by the Advertising Law, the Law on Protection of Consumer Rights and Interests, etc., the CSL and the E-commerce Law also enshrines new rights for individuals, including the right to access, right to cancel account, right to rectification and right to erasure.

- **Best Practice**

Some of the key suggestions which are particularly important are follows:

- For retailers, these can take advantage of pseudonymization, encryption or anonymizing personal data will be able to reduce their risk of non-compliance. This helps retailers mitigate risk, such as a data breach of personal consumer data.

- Consent must be freely given, specific, informed and unambiguous. It also requires a clear affirmative action by a consumer (as compared with the 'old' days of pre-ticked opt-in boxes and opt-out boxes consenting to marketing communications). Retailers now need to keep clear records of how and when consent was given.

- Contracts between retailers and their suppliers are required in writing and must include certain mandatory provisions, including requiring suppliers to implement appropriate technical and organizational security measures, or satisfy the requirement of the Cybersecurity

Protection 2.0 to protect data, obliging suppliers to report data breaches, only processing data on documented instructions from the retailer and allowing and contributing to audits by the retailer.

- Retailers need to have a data breach response plan in place which will enable them to respond quickly and effectively in the event of a breach, to ensure damage limitation to both the brand and its customers.

D. Transportation

Transportation is a leading and strategic industry of the national economy, and it plays a significant role in development and public welfare. As an industry closely related to "critical information infrastructure"[30], it is facing serious threats in cyberspace no matter for reasons such as national security confrontation or challenges posed by illegal organizations or individual behaviors. Meanwhile, transportation industry covers various areas in everyday life such as highways, railways, civil aviation, shipping services, and post services, and therefore has strong demands for data privacy protection and cybersecurity.

Although China is developing rapidly in terms of smart transportation, telematics, intelligent connected vehicle, and autonomous driving in recent years, data protection and cybersecurity in this area is still is its early days.

• Cybersecurity as a basic policy of smart transportation

The National Development and Reform Commission and the Ministry of Transport jointly issued the Implementation Plan for Promoting the "Internet Plus" of Convenient Transportation and Development of Intelligent Transportation in August 2016[31]. This policy document established the basic principles of including cybersecurity in the field of smart transportation. It made a few requirements regarding cybersecurity in the field of smart transportation: to improve the cybersecurity protection mechanism; to strengthen the prevention and control of cybersecurity risk; to expand the technical support capabilities; to level up the operational safety monitoring and early warning system of key websites, information systems, and clients; to conduct security risk and hidden danger investigations regularly; to enhance emergency response capacity; and, to prevent violations of privacy and abuse of users' information. In addition, the plan also specifically requires that the servers of data platforms providing transportation services must be located in China, which corresponds with Article 37 of the CSL[32].

In September 2019, the Central Committee of the Communist Party of China and the State Council jointly issued the Outline of Building a Powerful Country for Transportation[33]. This policy

[30] Under the Chinese law, "critical information infrastructure" refers to which relates to national security, national economy and people's livelihood and, if destroyed or if its functionality is lost, or if data is leaked, will seriously damage national security and public interests.

[31] http://www.gov.cn/xinwen/2016-08/05/content_5097842.htm

[32] Article 37 of the Cybersecurity Law of China: The operator of a critical information infrastructure shall store within the territory of the People's Republic of China personal information and important data collected and generated during its operation within the territory of the People's Republic of China.

[33] http://www.gov.cn/zhengce/2019-09/19/content_5431432.htm

document clearly states: "it is necessary to improve the cybersecurity protection system" and "to strengthen the security protection of traffic information infrastructure". The important status of cybersecurity in China's development of transportation industry, especially smart transportation, has been further established.

- **Transportation infrastructure and equipment**

In 2019, the infrastructure and equipment of transportation still faces various cyber threats. For example, attacks on smart terminal equipment and devices such as video surveillance cameras occur from time to time. Once a cyber-attack breaks out, a large number of equipment can be infected. Currently, there are still various loopholes and backdoors in a diverse category of smart terminals, requiring targeted solutions. Otherwise, the shutdown of the video surveillance system can have an adverse impact on traffic order, crime prevention and even public safety.

As another example, traffic guiding displays (usually are LED displays) as an infrastructure commonly have security risks in using default or factory-set passcode, such as 4-letter password "DOTS". Even with some encryption technology, weak passcodes are easily be cracked. This vulnerability can be exploited by hackers at home and abroad, which may not only lead to pranks, but also impact on social governance, traffic safety and even national security.

- **Intelligent connected vehicle (ICV) and telematics**

As a priority of automobile development, automotive information security has been valued by the industries of telecommunications, the automotive, the automotive electronics, and Internet service providers from the beginning.

However, ICVs and telematics inherit existing computing and networking architectures, and therefore may have the embedded security flaws of these systems. With the increase of electronic control units and connections in vehicles, the vulnerability that can be taken advantaged by hackers has also greatly increased, especially when the vehicle is connected to the cloud through networks because each computing, control, and sensing unit and connection path are possible to be exploited due to a security breach.

In addition to the intelligent system of vehicles, the security issues of smart terminal devices are also very prominent. It is mainly reflected in two aspects: First, the terminal devices are often connected to the in-car Wi-Fi or LAN, which can be used as a bridge for launching attacks. At present, no matter whether the terminal devices

are Android-based or iOS-based, there is always a risk of being hacked with malicious code. Second, the terminal devices usually store sensitive customer data, such as data about the driving records, image and voice data, service account, and authentication credentials, and there is also a risk of data breach in case of attacks.

- **Car-hailing**

China has a huge market for car-hailing. According to statistics[34], as of June 2019, the number of taxi-hailing users in China has reached 337 million, and the number of tailored taxi or fast ride users in China has reached 339 million. At the same time, there are also many problems with the data privacy of car-hailing, such as: privacy issues caused by in-car cameras to ensure passenger safety, drivers' access to passenger personal information, and confidentiality of passengers' car-hailing records and driving trajectories.

In recent years, the data privacy protection of the car-hailing industry has also been put on the legislative agenda. In July 2016, eight Ministries and Departments jointly issued the Interim Measures for the Management of Car-hailing Operating Services[35]. It aims to promote the integrated development of the taxi business and the Internet industry, to standardize the operation of car-hailing services, and to protect the rights and interests of passengers. Among them, the regulation focuses on standardizing the collection, storage, use, and sharing of passengers' data and ensuring the security of personal information and sensitive national information.

