LLINKS Law Offices
通力律师事务所

上海
上海市银城中路 68 号
时代金融中心 16 楼和 19 楼
邮编：200120
电话：+86 21 3135 8666
传真：+86 21 3135 8600

SHANGHAI
16F/19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
邮编：100005
电话：+86 10 8519 2266
传真：+86 10 8519 2929

BEIJING
4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话：+852 2592 1978
传真：+852 2868 0883

HONG KONG
27F, Henley Building
5 Queen's Road Central
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

伦敦
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

LONDON
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com
master@llinkslaw.com

Llinks Corporate and M&A Bulletin
June 2019

A Summary and Innovation of Data Security Legislation

——A Review of Data Security Administrative Measures (Draft)

By David Pan | Nigel Zhu

The Office of the Central Cyberspace Affairs Commission (Cyberspace Administration of China) (hereinafter "**CAC**") plays a pivotal role in China's legislation and enforcement of cyber security laws. Since the Cyber Security Law ("**CSL**") took effect on June 1, 2017, the CAC has issued more than 30 regulations (including drafts), among which some attracted considerable attentions from the public, such as the *Measures on Protection of Critical Information Infrastructures (draft)*, *Measures on Assessment of Cross-border Transfer of Personal Information and Important Data (draft)* and *Measures on Administration of Blockchain Information Services*.

As the CSL is approaching its second anniversary, the CAC issued on May 28, 2019 *Data Security Administrative Measures* (draft) (the "**Measures**"). At a first glance, the Measures appear to be merely "highlights" and a compilation of existing cyber security laws and regulations. A closer look, however, reveals that the Measures are a comprehensive "enhancement" to the existing cyber security laws and regulations.

如果您需要本出版物的中文本，
请与下列人员联系：

郭建良: +86 21 3135 8756
Publication@llinkslaw. com

For more Llinks publications,
please contact:

Roy Guo: +86 21 3135 8756
Publication@llinkslaw. com

Llinks Law Offices
www. llinkslaw. com

Upon the issuance of the Measures, Llinks Cyber Security and Data Service Team attempt to, in light of the Measures, interpret some of the long-lasting issues since the enactment of the CSL.

1. Relationship Between the Measures and Existing Laws

The Measures provide for 1) application scope; 2) protection of personal information and important data; 3) network operators' obligations in data practices; and labilities for illegal data practices, all of which are already covered by some existing laws and regulations.

Nevertheless, not a mere repetition of existing laws, the Measures incorporate provisions of innovation and enhancement based on existing laws. The Measures provide for a number of new obligations for network operators; enhance requirements in the CSL in relation to protection of important data and personal data, and expand the scope of obligees; and in response to the development of network technologies, start to regulate on new issues such as data scraping and automatic compilation.

It is worth pointing out that currently the Measures, *Measures on Assessment of Cross-border Transfer of Personal Information and Important Data* and several other regulations are still at the phase of exposure drafts, and they can be subject to changes before they are officially issued. The Measures and other draft laws may need to be aligned and thus can affect one another in the process. In any event, the innovation and improvements reflected by the Measures are worth attention.

2. Definition of Data

Legal practitioners in the cyber security area must be familiar with "personal data" and "important data", yet few are able to define what data is. Thus, the question is, other than personal information and important data, are there any other types of data regulated under the current legal framework?

The Measures define "network data" as "electronic data that has been collected, stored, transferred, processed or generated via network", which matches exactly the definition given by the CSL. But either the

Measures nor any other current laws and regulations fail to define where the boundaries of data are. In the CSL, only personal information and important data are specifically mentioned, but this does not mean data only comprises these two types. First of all, *Information Security Technology – Data Cross-border Transfer Security Assessment Guidelines* (draft) exclude state secret from important data, and the Measures also provide that regulation on state secret shall be deferred to other relevant laws. This clearly shows that state secret is not an independent type of data. Secondly, the Measures generally exclude "companies' operational data and internal administrative data" from important data. In summary, it can be inferred that under the current legal framework, data can be divided into at least the following categories: state secret, personal information, important data, and "companies' operational data and internal administration data" and other data that does not amount to important data (tentatively "non-important data").

