Data Collection and Processing Personal Information on Mobile Apps (China)

By Xun Yang | Yara Yang

China (PRC) is undergoing an economic revolution of digitalisation. Owing to the country's highly engaged mobile population and booming mobile e-commerce, mobile applications or apps, including mini-programs and public accounts on WeChat, and H5 pages (commonly known as mobile websites that can be seamlessly integrated into WeChat profiles to create interactive marketing campaigns) have increasingly become important tools for business operators to boost their brands and to promote their products.

Meanwhile, the Chinese government is making efforts to strengthen the protection of the personal information of residents in China, including the protection of personal information on mobile apps. In particular, the *Personal Information Protection Law of the PRC 2021* (2021 PIPL), effective on 1 November 2021, significantly enhances the personal information protection standard on mobile apps.

This note provides an overview of the regulatory regime for the collection and processing of personal information by apps in China. It discusses enforcement activities against non-compliant apps, compliance requirements, and the consequence for violating personal information rules by apps. The note also provides practical guidance for app operators to mitigate the risks of breaching personal information protection requirements.

Personal information protection regime on apps

The *2021 PIPL* is the first comprehensive law to regulate activities related to personal information in China and protect the personal information of residents in China. However, it is not the only law or

如果您需要本出版物的中文本，
请联系:

Publication@llinkslaw. com

For more Llinks publications,
please contact:

Publication@llinkslaw.com

regulation on personal information protection. China started to regulate behaviours related to personal information more than a decade ago. With the effectiveness of the 2021 PIPL, China has established a relatively complete personal information protection system, and personal information is now protected in all of the criminal, civil, and administrative law regimes.

Criminal law regime

In contrast to western countries, China started protecting personal information through its Criminal Law:

- The *Amendment VII to the Criminal Law of the PRC 2009* criminalises the stealing, illegal provision and sale of personal information by government officials and by staff of telecoms and public utility companies.
- The *Amendment (IX) to the Criminal Law of the PRC 2015* (2015 Criminal Law Amendment (IX)) further expands the scope of subjects. All individuals, regardless of their jobs or positions, are eligible for the offence of stealing, illegal providing and selling personal information. The 2015 Criminal Law Amendment (IX) also includes an offence that failing to perform cybersecurity obligations resulting in significant leakage of user information will be subject to the criminal liability of up to three years imprisonment. (For more information, see *Legal update, Criminal Law amendment: new individual and corporate offences for data privacy and cybersecurity violations*.)

  On 9 May 2017, the *Supreme People's Court* and the *Supreme People's Procuratorate* jointly released the *Interpretation on Several Issues on the Application of Law to the Adjudication of Criminal Cases involving the Infringement of Citizens' Personal Information 2017*, which clarifies certain terms related to criminal infringement of citizens' personal information under the 2015 Criminal Law Amendment (IX) (see *Legal update, SPC and SPP release interpretation on criminal infringement of personal information*).

Therefore, breach of personal information protection requirements by app operators, in serious cases, may constitute a criminal offence.

Civil law regime

The *General Provisions on the Civil Law of the PRC 2017* (2017 Civil Provisions), for the first time, recognised an individual's right to personal information as a type of personal rights. As a result, infringement of personal information may result in civil liability. The 2017 Civil Provisions were merged into and superseded by the *Civil Code of the PRC 2020* (2020 Civil Code, with effect from 1 January 2021). A specific chapter of the 2020 Civil Code stipulates the rights of individuals to personal information and the lawful ways to use personal information (see *Practice note, Chinese Civil Code: privacy and personal information protection*).

Additionally, where personal information processing activities infringe on personal information rights and cause damage, the infringing processor is presumed to be liable unless it can prove its compliance (*Article 69, 2021 PIPL*). Therefore, app operators must ensure the compliance of their apps to avoid possible civil liability.

Administrative law regime

China has several administrative laws and regulations on personal information protection, which stipulate detailed rules for personal information collecting and processing activities.