- **Autonomous driving**

Autonomous driving cars collect a large amount of personal data. From the perspective of data and privacy protection, this usually cause two issues:

First, if autonomous driving cars designed and produced in other countries operate in China, their network services and back-office services will inevitably be provided by foreign companies and servers. Some people believe that sensitive data such as driving records, traffic, and geographical environment data may be leaked or illegally used if transmitted overseas, endangering China's national security. Second, during the travel process, a large amount of user interaction data, including usage time, precise positioning, preferences, communication information, etc., contains great commercial

[34] http://free.chinabaogao.com/qiche/201912/1294C3J2019.html

[35] http://www.chinanews.com/gn/2016/07-28/7954840.shtml

value and may be used illegally by enterprises.

At present, China's legislation has not specifically provided for autonomous driving. However, in February 2017, the China Automotive Information Service Industry Application Alliance, a pilot standard-making group authorized the *National Standardization Management Committee, issued the Guidelines for the Security Protection of Vehicle Networking (Draft for Comments)*[36]. The Guidelines, as an organization standard formulated by legally recognized procedures, have certain reference significance. For example, the *Guidelines* proposes measures for cybersecurity based on the perspective of smart cars from multiple aspects, including software security, identity authentication, remote access, physical and environmental, security monitoring, data encryption, and so on. Considering that in the context of automotive intelligence, the Internet of Vehicles and autonomous driving technology are inseparable from each other. Although the aforementioned measures are aimed at the Internet of Vehicles, it may also be worthy of reference in the data privacy protection of autonomous driving.

- **Best Practice**

Based on the aforementioned risks and regulatory practices of data privacy protection and cybersecurity in the transportation industry, we have the following compliance tips:

- conduct self-assessment as to whether the company is a critical information infrastructure operator);

- carry out "multi-level classification assessment of network security" and adopt corresponding security protection requirements;

- long-term monitoring and regular maintenance of the network security status of internal and external information systems;

- take measures and techniques to prevent cyber-attacks;

- incorporate data privacy protection issues into the product or service development stage, and;

- pay attention to the trends of legislation and standard making of the transportation industry, such as rules and guidance issued by the Ministry of Transport and the National Technical Committee of Auto Standardization.

[36] http://www.tiaa.org.cn/xq.aspx?newsid=536&typeid=1

E. Internet of Things

Internet of ("**IoT**") things means the Internet which connects things to things. The business logic under IoT is that according to the agreed protocols, by using a variety of information sensing devices to connect various items via Internet to exchange information and communicate, it can automatically achieve intelligent identification, positioning, tracking, monitoring and management of items. Essentially, there are two basic business models under IoT, smart label recognition of objects and intelligent control of objects. These two basic application modes combined with multiple technologies such as intelligent induction and automation systems make a comprehensive IoT management system used for daily life, industrial control, and municipal management.

• Application Scenarios

In the applications of IoT, data is mainly collected, processed, and transmitted through the next three internet layers:

- data collected through intelligent sensing: that is, to obtain information by using a variety of automatic identification technologies (such as QR codes, electronic tags, voice recognition, etc.) or sensing technologies (such as wireless sensors, NFC, etc.) via sensing internet;

- data transferred via network: that is, connecting things to internet by technologies, services, cloud computing or other technological measures according to relevant internet protocols, so that to achieve internet-based items connection and interaction;

- data processing through the application layer: that is, to calculate and process the data collected through intelligent sensing in the application layer so that to achieve real-time control, accurate management, and scientific decision-making of the physical world.

There is a wide range of usages of IoT including smart transportation, environmental protection, government work, public safety, safe home, smart fire protection, industrial monitoring, environmental monitoring, elderly care, personal health, flower cultivation, water system monitoring, food traceability, enemy detection and intelligence gathering and so on. However, while this new technology provides convenience, this technology also brings new legal challenges.

• Legal Challenge

a) Personal Privacy

The core of IoT is the collection, analysis, and use of data, which provides the global vision potential of the entire organization and has unprecedented insights into customer behavior,

business operations, and work habits. While it's easy to understand why businesses are excited about the IoT model, accessing such large-scale data also carries significant risks.

The challenges of IoT to personal privacy protection are mainly reflected in the next five aspects:

- There is no a special law for IoT to protect personal's information, and considering the internet has no boundaries, for multinational IoT enterprises, when data collection and processing occur in different jurisdictions, there may be different countries' laws and regulations applicable.

- When IoT is installed in some public places, it is nearly impossible to obtain informed consent from people other than the device owner. The interactive interface provided by the IoT device to the user is not shown, nor does it provide data and function control options. In addition, people may be unaware of the existence of IoT devices and have no ability to withdraw from passive data collection.

- IoT applications such as wearables and smart homes blur the boundaries between private and public spaces.

- The monitoring and recording capabilities of IoT devices are often opaque, hidden, and difficult to detect. This brings challenge to users' right to know.

- It brings challenges the principle of transparency in privacy protection. Unlike websites, APPs, etc., IoT may not be able to show users the action of data collection, processing and relevant privacy policies.

b) Data Security

Based on the business logic of IoT, in this interconnected world, protecting data becomes very difficult because data can be transferred between multiple devices in seconds and the infinite new connections between devices also brings great challenges to the security of data. Other than the possibility of data breaches due to security bugs, hacking is more likely. Meanwhile, considering all data is transmitted over the Internet, and not all devices are secure, this may also lead to data leakage. In addition, even if data is not leaked from the user side, the acts of disobeying laws and regulations of service providers may as well as lead to security incidents.

- **Best Practice**

a) Personal Privacy Protection

For IoT enterprises, considering the large number of sensing devices used to collect data, enterprises need to be clear about how, where and what data is collected, and how to protect the data. According to China's existing relevant laws and regulations, IoT enterprises need to follow the basic principles about collection and process of personal information. IoT enterprises should classify data first and due to the intelligent identification and sensing system in IoT, the information collected will inevitably involve some personal sensitive information and important data. For such data, the IoT enterprises should pay special attention and undertake demanding obligations.

Besides, due to the efficiency and convenience of IoT, informed consent to process personal data in IoT networks may be difficult to obtain. In the case where there is no interactive connection with the personal information subjects, if it is difficult to obtain the user's informed consent, it is suggested to collect the de-identified non-personal information by using technical means rather than collect identified personal information directly.

b) Data Security Protection

For data security, considering IoT enterprises fall under to the definition of network operator under the CSL, IoT enterprises shall comply with the general and basic principles about cybersecurity protection and undertake the obligations of cybersecurity classified protection and strengthen cybersecurity protection. IoT enterprises should conduct regular network security inspections and employee training regularly to avoid cyber security vulnerabilities or employee leakage leading to data breach.

In addition, due to the wide application of IoT, it is also continuously deepening into some important areas, such as government work, public safety, fire protection, electricity, etc. Inevitably, some IoT enterprises fall under the definition of critical information infrastructure operator, and the corresponding cyber security protection obligations are also stricter.

