

Exploring Trends of App Privacy Policy Updates Under China's Personal Information Protection Law

This paper provides new perspectives and views to companies in need of establishing or revising their privacy policies. We selected 15 apps (referred to as "sample apps" hereafter) among the top 50 popular apps based on Apple Store's real-time download statistics for China as of April 20, 2022, from the categories "Business," "Social," "Shopping," "Photography," "Entertainment," "Music," and "Finance," to examine their privacy policy updates, and particularly generic key terms and industry-specific provisions. Below is a summary of the paper. For the full version (in Chinese only), please contact the authors.

1. Summary of key provisions of app privacy policies

Provisions of significant connection to users' rights and interests are usually highlighted in a conspicuous way (e.g., bold, italic, underlined) to draw users' particular attention. Four types of key provisions appear quite frequently in our research of the sample apps' privacy policies, which corresponds with our real-life experience.

1.1 Privacy protection for minors

All 15 sample apps included privacy provisions for minors in their privacy policies. WeChat has one of the most stringent requirements regarding guardian consent, which explicitly requires that minors under the age of 18 obtain “written consent” from their parents or guardians. QQ Music has a more relaxed approach, allowing minors aged above 14 and under 18 to authorize their own consent.

Eleven of the sample apps have privacy protection rules specific to children under 14 years old. The PIPL does not specify whether “special rules for handling personal information” have to be in the form of a separate document. However, the practice of those 11 sample apps suggests that if a company has, or may have, users under the age of 14, it is advisable to have in place specific privacy protection rules for children in addition to the general privacy policy to prepare for increasingly stringent regulatory requirements.

1.2 Biometric information processing

According to the Information Security Technology—Personal Information Security Specification (GB/T 35273-2020), biometric information includes human genomics, fingerprints, voice samples, and palm prints as well as ear, iris, and facial-recognition features. Because it is defined as sensitive personal information, biometric information is regulated under a different set of legal requirements. According to the PIPL, individual consent must be obtained to process sensitive personal information. The individual must be informed of the necessity of such processing as well as its impact on the individual’s rights and interests.

Based on the privacy policies of the 15 sample apps, we categorized the functions involving biometric information into facial beautification, verification and login (exclusive of real-name/real-person authentication) and other functions. The main types of biometric information involved in those functions are fingerprint, voice print, and facial-recognition features. Facial beautification is a frequent scenario where some sample apps processed biometric information. A common approach to storing biometric information is to store it locally on the user’s device, or to upload the information on a network server after de-identification/anonymization, to help mitigate and avoid the risks a company may face when handling

biometric information.

~~1.3 Real-name/real-person authentication~~


The real-name/real-person authentication provisions consist mainly of the types of personal information collected and the scenarios where the personal information is used. Among the sample apps, the main types of personal information collected for real-name/real-person authentication include name, ID number, and facial information, followed by mobile phone number and bank information. Companies need to determine whether the specific types of personal information collected involve sensitive personal information and, if so, carry out their legal obligations accordingly.

We combed through the privacy policies of the 15 sample apps and identified the main scenarios for real-name/real-person authentication. They are account registration, content publishing when logged in using a third-party account, and livestreaming.

In addition, certain sample apps specify the method of authentication (e.g., autonomous authentication, help from a third party, and manual authentication), the handling of information by third parties, and the disposal of information after the authentication is completed (i.e., storage or deletion). Tencent Meeting's livestreaming function requires the broadcaster to undergo real-person authentication but does not store the relevant information. Some of Taobao's functions involve real-name/real-person authentication and will store the authentication information and the authentication results. Apps that store authentication information state that the storage is for authentication purposes only and will not be used beyond that scope.

~~1.4 Automated decision-making~~

Automated decision-making is the activity of automatically analyzing and evaluating an individual's behavioral habits, interests, and/or financial, health, and credit status, and making decisions through computer programs. An analysis of the sample apps' privacy policies shows that the automated decision-making clause consists mainly of the type of personal information collected, the user's management of the automated



decision-making function, and the way the information is processed.