State secret is regulated under State Secret Law and other related laws. Data that is directly related to cyber security and is thus directly regulated under cyber security laws is personal information and important data, which means any discussions on these two types of data shall be premised on a clear definition of them.

2.1 Definition of Personal Information

The Measures follow the definition of "personal information" in the CSL, i.e. "all kinds of information recorded electronically or in other ways that can, independently or in combination with other information, identify a natural person." The definition of personal information is scattered in many laws and regulations. We summarize the definition of "personal information" in some major existing laws and regulations, as shown in Table 1 below.

Data Security Management Measures (Draft for Comment) (2019)	Personal information is all kinds of information recorded electronically or in other ways that can, independently or in combination with other information, identify the personal identity of natural persons.
CSL (2017)	Personal information is all kinds of information recorded electronically or in other ways that can, independently or in combination with other information, identify the personal identity of natural persons.

A Summary and Innovation of Data Security Legislation-A Review of Data Security Administrative Measures (Draft)

Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Laws in Handling Criminal Cases of Infringing Citizens' Personal Information (hereinafter referred to as "SPC & SPP Judicial Interpretations") (2017)	"Personal information of citizens" stipulated in Article 253 of the Criminal Law refers to all kinds of information recorded electronically or in other ways that can, independently or in combination with other information, identify a particular natural person or **reflect the activities of a particular natural person**.
Measures for Security Assessment of Cross-border Transfer of Personal Information and Important Data (Draft for Comment) (2017)	Personal information is all kinds of information recorded electronically or in other ways that can, independently or in combination with other information, identify the personal identity of natural persons.
Information security technology - Personal information security specification (hereinafter referred to as "Personal Information GB Code") (2017)	Personal Information is all kinds of information recorded electronically or in other ways that can, independently or in combination with other information, identify a particular natural person or **reflect the activities of a particular natural person**.

Table 1: Comparison of "personal information" definitions

As can be seen from the above table, the SPC & SPP Judicial Interpretations (effective before the CSL) and the Personal Information National Standard (effective after the promulgation of the CSL) both incorporate "information reflecting the activities of a particular natural person" into the definition of "personal Information". The "personal information" here includes two categories: one type of personal information which can identify a particular natural person by the specific nature of the information itself, and the other type of personal information which is generated by a particular natural person in his/her activities, including personal location information, personal call record, personal browsing record, etc. The definition of "personal information" in the Measures follows the definition of the CSL, which does not include "information reflecting the activities of a particular natural person". Consequently, which limits the scope of personal information to a certain extent.

Personal information that can independently identify a natural person is well understood, but all of the above laws and regulations also include information that can identify a natural person "in combination with other information" as personal information. "In combination with other information" here is a

qualitative rather than a quantitative rule, so the question is that to what extent does "personal information" require the combination of other information to reach the legal "identifiable" standard, thus constituting the "personal information" prescribed by laws and regulations? In other words, if one piece of information only needs to be combined with 5 pieces of other information to identify a particular natural person, and another piece of information needs to combine 50 pieces of other information to identify a particular natural person, then are these two pieces of information "personal information"? If the answer is yes, does the protection of these two personal information vary because of their identifiable degree in combination with other information? Obviously, the more other information that one piece of information needs to be combined with in order to identify a particular natural person, the less likely the piece of information constitutes personal information itself, and the less legal protection it should receive. As for the degree of information combination, EU GDPR requires to consider in combination with objective factors, such as the time needed to identify individuals in combination with other information, the available technology to process data, etc. However, there are no similar provisions in Chinese law so far. We expect a further elaboration on this issue in the formal draft of the Measures or other laws.