V. Typical Regulatory Hurdles & Compliance Tips

Data security and privacy protection run through every stage of the business, and different business scenarios may involve different data compliance issues. With the promulgation of the CSL, China has established a framework for data protection system. In the coming future, the release of a series of supporting regulations and standards will further improve the system. In this regard, systemic and general compliance can no longer meet regulatory requirements, and companies shall conduct specific compliance based on different business scenarios.

A. Privacy Policy

Privacy policy is a statement made by a company to demonstrate its commitment to protect users' privacy and to fully disclose what information is collected and how to use it. By obtaining the consent of the users on privacy policy, the subsequent collection and use of personal information will be justified with a legal basis.

As above-mentioned, in the past year, China data protection authorities have put a lot of effort in investigating and punishing illegal collection and use of personal information, especially by Apps, and the core of it is the authorities' assessment on the construction and demonstration of privacy policy. Here in this part, we will discuss the requirements under Chinese laws and regulations on privacy policy and the current best practices for reference.

• General Laws and Regulations

The CSL requires companies to obtain the users' informed consent before collecting and using their personal information. Otherwise, administrative punishments, such as fines and suspension of business may be imposed, and civil damages may be pursued due to the

violation. On this basis, the national standard, *Information Security Technology - Personal Information Security Specification* (《信息安全技术 个人信息安全规范》in Chinese, "**PISS**") provides an example of privacy policy in its attachments for reference, which is the most widely-used template by companies currently. It is noted that an updated version of PISS has been issued on March 6, 2020, and will come into force on October 1, 2020.

Along with the frequent enforcement activities, more specific and detailed rules on privacy policy are introduced, as the four major authorities, CAC, MIIT, MPS and SAMR launched their special campaign on illegal collection and use of personal information by Apps. Therefore, in addition to the PISS, companies shall also consider the requirements under the *Guide to the Self-Assessment of Illegal Collection and Use of Personal Information by Apps* (《App 违法违规收集使用个人信息自评估指南》in Chinese, "**Guide**"), the *Methods for Determining the Illegal Collection and Use of Personal Information by Apps* (《App 违法违规收集使用个人信息行为认定方法》in Chinese, "**Methods**") as well as the draft national standard *Information Security Technology - Basic Specification for the Collection of Personal Information by Mobile Internet Application (App) (Exposure Draft)* (《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范（征求意见稿）》 in Chinese) [37] when preparing privacy policy.

- **Key Concerns in Enforcement Activities**

It can be seen from the current enforcement activities that the following issues are the top concerns of the authorities, when determining illegal collection and use of personal information:

- the independence and readability of privacy policies;
- the description of the purpose, method and scope of collecting and using personal information;
- the necessity of the collection and use of personal information;
- the security protection measures adopted; and
- the protection of users' rights.

- **Best Practice**

In general, when constructing a privacy policy, two aspects shall be taken into consideration in accordance with the PISS, the Guide and the

[37] The draft national standard *Information Security Technology - Basic Specification for the Collection of Personal Information by Mobile Internet Application (App) (Exposure Draft)* was exposed for comments on Jan 20th, 2020.

Methods, namely the demonstration of privacy policy and the key elements therein.

As for the demonstration of privacy policy, it is suggested to:

- make the policy easy to read and understand, using consumer-friendly language;
- ensure that the policy can be found easily in the forms such as pop-up prompts, text links, and FAQs;
- update the policy as needed to stay current with changes in business practices and legal requirements, and notify the users in a timely manner.

Structurally, the following elements shall be included in a privacy statement:

- how to collect and use a user's personal information (including purpose and necessity of collection and use);
- how to use cookies and similar technologies;
- how to share, transfer, and disclose a user's personal information;
- how to store and protect a user's personal information;
- how to protect a user's personal information;
- a user's rights to his/her personal information;
- how to process a child's personal information;
- cross-border transfer of personal information;
- how a user can learn of privacy policy changes; and
- contact information.

B. Employee Privacy

Employers usually collect a large amount of information of employees, and most of this information will fall within the scope of "personal information" as defined by the CSL. Since there is no exemption for the collection and use of employees' personal information under the Chinese laws and regulation, general rules shall apply. However, due to the relationship between employers and employees, additional scenarios shall be considered when dealing with employees' personal information.

• Recruitment

In the process of recruitment, employers need the candidates to provide his or her personal information to determine whether he or she is qualified. Before collecting, employers should clearly inform the candidates in advance that their personal information may be collected before they are employed for human resource management, background checks, and other employment-related purposes, and obtain written consent from employees. The scope of candidates' personal information collected should be limited to basic information directly related to labor relations, such as the candidate's age, gender, work experience, educational background, etc. At the same time, due to the different nature of specific jobs, employers can also collect other personal information, such as health information, criminal records, etc. Employer should avoid collecting personal information not related to the performance of labor contracts, such as marital status, birth status, family background, etc. Employers should delete the information of candidates who failed to pass the recruitment assessment timely.

• On-boarding

Employers should clearly inform employees when they are on-boarding that their personal information may be collected for human resource management, salary or benefit arrangements, performance management, IT support and services, internal monitoring or investigation and other purposes related to employment or business arrangement, and obtain the written consent of the employees.

• Internal Monitoring and Investigation

For the purposes of internal monitoring or investigation, employers should clearly inform the employee that the work email, work computer and other network or electronic equipment used by the employee during the employment period are provided by the employer and belong to employers, and the employee should use it only for work purposes. Moreover, the employees shall be informed that

information of their use of the above-mentioned network or electronic equipment may be collected and used for internal monitoring or investigation purposes.

If there are any monitoring equipment or smart devices in the office, employers should limit the scope of monitoring open or semi-open office areas, such as public office areas, conference rooms, front desks, etc. Employers should inform employees in advance about the installation and use of monitoring equipment or smart device in the office, and clearly identify the office area where the monitoring equipment is installed to draw employees' attention. Employers should ensure that the contents obtained from monitoring is not arbitrarily obtained or disclosed. Employers should ensure that among the personal information of employees collected through intelligent monitoring, only the content related to work and performance of duties is used, and information that is unintentionally collected and related to employee privacy should be promptly destroyed.

- **Storage and Cross-border Transfer**

In practice, some employees of multinational companies will be required to fill in personal information on a global personnel management electronic system. However, the servers of such systems in foreign companies are often installed overseas. In addition, some companies may need to transfer personal information collected in China abroad.

From the perspective of compliance and reducing legal risks, for employers that may need to transfer personal information data overseas, they should clearly inform employees of the purpose, scope, type of information to be transferred and the country or region in which the recipient is located and obtain employees' written consents.

