LLINKS Law Offices
通力律师事务所

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

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

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

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
May 2019

Seven Alerts in Relation to Draft Measures for Management of Data Security

By Xun Yang

The Cyberspace Administration of China (***CAC***) issued on the morning of 28 May 2019, for public consultation, a draft *Measures for Management of Data Security*. The Draft upgrades the protections for cyber security and personal information onto a historical level. On one hand, the Draft provides that the Office of the Central Cyberspace Affairs Commission supervises the national cyber security works, which commission is one of the divisions of the Communist Party of China led by President Xi Jinping. This provision indicates that the Party and national leader pay great attentions to cyber security works. On the other hand, the Draft proposes a heavy burden on network operators to protect data security. Below sets out a non-exhaustive list of key requirements under the Draft.

I. Network operators must clarify data collection and using rules and must not mislead data subjects into giving consents to collection of personal data or discriminate the subject who refuses to consent to data collections

For more Llinks publications, please contact:

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

Llinks Law Offices
www.llinkslaw.com

In response to the issues discovered during the inspection on data protection on websites and APPs performed by CAC, the Draft imposes the following requirements on network operators in relation to collection and use of personal data: (1) to include required contents into the rules for collecting and using personal data; (2) to display the rules for collecting and using personal data in a centralized and reader-friendly way (according to recent cases, these rules must be included in a privacy policy but not a part of a tedious user agreement.); (3) to align functional designs of websites and Apps with the rules for the collecting and using personal data; (4) not to force or mislead data subject to consent to the collection of their personal data by, implied consents, bundled sales or otherwise; and (5) not to decline the provision of core business functions or reduce the service quality of core functions only because the refusal to give consents to data collections.

Data subjects in the Draft refer to individuals to whom the personal data are identifiable or related.

II. The collection of personal sensitive information and important data must be filed with the government

In accordance with the Draft, network operators, which collect personal sensitive information or important data for the purpose of business operations, must file with local offices of cyberspace affairs, among others, the rules for and the purpose, scale, method, scope, type and duration of collection and use of personal sensitive information. The term "personal sensitive information" is not clearly defined in any existing laws or regulations. According to the *Information security technology - Personal information security specification*, however, the term almost covers all types of information substantively related to persons, including personal financial information, health information, online account information, contact information, etc. The term "important data", as defined in the Draft, also covers a wide range of information. Therefore, absent of further restrictions of personal sensitive information and important data, in reality, any collection of personal information and other data in public domain for the purpose of operation will likely be required to be filed with the government.

III. Identification of "Targeted Advertisement" and "Synthetic Content"

In response to the application of big data in the field of targeted advertisement, the Draft provides for an identification requirement. In the event that a network operator uses users' data and algorithms to send news information, commercial advertisements or otherwise to targeted users, the operator must clearly identify such information or advertisement as "targeted advertisement," and also provide users with channels to stop receiving "targeted advertisement." Additionally, a network operator,

which uses big data, artificial intelligence or other technologies to automatically synthesize contents such as news, blogs, posts, comments, etc., must clearly mark on the content the label of "Synthetic Content". These two requirements are designed to protect users' right to be informed of and their right to consent to, receiving direct marketing materials, which is consistent with the rules under the advertisement laws. Nevertheless, it is still unclear about the definition of "users' data and algorithms", and thus whether the use of information collected by cookies for targeted advertisement or synthetic contents is captured by this requirement.

IV. Clarification on and protection for the identities of social media users

Based on the principle that social media users shall be responsible for the content they post, the Draft provides that network operators must verify and protect users' identities, including: (1) if users forward any content posted by other users, to automatically apply the account names of such other users on the forwarded content; and (2) when receiving complaints about using others' names to post contents, to respond to and deal with such complaints in a timely manner. These two requirements aim to establish direct connections between the contents and the users who post them, which require network operators to take these requirements into account when building the content platforms.

V. Security assessment is required when providing personal information to others

In addition to the "informed consent" requirement prescribed in the existing *Cybersecurity Law* and relevant guidelines, the Draft also requests network operators to assess the security risk before providing personal information to others, which undoubtedly increases the burdens of network operators on protection of personal information. However, the rules on how to conduct security assessment has yet been elaborated.

VI. Publication or cross-border transfer of important data requires security assessment and approval by competent authorities

With the continuous delay in promulgating the *Measures for Security Assessment of Cross-border Transfer of Personal Information and Important Data*, the Draft proposes security assessment and approval requirements on the publication and cross-border transfer of important data again. These requirements may be related to the fact that the United States passed the *Cloud Act* to adopt unfair hegemony to internet information. In comparison with the *Measures for Security Assessment of Cross-border Transfer of Personal Information and Important Data*, the Draft provides for a wider scope of assessment, including not only cross-border transfers of important data, but also their publication, sharing and trading, without any threshold on quantity.

VII. Platform operators will be presumed faulty during a data breach

The Draft strengthens the security management responsibilities of platform operators. Platform operators are required to supervise third parties of which applications are posted on their platforms. Platform operators are also held partly or solely liable for any losses suffered by users arising out of the data security incidents incurred by third parties' applications, unless network operators are able to provide that they have performed their security management obligations. In other words, platform operators have increased burdens of proof to demonstrate that they have fulfilled security management and supervision obligations, which must be reflected not only in the agreement with third party users, but also in the daily practice.

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	
Xun Yang Tel: +86 21 3135 8799 xun.yang@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	