At the national law level, the *National People's Congress (NPC) Standing Committee* gradually promulgated legislation on personal information protection, including:

- The *Decision of the NPC Standing Committee on Strengthening Network Information Protection 2012* (2012 Network Information Decision), which is the first congress-level legislation on personal information protection, setting out the general principles for the collection of personal information.
- The *Cybersecurity Law of the PRC 2016* (2016 CSL, with effect from 1 June 2017), which adopts the same principles as the 2012 Network Information Decision and specifies the transparency, consent, and security requirements for personal information collection. The issuance of the 2016 CSL elevated personal information protection to the level of cybersecurity, and the government began to actively enforce personal information protection rules in cyberspace, especially those related to apps.
- The *2021 PIPL*, which is the most comprehensive law on personal information protection enacted by the NPC Standing Committee, raising the standard of personal information protection to a historically high level in China.

At the ministerial rule level, various government agencies issued administrative measures, particularly regulating the collection and processing of personal information on apps. Among these measures, the *Provisions on Protecting the Personal Information of Telecommunications and Internet Users 2013* (2013 Telecoms User Provisions), issued by the *Ministry of Industry and Information Technology* (MIIT), are the first ministerial-level rules specially designed to protect personal information on telecoms networks and the internet, including apps. The 2013 Telecoms User Provisions laid the foundation for the MIIT to enforce personal information protection. Although the 2013 Telecoms User Provisions were largely drafted as high-level rules, there are some implementing rules governing personal information-related behaviours, including in particular the time frame for responding to individuals' complaints concerning the protection of users' personal information (*Article 12*).

After the effectiveness of the 2016 CSL, the *Cyberspace Administration of China* (CAC, which is the leading authority in personal information protection), jointly with the MIIT and other relevant agencies, issued several ministerial-level rules on protecting personal information on apps, including:

- The *Measures for Determining Illegal and Non-compliant Collection and Use of Personal Information on Apps 2019* (2019 App Determination Measures), which elaborate on the ways to apply personal information protection rules on apps and set out the criteria for identifying violations of personal information (see *Legal update, CAC and other ministries provide guidance on illegal collection and use of personal information by apps*).
- The *Provisions for the Scope of Necessary Personal Information for Usual Types of Apps 2021* (2021 Necessary Information Provisions), which provide guidance on the scope of information allowed to be collected by apps with different functions (see *Legal update, CAC and other ministries identify scope of necessary personal information for mobile apps*).

On 1 November 2021, the same day as when the 2021 PIPL took effect, the MIIT issued the *Notice on Improving User Experience of Information Communication Services 2021* (2021 User Experience Notice), which, among others, addresses the issues regarding the implementation of personal information protection requirements under the 2021 PIPL on apps. This indicates that the protection of personal information on apps has become the top priority of enforcement on the effectiveness of the 2021 PIPL.

National standards

In addition to the formal sources of laws (including congress-made legislation and ministerial-level rules), some national standards and industrial standards were issued to help implement personal information protection requirements. These national standards are not law per se, but they reflect the government expectations on personal information protection. In other words, business operators are expected to make good efforts to follow these standards unless they have justifiable reasons.

One of the most important national standards is the *Information Security Technology – Personal Information Security Specification (GB/T 35273-2020)* (2020 PI Specification), issued by the *State Administration for Market Regulation* (SAMR) and the *Standardisation Administration of China* (SAC) in 2020. It provides for detailed rules for collecting, processing, transferring, and disposing of personal information. In particular, the 2020 PI Specification sets out the standards for determining bundled consent, specifies the requirements for transferring personal information, elaborates on the factors to be considered during a personal information impact analysis (PIA), and explains the criteria for erasing personal information. These rules are highly relevant to apps for their protection of users' personal information.

In July 2020, the National Information Security Standardisation Technical Committee (also known as TC260) issued the *Guidance for Self-assessment of Collection and Use of Personal Information by Apps (TC260-PG-20202A)* (2020 Self-assessment Guidance). The 2020 Self-assessment Guidance was prepared based on the *2019 App Determination Measures*, by making reference to personal information enforcement cases. It elaborates on six aspects for assessing the compliance of apps with personal information protection requirements, that is:

- Whether the rules for collecting and using personal information are disclosed.
- Whether the purpose, manner and scope of collecting and using personal information are clearly stated.
- Whether user consent is obtained before collecting and using personal information.
- Whether the principle of necessity is followed, and the collection of personal information is limited to the minimum scope related to the services provided by the apps.
- Whether user consent is obtained before sharing personal information to others.
- Whether channels and functions are provided to erase or to correct personal information as well as to communicate with the app operator.