- **Staff Demission**

Employers should protect the personal information of the employee who has left the company and should not use such information for other purposes or provide to any third party. After the statutory period (for example, the period for keeping web logs is not less than six months) or a reasonable retention period, employers should delete or anonymize such personal information.

Employers should clearly stipulate in the internal rules and regulations that employees should not copy or retain work information other than personal information after leaving the company. If employees require to copy personal information on work computers in the process of demission, employers may allow it and HR or

other employee should accompany to ensure that the information copied by employees is only their personal information so that to avoid leaking any work information or other employees' information.

C. Data Localization & Cross-border Data Transfer

Multinationals looking to centralizing and consolidating inter-organizational functions and resources face the imminent need to transfer different kinds of data globally for various business purposes. For example, a shared service center located in Singapore may process data collected from Shanghai, so as to help the headquarter in New York to formulate strategic plans. Under the Chinese law, certain entities bear the responsibility to store certain types of data locally. Under circumstances where it is necessary to transfer the data across border, a security assessment must be conducted prior the transfer.

• General Laws and Regulations

PRC laws do prohibit/restrict the cross-border transfer/export (including being accessed by entities/individuals outside Mainland China) of certain data. For example, State secrets are strictly prohibited from being disclosed or exported; and the export of trade secrets shall be subject to the agreement with the right holder of secrets.

Generally, when transferring personal information abroad, the informed consent of the data subject shall be obtained. Besides, according to the CSL, the personal information and important data collected and generated by CII Operators within the territory of China shall be stored locally in China. Where it is necessary to provide such data abroad due to business needs, security assessment shall be carried out according to the measures formulated by competent authorities. It is worth noting that, The *Security Assessment Measures on the Export of Personal Information and Important Data (Draft for Comments)* (《个人信息和重要数据出境安全评估办法（征求意见稿）》in Chinese) and the *Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comments)* (《个人信息出境安全评估办法（征求意见稿）in Chinese》further expand the subjects who shall fulfill obligations of data localization and data transfer security assessment from CII operators to all network operators.

• CII Operator

Article 31 of the CSL defines CII as "*information infrastructure that, in the event of damage, loss of function, or data leakage, may severely endanger national security, national economy, people's livelihoods or public interests*".

Further, the *Regulation on the Protection of Critical Information Infrastructure (Draft for Comments)*（《关键信息基础设施安全保护条

例（征求意见稿）》in Chinese） published in July 2017 provides that the following sectors and business areas are deemed to constitute CII: (i) government agencies and units in energy, finance, transportation, water utilities, sanitation and healthcare, education, social security, environmental protection and public utilities, etc.; (ii) information networks, such as telecommunications, radio and television, the Internet as well as businesses providing cloud computing, big data and other large-scale public information network services; (iii) scientific research and production in fields such as national defence, industrial equipment, chemicals, food and drugs; (iv) radio stations, television stations and other news agencies; and (v) other key operations.

- **Important Data**

The CSL itself does not contain a definition of important data. The *Security Assessment Measures on the Export of Personal Information and Important Data (Draft for Comments)* (《个人信息和重要数据出境安全评估办法（征求意见稿）》in Chinese) defines important data as "data that is closely related to national security, economic development and societal and public interests".

Further, the non-binding national standard *Information Security Technology -Guidelines for Data Cross-Border Transfer Security Assessment (Draft for Comments)* (《信息安全技术 数据出境安全评估指南（征求意见稿）》in Chinese) provides a detailed but non-exhaustive appendix listing important data of 27 sectors/industries, including electricity, steel, chemical, water conservancy, environment protection etc.

It is to be noted that, although the regulation and guidelines serve as references for entities to determine CII operators and their status of retaining important data, further specifications are to be made by competent authorities of respective sectors/industries, while the government has the last say and can intervene at any time deemed necessary.

- **Security Assessment**

At present, the non-binding national standard *Information Security Technology -Guidelines for Data Cross-Border Transfer Security Assessment (Draft for Comments)* (《信息安全技术 数据出境安全评估指南（征求意见稿）》in Chinese) stipulates detailed procedures of security assessment on the export of data. Although the standard is just a draft version, and no penalty has been imposed in this regard so far, it has practical guiding significance to employers.

It is also noteworthy that the *Measures for Personal Information Cross-Border Transfer Security Evaluation (Draft for comments)* (《个人信息出境安全评估办法（征求意见稿）》 in Chinese), the latest draft measures of the security assessment on the export of personal information expands its applicable scope to all network operators, indicating all network operators rather than only CII operators, shall apply to the local cyberspace administrations at the provincial level for security assessment for cross-border transfer of personal information before transferring the information abroad.

- **Best Practice**

Considering the rules for CII operator definition and the security assessment on the export of personal information and important data are still in the draft stage, and that no penalty has been imposed in this regard so far, it is advisable for companies to conduct a pre-review within China to identify the relevant data likely to be prohibited or restricted from cross-border transfer subject to the relevant laws, regulations and agreements. For personal information specifically, it is advisable to obtain the data subjects' informed consent at least and follow the procedures of security assessment stipulated by the draft national standard mentioned above before the cross-border transfer.

If a company is likely to be considered as a CII Operator in China, it shall be prepared to satisfy the localization requirement and may consult with the competent sectoral authorities if it is allowed to export important data.

Besides, if the cross-border transfer of data involves criminal proceedings (including evidence collection), the procedural requirements under the *International Criminal Judicial Assistance Law* (《国际刑事司法协助法》 in Chinese) shall be considered, as it prohibits entities/individuals from providing assistance in criminal proceedings without the consent of the competent authorities of China.

D. Classified Protection of Cybersecurity

On May 13, 2019, State Administration for Market Regulation and the Standardized Administration officially released three new national standards, namely the *Information Security Technology - Guidelines for Grading of Classified Protection of Cyber Security* (《信息安全技术 网络安全等级保护基本要求》in Chinese), the *Information Security Technology - Evaluation Requirement for Classified Protection of Cybersecurity* (《信息安全技术 网络安全等级保护测评要求》in Chinese) and the *Information Security Technology - Technical Requirements of Security Design for Classified Protection of Cybersecurity* (《信息安全技术 网络安全等级保护安全设计技术要求》in Chinese), which are called the standards for Cybersecurity Classified Protection 2.0. These standards have come into force as of 1 December 2019. Compared with Information Security Classified Protection 1.0, Cybersecurity Classified Protection 2.0 upgrades the requirements on security protection in several aspects.

