JUNHE BULLETIN

JUNHE

March 28, 2019

Data Protection and Cybersecurity Law Update

Strengthening Governance of the Collection and Use of Personal Information by Apps

On January 25, 2019, the Cyberspace Administration of China, the Ministry of Industry and Information Technology, the Ministry of Public Security and the State Administration for Market Regulation jointly issued the *Announcement of Launching a Special Crackdown on the Illegal Collection and Misuse of Personal Information by Apps*, launching what is proposed to be a one-year special crackdown.

Various organizations, namely the National Information Security Standardization Technical Committee, the China Consumers Association, the Internet Society of China and the Cybersecurity Association of China have subsequently established a Working Group for the Special Crackdown on the Illegal Collection and Misuse of Personal Information by Apps (the **"Working Group"**), and on March 1, 2019 released the *Self-Assessment Guidelines on the Illegal Collection and Misuse of Personal Information by Apps* (the **"Guidelines"**).

I. Key Points for Assessment

The Guidelines detail the requirements for App operators to self-regulate, by checking and correcting their own conduct in relation to personal information collection and use. There are 32 assessment items under nine headings, laid out in three main sections, namely: the text of the privacy policy; the actual practice in an App's collection and use of personal information; and the protection of user rights when using Apps.

The Guidelines' requirements are based upon various pre-existing legislative items, namely the *Cybersecurity Law,* the *Consumer Rights Protection Law,* and the *Information Security Technology - Personal Information Security Specification* (the **"Specification"**), and a more recent draft, revised version, *The Information Security Technology - Personal Information Security Specification Draft* (the **"Draft Revised Specification"**) which was released for comment on January 30, 2019. Compared with the Specification and the Draft Revised Specification, the requirements prescribed in the Guidelines are stricter and more detailed, and include a number of new items. Some of the key aspects of the Guidelines are summarized below:

1. The privacy policy shall clearly state each service and the types of the personal information collected for each function

Perhaps the most noteworthy aspects of the Guidelines are their emphasis upon and clear definition of the "necessity principle". Where Apps provide multiple services, and each service requires users to provide different types of personal information, the Guidelines clearly indicate that the personal information required by each function shall separately listed in the privacy policy, and should not of being summarized or abbreviated by terms such as "etc." and '"e.g.". In addition, personal information should be collected separately for each different service; it is not permitted that information collected for one service can be used across other business services.

2. Apps shall clarify the purpose of information collection before obtaining authorization for system use

The Guidelines require that, when an App is seeking system authorization (excluding those circumstances where a user voluntarily enables the authorization voluntarily in their system settings), the App shall make it clear that the authorization is for the purpose of personal information collection.

The Guidelines also provide that App operators shall not require users to accept and agree to a one-time authorization to collect personal information for multiple services through bundling multiple services.

3. The privacy policy shall explicitly describe how user profiles will be used to personalize the display of content

According to the Guidelines, if an App operator intends to use personal information for profiling or for personalizing the display of content, the privacy policy shall indicate the scenarios where the information will be used and its potential influence on a user.

The Draft Revised Specification stipulates various opt-out mechanisms for personalized display: if personalized display is being used to push news or an information service to a user, the user shall be provided with a simple and intuitive option to withdraw from this personalized mode; if personalized display is being used to provide services to the users, they shall be given the option of deleting or anonymizing the personal information on which the targeted push activity is based should they choose to exit the personalized display mode.

4. The types of personal sensitive information and the export of personal data shall be clearly marked in the privacy policy

According to the Guidelines, any content relating to sensitive personal information and the export of personal information shall be clearly marked in the privacy policy, for example through the use of bold font, asterisk, underline, italics, color or other methods that draw the user's attention. When collecting personal and sensitive information, an App shall explicitly indicate the purpose, method and scope of collection and use of personal information in a prominent way, such as through pop-up prompts.

5. An App shall provide users with the right to close their accounts

The Guidelines not only require App operators to clearly explain in the privacy policy the process whereby a user can close their account, but also require an App to provide the means to close the account, such as an online interface that links to a customer service line. App operators are required to timely anonymize and delete a user's personal information after the user has closed the account.