Typically, the privacy policies of the 15 sample apps fulfill the PIPL's requirements of restricting pushed information and commercial promotion by explaining to users how to manage and turn off the personalization features. In addition, because personalized decision-making is based on the various types of information collected by the app, deleting such information is also a way to manage personalized decision-making activities. Also, methods to limit the sources of personal information can help achieve a restrictive outcome.

In our view, there is no standard template for a privacy policy. Companies develop and update their own privacy policies that work for them, taking into account the company's business and actual needs, the breadth of the personal information collected, the manner in which personal information is handled, and the level of compliance with their own legal obligations.

2. Analysis of key provisions of app privacy policy


In the second part of this paper, we analyze the characteristics of the sample apps' privacy policies according to their categories: Business, shopping, social, financial, entertainment, music, and photography.

~~2.1 Business apps~~

Business apps usually expound scenarios for individual users, corporate users, and end-users separately. A section on the collection of personal information tailored to the target user group is also included based on the positioning of the product. To improve the user experience and the work-related functions, business apps usually enable connectivity with other applications for office use. Because business apps typically have access to more-sensitive company information, they must consider how to manage its information retention. In this regard, business apps may choose to give some level of autonomy to business users.

~~2.2 Shopping apps~~

Because shopping apps need to create and guide users' impulses to buy and then satisfy their needs of



purchase, they generally focus more on pushed information and commercial promotion and achieve automated decision-making through the information collected. As a result, how to ensure the automated decision-making process meets the increasingly tightened regulatory requirements for information protection has become a major concern for shopping app operators.

Shopping apps also push a select list of recommended items based on an analysis of users' browsing history, search history, and hot topics on the platform. Moreover, they typically collaborate with third parties on payment and delivery (core) functions. As a result, these apps must share users' information, including orders, addresses, and other personal information. Thus, when drafting their privacy policies, shopping app operators must consider distinguishing and separating their own policies from those of third parties.

~~2.3 Social apps~~

To enable interconnectivity, social apps allow the user some autonomy over whether and what information is collected by the app and disclosed to the public as well as to define the scope of information collected according to a user's needs.

~~2.4 Financial apps~~

One needs to submit an extensive range of required information, which is usually sensitive information, to be able to use the core functions of a financial app. Balancing between financial regulatory requirements and personal information protection is one of the key concerns of financial apps. The segregation of liability with services provided by third parties also needs to be handled discreetly and with an emphasis on measures and terms regarding information sharing and risk segregation.

~~2.5 Entertainment apps~~

There may be fewer types of required information that an entertainment app needs to collect. But when special activities such as livestreaming and cashflow are involved, users may be subject to real-name authentication. Entertainment apps are unique when setting targeted recommendations and user-profiling

terms, which are generally pushed audio/video content based on the positioning of the individual app rather than completely commercial advertisements.

2.6—Music apps

Music apps may collect users' voice print under specific circumstances when applying for special identity or occupational certification. Therefore, the collection and use of such biometric information that is special compared with other personal information is an emphasis and point of concern for music apps.

2.7—Photography apps

Facial-recognition information is required generally for photography apps to perform certain special functions. Photography app operators should take measures to inform users explicitly and enumerate the scope, content, and purpose of information collected, and apply de-identification and/or anonymization when processing facial recognition information to mitigate the compliance risks faced.

3. Conclusion

In sum, app operators need to keep abreast of the key provisions of the regulatory requirements relating to personal information protection, review them against industry practice, and adjust their user agreements and privacy policies to ensure compliance and minimize risks.

Authors



Andy Y.D. Pan
Equity Partner, Yuanda
Shanghai
+86 21 6105 0917

apan@yuandawinston.com



Kate Y.Y. Mao
Associate, Yuanda
Shanghai
+86 21 6105 0572

kamao@yuandawinston.com