2.2 Definition of Important Data

Ever since the issuance of the CSL, important data has been the "Sword of Damocles" for network operators. The CSL has explicitly provided critical information infrastructure operators' obligations of data local storage and security assessment for data cross-border transfer. The *Measures on Assessment of Cross-border Transfer of Personal Information and Important Data* (draft) expanded such obligations to all network operators, yet it has remained as a draft till now. Even though two years have passed since the CSL's issuance, for lack of clarity, the legal framework still does not offer a practical guidance on important data.

The Measures define important data as "data whose breach could directly affect national security, economic security, social stability, public health and safety, such as unpublished government data, population, genetic, geographic and mineral resources information on a massive scale." In contrast,

Information Security Technology – Data Cross-border Transfer Security Assessment Guidelines (draft) define important data as "data relevant organizations, institutions and individuals collect or generate within the PRC that is not related to state secret and is closely related to national security, economic development and public interests."

What is new about the Measures is that they include "consequence analysis" as an element in the definition of important data, specifying that the recognition of important data is mainly based on a judgment of potential consequential damages. At the same time, the Measures' requirement of "direct impact" restricts the scope of important data. In addition, the Measures as a general rule exclude a company's "operational data and internal administrative data" from the scope of important data.

Appendix A of *Information Security Technology – Data Cross-border Transfer Security Assessment Guidelines* (draft) lists a variety of types of important data in 26 industries. However, among the listed types, some are personal information, and some may constitute "operational data and internal administrative data" within the meaning of the Measures. With regard to such a difference, we hold that in recognizing important data, the size and permutation of data is as important as the data type. For example, if the size of a company's "operational and internal administrative data" is so massive, or a divulgence of the aggregated "non-important data" can cause a direct impact on national security, economic security, social stability, and public health and safety, such data may nonetheless be deemed as important data. The Measures clearly use the language "in general" to make reservation for such situations.

In our view, the Measures are more scientifically reasonable compared to relevant current laws. We believe that when the Measures and *Information Security Technology – Data Cross-border Transfer Security Assessment Guidelines* are officially issued, the combination of the two will offer an unambiguous and practical guideline to network operators.

3. Data Practice

The Measures define data practice as "the collection, storage, transfer, storage and use of data within the PRC via network", which also defines the applicability of this regulation. Due to the borderless nature of network, to define engaging in data practices "within the PRC via network" becomes a challenging task. For instance, currently many foreign companies solicit Chinese users by means of Chinese websites, RMB payment methods, and Chinese before and after sale services etc. Apparently such companies' website/app, servers, network devices, network infrastructure and place of incorporation are all located outside the PRC, yet under such circumstances Chinese user can complete transactions through the foreign website or app, and the foreign company collects, stores, transfers, processes and uses personal information of Chinese users. Does this constitute engaging in data practices "within the PRC via network"? The Measures offer no answer yet, and we hope that the formal version of the Measures would tackle this question directly.

In terms of data practices, Chapter 2 of the Measures regulates data collection and Chapter 3 regulates data process and use. In the following sections, we will briefly interpret the Measures' requirements in this regard.

3.1 Data Collection

Chapter 2 of the Measures regulates data collection, which mainly prescribes the responsibilities and obligations of network operators in the course of personal information collection. Compared with current laws and policies on protection of personal information, the Measures set forth specifications about certain requirements, and lay down guidelines for the perfection of personal information protection system for network operators from a pragmatic perspective; at the same time, the Measures also mandate brand new requirements to keep up with the latest development. We have summarized and compared the specific changes in the form of tables (see Table 2). Below we focus our analysis on the new rules and requirements put forward in the Measures.

3.1.1 **Network operators shall formulate different privacy policies for different channels.** Since the audiences and functions of network operators' websites and applications are different, the personal information collected and the processing method are different. Network operators shall not adopt an all-in-one privacy policy that is applicable to all its channels after the Measures come into effect.