• Classified Protection 2.0

There are several differences between Classified Protection 2.0 and Classified Protection 1.0. First, Classified Protection 2.0 extends the application scope of Classified Protection 1.0. Information Security Classified Protection 1.0 mainly emphasizes the protection of information systems and government websites; while the Cybersecurity Classified Protection 2.0 extends the objects of protection to adapt to the repaid development in emerging technologies, such as cloud computing, big data, the Internet of Things, mobile internet and so on, which Classified Protection 1.0 does not cover. Second, Classified Protection 2.0 improves the security requirements of Classified Protection 1.0. Third, Classified Protection 2.0 requires active prevention and control, while the 1.0 does not.

According to Article 59 of the CSL, implementing Classified Protection 2.0 is a statutory duty that all network operators must perform. Where a network operator fails to fulfill the obligations of cybersecurity protection, it shall be ordered to make rectification, warned and/or fined by the authorities. Meanwhile, the persons directly in charge and other persons directly liable might be subject to a fine as well.

• Determination of Classification

Classified Protection 2.0 follows the five-level security protection system established by the Classified Protection 1.0 (see as below), but further strengthens the protection of the legitimate rights and interests of citizens, legal persons and other organizations, by raising the

level from 2 to 3 where the infringement is particularly serious.

Infringed Subjects	Degree of Infringement		
	General	Serious	Particularly Serious
Legitimate rights and interests of citizens, legal persons and other organizations	Level 1	Level 2	Level 3
Social order, public interests	Level 2	Level 3	Level 4
National security	Level 3	Level 4	Level 5

- **Best Practice**

Multinationals, especially those with internal member systems and own a large number of users shall come into compliance with the requirements under Classified Protection 2.0. To prepare for Classified Protection 2.0, companies may follow the work procedures as below:

Step 1	Classification	– Determine objects – Assess classification independently – Reviewed by experts (≥ Level 2) – Examined and approved by competent authorities
Step 2	Record	– File for record with the public security authorities – Examine and issue record certification
Step 3	Construction and Rectification	– Analyze the gap between current security protection conditions and the requirements of classified protection 2.0 – Make construction and rectification
Step 4	Classified Evaluation	– Choose qualified evaluation agencies – Conduct annual classified evaluation (≥ Level 3) – Produce rectification report
Step 5	Supervision and Inspection	– Accept regular supervision and inspection from the public security authorities – Conduct regular self-inspection（≥1/Year）

E. Use of VPN

Due to China's restriction on international connection, Virtual Private Network ("**VPN**") is widely-used by multinational companies in daily operation. However, in recent years, local public security authorities have become proactive in the enforcement targeting the use of unqualified VPNs, and issued fines on both individuals and companies. There are several cases punishing individuals who use unqualified VPN services only for self-entertainment in 2019. Furthermore, it is noticeable that, in a recent case, a foreign trade company was punished by the local public security authority in Haining, Zhejiang Province, due to its use of unqualified VPN to access International Internet for business. As such, how to use VPN legally in Mainland China has become an important compliance issue for companies, especially multinationals to pay attention to.

• General Laws and Regulations

According to Article 5 and Article 6 of the *International Telecommunication Exchange Administration Regulations* (《国际通信出入口局管理办法》in Chinese), and Article 6 of the *Interim Provisions on Regulating International Networking of Computer Information Networks* (《计算机信息网络国际联网管理暂行规定》in Chinese), entities and individuals shall use legally qualified channels, which is approved by the competent authority, namely Ministry of Industry and Information Technology ("**MIIT**"), to access International Internet.

In other words, unapproved channels, such as those self-established, sub-leased or rented from overseas providers are not allowed from using to connect International Internet. Any entities or individuals who access international internet via unqualified VPN services shall be (i) ordered to cease international connection; (ii) issued with an administrative warning; (iii) imposed a fine of up to RMB15,000 (about USD 2,135); and (iv) confiscated illegal gains (if any).

• Key Concerns in Enforcement Activities

In enforcement activities, two major issues concerned by the authorities are whether the accessing of international Internet is conducted through qualified channels and whether the qualified channels are used in proper ways.

a) Qualified Channels in Mainland China

As mentioned above, entities and individuals shall use legally qualified channels, which is approved by MIIT to access international Internet. However, so far as we know, in addition to the top three big basic telecommunications service providers, few companies are qualified to provide international connection services. That is

to say, generally, to get access to international Internet in China, companies are suggested rent international gateway channels provided by China Unicom, China Mobile, or China Telecom.

b) Proper Ways to Use International Connection

Even a company has rented a qualified VPN, attentions should be paid on the use of VPN or the accessing of International Internet through VPN. According to the relevant laws and regulations, entities and individuals shall not use international connections to harm State security, disclose State secrets or engages in other illegal or criminal activities. It is also forbidden to produce, consult, duplicate or disseminate information prohibited by laws, such as violent, obscene or pornographic materials and other information that may present an obstacle to public order or state security, etc. In July 2016, an individual was sentenced to an eight-month imprisonment, in addition to a fine of RMB10,000 (about USD1,450) for downloading prohibited content via VPN and selling it, since it has constituted the crime of illegal possession of articles promoting terrorism or extremism under the Criminal Law.

- **Best Practice**

Based on the above, multinationals, as (potential) users of VPN, are suggested to consider the following tips, when accessing International Internet in China.

a) Accessing International Internet via Qualified VPN

As aforementioned, a company shall rent an international gateway channel from a provider with a corresponding certificate. Specifically, it is suggested to rent the channel from the top three big basic telecommunications service providers in China.

b) An IT Compliance Program to Regulate Employee's Accessing of International Internet

It is also advised that companies shall establish a well-rounded IT compliance program, which helps to perform the network security duties on the companies mentioned above. To be more specific, the IT compliance program shall include an IT administration system, an internal registration system, and a comprehensive IT handbook and regular training shall also be introduced. The IT compliance program shall ensure the security of the VPN services and the network, and also ensure that the employees should access international internet legally in a

proper way without unauthorized sub-leasing and without visiting, producing, duplicating or disseminating any information prohibited under the relevant laws and regulations in China.

c) Blocking Websites with Prohibited Information

A qualified VPN shall be used properly without violating the relevant laws and regulations. Currently, it is widely adopted by multinationals to block sensitive websites with certain information by a whitelist or blacklist mechanism. Specifically, such prohibited information includes without limitation:

- the information against the fundamental principles set out under the Constitution;
- the information endangers national security, leaks State secrets, or incites overthrow;
- the information damages the State's honor or harms the interests of the State;
- the information incites ethnic hatred or discrimination, or undermines solidarity among all nationalities;
- the information undermines the State's policies on religions, and advocates religious cults or feudal superstition;
- rumors to disrupt social or economic order, or undermine social stability;
- the information involves obscene or pornographic materials, gambling, violence, killing, or instigates others to commit crimes;
- the information humiliates or defames other persons, or infringes the legitimate rights and interests of others; and
- the information advocates terrorism or extremism.