The 2020 Self-assessment Guidance sets out detailed check points for complying with personal information protection requirements from the above aspects.

In November 2020, the Telecommunication Terminal Industry Forum Association (电信终端产业协会) (TAF) issued various technical standards for the review of user rights protection. Each of the standards addresses an area of personal information protection from technical aspects, including:

- Collection of personal information beyond permitted scope.
- Sending commercial notices to targeted users.
- Ways to collect personal information.
- Requests for permissions.
- Non-compliant collection and use of personal information.
- Posting apps for downloading.
- Management of app distribution platforms.
- Display of app information on app distribution platforms.
- Auto-run of apps.

These standards are not legally binding and the TAF is not a government agent. However, given that the TAF is a trade association comprising major telecoms companies and internet companies, these standards reflect good practice that the MIIT expects app operators to follow.

Enforcement campaigns against non-compliant apps

Since the effectiveness of the *2016 CSL*, the government launched many campaigns against apps that failed to comply with personal information protection requirements. In the course of these campaigns, hundreds of apps were reported to have breached personal information protection requirements and are required to take remedial measures.

From a procedural aspect, the government usually first announces the commencement of an enforcement campaign together with enforcement priorities, and then focuses on the announced areas in subsequent enforcement actions. Following one or several enforcement actions, the government issues further guidance, based on the findings during the previous actions, for determining non-compliant behaviours. Further guidance is usually more in-depth than those contained in the announcement initiating the enforcement campaigns and serves as a base for future enforcement actions.
From a substance aspect, the focuses of enforcement have become more substantial.

Enforcement actions

From January 2019 to September 2019, the CAC, MIIT, SAMR, and the *Ministry of Public Security* (MPS) jointly carried out a special rectification campaign against apps. More than 600 apps were found to have failed to meet personal information protection requirements and were ordered to rectify the failures.

Afterwards, the MIIT and CAC took enforcement actions separately. Although the issues which the MIIT and CAC look into largely overlap, the MIIT focuses on the technical aspects of apps while the CAC focuses on the scope

of collection. The MPS and SAMR also took some actions, with the MPS focusing on the security level of relevant apps and the SAMR focusing on consumer rights protection.

The MIIT has been launching enforcement action systematically since December 2019 and reporting non-compliant apps periodically. It had issued 19 enforcement reports until the end of 2021. Each enforcement report contains lists of non-compliant apps identified by the MIIT's local offices and each list contains information about the non-compliant apps, the channels for downloading the apps, and the violations identified. Taking the 19th enforcement *report* on 23 September 2021 as an example, the MIIT reported a total of 333 apps that violated personal information requirements, including 51 apps identified by the MIIT's commissioned testing institutions and 282 apps identified by the MIIT's local offices in nine provinces. These non-compliant apps were given one week to rectify their violations, otherwise they would face further administrative sanctions (for example, removal from app stores).

The CAC's local offices also carried out several enforcement actions and issued reports on violations. In contrast to the MIIT, the CAC reviews and reports non-compliant apps by the functions of apps. For example, according to the action *report* issued by the CAC in December 2021, the CAC's local office in Zhejiang Province announced that 87 apps in 17 categories failed to meet personal information protection requirements. These 17 categories include online shopping, online games, instant messaging, food delivery, home services, and so on.

According to the enforcement reports issued by the MIIT and CAC, when an app is found to have violated personal information protection requirements, the app will be publicised and required to make rectifications within a short period of time. Although the non-compliant apps are not taken down immediately, the actions taken by the MIIT and CAC still pose challenges for app operators, as the time period for apps to rectify their violations is usually very short, and the publication of the list of non-compliant apps may damage the reputation of app operators.

Enforcement guidance

Alongside with the enforcement actions, the CAC and MIIT issued several guidance, setting out their views on the determination of non-compliant behaviours. Some guidance is "indicative" in nature and provides for the key points on which a coming enforcement action will focus; other guidance is "summative" and sets out the common issues which the government identified during past enforcement actions.