A Summary and Innovation of Data Security Legislation-A Review of Data Security Administrative Measures (Draft)

3.1.2 **Network operators shall not take discriminative measures on personal information subject based on whether personal information subject authorizes it to collect personal information and the authorization scope.** Such discriminative measures include service quality and price difference. This stipulation is not exactly the same as "consumer discrimination" as we normally understand, since it aims at restricting the purpose and manner of network operators' collection of personal information.

3.1.3 **Network operators shall assume the same obligations for personal information collected indirectly as those for direct collection.** This means that, network operators shall ensure the protection of personal information subjects' rights, even though the personal information was not directly collected by the network operators. Enterprises shall be alert of this stipulation in the Measures, and shall improve the compliance work for personal information collected from third parties.

3.1.4 **Collection of important data and personal sensitive information shall be filed, and a person in charge of data security shall be appointed.** Article 15 and 17 puts forward for the first time that, network operators which collect important data and personal sensitive information "for the purpose of business operations" shall (1) file with the network and information departments where the network operators locate; (2) appoint the person in charge of data security. We believe that "collecting important data and personal sensitive information for the purpose of business operations" shall mean that enterprises can directly generate economic benefits from its use of important data or personal sensitive information collected. Network operators defined by the Measures may include commercial data collectors, developers and diggers such as big data analysis companies and data brokers. However, the specific meaning of "for the purpose of business operations" requires further interpretation by the official version or the regulatory departments.

3.1.5 **Regulating new data security issues such as data scraping.** Article 16 of the Measures strictly limits the use of data scraping to the extent "not affecting the normal operations of websites".

Also, data scraping shall be ceased when it seriously affects the operations of websites or when the websites prohibit automatic visiting and collection. Network operators providing searching or information integration services shall initiate requests at an appropriate frequency, so as to avoid security incidents caused by high request frequency.

Data Collection Process		**Difference**
Rules shall be formulated for collection of personal information	Article 7 of the Measures	Revision of current rules
	Article 7 of the Measures **Article 41** of the CSL	
Requirements on the formulation of collection and usage rules	**Articles 8, 9, 10** of the Measures	Reiteration of current rules
	4 e), 5.6 a), 5.6 c) of Information Security Technology - Personal Information Security Specification	
Misleading personal information subjects to give consent is prohibited	**Article 11** of the Measures	Revision of current rules
	5.1 a), b) of the Information Security Technology - Personal Information Security Specification	
Differentiating core business functions	**Article 11** of the Measures	Reiteration of current rules
	5.2 a) of Information Security Technology - Personal Information Security Specification	
Protection of minors, determining the age line	**Article 12** of the Data Security Management Measures	Reiteration of current rules
	5.5 c) of Information Security Technology - Personal Information Security Specification	
No discrimination	**Article 13** of the Measures	New rules
Taking responsibilities for "second-handed" personal information	**Article 14** of the Measures	New rules
Filing obligations	**Article 15** of the Measures	New rules
Take caution in data scraping	**Article 16** of the Measures	New rules
Person in charge of data security	**Article 17** of the Measures	New rules
	Article 21 of the CSL	

Table 2 The comparison between the Measures and current laws and regulations – Data collection

3.2 Data Process & Use

Chapter 3 of the Measures regulates "the Processing and Use of Data", which mainly specifies the responsibilities and obligations of network operators in using and processing personal information; cross-border data transmission and managing related third parties. Chapter 3 puts forward quite a few new requirements for network operators, including brand new provisions on emerging data application scenarios such as "push notification" and "automatic compilation". The details of such changes are summarized in the table below (see Table 3). Below we focus our analysis on some of the new rules and requirements:

3.2.1 Article 32 of the Measures for the first time regulates "push notification", which includes targeted news and commercials generated by user data and algorithms. It is worth noting that the Measures does not prohibit the network operator from using targeted push notification, but requires that the words "Push Notification" be marked on the information pushed, and the user needs to be provided with the function of rejecting targeted push information. When the user chooses to stop receiving such information, the relevant data already collected should be deleted.

