



Llinks Corporate and M&A Bulletin
August 2019

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

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

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

伦敦
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

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

master@llinkslaw.com

Review of the Provisions on the Cyber Protection of Children's Personal Information

By David Pan | Susan Deng | Shana Sha

In recent years, as the number of minor netizens continues to expand, personal information of minors are vulnerable due to increasingly diversified network platforms and use of big data. With low sensitivity to personal privacy and lack of protection capability, children often face a higher risk of information leakage in social activities. On August 22, 2019, the Cyberspace Administration of China (the "CAC") formally promulgated the *Provisions on the Cyber Protection of Children's Personal Information* (the "New Provisions"), which will become effective on October 1, 2019. As the first regulation of specifically protecting children's personal information in China, the *New Provisions* carries the public's attention and expectation.

I. Main Differences between the New Provisions and the Exposure Draft

On May 31, 2019, the CAC promulgated the *Provisions on the Cyber Protection of Children's Personal Information (Exposure Draft)* (the "Exposure Draft"). The *New Provisions'* modifications to the *Exposure Draft* are summarized as follows:

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

Review of the Provisions on the Cyber Protection of Children's Personal Information

1. Highlight the importance of children's information

The *New Provisions* highlights the importance of children's information, and provides that "no organization or individual may produce, publish or disseminate the information that infringes upon children's personal information security". The *Administrative Measures on Internet Information Services* promulgated by the State Council in 2011 enumerates eight types of network information that shall not be produced, published or disseminated, including the information on national security, social stability, obscene pornography, insult and slander, and violence and terrorism. The *New Provisions* incorporates children's personal information into this category, which reflects the importance hereof. The *New Provisions* requires network operators to establish sound information security management systems and prevent any violations of children's personal information.

2. Emphasize the guardianship responsibility of the guardian

The *New Provisions* emphasizes the guardians' responsibilities in the protection of children's personal information, and adds the new rule on the basis of the *Exposure Draft* that "guardians shall properly fulfill their guardianship responsibilities, and educate and guide children to enhance their personal information protection awareness and capacity, and protect children's personal information security".

Guardians are the most intimate people in children's daily life, and they know well children's participation in network activities. The *Exposure Draft* focuses on the responsibility of network operators instead of guardians' duties of guardianship for personal information protection. In contrast, the *New Provisions* requires guardians to offer proper guidance and help children in using their personal information in network activities, so as to enhance children's self-protection ability. By adding this new rule, children's information protection are two-fold: one "internally" by guardians and the other "externally" by others.

3. Change from "express consent" to "consent"

The change from "express consent" to "consent" is a significant change made in the *New Provisions* compared with the *Exposure Draft*. The *Exposure Draft* repeatedly emphasizes that where network operators collect, use, store, transfer or disclose children's personal information, they shall inform children's guardians in a noticeable and clear way, **and shall obtain the express consent of children's guardians**; such consent shall be specific, clear and unambiguous and shall be made voluntarily. The *Guidelines for Personal Information Protection in Public and Commercial Service*

Review of the Provisions on the Cyber Protection of Children's Personal Information

Information Systems (GB/Z 28828-2012) promulgated in 2012 points out that “when collecting personal general information, it may be deemed that the personal information subjects have given tacit consent; if the personal information subjects explicitly object, the collection of personal information shall be stopped or the personal information collected shall be deleted; when collecting personal sensitive information, it is required to obtain the express consent from the personal information subjects”. The *Personal Information Security Specification (GB/T 35273-2017)* promulgated in 2018 also states that before personal information is collected, it is required to obtain the authorized consent from personal information subjects; when personal sensitive information is collected, it is required to obtain the express consent from personal information subjects. As we can see, although literally there is only minor difference between “express consent” and “consent”, the difference in special requirements on network operators' responsibilities is obvious. The deletion of the word “express” in the *New Provisions* substantially lowers the requirements for network operators.

Although the *Cybersecurity Law of the People's Republic of China*, the *Regulations on Protecting the Personal Information of Telecommunications and Internet Users* and other laws and regulations do not require the network operator to obtain “express” consent from the user in the course of collecting personal information. Children's information, as a special category of personal information, should be given adequate protection. The *Information Security Technology Personal Information Security Specification* stipulates that “personal information of children aged 14 and under is personal sensitive information”; “in the course of collecting personal sensitive information, express consent shall be obtained from the personal information subject; prior to the collection of the personal information of a minor aged 14 or above, express consent shall be obtained from either the minor or its guardian; otherwise from its guardian merely.” The *Exposure Draft* requiring “express consent” is a reflection of the above provisions in the national standard.