2019

In January 2019, the CAC, MIIT, SAMR and MPS jointly issued the *Announcement on Conducting Special Rectification Campaign against Illegal Collection and Use of Personal Information by Apps 2019* (2019 Public Notice). The 2019 Public Notice announced the commencement of a one-year enforcement action and indicated the following priorities in the enforcement actions during 2019, that is, where an app operator:

- Collects personal information unrelated to the services provided.

- Fails to inform data subjects of the rules for collection and use of personal information in a clear way and an easy-to-read language.
- Does not allow data subjects to decide whether to consent to the collection of their information.
- Coerces data subjects to consent to the collection of their personal information.
- Collects personal information in violation of personal information protection rules or in breach of the agreement with data subjects.
- Does not provide an opt-out option for users when sending push notifications regarding news and commercial advertisement.

The 2019 Public Notice addresses only those apparent non-compliant activities, with a high-level description.

After ten months of enforcement actions, the MIIT issued the *Notice on Special Enforcement Work against the Infringement of User Rights by Apps 2019* (2019 MIIT Enforcement Notice), launching further enforcement actions from 31 October 2019 to 20 December 2019 and summarising the major non-compliant behaviours of apps identified in previous actions, including:

- Illegal collection of users' personal information, including where an app operator:
  - fails to clearly inform users of the purpose, method and scope before collecting the user's personal information; and
  - collects personal information beyond the scope of user consent or frequency, which is not necessary for the services it provides.
- Illegal use of personal information, including sharing personal information without consent and delivering customised marketing materials without an opt-out option.
- Unreasonable request for permissions, including forced activation of permissions, frequent requests for permissions, and requests for unnecessary permissions.
- Imposition of unreasonable conditions on account cancellation.

Most of the non-compliant behaviours illustrated in the 2019 MIIT Enforcement Notice are the same as those mentioned in the 2019 Public Notice. However, the 2019 MIIT Enforcement Notice contains illustrative samples for each type of non-compliance.

Shortly after the issuance of the 2019 MIIT Enforcement Notice, the CAC, MIIT, SAMR, and MPS jointly issued the *2019 App Determination Measures* in November 2019, providing detailed guidance on the determination of six categories of non-compliant behaviours of apps based on past enforcement actions, including:

- Failure to publicise the rules for the collection and use of personal information.
- Failure to clearly state the purpose, manner and scope of the collection and use of personal information.
- Collection and use of personal information without user consent.
- Collection of unnecessary personal information.
- Provision of personal information to others without consent.
- Failure to provide channels to erase or correct personal information or failure to publish information, such as complaints and reporting methods.

Compared to the 2019 MIIT Enforcement Notice, the 2019 Determination Measures provide additional and more specific illustrative samples for each non-compliant behaviour. To expand the 2019 Determination Measures, the government enacted the *2020 Self-assessment Guidance*, which covers the same six categories of non-compliant behaviours of apps and provides much more specific explanations of the criteria for determining these non-compliant behaviours.

2020

In July 2020, the MIIT issued the *Notice on Promoting Deepened Special Enforcement Actions against the Infringement of User Rights by Apps 2020* (2020 Deepened Action Notice), which clarified the key areas of enforcement actions by the MIIT in the next stage.

Unlike previous notices and rules issued by the MIIT, the 2020 Deepened Action Notice raised concerns about the compliance of technical designs with personal information protection requirements, including, the collection of personal information by software development kits (SDKs, which are third party codes built into apps) without disclosing the rules for using personal information, technical barriers for withdrawing consent to the collection of personal information, and cheating users into downloading apps through dummies.

2021

On 1 November 2021 when the *2021 PIPL* took effect, the MIIT issued the *2021 User Experience Notice*, requiring 39 identified big internet companies to improve, among other aspects, personal information protection practice within the time frame specified in the notice.

The 2021 User Experience Notice provides guidance on how to implement some of the personal information protection rules under the 2021 PIPL, including, for example, the way to display a privacy policy, alert the collection of sensitive information, and inform data subjects of the external provision of personal information collected by apps.

Although the MIIT identified only 39 big internet companies that must comply with the requirements in the 2019 User Experience Notice, the requirements reflect the good practices that the government expects all businesses to make efforts towards.

Enforcement priorities

Guidance and enforcement reports issued in previous enforcement actions indicate that the government has been adopting a step-by-step approach to gradually deepen enforcement priorities.