In addition, the Measures stipulate that the targeted push activities should abide by laws and administrative regulations, respect social ethics, business ethics, public order and good customs. Acts of discrimination and fraud are prohibited. With the advent of big data era, discrimination caused by algorithmic systems has gradually become public concern. Discrimination resulted from targeted pushes may harm the user's personal feelings, cause monetary damages, and may even seriously interrupt the normal life of the user. Although it is of epoch-making significance to bring up the idea to regulate targeted push, it still requires more mature legislation by the authorities and accurate technical adjustments and innovations by network operators.

The *Guidelines for Internet Personal Information Security Protection* promulgated by the Ministry of Public Security stipulates that "If user profile technology that entirely relies on automated processing is used for value-added applications such as precision marketing, search

result ranking, personalized push news, targeted advertising, etc., it may not be necessary to obtain explicit authorization from the users in advance". The network operators shall deliberate on the implementation of this requirement and the new requirement mentioned in the Measures.

3.2.2 The Measures for the first time give guidelines on "automatic compilation" from the perspective of cyber security. In 2018, the National Copyright Administration and other four ministries launched the campaign of "Jian Wang 2018", cracking down on plagiarisms committed by "automatic compilation". "Automatic compilation" refers to the use of big data, artificial intelligence and other technologies to automatically synthesize news, blog posts, comments and other information. The Measures requires that such synthesized information shall be marked "automatic compilation", and such synthesized information shall not be "for profit" or harm others' interest.

3.2.3 The Measures reinforce the network operator's administrative obligations on third-party applications accessing their platforms. Article 30 of the Measures stipulates that if a third-party application causes a data security incident and causes loss to the user, the network operator shall take part or all of the liabilities unless the network operator can prove its non-fault otherwise. Operators of relevant platforms should tighten the conditions and qualification requirements for third-party applications to go online, and strengthen the management and supervision of application data security in their platform.

3.2.4 The Measures set forth stricter requirements on the release, sharing, trading and cross-border transmission of important data. The available legal regime only covers the local storage of important data and security assessment requirements of data cross-border transmission. The Measures attempts to incorporate concepts of "publishing, sharing and trading" of important data into the law. Comparing with the CSL, the *Measures for the Security Assessment of Cross-border Personal Information and Important Data Transmission (Exposure Draft)* expands the security assessment subjects of personal information and important data export from Critical Information Infrastructure operators ("CIIO") to all network operators. Similarly, the Measures extends the obligations related to important data to all network operators, Moreover, the Measures require the transmission of important data to be reported to the industry supervisory authorities for approval. In addition to the cross-border transmission of important data, the publication, sharing

and trading of important data also requires a security assessment and report to the industry's competent regulatory authorities for approval.

It is worth exploring whether the Measures has created a new administrative license for the important data to be reported to the industry's supervisory authority for approval. The CSL, as upper-level law, puts forward regulations on exporting important data by CIIO, but it does not create an administrative license or authorize local lower-level regulations to further regulate this matter. According to the rules for the establishment of administrative licenses, no administrative license may be created by the lower-level law for matters which are already prescribed by upper-level law. Under this circumstance, it is debatable how the new license created by the Measures complies with the *Administrative Licensing Law* needs further consideration.

3.2.5 The Measures introduce a new provision that has never appeared in the CSL. Article 29 of the Measures stipulates that the traffic generated by domestic users accessing the domestic Internet shall not be routed outside China. The relevant authorities did not explain the reasons for adding this article and its specific meaning. We understand that this article may be related to Article 28, because domestic users will initiate data transmission and exchange when accessing the domestic Internet, which of course may also include important data. If the related traffic is routed overseas, there is a risk that important data will be transmitted outside the country without a security assessment. In addition, routing traffic abroad may also cause line congestion, resulting in traffic being stolen and monitored. Thus, such provision may prevent route leakage, traffic misdirection and traffic hijacking. We expect this article to be refined in the final draft of the Measures.