F. Data Breach

In recent years, data breach and leakage have become one of the top concerns in the world. According to a report from the security intelligence provider Risk Based Security for the Q3 quarter of 2019, from January 1, 2019 to September 30, 2019, there were 5,183 data breaches disclosed globally, and the amount of data leaked reached 79.95 100 million records. Any business that utilizes the Internet may experience data breach, therefore data security and breach prevention have become more and more important in internal compliance programs.

• General Laws and Regulations

The CSL requires entities to prevent personal information and network data from being disclosed, stolen or tampered, by performing obligations of security protection. Any violation of such requirements may lead to administrative punishments, like warning and fines, as well as civil compensation. Besides, intentional data leakage may bring criminal liabilities for both individuals and entities.

• How to Prevent Data Leaks

To prevent data leakages, enterprises should take the obligations of data security protection, to be specific, the following five aspects can be noted:

- perform duties of Classified Protection 2.0
- adopt data classification and identify critical data;
- introduce comprehensive data protection system;
- find and repair system vulnerabilities in a timely manner;
- monitor and record cybersecurity risks;
- make data breach response plan; and
- organize employee training about breach prevention and response.

• Best Practice

When a data breach occurs, the following aspects shall be considered in order to address and minimize the potential influence.

a) Internal Investigation and Timely Remedy

After discovering a security incident, enterprises should immediately deploy an incident handling team in accordance with the emergency mechanism set before to investigate the cause of the data leakage, identify the type, quantity and the sensitivity of the data involved, determine the scope of the affected personal information

subject, and analyze whether the data involved is encrypted and whether the prevention measures have effectively defended against attacks. Based on these, assess the degree of impact on the rights and freedoms of the personal information subject and other possible consequences. At the same time, enterprises should immediately protect cyber systems, repair vulnerabilities that may cause data leakage, and prevent further data leakage. In the process, enterprises can hire external legal and technical teams to assist with electronic data forensics and retain evidence for possible subsequent investigations and disputes.

b) Notification to Regulators and Personal Information Subjects

Based on the assessment of the impact and risk of security incidents and relevant laws and regulations, enterprises should determine whether they need to report to the regulatory agencies and whether they need to notify the affected personal information subjects. If necessary, enterprises should quickly determine whether the security incident is under the jurisdiction of extraterritorial laws and whether there are special provisions in the extraterritorial laws involved, which regulatory agency(s) to report, whether to include regulatory agencies outside the region, the scope of the data subject to be notified and the method of notification, and the contents of the report and the notice. Enterprises can commit professional law firms to handle this. After confirming the above contents, enterprises should timely report and notify according to relevant laws and regulations.

c) Recording and Filing

Regardless of whether a security incident needs to be reported to the supervisory authority or notified to the affected subjects, enterprises should keep a record of the security incident. If the enterprise does not report and notify according to the evaluation decision, the enterprise should record the analysis process and results of the evaluation. Enterprises should also keep relevant records of the facts related to the security incident, the cause of the incident, the relevant impact, the remedial measures taken, and the relevant web logs should be retained for at least six months. This is not only a requirement of laws and regulations, but also becomes an important reference and evidence for supervisory agencies.

d) Accountability

If it is verified that a data leakage has indeed occurred, the enterprise should promptly trace the source of the breach in a timely manner and investigate the causes. If it is the responsibility of the enterprise's internal staff, enterprise should take the internal review in a timely manner, save

the evidence, and deal with this in accordance with the enterprise's internal regulations, and initiate a lawsuit if necessary; if due to an external hacker attack, the enterprise should review the enterprise's system while investigating whether the enterprise's system exists loopholes and whether it has fulfilled the statutory obligations， such as Classified Protection 2.0. At the same time, the enterprise should actively assume responsibility to the relevant subjects, compensate for the losses, and actively obtain the understanding of the relevant subjects.

G. Privacy by Design & Privacy by Default

Actually, Privacy by design is an old and broad concept in systems engineering which is described as "not about data protection" but rather "designing so data doesn't need protection" with the "root principle based on enabling service without data control transfer from the citizen to the system" in Wikipedia.

Privacy by Design and Privacy by Default is more popular with effective as of the GDPR. In short, the GDPR requires:

- Data protection by design: data controllers must put technical and organizational measures such as pseudonymization in place – to minimize personal data processing and personal data collection.

- Data protection by default: data controllers must only process data that are necessary, to an extent that is necessary, and must only store data as long as necessary.

Principles of Privacy by Design may be applied to all types of personal information, but should be applied with special vigor to sensitive data such as health information and financial information. Privacy by Design aims to give data subjects more power over their personal data. For Privacy by Default, offering the most privacy friendly option as a default setting will give people an actual say over which parts of their personal data can be used.

Although, the concept of Privacy by Design and Privacy by Default are not detailed in related PRC laws and regulations, companies which provide product to users shall put the principles of Privacy by Design in the early stages of any project from transparency, users' control and data security.

- **Best Practice**

We encourage companies shall ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle. For example, when:

- building new IT systems for storing or accessing personal data;

- developing legislation, policy or strategies that have privacy implications;

- embarking on a data sharing initiative; or

- using data for new purposes.

H. Data Crawling

Data crawling (i.e. conducting automatic data extraction from websites or servers by robots or other tools) is widely used by content platforms and big data companies. Generally speaking, data crawling is an efficient way to acquire massive data from the Internet. However, according to the relevant and regulations, excessive extraction of data and improper use of data crawling may lead to criminal liabilities, administrative liabilities and civil liabilities.

• Criminal Liabilities

a) The crime of illegally obtaining data from computer information system

If a data crawler hacks into a computer information system, such as breaking through a firewall and bypassing anti-scraping measures to achieve its purpose of illegally acquiring data, it may violate Article 285 (2) of the *Criminal Law*.

In a case, four employees of an IT company based in Shanghai cracked the anti-scraping measures of Beijing Bytedance Technology Co., Ltd., used "tt_spider" files to scrap video data, forged "device_id" to bypass the server identity check, and forged the UA and IP to bypass the server's access frequency restrictions. The court ruled that the IT company and the four employees were all found guilty for committing the crime of illegally obtaining data from computer information system. Therefore, the company was fined 200,000 CNY, and four employees were each sentenced to 9 months to 1 year in prison and received a fine.

b) The crime of illegally hacking into computer system

If the computer information system hacked by the data scraper concerns state affairs, national defense, and cutting-edge science and technology, the scraper can be found guilty for this crime even if no data is scraped, pursuant to Article 285 (1) of the *Criminal Law*.

c) The crime of infringing on citizens' personal information

If the data scraper crawls non-public personal information without the consent or authorization and the personal information involved in the case reaches a certain amount, this may constitute the crime of infringing on citizens' personal information specified in Article 253 of the *Criminal Law*.