Privacy policy

During the first stage of enforcement, roughly from the effectiveness of the *2016 CSL* until early 2019, enforcement actions focused on the privacy policies or notices of apps. In particular, the CAC, MIIT, SAMR and

SAC launched a special campaign on privacy policy provisions (隐私条款专项工作) in July 2017, to review, analyse and improve the privacy policies of big internet companies for the purpose of setting them as model policies for other internet companies.

During this stage, the government also engaged testing and research institutions to review apps on the market. These institutions issued reports on their findings and urged operators whose apps were found non-compliant to make rectifications. A report issued by the Nandu Personal Information Protection Research Center (PIPRC) on 25 December 2018 revealed that, out of 1000 apps, 70% failed to have privacy policies satisfying the requirements under the 2016 CSL and 21% had no privacy policies at all.

Scope of personal information and user consent

After the first stage of enforcement, most of the apps on the market were equipped with privacy notices, and most of the notices contain the necessary information required by personal information protection laws.

The government then expanded its review during the second stage to the way that app operators collect personal information. In other words, the government looked into the scope of personal information actually collected by apps, and compared them against the scope of personal information to which users consented and the scope of personal information necessary to achieve the designed functions of apps.

For example, according to the *Announcement* of the First Batch of Reported Non-compliant Apps issued by the MIIT in December 2019, out of the 41 apps which were found non-compliant, 30 were reported to collect personal information beyond the scope of necessity or the scope to which users consented.

During this second stage, the government also gradually looked into the way in which app operators seek users' consent. In particular, the government reviewed whether app operators coerced users into consent. In the reports issued by the MIIT during 2019 and early 2020, failure to seek users' explicit consent is a commonly identified issue, in addition to the collection of personal information beyond allowed scope.

Technical designs

In 2021, while the CAC continued looking into the scope of information collection, the MIIT further expanded its focus to the technical design of apps. In the MIIT's enforcement reports in 2021, several apps were reported to have breached personal information protection requirements, including:

- Asking for mobile permissions in excessive, frequent or compulsory manners.
- Sending customised message without users' consent.
- Frequent automatic running or automatic activation of other programs.

Consequently, compliance work for apps should no longer be restricted to reviewing paper-based legal documents, but to also include the review of the designs of apps.

User experience

With the effectiveness of the *2021 PIPL*, the focus of enforcement appears to have been shifted to user experience. According to the *2021 User Experience Notice*, the MIIT looks into whether an app:

- Displays its privacy notice in a clear, precise, and an easy-to-understand manner.
- Informs users of the purpose of granting access to their camera, contact list, location, or other sensitive information.
- Optimises the display of its pop-up windows.
- Clearly lists the information it collects and shares with third parties.

Key requirements for compliance with personal information rules

China has a comprehensive set of requirements for apps to protect personal information. Despite the gradually deepened areas of focus and increasingly stricter enforcement, at this stage, the following are the key areas of enforcement which apps should pay attention to.

Display of privacy notices

Apps are required to display their privacy notices in a clear, precise, and easily accessed manner. According to Article 41 of the *2016 CSL*, network operators must publicise the rules for collecting and using personal information, and explicitly disclose the purposes, manner and scope of the information collection and use. Article 17 of the *2021 PIPL* further requires that, before processing personal information, personal information processors must inform data subjects genuinely, accurately, and completely, in prominent ways and in clear and understandable languages, of the following information:

- The name and contact information of the processors.
- The purposes and manners of processing personal information, the type of personal information being processed, and the retention period of personal information.
- The manners and procedures for data subjects to exercise their rights in personal information.

The information which is required to be disclosed to data subjects is usually compiled into a document known as a privacy notice or personal information protection policy. Obviously, since app operators collect and use users' personal information, they need to display the privacy notices to users in proper ways.

Based on the guidance issued by the government and enforcement cases, an online privacy notice should be:

- **Displayed within the app.** It is not sufficient to merely display the privacy notice on the official website or app store. Users should be allowed to view privacy notices on relevant apps. The common practice is to have a privacy notice pop up when users log into an app for the first time.
- **Easily accessible.** Users should be able to view the privacy notice both when registering and using the app. An app's privacy policy is not determined to be easily accessible unless it can be found by no more than four clicks from the app's homepage.

