君合研究简讯

JUNHE

2020 年 8 月 7 日

信息保护和网络安全法律热点问题

标准确立与执法并进——APP 数据保护监管进一步加强

2020 年 7 月底，一系列标准制定与执法活动进一步释放出 APP 隐私保护监管加强的信号：

- 2020 年 7 月 22 日，中央网信办、工业和信息化部、公安部、国家市场监管总局（以下简称**“四部委”**）在京召开会议，启动 2020 年 APP 违法违规收集使用个人信息治理工作[1]；
- 同日，工业和信息化部也宣布开展纵深推进 APP 侵害用户权益专项整治行动[2]；
- 全国信息安全标准化技术委员会（以下简称**“信安标委”**）也于同日发布标准相关技术文件《网络安全标准实践指南—移动互联网应用程序（APP）收集使用个人信息自评估指南》（以下简称**“《信安标委自评估指南》”**）正式生效版本，以六大评估点为 APP 运营者进行个人信息使用自评估提供参考与方向[3]。

一、标准及执法情况回顾和进展

2019 年 3 月 3 日，在宣布开展 APP 违法违规收集使用个人信息专项治理后，为推进 APP 运营者对其收集与使用个人信息的情况进行自查自纠，受四部委委托的 APP 违法违规收集使用个人信息专项治理工作组发布《APP 违法违规收集使用个人信息自评估指南》（以下简称**“《工作组自评估指南》”**），成为 APP 运营者开展隐私实践合规的重要指导性文件。此后，四部委又于 2019 年 12 月 30 日发布《APP 违法违规收集使用个人信息行为认定方法》（以下简称**“《认定方法》”**）。而此次《信安标委自评估指南》则是在《网络安全法》和《认定方法》等一系列法律法规要求的基础上，结合目前所开展的 APP 检测评估经验所归纳总结的 APP 运营者自评估要点。相比于一年前发布的《工作组自评估指南》，《信安标委自评估指南》结合了一年来开展 APP 隐私治理工作的经验要点，提供更为细化的落实要求。

四部委启动的 2020 年 APP 违法违规收集使用个人信息治理工作，在总结了 2019 年 APP 整治工作的基础上，也进一步强调了 2020 年 APP 治理工

1http://www.cac.gov.cn/2020-07/25/c_1597240741055830.htm

2http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057709/n3057714/c8027149/content.html

3信标委曾于 3 月 19 日公布该规定的征求意见稿。

作的重点。

工业和信息化部在 2019 年多批整改各类 APP 的基础上，开展纵深推进 APP 侵害用户权益专项整治行动，旨在督促相关企业强化 APP 个人信息保护，及时整改消除违规收集、使用用户个人信息和骚扰用户、欺骗误导用户、应用分发平台管理责任落实不到位等突出问题，净化 APP 应用空间，并拟于 2020 年 8 月底前上线运行全国 APP 技术检测平台管理系统，12 月 10 日前完成覆盖 40 万款主流 APP 检测工作。

二、合规重点

基于以上的进展，我们建议企业特别重视以下 APP 合规要点：

1. 评审范围扩展：《信安标委自评估指南》明确，除 APP 运营者之外，小程序、快应用等运营者也可参考其中的适用条款进行自评估。工业和信息化部整治行动也提到将对小程序、快应用进行评估。值得注意的是，信安标委于今年 3 月份发布的《网络安全标准实践指南-移动互联网应用程序（APP）个人信息安全防范指引（征求意见稿）》中也提出建议小程序运营者参考适用该指引。因此，将小程序、快应用等纳入到评审范围的趋势逐渐凸显。

2. 强调儿童信息保护：《信安标委自评估指南》特别强调，若涉及收集使用儿童个人信息相关业务功能的，需制定针对儿童的个人信息保护规则，并举例如收集不满十四周岁未成年人个人信息的教育类 APP 应制定针对儿童的个人信息保护规则。该规定呼应了 2019 年国家互联网信息办公室发布的《儿童个人信息网络保护规定》，体现出儿童个人信息保护将可能成为监管重点之一。