• Administrative Liabilities

The CSL itself does not specify administrative liabilities for illegal use of data scraping. However, Article 16 of the *Data Security Management Measures (Draft for comments)*

(《数据安全管理办法(征求意见稿)》in Chinese, "**Measures**") recognizes data scraping used in a legal manner and sets a "one third of the average daily website traffic" as a tentative "safe harbor" rule which reflects the regulatory approach that may be officially adopted by the authority in the future.

a) A proposed "safe harbor" rule

Article 16 of the Measures stipulates that network operators using automatic means to access and collect website data must not hinder the normal operation of the website; where such acts are seriously affecting the operation of the website, e.g. the automatic access exceeds one-third of the average daily traffic of the website, the data scraping shall be stopped when the website operator requests. Although this provision is only a draft version, it has guiding significance when other laws remain silent about this issue.

b) Illegal access to personal information

Data scraping may also violate Article 44 of the CSL, that is, no individual or organization may steal or otherwise illegally obtain personal information. In violation of this provision, if not subjected to criminal liability, the public security department shall confiscate the illegal income and impose a fine of more than 1 to 10 times the illegal income. Where there is no illegal income, a fine of less than 1 million CNY shall be imposed.

- **Civil Liabilities**

Improper use of data crawling may also lead to civil lawsuits, of which the major claim is unfair competition. In *Dianping v Aibang (2011)*[38], the court ruled that customer reviews collected and sorted on dianping.com are the plaintiff's fruits of labor with high commercial value and should therefore be protected under the *Anti-Unfair Competition Law*. In *Dianping v Baidu Map (2016)* [39], the court established a "substantive substitute" test, which refers to that to establish an unfair competition claim, the content on the data scraper's website must be proved to be a substantive substitute of that on the data owner's[40] website, so that users could obtain a substantive part of the relevant data merely by accessing the data scraper's website and would therefore visit the data owner's website less frequently. In the end, the court ordered Baidu Map to pay 3 million CNY as a compensation for Dianping. After this judgment, the substantive

[38] Beijing First Intermediate People's Court (2011) Final Trial No. 7512 (北京市第一中级人民法院（2011）一中民终字第 7512 号)

[39] Shanghai Intellectual Property Court (2016) Final Trial No. 242 (上海知识产权法院（2016）沪 73 民终 242 号)

[40] Under Chinese law, "data owner" is not a formal legal term as the law does not recognize data ownership so far. For discussion purpose, data owner is adopted to refer to network/business operators who control, manage and have legal interested in the data.

substitute test was widely adopted by other courts in similar unfair competition cases concerning data scraping.

- **Best Practice**

Based on the needs of technological development and commercial competition, data crawling is a useful tool that may be difficult to give up. Therefore, we suggest companies to use data crawling in a legal manner and abide by the following principles:

- do not break through technical measures, firewalls and access controls;

- do not target personal information, trade secrets and copyrighted data;

- avoid imposing more than one third of the average daily website traffic;

- stop scraping and delete data in time once receive complaints;

- avoid substantial substitute of the service, and;

- keep operation logs and relevant documents for future verification.

I. Data Aggregation

Data aggregation is a formal framework in which are expressed means and tools for the alliance of data originating from different sources and it aims at obtaining information of greater quality. For enterprises, data aggregation can be used to analyze big data, improve user profiling, and enhance the value of data assets. Data aggregation may lead to a range of related data and privacy issues. Here we focus on two main aspects among them: (i) user consent, and (ii) due diligence in mergers and acquisitions (**"M&A"**).

• The Google Case

On January 21, 2019, the French Data Protection Authority (**"CNIL"**) imposed a fine of 50 million EUR on Google under the GDPR for its alleged failure to (i) provide notice in an easily accessible form, using clear and plain language, when users configure their Android mobile device and create a Google account, and (ii) obtain users' valid consent to process their personal data for ad personalization purposes[41]. Although CNIL did not clearly state that the case was directed at Google's data aggregation, the penalty decision pointed out that the cross-business data aggregation behind personalized advertising was one of the actions illegal.

• Invalid Consent to Data Aggregation

In this case, Google did mention data aggregation to users sometimes, such as in its Privacy and Terms: we will aggregate the personal data generated in our services and different terminals based on the purpose of data processing; for example, based on your account settings, we will serve you personalized ads based on your use of search results and YouTube-generated interests and a spell correction model based on massive data across services. However, in another Privacy Policy and other documents for users, Google is only vague about data aggregation. In this way, Google only informed the users of the existence of its data practice, sometimes even not mentioned data aggregation, and merely explained by ways of taking examples rather than refining the specific data types and how to use these data for which purposes.

Per the CNIL's view, the above statements in Google's privacy policy is relatively simplistic and completely prevents users from knowing what data is being used for what services and what the consequences will be. Specifically, on the one hand, Google did not allow users fully understand the specific consequences of processing; on the other hand, the processing of

[41] https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

Google personalized ads, which involved data aggregation as the technical means, is not "clear" and "understandable".

- **What is Valid Consent**

Google revised its privacy policy in 2012-2014 and has caused investigations by the EU's Article 29 Working Party and several national data protection authorities (including the CNIL). At that time, the Article 29 Working Party gave some recommendations to Google, some of which we think are valuable for compliance promotion:

- clearly inform users of the specific purpose of data aggregation and the type of data used for each purpose.

- to obtain the legal basis of data aggregation, that is, to obtain the explicit consent of the user through positive actions;

- provide users with a convenient and effective opt-out choice to data aggregation;

- ensure compliance with the data minimization principle, purpose limitation principle, and privacy by design requirements;

- isolate and distinguish the data collected via different data aggregation processes;

- the data retention period for data aggregation shall be consistent with the purpose.

- **Due Diligence in M&A**

Due diligence is a critical aspect of M&A, particularly in transactions concerning data aggregation and data assets. To accurately value the transaction and identify significant risks, a purchaser or investor (the **"Buyer"**) will typically conduct a comprehensive review of the corporation to be acquired (the **"Target"**). This due diligence process will also form the basis of the representations and warranties in the transaction documents.