Similarly, the *New Provisions* removes the word “express” in consideration of multiple factors. First of all, the existing effective regulations do not require the express consent given by the personal information subject before the collection of personal information. The *New Provisions* removes the word “express” to keep in line with the conservative standpoint of upper law, the *Cybersecurity Law of the People's Republic of China*, so as to ensure the enforceability of the law. Secondly, it could be laborious and costly if network operators are required to obtain “express” consent from the guardian in practice. The removal of the word “express” lowers the operational difficulty and lessens compliance costs of network operators. Otherwise, the onerous burden would probably discourage the network operators from fully complying with the law. Regardless of the changes, the network operators are not allowed to lower the protection level for children's personal information. On

Review of the Provisions on the Cyber Protection of Children's Personal Information

February 27, 2019, the Federal Trade Commission (FTC) announced that the operators of networking video APP, Musical.ly (later merged into the overseas version of Douyin, Tik Tok) have agreed to pay USD 5.7 million to settle the FTC's allegation that they violated *Children's Online Privacy Act (COPPA)*. According to the FTC, the operators of Musical.ly APP knew that a large portion of its users are children under 13 years old, yet they failed to notify parents of these children about the app's collection and use of these children's personal information, obtain parental consent before such collection and use, and delete personal information at the request of parents, and thus violated *COPPA*. The number of similar cases is also on the rise in China.¹ Although China's statutory fine is not as large as the U.S. one, network operators must still be cautious of the "Sword of Damocles" of children's personal information.

4. Remove situations of "without consent of guardians"

The *New Provisions* removes certain situations in which children's information can be obtained without the consent of the guardian. In the case of children's information disclosure, the *New Provisions* retains the article that "the information that shall be disclosed as stipulated by laws and administrative regulations or may be disclosed as agreed with the guardian" may no longer be subject to the consent of the guardian. This also means that the network operator must obtain the consent from the guardian to collect, use and transfer children's personal information. The *New Provisions* also removes the two exceptions mentioned in the *Exposure Draft*: "to protect national security or public interest" and "to eliminate the immediate danger of children per se or property". In the future, it is difficult for network operators to cite the above "legitimate" reasons to defend their infringement upon children's personal information. This change has also significantly enhanced the protection of children's information and highlighted the important role of guardians in the protection of children's information.

5. Others

- The *New Provisions* removes the provision that "network operators are required to appoint a personal information protection specialist for the protection of children's personal information" in the *Exposure Draft* and the requirement on user agreement for children.
- The *New Provisions* removes the provision regarding the situation where "network operators and third parties use children's personal information together" and forbids such kind of use and share.

Review of the Provisions on the Cyber Protection of Children's Personal Information

- The *New Provisions* adds the means of complaints and reporting for children and their guardians, the method of correcting and deleting children's personal information and the remedies for the guardian.

II. Comparison between *New Provisions* and Other Children's Information Protection Regulations and Policies

1. Ways to obtain the consent of the guardians

As analyzed above, there are differences between laws and national standards in the form of consent in terms of collection of children's personal information. The *Methods for Identifying Unlawful Acts of Applications (Apps) to Collect and Use Personal Information (Exposure Draft)*, the *Administrative Measures for Data Security (Exposure Draft)* and the *Regulations on Protecting Minors on the Network (Exposure Draft)* require that the collection of children's personal information shall be subject to the guardian's "consent". Consistent with the above legislation, the *New Provisions* does not require consent to be "express". In contrast, the national standard *Personal Information Security Specifications* requires that the guardian's consent must be "express". Express consent means the act of a personal information subject's clear authorization for processing of its personal information, either through a written statement or its voluntary affirmative action, which includes voluntarily making statements, voluntarily ticking or clicking "Agree", and so on.

As discussed above, the change from "express consent" to "consent" is not intended to weaken the protection on children's personal information. While this change is consistent with the upper law, it is a compromise with reality, because it is difficult for network operators to meet the "express consent" requirements in a short term. Onerous requirements may not bring healthy social effects, and may even weaken the capacity and willingness of network operators to provide relevant services or improve compliance measures. With the gradual formulation of China's personal information protection system, it is sensible for legislators to provide a certain buffer period provided that the national standard has already set a strict requirement. Probably, the regulator adds the "express consent" requirement to test the water. It is not the first time for the regulator to do so and this could imply that in the future, the personal information protection regulations would be stricter.