3. 强化 SDK 及第三方应用的合规要求：在《工作组自评估指南》的基础上，《信安标委自评估指南》进一步强调与细化了第三方代码及插件（如 SDK）收集个人信息的要求，包括：如嵌入第三方代码、插件（如 SDK）收集个人信息，需说明第三方代码、插件的类型或名称，及收集个人信息的目的、类型、方式；通过客户端嵌入第三方代码、插件（如 SDK）等方式向第三方发送个人信息时，需事先征得用户同意，但《信安标委自评估指南》特别规定，经匿名化处理除外。此外，《信安标委自评估指南》还规定了 APP 接入第三方应用并向其提供个人信息的相关要求，包括：在征得用户同意后向第三方应用提供个人信息，APP 运营者应对第三方应用收集个人信息的合法、正当、必要性等方面进行审核。

4. 进一步明确权限申请与收集个人敏感信息的告知方式：《工作组自评估指南》要求收集个人敏感信息时，APP 应通过弹窗提示等明显方式向用户明示收集、使用个人信息的目的、方式、范围。《认定方法》则进一步提出在收集上述信息时应同步告知用户收集的目的。在此基础上，《信安标委自评估指南》对上述告知要求进行了整合和强化：要求申请打开个人信息收集权限时及要求用户提供个人敏感信息时，通过显著方式同步告知用户其目的，对目的的描述明确、易懂，例如通过弹窗提示、用途描述等等显著方式告知。

5. APP 申请与使用系统权限的要求进一步加强、细化：《信安标委自评估指南》整合、强化了《工作组自评估指南》与《认定方法》中的要求，要求在打开可收集个人信息的系统权限时，应通过显著方式同步告知用户其目的，对目的的描述明确、易懂。

2020 年 7 月 29 日，信安标委发布《网络安全标准实践指南—移动互联网应用程序（APP）系统权限申请使用指引（征求意见稿）》（以下简称“**《权限使用指引》**”）。《权限使用指引》规定了 APP 申请、使用系统权限的基本要求及通用原则以及安卓系统典型权限的申请和使用要求，并在附录中介绍了安卓、iOS 系统常见的敏感系统权限、系统权限申请使用的常见问题，及常见服务提供的过程中不建议 APP 申请的安卓系统权限。《权限使用指引》针对当下 APP 运营者过度索权、滥用用户个人信息的现象，为 APP 运营者申请与使用用户权限提供了较为全面的参考。其中的一些具体要求，例如除安全风控场景外，APP 不应收集不可变更的设备唯一标识（如 IMEI 等），对小程序收集个人信息权限的要求都值得进一步关注。

6. 强调、细化必要原则要求：《信安标委自评估指南》将“是否遵循必要原则”作为一个单独的评估点，并进一步细化遵循必要原则的具体要求。包括不得收集与业务无关的个人信息、用户可拒绝非必要信息的收集、不得强迫收集用户个人信息、收集个人信息频度不得超过业务实际需要等。其中，《信安标委自评估指南》特别强调在浏览、游客等无需注册即可使用的模式下，不得以影响用户使用功能的方式促使用户同意个人信息收集行为。此外，必要性原则的强化也体现在《权限使用指引》中，最小必要原则是 APP 权限申请的基本原则之一并体现在《权限使用指引》的具体要求中。由此可见必要原则将成为 APP 运营者个人信息收集与使用过程中应关注的重点。

7. 用户画像与定向推送：《工作组自评估指南》要求“应说明个人信息用于用户画像、个性化展示的应用场景及其对用户权益产生的影响”。在此基础上《信安标委自评估指南》进一步要求如部分业务功能不涉及用户画像、个性化展示，可在规则中明确说明。关于定向推送，《信安标委自评估指南》强调，存在利用用户个人信息和算法定向推送信息情形时，需为用户提供拒绝接收定向推送信息，或停止、退出、关闭相应功能的机制，或不基于个人信息和个性化推荐算法等推送的模式、选项。这也与《认定方法》的要求一致。