6. Embedding third-party code plug-ins to collect personal information

According to the Guidelines, if personal information is transmitted to the server of a third party via an embedded third-party code, a plug-in or other means, the user shall be explicitly informed through a method such as a pop-up prompt. According to the Specification, if a personal information controller deploys a third-party plug-in that does not separately seek authorization from the subject to collect and use their personal information, then the personal information controller and the third party shall be regarded as joint personal information controllers and shall bear the obligation of explicitly informing the personal information subject. This requirement of the Guidelines also reflects the principle of the Specification above.

7. Continuing to ask for authority and pester users having already been explicitly refused

According to the Draft Revised Specification, a personal information controller shall not *repeatedly* solicit the consent of the personal information subject who rejects, turns off or quits specific services. The Guidelines set an even higher requirement, that is an App shall not ask the user again whether to turn on the corresponding authority for certain services.

8. Other requirements

Among some of the other requirements included in the Guidelines are that the privacy policy shall be presented separately and shall be easy to read and visit, and be accessible within four clicks of the main function interface; the privacy policy shall explicitly list the App operator's basic information, including the responsible person's name, registered address and contact information; it is prohibited to include unreasonable conditions; and an App shall provide methods of searching, correcting, and deleting personal information.

II. Our Observations

The Guidelines include and on certain points go beyond the requirements already outlined in the Cybersecurity Law, the Specification and the Drafted Revised Specification, proposing detailed and stricter assessment standards. It seems many Apps in the market would currently be unlikely to meet the requirements laid out in the Guidelines unless further improvement is made.

At present, the Working Group suggests App operators should self-regulate through voluntarily conducting self-inspection, making corrections regarding the collection and use of personal information, and improving protection for personal information. In practice, we have not as yet come across any administrative penalty precedents based on the Guidelines.

Marissa DONG	Partner	Tel: 86 10 8519 1718	Email:dongx@junhe.com
Lena YUAN	Associate	Tel: 86 10 8553 7663	Email:yuanq@junhe.com
Junjie DONG	Associate	Tel: 86 10 8540 8722	Email: dongjj@junhe.com

This document is provided for and only for the purposes of information sharing. Nothing contained in this document constitutes any legal advice or opinion of JunHe Law Offices.. For more information, please visit our official website at www.junhe.com or our WeChat public account “君合法律评论”/WeChat account “JUNHE_LegalUpdates”.

君合研究简讯

JUNHE

2019 年 3 月 28 日

信息保护和网络安全法律热点问题

四部委加强 App 个人信息收集使用治理

2019 年 1 月 25 日，中央网信办、工信部、公安部与市场监管总局四部门联合发布《关于开展 App 违法违规收集使用个人信息专项治理的公告》，拟针对目前 App 收集与使用个人信息的乱象，开展为期一年的专项治理。据此，全国信息安全标准化技术委员会、中国消费者协会、中国互联网协会、中国网络空间安全协会成立 App 违法违规收集使用个人信息专项治理工作组（以下简称“**工作组**”），工作组于 2019 年 3 月 1 日编制发布了《App 违法违规收集使用个人信息自评估指南》（以下简称“**《指南》**”）。

一、 评估重点

《指南》主要用于 App 运营者对收集与使用个人信息进行自查自纠，分别从隐私政策文本、App 收集使用个人信息行为、App 运营者对用户权利的保障三个方面提出了 9 大评估事项共计 32 个评估点。《指南》中的要求主要参照《网络安全法》、《消费者权益保护法》、《信息安全技术 个人信息安全规范》（GB/T 35273-2017，于 2018 年 5 月 1 日实施，以下简称“**《信安规范》**”），以及于今年 1 月 30 日发布征求意见的新修订的《信息安全技术 个人信息安全规范（草案）》（以下简称“**新《信安规范》（草案）**”）。从整体来看，《指南》提出的要求更加严格和细致，其中有多项要求系首次提出，其中重点梳理如下：

1、 隐私政策需清晰说明各项业务功能及其所收集个人信息类型

《指南》最值得注意的要求在于强调、细化和明确了“必要性”原则，对 App 提供多项功能、多项功能分别要求用户提供不同类型的个人信息的情况，《指南》明确提出隐私政策中应当将收集个人信息的业务功能**逐项列举**，每个业务功能在说明其所收集的个人信息类型时，应在隐私政策中**逐项列举**，不得使用“等、例如”等方式概括说明；并且，每个业务功能都应说明其对应的收集的个人信息类型，不应出现多个业务功能对应一类个人信息的情况。这种“穷尽式”的列举要求在实践中可能给 App 运营者带来很大的挑战和实操难度。