Review of the Provisions on the Cyber Protection of Children's Personal Information

2. Supervise Off-campus Online Training and Learning APP

In recent years, online educational network operators and educational apps mushroomed. Convenient to students though, these online educational platforms contain a lot of risks. Starting from the third quarter of 2018, the Ministry of Industry and Information Technology (MIIT) has added “Problems in users’ personal information protection inspections” to the *Notice of the MIIT on the Quality of Telecommunications Services*, which exposed many Apps’ abuse of mobile phone users’ personal information.² On July 1, 2019, MIIT published results of the supervision on personal information protection of telecommunications and Internet users (No. 2 of 2019)³. In a random inspection of 106 Internet services of 100 Internet enterprises, 18 Internet enterprises failed to publicize the rules for collecting and using users’ personal information, failed to inform the methods for inquiring and correcting information, and failed to provide account cancellation services. The enterprises involved include entities closely related to children’s information, such as XRS online school. According to the evaluation of 30 popular K12 online educational Apps by the Southern Metropolis Daily New Business Law Research Center in 2018, many educational Apps invaded privacy in the process of collecting, storing and using users’ information. For example, 14 Apps did not have specific privacy policy. Some neither adopted user agreement, privacy policy, nor committed to data protection. 20 Apps did not allow users to cancel their accounts by themselves. Even after users canceled their accounts, the backstage server of these apps still stored user’s personal information to do course promotion.⁴

In view of many problems existing in the online education business, in December 2018, the Ministry of Education issued the *Notice on Strictly Prohibiting the Introduction of Harmful Applications (APPs) into Primary and Middle Schools*, requiring that educational Apps entering schools must ensure information and data security of students and prevent the disclosure of students’ privacy. In July 2019, six departments including the Ministry of Education issued the *Implementation Opinions on Standardizing Off-Campus Online Training*, requiring off-campus online training institutions to ensure student information security. The online operators shall implement the cyber security graded protection system, cyber security alerting and notification system and users’ information protection system, and take technical measures in place for security protection; shall be prohibited from illegally selling or providing student’s information. In contrast, the *New Provisions* is more detailed and sets out clear requirements on the collection, use, storage, transfer and disclosure of children’s personal information. Online operators that provide educational and training services for children aged 14 or under should promptly comply with the *New Provisions*.

Review of the Provisions on the Cyber Protection of Children's Personal Information

III. Conclusions

Before the implementation of the *New Provisions*, penalty cases already happened in the education business. For example, in 2017, Hangzhou Administration for Market Regulation investigated a number of educational institutions including Meishule Education Consulting Co., Ltd. and Jingying Education Technology Co., Ltd. Some administrative penalties amounted to 300,000 yuan. These educational institutions collected information such as the child's name, gender, date of birth, and the child's parent's name, address, telephone number, etc., for the purpose of developing students and marketing training courses. When collecting such personal information, they did not keep record of consent or authorization of the child's parents or "disclosed the purpose, method and scope of collection and use of the information".

The *New Provisions* provides more targeted and detailed guidelines on information protection, and provides the law enforcement agencies with a more solid and clear law enforcement basis to crack down abusive activities relating to children's personal information. Network operators from industries such as education, consumer goods, or information services engage in the marketing and management of children's personal information. It is advisable for those network operators to get themselves familiar with the *New Provisions* and carry out gap analysis and rectification as soon as possible.

Review of the Provisions on the Cyber Protection of Children's Personal Information

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	

Review of the Provisions on the Cyber Protection of Children's Personal Information

¹ See the conclusion part.

² See Notice of the MIIT on the Quality of Telecommunications Services(No. 4 of 2018)
<http://www.miit.gov.cn/n1146290/n1146402/n7038720/c7048061/content.html>

³ See Notice of the MIIT on the Quality of Telecommunications Services(No. 2 of 2019)
<http://www.miit.gov.cn/n1146295/n1652858/n1652930/n4509627/c7021505/content.html>

⁴ See Individual online education apps are hard on the eyes! Amazingly a lot of soft pornography!
<https://mp.weixin.qq.com/s/bSFEZxKkp25dDXnsZmkHpg>