8. 隐私政策的展示与同意：在《工作组自评估指南》与《认定方法》的基础上，《信安标委自评估指南》进一步要求，尽可能在界面的固定路径展示隐私政策（或其链接），不频繁变更展示隐私政策的路径；不得以默认选择同意隐私政策等非明示方式征求用户同意，除在首次运行、用户注册时，通过弹窗等明示方式提醒用户阅读隐私政策，若通过设置“下一步”、“注册”等方式征求用户同意，还需明确上述动作与同意隐私政策之间的逻辑关系。

9. 用户个人信息保护权利行使的回应及投诉、举报渠道：《信安标委自评估指南》重述了《认定方法》中对用户有关个人信息权利行使的回应与投诉、举报的处理应承诺时限不超过 15 个工作日的要求。在用户有关个人信息的投诉、举报渠道中，将《工作组自评估指南》原有的“传真”方式替换为“即时通讯账号”。

三、我们的观察

《信安标委自评估指南》的出台及近日执法部门针对 APP 违法违规收集使用个人信息的整治活动进一步说明 APP 隐私实践的相关执法与监管力度不断加大，小程序、快应用等运营者也逐步成为监管重点关注的对象。建议各类 APP、小程序等运营者应尽快加强对收集与使用用户个人信息的合规工作，并随时关注相关的立法与监管动态。

董　潇　合伙人　电话：86 010 8519 1718　邮箱地址：dongx@junhe.com
郭静荷　律　师　电话：86 010 8553 7947　邮箱地址：guojh@junhe.com
董俊杰　律　师　电话：86 010 8540 8722　邮箱地址：dongjj@junhe.com

JUNHE BULLETIN

August 12, 2020

Data Protection and Network Security

Regulations on App Data Protection are Further Strengthened

At the end of July 2020, the supervision of the privacy protection of apps is strengthened, signaled by a series of standard formulation and law enforcement activities.

- On July 22, 2020, the Cyberspace Administration of China ("**CAC**"), the Ministry of Industry and Information Technology of the People's Republic of China ("**MIIT**"), the Ministry of Public Security of the People's Republic of China and the State Administration of Market Regulation ("**Four Ministries**") held a meeting in Beijing to launch the work of governing the illegal collection and use of personal information by apps in 2020[1];

- On the same day, MIIT also announced the launch and promotion of rectification action for the infringement of users' rights and interests by apps[2];

- The National Technical Committee of Information Security Standardization ("**TC 260**") also issued on the same day a document titled *Network Security Standard Practice Guidelines - Self-Assessment Guidelines on the Collection and Use of Personal Information by Mobile Internet Applications* (formal effective version) ("**TC260 Guideline**"). It provides reference and direction for app operators to conduct self-assessment on the use of personal information, in the form of six evaluation points[3].

1. Review and progress of standards and law enforcement

After the announcement of the launch of the special governance on the illegal collection and use of personal information by apps on March 3, 2019, in order to push app operators to conduct self-examination and self-correction on the collection and use of personal information, the app special governance working group on the illegal collection and use of personal information entrusted by the Four Ministries issued the *Guidelines on Self-assessment on the Illegal Collection and Use of Personal Information by*

[1] http://www.cac.gov.cn/2020-07/25/c_1597240741055830.htm

[2] http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057709/n3057714/c8027149/content.html

[3] The T260 released the draft version of such Guidelines for public consultation on March 19th.

Apps ("**Working Group Guidelines**"), which has become an important guiding document for app operators to develop privacy practices and compliance. The Four Ministries issued the *Determination Rules for Identifying the Illegal Collection and Use of Personal Information by Apps* ("**App Determination Rules**") on December 30, 2019. The TC260 Guidelines summarized the main points of self-assessment for app operators based on the requirements of a series of laws and regulations such as *Cybersecurity Law* and the App Determination Rules, in combination with the existing app testing and evaluation. Compared with the Working Group Guidelines issued a year ago, the TC260 Guidelines combine key points obtained from the experience of app privacy governance over the past year and provides more detailed implementation requirements.

On the basis of summarizing the app governance work in 2019, the 2020 governance work on the illegal collection and use of personal information by apps launched by the Four Ministries further emphasizes the key points of the app governance work in 2020.

MIIT carried out special in-depth rectification actions on the governance of the infringement of user rights and interests by apps, aiming to urge relevant enterprises to strengthen the protection of personal information by apps. It urged them to conduct rectification and eliminate problems such as the illegal collection and use of a user's personal information, and the harassment, deception and misleading of users. It also discussed the inadequate implementation of management responsibilities by application distribution platforms, with the aim to purify the space of apps. MIIT also plans to run a national app technology testing platform management system before the end of August 2020, as well as complete all testing work covering 400,000 mainstream apps by December 10.

2. Key Points in Compliance

Based on the above, we recommend that enterprises pay special attention to the following app compliance points:

1) Expansion of the evaluation scope: the TC260 Guidelines clarify that in addition to app operators, operators of mini-programs and fast applications may also conduct self-assessment with reference to the applicable terms. An assessment on mini-programs and fast applications is also required in MIIT's governance action. It is noticeable that the *Network Security Standard Practice Guideline-Mobile Internet Application (App) Personal Information Security Prevention Guidelines (Draft for Comment)* issued by TC260 in March also suggests that mini-program operators should refer to the guidelines. Therefore, the trend to include mini-programs and fast applications in the scope of the evaluation has become more prominent.

2) Emphasis on the protection of children's information: The TC260 Guidelines emphasize that if an app has a function of collecting and using a child's personal information, it is necessary for the app operators to formulate specific personal information protection rules for children. For example, educational apps which collect the personal information of minors under the age of 14 should formulate personal information protection rules for children. This regulation echoes the *Provisions on the Network Protection of Children's Personal Information*, which was issued by CAC in 2019, indicating that the protection of children's personal information is likely to become a focus of the regulation.

3) Strengthening the compliance requirements of SDK and third-party applications: On the basis of the Working Group Guidelines, the TC260 Guidelines further emphasize and refine the requirements for collecting personal information by third-party codes and plug-ins (such as SDK), including: when collecting personal information through embedded third-party codes and plug-ins (such as SDK), app operators should explain the type

and the name of the third-party code or the plug-in, as well as the purpose, type and method of the personal information collection; when sending information to a third party through third-party codes and plug-ins (such as SDK) embedded in the client side, the user's consent should be obtained in advance, though the personal information which has been anonymized is excluded from the above requirements. In addition, the TC260 Guidelines also stipulate the relevant requirements for an app regarding its connection with third-party applications and providing them with personal information. For example, an app should provide personal information to third-party applications after obtaining the user's consent, and the app operators should check the legality, legitimacy and necessity of personal information collection by third-party applications.

4）Further clarify the notification method for permission applications and the collection of personal sensitive information: The Working Group Guidelines require that when collecting sensitive personal information, apps should clearly indicate to the users the purpose, method and scope of the collection and the use of personal information through pop-up prompts or other obvious methods. The App Determination Rules further propose that users should be notified of the purpose of the collection at the same time when collecting the above information. On this basis, the TC260 Guidelines combine and strengthen the above notification requirements by requiring that when applying to enable permission for personal information collection or requesting users to provide personal sensitive information, the user should be simultaneously notified of the purpose of the personal information collection in a significant way and the description of the purpose should be clear and easy to understand; the notification may be conducted through pop-up prompts, descriptions of the purpose, etc.

5) Further strengthening and refining the requirements for apps to apply for and use system permissions: the TC260 Guidelines combine and strengthen the requirements in the Work Group Guidelines and App Determination Rules. It states that when enabling the system permission for collecting personal information, users should be informed of its purpose at the same time and in an eye-catching way, and the description of the purpose should be clear and easy to understand.

On July 29, 2020, the TC 260 issued the *Network Security Standard Practice Guidelines-Guidelines on the Application and Use of Mobile Internet Application (APP) System Permission (Draft for Comment)* ("**Permission Use Guidelines**"). The Permission Use Guidelines stipulate the basic requirements and general principles for apps to apply for and use system permissions, as well as the application and use requirements for typical permissions of the Android system. Furthermore, it also introduces common sensitive system permissions of Android and iOS systems, common issues in the application and use of systems permissions, and system permissions which are not recommended to be applied for by apps in the provision of services. The Permission Use Guidelines provide a comprehensive reference for app operators to apply for and use users' permissions in response to the current phenomenon of excessively claiming rights and abusing users' personal information. Some of these specific requirements are worthy of further attention such as except for security risk control situations, an app should not collect unique device identifiers that cannot be changed (such as IMEI); and the different requirements for personal information collection permission for mini-program operators.

6）Emphasizing and refining the requirements of the necessity principles: The TC260 Guidelines stipulate "whether to follow principles of necessity" as an independent evaluation point, and further refine the specific requirements for following the necessity principles, including: operators should not collect personal information

irrelevant to their business, users can refuse the collection of unnecessary information, operators are not allowed to force users to collect personal information and the frequency of collecting personal information should not exceed the actual needs of the business. The TC260 Guidelines particularly emphasize that users should not be prompted to consent to the collection of personal information in a way that affects the user's use of functions under the mode of browsing, tourist or other modes that can be used without registration. In addition, the strengthening of the principle of necessity is also reflected in the Permission Use Guidelines. The principle of minimum necessity is one of the basic principles of app permission applications and is reflected in the specific requirements of the Permission Use Guidelines. It shows that the principle of necessity should become the focus of attention in the process of the collection and use of personal information by app operators.

7） User portraits and targeted push notifications: The Working Group Guidelines require that "application scenarios where personal information is used for user portraits and personalized display and the impact of such use on users' rights should be explained". On this basis, the TC 260 Guidelines further require that if some business functions do not involve user portraits and personalized displays, it should be stated in the rules. Regarding targeted push notifications, the TC260 Guidelines stress that when a user's personal information and algorithms are used to push information, the mechanisms for refusing to receive targeted push information, or stopping, exiting and turning off the corresponding function should be provided to the user as well as the pushing mode and option which is not based on personal information and personalized recommendation algorithms. This is also consistent with the requirements of the App Determination Rules.

8） Requirements on displaying and consenting to privacy policies: On the basis of the Working Group Guidelines and App Determination Rules, the TC260 Guidelines further require that privacy policies (or links) should be displayed in a fixed way on the interface and this should not be changed frequently; the operators should not obtain consent from users by non-expressive methods such as agreeing to privacy policies with tacit consent.

Except for the requirement that users should be notified to read privacy policies through express methods such as pop-ups at the first time of running the app or registration, if the users' consent is obtained through settings such as a "next step" or "registration", the logical relationship between the above actions and the privacy policy consent should also be clarified.

9) Responses, complaints and reporting channels for users to implement their rights on personal information protection: the TC260 Guidelines reiterate the requirements that the time limit for dealing with responses, complaints and tip-offs should not exceed 15 working days which was provided in the App Determination Rules. As for the channels for user complaints and reports on personal information, the original "faxing" method stipulated in the Working Group Guidelines has been replaced with "instant messaging account".

3. Our observations

The introduction of the TC260 Guidelines and the recent governance activities of law enforcement authorities further illustrate the continuous strengthening of the law enforcement and supervision related to app privacy practices. Operators such as mini-programs and fast applications have also gradually become the focus of supervision. It is recommended that operators of various apps and small programs should strengthen compliance in the collection and use of users' personal information as soon as possible and pay close attention to the relevant legislation and regulatory developments.

Marissa DONG	Partner	Tel: 86 10 8519 1718	Email:dongx@junhe.com
Jinghe Guo	Associate	Tel: 86 10 8553 7947	Email:guojh@junhe.com
Junjie DONG	Associate	Tel: 86 10 8540 8722	Email: dongjj@junhe.com