- **Easy to read and understand.** In terms of format, the font of the privacy notice should not be too small, the colour of the text should contrast with the background, and the layout of the privacy notice should not exceed the boundary of the apps. The usual practice is to display the privacy notice in the same or similar way as the main content of the apps. From the language aspect, since privacy notices are designed for laypeople, they should be written in an easily understood way. Legal or technical jargon without explanation is inappropriate. Some enforcement cases also indicate that privacy notices must be displayed in simplified Chinese.

The government also expects apps to display a summary of their privacy notices. As Chinese laws increasingly require privacy notices to contain sufficiently detailed information about personal information processing rules, the privacy policies of some sophisticated apps are more than ten pages. A layperson will have difficulty in reading and understanding long documents. On a pilot basis, the *2021 User Experience Notice* requires 39 top apps to display a summary of their privacy notice in addition to the privacy notice itself. The requirements may be expanded to apply to all apps in the future.

Scope of information to be collected

Minimum necessity is always the principle of personal information collection. Article 41 of the *2016 CSL* provides that network operators must not collect personal information irrelevant to the services they provide. Article 6 of the *2021 PIPL* further provides that the collection of personal information must be limited to the minimum scope which is necessary to achieve the purpose. Since apps may collect personal information to perform their functions, they must adhere to the minimum necessity principle.

Pending detailed clarification of the standard of necessity, the 2021 PIPL specifies certain circumstances that reflect the necessity standard, for example:

- Where certain personal information is necessary for performing a contract to which the data subject is a party, the processing of the personal information does not require the consent from the data subject (*Article 13*). The necessity standard stipulated in this provision is that the relevant contract cannot be performed without such personal information, that is, such personal information is irreplaceable for achieving the purpose of the contract. It implies that if personal information is collected on the basis of consent, the necessity standard does not require such personal information to be irreplaceable.
- Personal information processors must only process sensitive personal information when they have a specific purpose and sufficient necessity (*Article 28*). The standard of sufficient necessity in this provision may be interpreted as that the information to be collected cannot be substituted by less sensitive information. It appears that the processing of non-sensitive personal information only requires that such information is reasonably used in business processes to provide the services to which the data subject subscribes. Such information is not required to be irreplaceable.

The *2021 Necessary Information Provisions* set out the scope of "necessary" personal information which 39 categories of apps are allowed to collect, for the purpose of addressing which information, in the mind of the promulgating government agencies, satisfies the minimum necessity standard. However, since the 2021

Necessity Information Provisions fail to consider specific business scenarios, some provisions are not practically enforceable. For example, the information required for know your client (KYC) verification in the provision of financial services is not included in the scope of information which financial apps are allowed to collect.

Ways to demonstrate data subjects' consent

Article 41 of the *2016 CSL* requires network operators to obtain data subjects' consent before collecting and using their personal information. Article 13 of the *2021 PIPL* expands the basis for processing personal information, but data subjects' consent remains the primary basis. Apps, as a channel to collect personal information, must have a mechanism to seek and demonstrate data subjects' consent to the collection. The consent must be explicit and freely given. The following two types of consent are usually considered to be not explicit or not voluntary:

- **Default consent.** Article 14 of the 2021 PIPL requires the consent of a data subject to be explicit. This is consistent with the position under the *2020 PI Specification*. However, neither the 2021 PIPL nor the 2020 PI Specification further defines the term "explicit".

  The *2019 App Determination Measures* consider that default consent is not a way to demonstrate explicit consent of a data subject. In other words, apps must not assume that users agree to the collection of their personal information, for example, by displaying a pre-ticked consent box on behalf of users. Rather, apps should be designed to demonstrate a user's consent through specific acts, such as allowing users to tick a checkbox or click an "agree" button to express the consent to the collection and use of their personal information.
- **Bundled consent.** Article 14 of the 2021 PIPL requires that consent must be granted by data subjects on a voluntary basis. If users are forced to consent to the collection of personal information that is not necessary for performing the app function to which the users subscribe, such consent will be found involuntary. Similarly, if an app has multiple functions with each function requiring the collection of different types of personal information, the app must seek consent to collect these different types of personal information separately. Otherwise, if an app seeks consent to collect personal information for different functions in a package, this is called bundled consent and is not considered to be voluntary consent.

