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
March 2019

APP: from "Prying" to "Protection"

By David Pan | Nigel Zhu | Susan Deng

On February 27, 2019, the Federal Trade Commission (FTC) announced that the operators of networking video APP, Musical.ly (now 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 USD 5.7 million settlement payment constitutes the largest civil penalty ever obtained by the FTC in children's privacy case, and therefore quickly caught the public's attention. In fact, Douyin is not alone in getting penalized for violating personal information protection laws. Even though 2019 has just witnessed its third month, a number of foreign and domestic companies have troubled themselves with personal information violations.

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

On January 21, 2019, France's data protection watchdog La Commission nationale de l'informatique et des libertés (CNIL) fined Google EUR 50 million for violations of EU's General Data Protection Regulation (GDPR). According to CNIL, the penalty imposed on Google was based on two grounds: 1) Google failed to provide users with transparent and comprehensive information about how it handles user data; and 2) Google failed to validly obtain user's consent with the processing of their data for ads personalization.

Based on announcements by other EU data protection authorities, Facebook is facing 10 probes launched by the Irish Data Protection Commission for GDPR violations, which include probes against Facebook itself as well as its subsidiaries, Whatsapp and Instagram. In addition, EU data protection authorities are probing Apple, Microsoft and Twitter, and penalty decisions for these giants' personal data law violations may be issued later this year.

On December 16, 2019, a Weibo user claimed that he found in the cache files of JD Finance Android version pictures generated by the phone's snapshot tools and other camera Apps, and he suspected that the JD Finance App has been collecting and updating user pictures, and thus infringed users' privacy. After having made a self-investigation, Jing Dong concluded that "there are some technical issues in developing JD Finance App's functions", and issued an official apology, claiming that it "never sought to collect user pictures without authorization … has never before, and will never in the future upload user pictures without authorization." It is unclear at the moment whether government authorities will investigate the incident or impose any penalties on Jing Dong for the "technical issues", but this incident definitely heightened the public's attention on compliance issues related to App's collection and use of personal information.

The aforementioned cases show that, with strengthened regulation, improvement of law enforcement technology and increase of user awareness of personal information protection, the era in which APP operators can make profit by unlawfully collecting or using personal data without any liabilities is in the rear-view mirror.

I. Law and Enforcement

In recent years, accompanying the development of big data related technology and the deepening of the exploitation of data value, the thirst for and reliance on user personal information by operators in all industries has caused the unlawful collection and use of personal data to go viral. To curb such acts, China's legislation and enforcement actions for personal data protection also skyrocketed in this period.

1. Criminal Law

Most APP operators are probably familiar with the administrative penalties for unlawful collection and use of personal data, believing that the consequences for violation are just warning, rectification or fine. What they did not know is that personal information violations may bear criminal liabilities since

2015, and offenders may face criminal penalties of up to seven years of imprisonment.

Subsection 1 of Article 253 of the *Criminal Law* provides that "whoever sells or provides citizen's personal information to others in violation of applicable laws and regulations shall be imprisoned no more than three years or detained, or fined in addition to the preceding sentence or independently, in a case of severe nature; or, in a case of extremely severe nature, imprisoned no more than seven years, and fined." It also provides that "whoever steals or otherwise illegally obtains citizen's personal information shall be penalized according to the preceding provision".

The Supreme People's Court and the Supreme People's Procuratorate on May 8, 2017 jointly issued *Interpretations to Issues relating to Application of Law in Criminal Cases involving Infringement on Citizen Personal Information*, which further articulates the recognition and penalties of the crime. The judicial interpretation provides that "cases of severe nature" provided in Section 1, Article 253 of the *Criminal Law* includes "illegal collection, sale or supply more than 50 pieces of tracking information, communication correspondence, credit information or property information over 50 pieces", "illegal collection, sale or supply of more than 500 pieces of accommodation information, communication records, health and physiological information, transaction information or other personal information that may affect citizen's personal or proprietary safety" and "illegal collection, sale or supply of more than 5,000 pieces of information other than listed in the preceding two provisions", or that "illegal gains exceed RMB 5,000", while "cases of extremely severe nature" includes cases in which the number of pieces of information or the illegal gains exceed 10 times of the numbers provided in "cases of severe nature". According to this judicial interpretation, the threshold for the crime is reduced to half of the relevant numbers, in the event that personal information collected from providing services is sold or supplied to others.