Data Process & Use		**Difference**
Data protection reciting national standard	Article 19 of the Measures.	Reiteration of current rules
Storage and use of personal information shall be bound by rules in relation to storage and use	Articles 20 and 22 of the Measures.	Reiteration of current rules
	6.1 and 7.3 c) of Information Security Technology - Personal Information Security Specification	
Responding to data subject's requests	Article 21 of the Measures	Reiteration of current rules

	Article 43 of the CSL **7.4 7.5 7.6 7.8 7.11** of Information Security Technology - Personal Information Security Specification	
Restricting push notifications	Article 23 of the Measures **7.7 b)** of the Information Security Technology - Personal Information Security Specification	Reiteration of current rules
Restricting automatic compilation	Article 24 of the Measures	New rules
Exceptions to data subject's consent	Article 27 of the Measures **5.4** of the Information Security Technology - Personal Information Security Specification	Reiteration of current rules
Risk assessment of important data export	Article 28 of the Measures Article 37 of the CSL	Revision of current rules
No domestic network traffic routed outside the PRC	Article 29 of the Measures	New rules
Third-party management obligations	Article 30 of the Measures	New rules
Obligations of data recipient	Article 31 of the Measures **8.3** of the Information Security Technology - Personal Information Security Specification	Reiteration of current rules
Principles re data process	Article 32 of the Measures	Reiteration of current rules

Table 3 comparison between the Measures and current laws and regulations – data process and use

4. Epilogue

In conclusion, the Measures are not only an "interim summary" of existing important cyber security issues, but also an attempt to make innovations in this regard. The Measures is bound to have profound impact on all network operators. We look forward to the official issuance of the Measures, which we believe will provide clearer and more practical guidelines to network operators' compliance efforts.

A Summary and Innovation of Data Security Legislation-A Review of Data Security Administrative Measures (Draft)

Contact Details

If you would like to know more information about the subjects covered in this publication, please feel free to contact the following people or your usual Llinks contact.

Author	
David Pan Tel: +86 21 3135 8701 david.pan@llinkslaw.com	

Shanghai	
David Yu Tel: +86 21 3135 8686 david.yu@llinkslaw.com	**Bernie Liu** Tel: +86 21 3135 8678 bernie.liu@llinkslaw.com
Selena She Tel: +86 21 3135 8770 selena.she@llinkslaw.com	**Nicholas Lou** Tel: +86 21 3135 8783 nicholas.lou@llinkslaw.com
Dali Qian Tel: +86 21 3135 8676 dali.qian@llinkslaw.com	**Kenneth Kong** Tel: +86 21 3135 8777 kenneth.kong@llinkslaw.com
David Wu Tel: +86 21 6043 3711 david.wu@llinkslaw.com	**David Pan** Tel: +86 21 3135 8701 david.pan@llinkslaw.com
Elyn Jiang Tel: +86 21 6043 3710 elyn.jiang@llinkslaw.com	
Beijing	
David Yu Tel: +86 10 8519 2266 david.yu@llinkslaw.com	**Bernie Liu** Tel: +86 10 8519 2266 bernie.liu@llinkslaw.com
Yuhua Yang Tel: +86 10 8519 1606 yuhua.yang@llinkslaw.com	
Hong Kong(in Association with Dennis Fong & Co., Solicitors)	
David Yu Tel: +86 21 3135 8686 david.yu@llinkslaw.com	**Sandra Lu** Tel: +86 21 3135 8776 sandra.lu@llinkslaw.com
London	
Yuhua Yang Tel: +44 (0)20 3283 4337 yuhua.yang@llinkslaw.com	