移动应用(APP)的个人信息保护

作者：杨迅 | 杨蕾

中国正在经历一场数字化的经济革命。随着智能手机的普及和移动电子商务的蓬勃发展，移动应用程序 APP，包括微信上的小程序和公众号，以及 H5 页面(俗称移动网站，可以无缝与个人微信资料结合，构建微信营销平台)越来越成为企业经营者提升品牌形象和推广产品的重要工具。

中国相关的监管部门也正不断努力加强对中国居民个人信息的保护。与此同时，对 APP 上个人信息保护的监管要求也在不断加强。特别是在 2021 年 11 月 1 日《中华人民共和国个人信息保护法》(以下简称“《个保法》”)生效后， APP 上个人信息保护的标准显著提高。

本文概述了中国对 APP 收集和处理个人信息的监管要求。讨论了针对不合规 APP 的执法活动、APP 的合规要求以及其违反个人信息保护法规的后果。并为 APP 运营商提供实践指南，以降低运营商违反个人信息保护法规的风险。

一. APP 个人信息保护法律体系

2021 年《个保法》是中国首部规范与个人信息相关的活动并保护居民个人信息的综合性法律。但是，它并不是中国唯一一部关于个人信息保护的法律或法规。相反，中国早在十多年前就开始规范与个人信息相关的行为。随着 2021 年《个保法》的生效，中国已经建立了较为完善的个人信息保护体系。个人信息现在在刑法、民法和行政法中都能找到相应的救济途径。

For more Llinks publications, please contact:

Publication@llinkslaw.com

如您需要了解我们的出版物，请联系:

Publication@llinkslaw.com

(一) 刑法体系

与西方国家不同，中国的个人信息保护最先从刑法开始:

- 2009 年《中华人民共和国刑法修正案(七)》认定国家机关或者金融、电信、交通、教育、医疗等单位的工作人员窃取、出售或者非法提供个人信息是犯罪行为。
- 2015 年《中华人民共和国刑法修正案(九)》进一步扩大了主体范围。所有个人，无论其工作或职位如何，都有可能构成窃取、出售或者非法提供个人信息罪。《刑法修正案(九)》还包括网络服务提供者不履行信息网络安全管理义务导致用户信息严重泄露的罪名，最高可判处三年有期徒刑。

  2017 年 5 月 9 日，最高人民法院、最高人民检察院联合发布《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》，明确了 2015 年《刑法修正案(九)》下涉及刑事侵害公民个人信息的某些条款。

因此, APP 运营商违反个人信息保护要求，情节严重的，可能构成刑事犯罪。

(二) 民法体系

2017 年《中华人民共和国民法总则》首次从民事基本法层面确立了个人信息的民事权利。因此，侵犯个人信息可能需要承担民事责任。 2020 年颁布 2021 年 1 月 1 日起生效的《民法典》吸收了《民法总则》 。《民法典》第四编第六章专门规定了个人信息权以及个人信息处理的原则和条件。

此外，如果处理个人信息侵害个人信息权造成损害，除非个人信息处理者能够证明自己没有过错，否则将推定其承担损害赔偿等侵权责任(《个保法》第 69 条)。因此, APP 运营商必须确保其应用程序的合规性，以避免承担民事责任的风险。

(三) 行政法体系

中国有相当多的与个人信息保护相关的行政法规和规章。通过这些法律、法规及规章制度，中国逐步确立了个人信息收集和处理的详细规则。

在国家法律层面，全国人大常委会对个人信息保护的立法也呈现出逐渐详细的特点:

- 2012 年《全国人大常委会关于加强网络信息保护的决定》(以下简称“《网信保护决定》”)，这是第一部关于个人信息保护的国家级立法，规定了收集个人信息的一般原则。
- 2016 年《中华人民共和国网络安全法》(以下简称“《网安法》”，自 2017 年 6 月 1 日起生效)，沿用了 12 年《网信保护决定》的一般原则，并规定了收集个人信息的告知要求、同意要求和安全要求。《网安法》的发布将个人信息保护提升到网络安全的高度，预示着政府开始重视网络空间中个人信息保护，包括与 APP 相关的个人信息保护规则。

- 2021 年《个保法》是迄今为止全国人大常委会制定的最全面的个人信息保护法，将个人信息保护水平提高到了历史最高水平。

在国务院部委层级，针对 APP 上个人信息的收集和处理，各政府机构也发布了相关个人信息保护的规定。其中， 2013 年《电信和互联网用户个人信息保护规定》(以下简称"《电信用户规定》")是工业和信息化部(工信部)发布的第一部专门用于保护包括 APP 在内的电信网络和互联网个人信息的行政规章。 2013 年《电信用户规定》为工信部加强个人信息保护奠定了基础。尽管 2013 年《电信用户规定》在很大程度上是作为纲领性文件起草的，但对个人信息相关行为也有一些实施规则，特别是对与用户个人信息保护有关的投诉的答复时限(第 12 条)。

2016 年《网安法》实施后，国家网信办(网信办，个人信息保护的牵头机构)联合工信部等相关部门发布了多项关于个人信息保护的行政规章，包括:

- 2019 年《App 违法违规收集使用个人信息行为认定方法》(以下简称"《 App 违法违规行为认定方法》")将个人信息保护规则应用于 APP，并制定违反个人信息保护的标准。
- 2021 年《常见类型移动互联网应用程序必要个人信息范围规定》(以下简称"《必要信息规定》")，对不同功能 APP 允许收集的信息范围提供指导。

2021 年 11 月 1 日，《个保法》生效当天，工信部发布《关于开展信息通信服务感知提升行动的通知》， (以下简称"《服务感知通知》")，旨在解决在 APP 上实施 2021《个保法》下个人信息保护的相关问题。这表明，2021《个保法》生效后，保护 APP 上的个人信息已成为执法的重中之重。

(四) 国家标准

除了法律法规和规章之外，一些国家标准和行业标准也可以起到保护个人信息的作用。虽然这些标准本身不是法律法规，但它们反映了监管部门对个人信息保护的期望。这也就是说，除非有正当理由，经营者应努力遵守这些标准。

这些标准中，最重要的国家标准之一是《信息安全技术-个人信息安全规范》 (GB/T 35273-2020)(以下简称"2020 个保规范")，由国家市场监督管理总局(市场监管总局)和国家标准化管理委员会(国家标准委)于 2020 年发布。它规定了收集、处理、传输和处置个人信息的详细规则。具体而言，2020 个保规范规定了确定捆绑同意的标准，明确了传输个人信息的要求，详细说明了在个人信息影响分析 (PIA) 中要考虑的因素，并解释了删除个人信息的标准。这些规则在保护用户的个人信息方面与 APP 高度相关。

2020 年 7 月，全国信息安全标准化技术委员会(简称 TC260)发布《移动互联网应用程序 app 收集使用个人信息自评估指南》(TC260-PG-20202A)(以下简称"《自评估指南》")。 《自评估指南》是根据 2019 年《 App 违法违规行为认定方法》，参考个人信息执法案例编制而成的。指南详细阐述了评估 APP 是否符合个人信息保护要求的六个方面，即:

- 是否公开收集使用个人信息的规则。
- 是否明示收集使用个人信息的目的、方式和范围。
- 是否征得用户同意后才收集使用个人信息。
- 是否遵循必要原则，仅收集与其提供的服务相关的个人信息。
- 是否经用户同意后才向他人提供个人信息。
- 是否提供删除或更正个人信息功能，或公布投诉、举报方式等信息。

2020 年《自评估指南》从上述方面对遵守个人信息保护要求的检查点进行了详细的规定。

2020 年 11 月，电信终端产业协会(TAF)发布了 APP 用户权益保护测评规范系列标准。每个标准都从技术方面有针对性地规范个人信息收集使用，包括:

- 超范围收集个人信息。
- 定向推送。
- 个人信息获取行为。
- 权限索取行为。
- 违规使用个人信息。
- 违规收集个人信息。
- 下载分发行为。
- 移动应用分发平台管理。
- 移动应用分发平台信息展示。
- 自启动和关联启动行为

这些标准不具有法律约束力, TAF 也不是政府机构。然而，鉴于 TAF 是一个主要由电信公司和互联网公司组成的行业协会，这些标准反映了工信部对 APP 运营商合规的期望。

二. 针对 APP 个人信息保护合规的执法行动

自 2016 年《网安法》生效以来，相关监管部门针对不符合个人信息保护要求的 APP 展开了大量的执法行动。在执法过程中，有数百个 APP 因违反了个人信息保护要求，被要求采取补救措施。

从程序上看，监管部门通常会先预先发布本次执法的关注重点，然后在随后的执法行动中针对宣布的重点领域开展执法。在一次或多次执法行动之后，监管部门会总结之前的执法经验，并发布针对违规行为的指导意见。这种指导意见实践性更强并为之后的执法行动奠定基础。

从实质上看，针对不合规 APP 的执法重点日益深化和充实。

(一) 执法行动

2019 年 1 月至 2019 年 9 月，网信办、工信部、市场监管总局、公安部根据《关于开展 App 违法收集使用个人信息专项治理的违规公告》，联合开展应用专项整治。600 多款 APP 因不符合个人信息保护要求，被责令整改。

其后，工信部、网信办分别采取执法行动。虽然工信部和网信办在执法范围上存在很大的重叠，但工信部侧重于 APP 技术方面的合规，而网信办侧重于信息收集方面的问题。 公安部和市场监管总局也有相应的执法活动，公安部重点关注相关 APP 的安全等级，市场监管总局重点关注消费者权益保护。

工信部自 2019 年 12 月以来一直在系统性地开展执法行动，并定期报告不合规的 APP。截至 2021 年底，工信部已发布 19 份执法报告。执法报告中包含了由工信部各省市管理局认定的不合规 APP 列表，列表中包含有不合规 APP 的信息、下载途径以及违规事实。以 2021 年 9 月 23 日的发布的第十九次执法报告为例，工信部共通报了 333 款违反个人信息要求的 APP。其中，工信部委托第三方检测机构认定的 APP 51 款，工信部 9 省通信管理局认定的 APP 282 款。这些不合规的 APP 被要求限时一周内整改，否则它们将面临进一步的行政处罚(例如，从应用程序商店下架)。

网信办各地工作组也开展了多项执法行动并发布 APP 违规通报。与工信部不同，网信办按照应用功能对不合规 APP 进行审核和通报。例如，根据网信办 2021 年 12 月发布的《浙江关于闪修侠等 87 款 App 违法违规收集使用个人信息情况的通报》，这 87 款 APP 分别来自 17 个不同品类，包括网上购物、网络游戏、即时通讯、餐饮外卖、本地生活等。

根据工信部和网信办发布的执法报告，当发现某款 APP 违反个人信息保护要求时，将予以公示，并要求其限期整改。虽然这些不合规的 APP 没有立即下架，但工信部和网信办采取的措施仍然会对 APP 运营商产生影响，因为监管部门给予的整改时间通常很短，而且不合规名单的公布可能会损害运营商的声誉。

(二) 执法指导意见

在执法行动的同时，网信办和工信部发布了多项对违规行为认定的指导意见。一些指导本质上是“指示性的”，规定了即将采取的执法行动的关注重点；一些指导是"总结性的"，列出了监管部门在过去执法行动中发现的常见问题。

(1) 2019

2019 年 1 月，网信办、工信部、市场监管总局和公安部联合发布了《关于开展 App 违法违规收集使用个人信息专项治理的公告》，宣布开始为期一年的执法行动，并指出 2019 年执法行动中需要关注的以下重点事项，即 APP 运营商:

- 收集与所提供服务无关的个人信息。
- 未能以通俗易懂、简单明了的方式展示个人信息收集使用规则。
- 不允许用户决定是否同意收集其信息。
- 强迫用户同意收集其个人信息。
- 违反个人信息保护规则或违反与用户的约定收集使用个人信息。
- 在定向推送新闻、时政、广告时，不为用户提供拒绝的选项。

2019 年的这份公告仅针对那些明显不合规的行为，并对不合规活动进行了概要描述。这次执法行动结束后，工信部发布了《关于开展 App 侵害用户权益专项整治工作的通知》(以下简称"《专项整治通知》")，为其后的执法(2019 年 10 月 31 日至 2019 年 12 月 20 日)提供了指引，并总结了之前执法中发现的 APP 的不合规行为，包括:

- 违规收集用户个人信息方面

  1."私自收集个人信息"。即 APP 未明确告知收集使用个人信息的目的、方式和范围并获得用户同意前，收集用户个人信息。

  2."超范围收集个人信息"。即 APP 收集个人信息，非服务所必需或无合理应用场景，超范围或超频次收集个人信息，如通讯录、位置、身份证、人脸等。

- 违规使用用户个人信息方面

  3."私自共享给第三方"。即 APP 未经用户同意与其他应用共享、使用用户个人信息，如设备识别信息、商品浏览记录、搜索使用习惯、常用软件应用列表等。

  4."强制用户使用定向推送功能"。即 APP 未向用户告知，或未以显著方式标示，将收集到的用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或精准营销，且未提供关闭该功能的选项。

- 不合理索取用户权限方面

  5."不给权限不让用"。即 APP 安装和运行时，向用户索取与当前服务场景无关的权限，用户拒绝授权后，应用退出或关闭。

  6."频繁申请权限"。即 APP 在用户明确拒绝权限申请后，频繁申请开启通讯录、定位、短信、录音、相机等与当前服务场景无关的权限，骚扰用户。

  7."过度索取权限"。即 APP 在用户未使用相关功能或服务时，提前申请开启通讯录、定位、短信、录音、相机等权限，或超出其业务功能或服务外，申请通讯录、定位、短信、录音、相机等权限。

- 为用户账号注销设置障碍方面

  8."账号注销难"。即 APP 未向用户提供账号注销服务，或为注销服务设置不合理的障碍。

2019 年的联合公告中大部分的不合规行为与其后工信部发的通知中提到的不合规行为没有明显区别。但是，工信部的通知中包含有每种违规行为的示例。

在工信部的通知发布不久后，网信办、工信部、市场监管总局、公安部于 2019 年 11 月又联合发布了《App 违法违规收集使用个人信息行为认定方法》，就 APP 六类不合规行为的认定作出了详细指导。包括:

- 未公开收集使用规则。
- 未明示收集使用个人信息的目的、方式和范围。
- 未经用户同意收集使用个人信息。
- 违反必要原则，收集与其提供的服务无关的个人信息。
- 未经同意向他人提供个人信息。
- 未按法律规定提供删除或更正个人信息功能或未公布投诉、举报方式等信息。

与 2019 年工信部的通知相比，2019 年 11 月的认定方法对每一种不合规行为都提供了更多、更具体的说明样本。为充实该认定方法，相关监管部门制定了 2020 年《自评估指南》，涵盖了相同的六类 APP 的不合规行为，并对这些不合规行为的认定标准进行了更具体的解释。

(2) 2020

2020 年 7 月，工信部发布了《开展纵深推进 App 侵害用户权益专项整治行动的通知》(以下简称“《纵深行动通知》”)，明确了工信部下一阶段执法行动的重点领域。

2020 年《纵深行动通知》整治对象包括 App 服务提供者、软件工具开发包(SDK)提供者、应用分发平台三类，整治任务包括 App、SDK 违规处理用户个人信息，设置障碍、频繁骚扰用户，欺骗误导用户以及应用分发平台责任落实不到位的四大方面。

(3) 2021

2021 年 11 月 1 日，《个保法》生效之日，工信部发布 2021《服务感知通知》，明确要求 39 家互联网大公司在通知规定的时限内完善个人信息保护等方面的工作。2021《服务感知通知》就如何实施 《个保法》下的一些个人信息保护规则提供了指导，例如如何显示隐私政策、提醒收集敏感信息以及告知用户 APP 已经收集到的个人信息基本情况。尽管工信部仅要求 39 家互联网大公司必须遵守 2021《服务感知通知》，但这些要求反映了监管部门对其他相关企业合规的期望。

(三) 执法重点

以往执法行动中发布的指导和执法报告表明，相关监管部门一直在采取循序渐进的方式，逐步深化执法重点。

(1) 隐私政策

在执法的第一阶段，大致从 2016 年《网安法》生效到 2019 年初，执法行动侧重于隐私政策。特别是，2017 年 7 月网信办、工信部、公安部、国家标准委联合开展隐私条款专项工作，对大型互联网公司的隐私政策进行审查、分析和完善，以期将其作为其他互联网公司的示范。

在这个阶段，监管部门还聘请了测试和研究机构来检测市场上的应用程序，并根据这些机构发布的调查报告，敦促不合规的 APP 运营商进行整改。南都个人信息保护研究中心(PIPRC)于 2018 年 12 月 25 日发布的一份报告显示，在 1000 个 APP 中，70% 的 APP 没有满足 2016 年 《网安法》的隐私政策的要求，21% 的 APP 根本没有隐私政策。

(2) 个人信息范围和用户同意

第一阶段执法后，市场上的大部分 APP 都配备了隐私声明，并且大部分通知都包含个人信息保护法所要求的必要信息。

监管部门随后在第二阶段将审查范围扩大到 APP 运营商收集个人信息的方式。也就是说，监管部门将 APP 实际收集到的个人信息与用户同意的个人信息和实现 APP 设计功能所需的个人信息进行了比较。例如，根据工信部 2019 年 12 月发布的《关于侵害用户权益行为的 APP(第一批)通报》，在被查明不合规的 41 个 APP 中，30 个 APP 被查出超出必要范围或用户同意的范围收集个人信息。

在这第二阶段中，相关监管部门也逐渐研究 APP 运营商寻求用户同意的方式。特别是，监管部门审查了 APP 运营商是否强迫用户同意。在 2019 年和 2020 年初工信部发布的报告中，除了收集超出允许范围的个人信息外，未征得用户明确同意是一个普遍存在的不合规问题。

(3) 技术设计

2021 年，在网信办持续研究个人信息收集范围的同时，工信部进一步将重点扩展到 APP 的技术设计。工信部 2021 年执法报告中，有不少 APP 被查出违反个人信息保护要求，包括:

- 以过度、频繁或强制的方式请求移动权限。
- 未经用户同意发送自定义消息。
- 频繁自动运行或自动激活其他程序。

因此，APP 的合规工作不应再局限于审查纸质法律文件，还应包括对 APP 设计的审查。

(4) 用户体验

随着 2021《个保法》的生效，执法的重点似乎已转移到用户体验上。根据 2021《服务感知通知》，工信部调查 APP 是否:

- 以简洁、清晰、易懂的方式，向用户提供 APP 产品隐私政策摘要。
- 以适当方式告知用户调用对其相册、通讯录、位置等敏感权限的访问权限的目的。
- 优化 APP 开屏弹窗信息展示方式。
- 简洁、清晰列出 APP 与第三方共享的用户个人信息基本情况。

三. 遵守个人信息保护法规的关键要求

中国对 APP 中的个人信息保护有一套全面的要求。尽管重点领域逐渐深化，执法力度越来越强，但现阶段，以下是 APP 运营商应注意的重点执法领域。

(一) 显示隐私声明的方式

APP 必须以清晰、准确且易于访问的方式显示其隐私声明。2016 年《网安法》第 41 条，网络运营者必须公开个人信息收集、使用规则，明示收集、使用信息的目的、方式和范围。 2021 年《个保法》第 17 条进一步要求，个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项:

(一) 个人信息处理者的名称或者姓名和联系方式;
(二) 个人信息的处理目的、处理方式，处理的个人信息种类、保存期限;
(三) 个人行使本法规定权利的方式和程序;
(四) 法律、行政法规规定应当告知的其他事项。

需要向用户披露的信息通常被编纂成一份名为隐私政策或个人信息保护声明的文件。显然，由于 APP 运营商收集和使用用户的个人信息，他们需要以适当的方式向用户展示隐私政策。

根据政府发布的指导和执法案例，运营商披露的方式应该:

- **显示在应用程序内。**仅在官方网站或应用商店上显示隐私声明是不够的。应允许用户查看相关 APP 的隐私声明。 通常的做法是在用户首次登录 APP 时弹出隐私通知。
- **易于访问。**用户在注册和使用 APP 时应该能够查看隐私声明。一个易于访问的隐私政策应当在 APP 主页点击四次之内就可以找到。
- **易于阅读和理解。** 格式方面，隐私声明的字体不宜过小，文字颜色应与背景形成对比，隐私声明的布局不应超出 APP 的边界。通常的做法是以与 APP 的主要内容相同或相似的方式显示隐私声明。语言方面，由于隐私声明是为普通大众设计的，因此它们应该以易于理解的方式编写，如一些法律和技术术语应当有相应的解释。此外，执法案例还表明隐私声明必须以简体中文显示。

政府还希望 APP 显示其隐私声明的摘要。随着中国法律对隐私声明中个人信息处理规则的要求日益严格，一些大型 APP 的隐私政策长达十多页。外行很难理解和阅读这些长文档。作为试点，2021《服务感知通知》要求 39 个热门 APP 除了隐私声明本身，还应显示其隐私声明的摘要。这些要求将来可能会扩展适用于所有 APP 上。

(二) 收集信息的范围

最小必要始终是个人信息收集的原则。 2016 年《网安法》第 41 条规定，网络运营者不得收集与其提供的服务无关的个人信息。2021 年《个保法》第 6 条进一步规定，收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。由于 APP 需要收集个人信息以执行其功能，因此它们必须遵守最小必要性原则。

虽然对必要性标准更详细的说明暂付阙如， 2021 年《个保法》规定了的某些情况反映了必要性标准，例如:

- 如果某些个人信息是订立、履行个人作为一方当事人的合同所必需，则个人信息处理者不需要个人的同意(第十三条) 。本条规定的必要性标准是，如果没有该个人信息，相关合同就无法履行，即该个人信息对于实现合同目的是不可替代的。这意味着如果个人信息是在同意的基础上收集的，必要性标准并不要求此类个人信息是不可替代的。
- 个人信息处理者只有在具有特定的目的和充分的必要性的情况下，才能处理敏感的个人信息(第二十八条) 。本条中的充分必要性标准可以理解为所收集的信息不能被不那么敏感的信息所替代。而非敏感个人信息的处理只需要在业务过程中合理使用此类信息，并为用户提供其所认购的服务。此类信息不需要是不可替代的。

2021 年《常见类型移动互联网应用程序必要个人信息范围》规定了允许 39 类常见类型 App 的必要个人信息范围，为最低必要性标准提供了参考。但是，由于该规定没有考虑到具体的业务场景，一些规定实际上不具备执行力。例如，在提供金融服务时，了解客户(KYC)验证所需的信息没有被包括在金融应用程序可以收集的信息范围内。

(三) 表明数据主体同意的方式

2016 年《网安法》第 41 条要求网络运营者在收集、使用个人信息前必须征得被收集者的同意。2021 年《个保法》第 13 条扩大了处理个人信息的基础，但个人的同意仍然是主要依据。APP 作为收集个人信息的渠道，必须有一种机制来寻求和证明用户对其信息收集的同意。这种同意必须是明确的和自愿的。以下两种类型的同意通常被认为是不明确的或不自愿的:

- **默认同意。** 2021 年《个保法》第 14 条要求数据主体明确同意。这与 2020 PI 规范下的立场一致。但是， 2021 年《个保法》和 2020 PI 规范都没有进一步定义术语“明确” 。

2019 年《 App 违法违规行为认定方法》认为默认同意不是证明用户明确同意的一种方式。也就是说， APP 不得推定用户同意收集他们的个人信息，例如，代表用户显示预先勾选的同意框。相反，APP 的设计应能够让用户通过特定行为表明同意，例如勾选复选框或单击“同意”按钮以表示同意收集和使用其个人信息。

- **捆绑同意。**2021 年《个保法》第 14 条要求个人必须在自愿的基础上给予同意。如果被迫同意收集不是用户订阅的执行 APP 功能所必需的个人信息，此类同意将被视为非自愿的。同样，如果一个 APP 具有多个功能，并且每个功能都需要收集不同类型的个人信息，则该 APP 必须分别征得同意才能分别收集这些不同类型的个人信息。如果 APP 不这么做的话，这种同意称为捆绑同意，不被视为自愿同意。

  因此，正如 2020 个保规范所建议的，为避免捆绑同意的风险，APP 要区分其核心功能和辅助功能，分别取得用户同意，收集用于核心功能和辅助功能的个人信息.

(四) 获取权限的方式

2016 年《网安法》和 2021 年《个保法》或其他法规都没有对于允许访问或激活 APP 模块的专门规定，例如授予 APP 访问用户手机上的相册、位置和联系人列表的权限。然而，鉴于授予权限的目的是通过这些模块收集信息，根据 2019 年工信部发布的《专项整治通知》和 2020 年《纵深行动通知》，在移动设备上获取权限应与寻求同意收集个人信息遵循相同的规则。

根据以往的执法指导和执法案例，以下行为是不合规的:

- 在未通知用户或征得用户同意的情况下激活功能或访问 APP 模块。
- 请求打开 APP 功能不必要的权限。
- 在用户激活需要开启某项权限的功能之前获取权限。
- 请求权限过于频繁，影响 APP 的正常使用。

例如，如果基金管理 APP 具有自动定位附近基金柜台的功能，需要启动定位模块，则该 APP 不得:

- 在不通知应用用户的情况下访问位置模块。
- 当用户不在寻找附近的柜台时访问位置模块。
- 每次操作 APP 时，寻求用户对位置模块的许可。

(五) 个人信息共享的通知

2016 年《网安法》第 41 条要求网络运营者告知被收集者使用其个人信息的方式。但是，2016 年《网安法》的重点是规范网络运营者对个人信息的使用，并未具体规范个人信息的共享。

2020 年《纵深行动通知》明确了 SDK 收集个人信息的要求。APP 通过 SDK 向他人传输个人信息的，必须明确传输给 SDK 的个人信息范围，以及 SDK 收集个人信息的目的和方式。在实践中，为满足此类要求，嵌入 SDK 的 APP 的隐私声明通常包含一个表格，显示 APP 中使用的所有 SDK、SDK 开发者的名称、SDK 的功能、SDK 收集的个人信息、以及这些 SDK 隐私声明的超链接。

2021 年《个保法》生效后，2021《服务感知通知》要求建立双清单制度，即 APP 的隐私政策必须明确其收集的个人信息(包括内嵌第三方软件工具开发包 SDK)及其传递给第三方的信息(包括 SDK 发出的信息)。同样，2021《服务感知通知》适用于 39 款热门应用，未来有可能扩大到规范所有应用。

(六) 个性化显示和消息推送

根据 2021 年《个保法》第 24 条，如果 APP 运营商基于自动化决策向个人推送消息和商业营销信息，必须向个人提供不接收消息和商业营销信息的选项，或提供此类推送的便捷拒绝方式。

自动化决策被定义为通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。(第 73 条，《个保法》)。该要求源自 2020 年个保规范，该规范还要求运营商授予个人反对展示根据个人特征(例如购买习惯和兴趣)定制商品和服务的权利。

APP 通常会根据用户的行为数据向用户推送定制化通知，并根据用户的偏好(例如，之前察看的商品和服务)展示商品和服务。实际上，APP 通常遵循以下协议来满足自定义显示和发送自定义消息的要求:

- 当 APP 向用户发送商业营销(例如，以电子邮件或短信的形式)时，其隐私声明应包含用户同意接收此类商业营销。此外，此类商业营销应包含拒绝进一步接收此类消息的链接或按钮。
- 如果 APP 具有根据用户习惯或其他特性展示商品或其他商品的功能，其隐私声明应明确列出其为个性化展示而收集的信息。
- 当 APP 根据用户的习惯或其他个人信息显示商品和其他展示时，它应该提供替代选项(例如按价格或字母显示)，以便用户选择不基于他们的习惯或其他个人信息展示商品或服务。

(七) 沟通渠道

根据 2013 年《电信用户规定》第 12 条，电信业务经营者、互联网信息服务提供者应当建立用户投诉处理机制，公布有效的联系方式，接受与用户个人信息保护有关的投诉。此外，根据 2021 年《个保法》，个人对其披露的个人信息享有一系列权利，包括查阅权、复制权、更新权、撤回同意权等。因此，个人信息处理者必须提供和维护个人与他们沟通的渠道。

对于通过 APP 收集和处理个人信息，由于 APP 运营商与用户没有线下接触，因此与用户的所有通信都必须在 APP 上进行。在实践中，APP 可以通过以下渠道与用户交流:

- 对于用户个人信息的查阅、复制和更新的权利，APP 运营商应维护用户可以复制和更新的个人资料页面，并显示 APP 收集的用户个人信息。
- APP 的注销页面应易于查找。用户可以在这些页面中注销其 APP 帐户，并且在注销后，其个人信息将从日常商业运营的数据库中删除。
- APP 的隐私声明应明确说明:
  - 用户与 APP 运营商沟通和行使个人信息权利的渠道；和
  - 注销用户帐户后可能使用个人信息的目的和方式(例如，为售后服务保留交易记录) 。
- APP 应提供在线热线或电子邮件地址，通过该热线或电子邮件地址可以联系到专门的团队来处理用户关于个人信息的问题。

四. 合规建议

APP 不仅是电子商务企业的平台，也是企业拉近客户的最重要工具之一。自 2016 年《网安法》生效以来，APP 一直是个人信息保护执法的主要目标。随着 2021 年《个保法》生效，APP 可能会继续成为个人信息保护执法的重点。

如果 APP 违反政府的个人信息保护要求，根据以往的执法案例，它将被列入监管部门发布的执法报告中。这会严重损害 APP 运营商的声誉。如果不合规的 APP 未能在执法机关规定的时间(通常是一周)内进行整改，则该 APP 可能面临被下架的风险，从而对运营商的业务造成更严重的损害。

此外，根据 2021 年《个保法》，严重违反个人信息保护法的行为，包括 APP 的违规行为，可能会被处以巨额罚款(可能是去年营业额的百分比)。

在政府对企业个人信息保护要求日益严苛的当下，合规审查对于降低 APP 不合规的风险非常重要。

(一) 何时开始审查?

APP 运营商应在发布新的 APP、向现有 APP 添加新功能或当 APP 的个人信息处理活动发生重大变化之前进行合规审查。

根据 2021 年《个保法》第 55 条，在处理敏感个人信息、利用个人信息进行自动化决策以及与第三方共享个人信息等情况下，需要 PIA。

由于大多数 APP 都符合上述的收集个人信息的场景，大多数 APP 的发布都需要提前 PIA。审查 APP 的个人信息处理活动的合规性是 PIA 的一部分。即使目前 PIA 还不是法律法规的强制性要求，早期的合规审查仍然是重要的，因为它可能有助于降低 APP 在执法行动中被发现不合规的风险，从而避免运营商声誉受损和 APP 下架的风险。

(二) 谁参与审查?

合规审查应由来自法律、合规、IT 和业务部门的代表组成的团队进行，以确保将业务需求、IT 风险以及法律和合规要求全部考虑在内。外部顾问可能会在重要 APP 发布时参与进来，帮助设定审查基准。

(三) 如何进行审查?

应用程序的合规审查通常分为三步:

- 第一步是了解 APP 的个人信息处理活动，其中包括:
  - 收集、处理、使用和传播的个人信息的类型和数量;
  - 使用个人信息的目的;
  - 个人信息的传输方式；和
  - APP 的设计、功能和业务期望。

- 第二步是将个人信息处理活动与“合规”标准进行比较，来发现一些不足或漏洞。 “合规”的标准主要考虑以下因素:
  - 法定要求;
  - 现有案例所反映的规则；和
  - 行业实践。

- 第三步是构建平衡合规和业务需求的解决方案，解决第二步中发现的不足或漏洞。

如您希望就相关问题进一步交流，请联系:

杨 迅
+86 21 3135 8799
xun.yang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系: **master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野