2. Civil Law

Article 111 of the General Part of *Civil Law* provides that "a natural person's personal information is protected by law. Organizations or individuals shall legally collect others' personal information and ensure the security of such information, and shall not illegally collect, use, process or transfer personal information, or illegally buy or sell, supply or disclose others' personal information".

Although Chinese legislation has not made "right to personal information" a statutory right yet, personal information subjects undoubtedly enjoy the right under the *Civil Law* to be free of unlawful collection and use of their personal information. For those who infringe on a natural person's personal information, the personal information subject can seek civil damages from the infringer, including but not limited to cessation of infringement, removal of hindrance, indemnification, removal of adverse effect, restitution of reputation and apologies.

Moreover, the right a personal information subject may have overlap with his statutory rights, such as portrait right and privacy right. Under such circumstances, the personal information subject may seek damages under the *Tort Liability Law* for infringement on his/her portrait right and privacy right.

3. Administrative Law

It is not an exaggeration to say that currently the area of administrative law is the main "battle field" for personal data protection. The number of laws and regulations and enforcement actions, as well as APP operators' awareness level are much higher in the administrative area than criminal and civil area.

The *Cyber Security Law* (CSL) lays out the basic principles of personal information protection. According to the CSL, "network operators shall collect and use personal information based on the principles of legality, legitimacy and necessity, publicize rules for collection and use, inform the purpose, method and scope of collection and use, and obtain information subject's consent". In addition, "network operators shall not collect personal information irrelevant to their services, not collect or use personal information in violation of laws and regulations and the agreement between parties, and shall process the personal information they collect pursuant to laws and regulations and the agreement between the parties", and "shall not supply personal information to others without the personal information subject's consent, except information that has been processed so that it cannot identify specific individuals and cannot be restored".

In the administrative law area, the suggestive national standard *Information Security Technology Personal Information Security Specifications* (GB/T 35273-2017) (Personal Information Standards) is of substantial significance. The Personal Information Standards define "personal information" and raise the concept of "personal sensitive information", as well as setting detailed requirements on the collection, storage, use and third-party processing, sharing, assignment and disclosure of personal information. Although the Personal Information Standards are suggestive standards and lack inherent enforceability, it is worth mentioning that under the current circumstances that the CSL and other personal information protection laws lack detailed implementation rules, they will be referenced by administrative and judicial authorities for factual findings and to access whether certain legal elements have been met, so that recognitions and penalties will be passed down accordingly and APP operators will bear civil, administrative and even criminal liabilities accordingly. Furthermore, as a suggestive national standard, the criteria raised in the Personal Information Standards are generally more stringent than those required by law, hence, if APP operators fulfill its personal information protection obligations according to the Personal Information Standards, they would be reasonably confident that they are unlikely to violate relevant laws and regulations, and they may take the compliance of such standards as a defense when facing government investigation or third-party claims.

In addition to the CSL and the Personal Information Standards, many separate regulations for various areas and industries rule specifically on personal information protection, such as the *National People's Congress's Decision on Strengthening Protection of Internet Information*, *Telecommunication and Internet User Information Protection Rules*, *Courier Services User Personal Information Security Administrative Rules*, *Peoples Bank of China Notice on Better Personal Financial Information Protection by Banking Financial Institutions*, and *Internet Personal Information Security Protection Guidelines*. Some other laws and regulations also contain provisions of personal information protection, such as the *Consumer Rights Protection Law, Minor Protection Law, Commercial Banks Law, Resident ID Law, Passport Law, Tourism Law, Electronic Signature Law, Credit Administrative Rule*.