  Therefore, as suggested by the 2020 PI Specification, to avoid the risk of bundled consent, an app must first distinguish its core functions from ancillary functions, and maintain two channels to seek user consent to collect personal information used for core functions and ancillary functions separately.

Ways to seek permission

Neither the *2016 CSL* nor the *2021 PIPL* or other legislation specifically regulates the permission to access or activate an app's modules, such as granting permission for an app to access the camera, location and contact list on a user's phone. However, given that the purpose of granting permission is to collect information through these permitted mobile modules, the government considers that seeking permission on mobile devices should follow the same rules for seeking consent to collect personal information, according to the *2019 MIIT Enforcement Notice* and the *2020 Deepened Action Notice*.

In accordance with the past enforcement guidance and enforcement cases, the following behaviours are considered non-compliant:

- Activating functions or accessing app modules without notifying users or seeking users' consent.
- Requesting permissions unnecessary for performing the function of apps.
- Obtaining permission before users activate the function which requires that permission.
- Requesting permission in an excessively frequent manner, interrupting the normal use of apps.

For example, if a fund management app has the function of automatically locating nearby fund counters which needs the activation of the location module, the app must not:

- Access the location module without notifying the app user.
- Access the location module when users are not looking for nearby counters.
- Seek users' permission on the location module on every act on the app.

Notification of personal information sharing

Article 41 of the *2016 CSL* requires network operators to inform data subjects of the ways to use their personal information. However, the 2016 CSL focuses on regulating the use of personal information by network operators but not specifically regulating the transfer of personal information.

The *2020 Deepened Action Notice* clarifies the requirements for SDKs to collect personal information. Where an app collects personal information to transfer it to SDK developers, the app must specify the scope of personal information to be transferred to the SDKs, as well as the purpose and manner of collecting personal information by the SDKs. In practice, to meet such requirement, the privacy notices of apps which are embedded with SDKs usually contain a table showing all SDKs used in the app, the names of the SDK developers, functions of the SDKs, the personal information collected by the SDKs, and hyperlinks to the privacy notices of these SDKs.

After the effectiveness of the *2021 PIPL*, the *2021 User Experience Notice* requires the establishment of a dual-list system, that is, the privacy policy of an app must specify both the information it collects (including the information collected by the SDK embedded in the app) and the information it delivers to third parties (including the information send out by SDKs). Again, the 2021 User Experience Notice applies to 39 top apps and there is a possibility that it will be expanded to regulate all apps in the future.

Customised display and message

According to Article 24 of the *2021 PIPL*, if an app operator sends push notices of customised messages or commercial advertisement based on automated decision-making to an individual, it must provide the individual with the option not to receive the customised message or commercial notice, or convenient opt-out methods for such push notices.

Automated decision-making is defined as the activity of making decisions through automated analysis and assessment by computer programs of an individual's habits, interests or economic, healthcare, credit status and

so on (*Article 73, 2021 PIPL*). The requirements derive from the *2020 PI Specification*, which also requires operators to grant individuals the right to object to the display of goods and services customised according to personal characteristics, such as purchasing habits and interests.

It is a common practice for apps to push customised notifications to users based on their behavioural data, and display goods and services based on user preferences (for example, prioritising posts). In practice, apps usually follow the protocol below to meet the requirements of customised display and sending customised messages:

- When an app sends commercial messages (for example, in the form of emails or short messages) to users, its privacy notice should contain a request for users' consent to receiving such commercial messages. In addition, the commercial messages should contain links or buttons that users can click to reject further receiving such commercial messages.
- If an app has the function of displaying goods or other posts according to users' habits or other features, its privacy notice should clearly list the information that it collects for customised display.
- When an app displays goods and other posts according to users' habits or other personal information, it should provide alternative options (such as display by price or alphabet letters) so that users can select not to display the posts based on their habits or other personal information.

Communication channels

According to Article 12 of the *2013 Telecoms User Provisions*, telecoms and internet service providers must provide users with channels to report personal information breaches. Further, under the 2021 PIPL, data subjects have a series of rights to the information they disclose, including the right to enquiry, right to make a copy, right to update, right to withdraw consent and so on. Therefore, personal information processors must provide and maintain channels for individuals to communicate with them.