2、 App 使用系统权限应说明该权限将收集个人信息的目的

《指南》要求当 App 打开系统权限时（不包括用户自行在系统设置中打开权限的情况），**App 应当说明该权限将收集个人信息的目的**。

《指南》还要求 App 运营者不应通过捆绑多项业务功能的方式，要求用户一次性接受并授权同意多项业务功能收集个人信息的请求。

3、 隐私政策需明示用户画像与个性化展示的使用

《指南》要求，如果 App 运营者将个人信息用于用户画像、个性化展示等，隐私政策中应说明其应用场景和可能对用户产生的影响。 我们注意到，与之相关的，新《信安规范》（草案）对个性化展示的退出机制进行了规定：在向个人信息主体推送新闻或信息服务的过程中使用个性化展示的，应为个人信息主体提供简单直观的退出个性化展示模式的选项；在向个人信息主体提供业务功能的过程中使用个性化展示的，当个人信息主体选择退出个性化展示模式时，应向个人信息主体提供删除或匿名化定向推送活动所基于的个人信息的选项。

4、 隐私政策里个人敏感信息类型与个人数据出境情况需显著标识

《指南》要求，隐私政策里涉及个人敏感信息及个人信息出境的情况均需显著标识，可采用字体加粗、标星号、下划线、斜体、颜色等方式，提醒用户高度关注。其中，在收集个人敏感信息时，App 应以弹窗提示等显著方式向用户明示收集、使用个人信息的目的、方式、范围。

5、 App 需提供用户注销账号的权利

《指南》不仅要求 App 运营者在隐私政策里对用户注销账户的操作方法进行明确的说明，同时要求 App 应提供注销账号的途径（如在线功能界面、客服电话等），并在用户注销账号后，及时删除其个人信息或进行匿名化处理。

6、 嵌入第三方代码插件收集个人信息

《指南》要求，如果通过嵌入第三方代码、插件等方式将个人信息传输至第三方服务器，应通过弹窗提示等方式明确告知用户。根据《信安规范》，个人信息控制者在提供产品或服务的过程中部署了收集个人信息的第三方插件，且该第三方并未单独向个人信息主体征得收集、使用个人信息的授权同意，则个人信息控制者与该第三方为共同个人信息控制者，并应履行向个人信息主体明确告知的义务。《指南》该项要求也体现了上述规定的精神。

7、 被明确拒绝后不得继续索要权限、打扰用户

《指南》提出，对用户明确拒绝使用、关闭或退出的特定业务功能，App 不应再次询问用户是否打开该业务功能或相关系统权限。新《信安规范》（草案）规定，若个人信息主体不同意使用、关闭或退出特定业务功能，个人信息控制者不得频繁征求个人信息主体的同意。《指南》明确提出了更高的要求，即“不应”再次询问用户是否打开相应权限。

除了上述要点之外，《指南》还提出了隐私政策需单独成文并易于阅读、容易访问（从 App 主功能界面通过 4 次以内的点击应当能访问到隐私政策）、隐私政策应列明 App 运营者基本情况（包括名称、注册地址、负责人联系方式）、不得设不合理条款、App 应提供查询、更正、删除个人信息的途径等要求。

二、我们的观察

《指南》细化了《网络安全法》、《信安规范》的要求，并提出了一些相对法律法规的原则性要求更加细致和严格的评估标准，按照《指南》的标准，目前很多 App 在实践之中可能并未能达到《指南》的具体要求。

目前，工作组建议 App 运营者参照《指南》对其收集使用个人信息的情况进行自查自纠，主动提升个人信息保护水平。但实践中尚未看到有明确的根据《指南》的处罚案例。

董　潇　合伙人　电话：86 10 8519 1718　邮箱地址：dongx@junhe.com
袁　琼　律　师　电话：86 10 8553 7663　邮箱地址：yuanq@junhe.com
董俊杰　律　师　电话：86 10 8540 8722　邮箱地址：dongjj@junhe.com

本文仅为分享信息之目的提供。本文的任何内容均不构成君合律师事务所的任何法律意见或建议。如您想获得更多讯息，敬请关注君合官方网站“www.junhe.com” 或君合微信公众号“君合法律评论”/微信号“JUNHE_LegalUpdates”。