Another notable trend is that in addition to strengthening ex post penalties, the authorities have been emphasizing on ex ante supervision. On January 25, 2019, the Cyberspace Affairs Commission, Ministry of Industry and Information Technology, Ministry of Public Security and State Administration of Market Regulation jointly issued the *Announcement on Special Operations against Unlawful Collection and Use of Personal Information through APP* (the Announcement). The Announcement emphasizes the principles regarding personal information protection provided in the CSL etc., the responsibilities of respective government authorities in combating personal information violations, and innovated in providing an assessment for unlawful collection and use of personal information to be formed jointly by the National Information Security Standardization Technical Committee, China Consumer Association, China Internet Association and China Cyberspace Security Association (the APP Special Taskforce), and to arrange for professional institutions to assess the personal information collection and use status of APPs with massive numbers of users and closely related to people's life. It is also encouraged for APP operators to conduct self-inspection and reception in accordance with the APP Assessment Guidelines (see definition below) so as to increase their personal information protection capabilities.

The APP Special Taskforce issued *Guidelines on Self-Assessment for APP's Unlawful Collection and Use of Personal Information* (APP Assessment Guidelines), which guide APP operators from three major aspects: privacy policy, APP's collection of personal information and user rights protection provided by APP operators. In terms of privacy policy, the APP Assessment Guidelines point out 1) the independence and readability of the privacy policy; and 2) clear articulation of the functions of each service and the personal information collected; and 3) specify rules for personal information processing and user rights protection. In terms of APP's collection of personal information, the APP Assessment Guidelines touch on the following topics: 1) the purpose, method and scope of personal information collected; and 2) collection and use of personal information shall be subject to voluntary user consent, and mandatory bundled authorization is not allowed; and 3) collection of personal information shall be subject to necessity. With regard to user rights protection provided by APP operators, the APP Assessment Guidelines require that APP operators shall 1) enable users to

deregister user account, correct or delete personal information; and 2) respond to user complaints in a timely manner.

The APP Special Taskforce also established a public WeChat account called "APP Personal Information Complaint" to encourage APP users to report unlawful collection and use of personal information by APPs.

II. Compliance Tips

The cases at the beginning of this article regarding unlawful collection and use of personal information are in a way alarming to the APP operators. By drawing a boundary of legitimate collection and use of personal information, the cases point out the direction for APP operators of how to use personal information legally and how to adjust business plans accordingly.

As mentioned above, the Announcement provides a very clear and operational guideline for APP operators to lawfully collect and use personal information. According to the Announcement, when an APP operator collects and uses personal information, it must not collect personal information that is irrelevant to the services provided; "when collecting personal information, it is necessary to display rules regarding personal information collection and use in an easy-to-understand, simple and clear manner, and obtain personal information subject's autonomous consent; shall not coerce the user to authorize in a disguised form by means of defaulting, bundling, or threatening to stop installation and use, and the operators may not collect personal information in violation of laws and regulations and agreements with users. The above requirements are already reflected in the CSL, Consumer Rights Protection Law, the Personal Information Standards and other laws, regulations and national standards. In the rest of this article, we propose a number of compliance tips regarding the collection and use of personal information for APP operators based on the above cases, relevant laws and regulatory situations and trends.

1. Improve Privacy Policy

   1) Be concise and user-friendly. Tables and charts could be used to facilitate demonstration. According to the review results of the "Privacy Policy Special Project" conducted by the CAC, the Ministry of Industry and Information Technology of the People's Republic of China, Ministry of Public Security, the National Standards Committee and other departments jointly during the "Personal Information Protection Enhancing Action" in 2017, companies should make concise and readable privacy policies and should enable users to locate and comprehend the critical contents.

   2) Use enhanced notice which contains the core contents regarding collection of personal

information before installation, registration, and first use by users. Enhanced notice does not contain the full content of the privacy policy, but it condenses the core of the privacy policy and shall highlight the information that the user is most concerned about, such as the scope of personal information collected, the purpose and the subject of use.

3) User-oriented. Provide "one-stop" authorization withdrawal and closure, online access, correction and deletion of user personal information, online cancellation of accounts and other functions. Proactively distinguish between core functions and peripheral functions for users to make their decisions.

2. Obtain Informed Consent

1) The collection and use of personal information by APP operators shall follow the principles of legality, legitimacy and necessity. APP operators shall clearly indicate the purpose, methods and scope of the collection and use of such information, and shall obtain consent from the data subject. The information shall not be collected or used in violation of the laws and regulations and the agreement between both parties.

2) The user should not be required to accept and authorize multiple business functions to collect personal information at one time by bundling these business functions of the APP.

3) Do not use implied consent. Do use the user's initiative to fill in, click or check as the pre-condition for activating business function or personal information collection of the product or service.

3. Special Protections for Minors

1) Establish an age authentication and identification system, or use a real identity registration verification mechanism to effectively identify minor users. Before collecting the personal information of a minor, it is strictly required for the user to show his/her express consent, or the same from his/her guardian, and a reminder should be shown conspicuously via the APP. For minors under the age of 14, express consent of their guardian shall be obtained.

2) Set up screening and inspection mechanism, timely discover the personal information of minors collected without proper consent, and delete relevant data in time.

4. Avoid Excessive Collection

In practice, some companies mistake the consent of the personal information subjects as a sufficient

condition for compliance of their use of personal information. These companies ignore the "necessity" principle of using personal information mandated by the CSL, and also overlook the "minimization requirements" proposed in Section 5.2 of the Personal Information Standards. The "necessity" principle and the "minimization requirements" suggest that:

1) The types of personal information collected should be directly related to the realization of the business functions of a product or service. "Directly related" means that the functions of a product or service cannot be fully realized in the absence of such information.

2) The frequency of automatic collection of personal information should be the minimum frequency necessary to fulfil the business function of the product or service; and

3) The amount of personal information indirectly obtained should be the minimum necessary to fully fulfil the business functions of the product or service.

In addition, APP operators should notice that personal property information, personal health physiological information and face recognition information are personal sensitive information. Prior to collecting personal sensitive information, the APP operators shall:

1) Notify personal information subjects about the core business functions of the product or service, the personal sensitive information that must be collected, as well as the impact brought by refusal to provide or give consent. Allow personal information subjects to choose whether to provide or consent to automatic collection;

2) If a product or service provides additional functions and needs to collect personal sensitive information, it should, prior to the collection, explain to each personal information subject about the additional functions of which full exercise needs personal sensitive information, and allow the individuals concerned to select whether to provide or agree with the automatic collection thereof. When an individual concerned refuses, such additional functions may not be activated, provided that the core business functions are not interfered with for such reason, as well as the service quality shall be maintained at the usual level.

Excessive collection of personal information may result in administrative penalties, and may even constitute a criminal offence. In order to avoid such consequences, the company shall distinguish core functions and additional functions of products or services based on the casual relationship between personal information and the realization of various functions, and ensure that the users may continue to use other business functions which are irrelevant with those parts of personal information.

5. Inform Users of Automatic Data Collection Tools

Besides the user's basic personal information, the user's online activity information, such as the pages visited by the user, the products viewed, and the comment posted may be collected by the built-in automatic data collection tools in the APP.

If users' online activity information is collected during the use of the APP or its background operation, as a starter, APP operators shall ensure that collection of such information is made moderately, confined to the scope and purpose as agreed by the users. The APP operator shall have a detailed description of the technical mechanism in its privacy policy, explain the purposes of adoption of automatic tools to collect personal information, and provide to users the methods and detailed guide for them to restrict data collection by automatic tools.

6. Jurisdiction of Foreign Law

In addition to the laws of the country in which APP operators are located, the cross-border operations and use of the APP require the APP operators to comply with foreign laws. For example, if the APP users include EU residents, the APP operator also needs to comply with the relevant provisions of the GDPR. Extraterritorial laws such as GDPR differ from Chinese laws and policies in the definition and protection system regarding personal information, and such laws may impose stricter responsibilities on operators in certain areas. For instance, when making automated individual decision-making and profiling, the operator should inform the subject of relevant personal information processing, and provide him/her with a convenient manual intervention or questioning method. Regular checks shall be made to ensure that automated personal decision-making and portrait systems operate as intended.

III. Conclusion

Compliance is not a mere formality to respond to legal requirements. Rather, as a lifeline of the companies, compliance creates value. APP operators, especially those that rely on user personal information shall make personal information compliance a first priority. Only by lawfully collecting and using personal information will APP increase user stickiness and preference, which in return brings profit to APP operators. If APP operators continued to collect and use personal information unlawfully, they would pay for a heavy price for their contempt for users and violations of laws.

APP: from "Prying" to "Protection"

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	