- **What is "Proper Due Diligence"**

Due diligence on data privacy protection and cybersecurity, is not a one-size-fits-all exercise - the Buyer needs to have a basic understanding of the Target's business to focus on key issues. For instance, if a Target only does business-to-business deals, due diligence focusing on the protection of personally information is less important than due diligence focusing on the protection of "important data"[42]. Conversely, important data and trade secrets diligence is

[42] "Important data" refers to data that is closely related to national security, economic development and societal and public interests in Chinese laws.

probably less important for a consumer-facing Target that collects significant amount of personal information. Overall, the Buyers should consider the nature of the Target and its data to properly scope and structure due diligence. Here are some of the major aspects to consider:

- identify the target's digital assets (e.g. personal information, important data, trade secrets);
- evaluate the target's internal and external data privacy and cybersecurity programs;
- identify ongoing or past incidents and breaches;
- assess regulatory compliance (e.g. compliance on mobile application, "classified protection scheme" and cross-border transfer); and
- assess potential liabilities (e.g. civil, administrative and criminal liabilities).

- **Due Diligence and Transaction Terms**

In the digital age, ever company is vulnerable to data incidents, regardless of the strength of its policies and the sophistication of its IT security infrastructure. For Targets with significant data, due diligence, no matter how in-depth and comprehensive it is, may not identify all the risks regarding data privacy and cybersecurity.

Therefore, in the process of formulating and signing transaction documents, to include representations and warranties clauses based on due diligence results can change information asymmetry and prevent unknown risks of the Target.

In addition, the Buyer may also propose further protection terms such as compensation liability, security deposits, escrow accounts, and the right to opt-out, thereby mitigating potential damages.

J. Big Data & Competition

Companies now compete for data assets. Some companies have generated and accumulated a huge amount of customer-data, which become their critical competitive edge. Some have to rely on access to others' data, which is the basis of their analytics, machine learning, or any other kind of algorithm services. Consequently, clashes are unavoidable. To name a few, in 2017 Alibaba's logistic platform temporarily closed its API to SF Express, a top shipping service provider in China, and the same year Huawei and Tencent argued on whether Huawei's handset can have access to users' data generated in Tencent's app, Wechat. Similar incidents also occurred in the past year.

The battles over data present legal issues concerning data's ownership or competition law, which cannot be resolved under traditional rules due to its intangible, non-rivalrous nature. Although the relevant laws lag behind, in practice some looming rules have been drawn to help refine the boundary of what can and what cannot be done about data assets.

• Data Scrapping or Crawling

In China, the past years have seen quite some civil disputes concerning data scrapping or crawling. For example, CCTV sued a website Zhibo.tv for unlicensed live show of 2016 Rio Olympic Games, which were actually retrieved from CCTV but additionally accompanied by a livestream broadcaster and commentary of Zhibo itself. Last year, the case was decided. The court handed down the judgment holding that Zhibo's conduct is "free-riding" and constitutes unfair competition under the *Anti-Unfair Competition Law*. Similarly, most crawling related civil cases are also decided according to the *Anti-Unfair Competition Law*, based on whether the scrapper is taking unfair advantage of others. Various standards are developed following this rule, such as whether industry norms like web search robots are obeyed (*Baidu v. Qihoo* 360, 2014), or whether users' consents are properly obtained (*Sina v. Maimai*, 2017).

Excessive crawling of others' data may even constitute the crime of "illegally accessing computer system data," which could lead to up to 7 years' sentence plus fines in China. Judging from some typical cases last year, the question is whether the defendant is legally accessible to such data, or the defendant knowingly bypasses the anti-crawling measures placed by the victim.

• Data as "Essential Facility"

Antitrust law around the world is increasingly and inevitably overlapping with data regulation. Inspired by the U.S. case, *HiQ Labs v.LinkedIn*,

the right to access others' data is considered under the essential facility doctrine of antitrust law. However, there are still many obstacles that need to be overcome in order to apply the antique theory in a digital era. For example, the doctrine requires that a competitor is unable to duplicate the essential facility, which is opposite to the non-rivalrous nature of data. In addition, the rules on privacy protection and the lack of user consent may also prevent forced sharing.

- **Best Practice**

With the gap in law, what companies can do is to make avail of the existing rules to the extent possible. First of all, contract is always the basis in data sharing. Detailed clauses on each parties' rights and duties can provide certainty where the law fails. In addition, intellectual property rights, such as copyrights or trade secrets, may help protect data assets when data ownership is not defined. Specifically for data scrapping or scrawling, anti-crawling measures are always recommended to safeguard data, not only technically but also in the legal sense that an infringer's bypassing such measures can help demonstrate it is unjustified.

VI. Looking Forward

In recent years, we have seen an unprecedented expansion in data privacy and security regulations globally. Major jurisdictions around the world have made or updated their regulatory requirements with differences in approaches and priorities. Therefore, MNCs are facing greater challenges in applying divergent global data privacy and security regulations.

China, ever since the implementation of the CSL on June 1, 2017, has entered a new era for data protection, with legislators continuously rolling out laws and proposals, and regulators stepping up enforcement. It is believed that, the "Personal Information Protection Law" and the "Data Security Law", which are in the pipeline for the moment and expected to be promulgated in the coming three years, shall bring China's data protection and security regulation to a new height, where enforcement activities will be more normal and general.

Meanwhile, along with the improvement of legislation and supervision, private litigations initiated by individuals and entities, as well as public interest organizations are estimated to increase, for the purpose of damage compensation, business competition, etc. The unprecedented attention paid by the capital market to data protection has shown that, data compliance should be incorporated in the beginning of the product's design and run through the entire life cycle of the product, rather than considering data compliance assessments after the listing of products or the establishment of business models.

As such, for companies with businesses in China, it is the time to take China's data privacy and security laws more seriously than ever.

Authors

Ken Dai - Partner, Shanghai Office

Location	Shanghai
Direct Line	+86 21 5878 1965
Email	jianmin.dai@dentons.cn
Mobile	(86) 139 1611 3437
Practice Areas	Antitrust | Data Privacy Protection and Cybersecurity | Anti-Corruption and Anti-commercial Bribery

Jet Deng - Partner, Beijing Office

Location	Beijing
Direct Line	+86 10 58137038
Email	zhisong.deng@dentons.cn
Mobile	(86) 135 2133 7332
Practice Areas	Antitrust | Data Privacy Protection and Cybersecurity | Anti-Corruption and Anti-commercial Bribery

ABOUT DENTONS

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognized by prominent business and legal publications for its innovations in client service, including founding Nextlaw Enterprise, Dentons wholly owned subsidiary of innovation, advisory and technology operating units. Dentons' polycentric approach, commitment to inclusion and diversity and world-class talent challenge the status quo to advance client interests in the communities in which we live and work.

dentons. com

dentons. com