For the collection and processing of personal information via apps, since the app operators have no physical contact with users, all communications with users must be carried out on apps. In practice, apps may communicate with users via the following channels:

- For the right to enquiry, copy and update users' personal information, apps should maintain a profile page that displays users' personal information collected by the app, which can be screen-copied and updated.
- Apps should maintain easy-to-find pages where users can cancel their accounts with the apps and, on the cancellation, the users' personal information will be removed from the databases used for the normal course of business.
- Privacy notices of apps should clearly state:
  - the channels for users to communicate with the app operators and to exercise their data subject rights; and
  - the purposes and manner by which personal information may be used after cancellation of user accounts (for example, the retention of transaction records for after-sales services).
- Apps should provide an online hotline or email address by which dedicated teams can be reached to address users' reports on personal information matters.

Consequence of non-compliance

Apps are not only platforms for e-commerce businesses, but also one of the most important tools for companies to get closer to their customers. Since the effectiveness of the *2016 CSL*, apps have been the main target of personal information protection enforcement. With the effectiveness of the *2021 PIPL*, apps may continue to be the focus of enforcement of personal information protection.

Should any app breach personal information protection laws, according to past enforcement practices, it will be included in an official enforcement report as a non-compliant app together with the identified non-compliant issues. This will cause significant reputational damage. If an app identified as non-compliant fails to make rectifications within a prescribed time period (usually a week) set by the enforcing government agent, the app may face the risk of being taking down from the app store, which causes more serious damage to the app operator's business.

According to the *2021 PIPL*, serious breaches of personal information protection requirements, including those breaches by apps, may be subject to hefty fines (which could be a percentage of last year's turnover). For more information, see *Practice note, Personal information collection and processing in China: Liabilities and penalties for breach*.

Compliance reviews

A compliance review is important to mitigate the risk of apps being found non-compliant with personal information protection requirements.

Starting a review

App operators should perform a compliance review before launching an app, adding a new function to an existing app, or when the personal information processing activities of an app will change significantly.

According to Article 55 of the *2021 PIPL*, a PIA is required, among other situations, for the use of sensitive personal information, the collection of personal information for automated decision-making, and the sharing of personal information with third parties.

Since most apps collect personal information in one of the above scenarios, the launch of most apps requires a PIA in advance. Reviewing the compliance of an app's personal information processing activities is part of a PIA. Even if a PIA is not statutorily required, an early compliance review is still advisable as it may help mitigate the risk of an app being found non-compliant in enforcement actions and avoid reputational damage and possible business disruption.

Who is involved in a review?

A compliance review should be conducted by a team comprising representatives from legal, compliance, IT and business departments to ensure that business needs, IT risks, and legal and compliance requirements are all taken into account. External consultants may be involved in launching important apps to facilitate benchmark reviews.

How to conduct a review?

A compliance review of an app is usually a three-step process:

- The first step is to understand the personal information processing activities of the app, including, among others:
  - the types and quantity of personal information to be collected, processed, used, and communicated;
  - the purpose for using the personal information;
  - the way that the personal information is transmitted; and
  - the design, functionality, and business expectations of the app.
- The second step is to compare the personal information processing activities against a "compliance" standard and to discover any gaps or loopholes. The "compliance" standard is determined by considering:
  - the statutory requirements;
  - the rules indicated by enforcement cases; and
  - industrial practice.
- The third step is to build a solution that balances compliance and business needs, addressing the gaps or loopholes identified in the second step.

If you would like to know more information about the subjects covered in this publication, please contact:

Xun Yang
+86 21 3135 8799
xun.yang@llinkslaw.com

SHANGHAI

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

BEIJING

30F, Central Tower, China Overseas Plaza, 8 Guanghuadongli,
Chaoyang District
Beijing 100020 P.R.China
T: +86 10 5081 3888
F: +86 10 5081 3866

SHENZHEN

18F, China Resources Tower
2666 Keyuan South Road,
Nanshan District
Shenzhen 518063 P.R.China
T: +86 755 3391 7666
F: +86 755 3391 7668

HONG KONG

Room 3201, 32/F, Alexandra House
18 Chater Road
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

LONDON

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

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD