App 个人信息保护的五大要点

作者：杨迅 | 杨坚琪

针对 App 收集使用个人信息的合规监管一致是网信办、公安部、工信部以及国家计算机病毒应急处理中心等政府部门或者协会整治个人信息收集使用违规行为的前沿阵地。各部门也经常性公布 APP 违反个人信息保护的案例。在此背景下，本文结合正式生效版本的《个人信息保护法》以及此前的不同部门的监管经验，探求 APP 个人信息保护的要点。

要点 1: “知情同意”要求的完善

虽然《个人信息保护法》第 13 条在“知情同意”之外，列举了 6 项无需个人同意即可处理个人信息的正当理由(就此请见我们在***第一篇文章***中的分析)。但对于作为商事主体的一般 App 运营者而言，“知情同意”毫无疑问仍然是最为重要的“合法处理依据”。在《个人信息保护法》出台之前，无论是《民法典》第 1035 条的规定还是《网络安全法》第 41 条的规定，均仅原则性地设定“知情同意”要求，即要求收集个人信息的主体，应当“公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意”。但就规则中应当具体涵盖的内容，上述法律并没有进一步的明确规定：**而《个人信息保护法》则对此进行了直接回应，明确对《隐私政策》应当包含的内容提出了要求(“内容性”要求)**。

根据《个人信息保护法》的规定，如下的内容应当包含在 App 运营者提供的《隐私政策》或《个人信息保护声明》中:

- App 运营者的名称和联系方式
- 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;
- 个人行使本法规定权利的方式和程序;
- 个人信息保护负责人的联系方式(若处理个人信息的数量达到法定要求);
- 其他法律要求公开的内容。

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

实际上，第 17 条的规定并未超出之前颁布的《个人信息安全规范》《App 违法违规收集使用个人信息自评估指南》等非强制性指南的范围。不过过去很多 App 运营者考虑到前述指南的要求并非是强制性要求，因而未能在 App 的《隐私政策》中说明相关的内容(或者**仅选择性地说明相关的内容**)。而在《个人信息保护法》正式将该等内容要求明确列为法律要求后，App 运营者则不再有“借口”，必须确保《隐私政策》或《个人信息保护声明》的内容满足法律要求。

不仅仅是对于内容调整，《个人信息保护法》还对“知情同意”提出了更高的**“操作性”要求**：例如，《个人信息保护法》第 17 条第 3 款要求将“处理规则应当公开，并且便于查阅和保存”。根据上述的法律要求，App 运营者应当在 App 中设置专门的页面以供用户查询相关的处理规则(**这点在实践中大部分 App 已经做到**)，同时应当向用户提供下载方式，以满足“保存”要求。我们理解，后者目前大部分 App 还未实现该等功能。实际上，在《个人信息保护法》之外，现有的《App 违法违规收集使用个人信息行为认定方法》(“**《App 违法违规认定方法》**”)等，亦提出了有关“知情同意”的操作性要求，包括：

- 是否在首次运行时通过弹窗等明显方式提醒用户阅读隐私政策；
- 是否能够实现“4 次点击”即可访问收集使用个人信息规则；
- 是否满足“清晰易懂”“阅读便捷”“中文版本”要求。

我们建议 App 运营者尽快对“内容性”要求和“操作性”要求进行自查，以保证“知情同意”要求的合规。

要点 2：重申正当授权要求

《个人信息保护法》再次重申了授权正当性的要求。无论是工信部主导的“侵害用户权益行为 App 通报”系列，还是网信办主导的“App 违法违规使用个人信息”系列，实际上都对 App 申请权限的正当性提出要求：例如，“**App 强制、频繁、过度索取权限**”作为一种违法行为，几乎每次都会出现在各类通报之中。

在梳理监管经验的《网络安全标准实践指南-移动互联网应用程序(App)系统权限申请指南》中，“一揽子授权”“强迫授权”和“私自调用权限”等行为均已经被监管部门认定为违法违规收集使用个人信息的行为。而《个人信息保护法》在第 5 条提出的“处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过**误导、欺诈、胁迫**等方式处理个人信息”要求，则将 App 运营者的“正当授权”要求上升为法律层面的要求。

考虑到《个人信息保护法》下近乎“严苛”的行政责任，结合 2021 年 4 月发布的《移动互联网应用程序个人信息保护管理暂行规定(征求意见稿)》(“**《App 个人信息保护规定(征)》**”)和《App 违法违规认定方法》中的规定，我们建议 App 运营者应当尽快审核 App 调取权限存在“误导、欺诈、胁迫”的情形，尤其是：

- 是否在调用权限前，明确告知用户权限申请目的；
- 在用户同意前已经默认打开权限的情形；
- 故意欺瞒、掩饰收集使用个人信息的真实目的，向用户调取权限；
- 用户不同意后，仍然频繁征求用户同意；
- 实际打开权限的范围大于声明的权限范围；
- 是否存在“默认勾选”同意的情况；

- 是否根据实际使用情况进行“动态申请”;
- 是否存在版本更新后，自动调整用户设置的权限设置状态的情况;
- 是否要求用户必须一次性打开多个系统权限。

要点 3: “最小必要”要求的再一次明确

《个人信息保护法》对于 App 治理的第 3 个关键要点，则是“最小必要原则”的一再重申，例如:

- 个人信息处理应当具有**明确、合理的目的**，并与处理目的直接相关，采取对**个人信息影响权益最小的方式**(第 6 条)
- 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(第 6 条)
- 除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的**所必要的最短时间**(第 19 条)
- 只有在**具有特定的目的和充分的必要性**，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息(第 28 条)

可以说，《个人信息保护法》从**处理目的、处理方式、收集范围、保存期限**等“四大方面”总结了处理个人信息的“最小必要原则”要求。实际上，上述要求并非是“凭空而来”，而是基于已有的立法和监管实践上总结的经验。例如，就收集个人信息“限于实现处理目的的最小范围”，2021 年 3 月发布的《常见类型移动互联网应用程序必要个人信息范围规定》就对 39 类 App 的基本功能和相应的“必要个人信息”范围作出了规定(当然，不同的 App 仍然应当结合自身的业务类型进行判断)。此外，2021 年 4 月的《App 个人信息保护规定(征)》亦更深入地对 App 的后台处理行为提出了更高的要求: 例如，App 运营者需要审核“处理个人信息的数量、频次和精度是否满足服务所必须”的要求。

如果说“知情同意”还仅仅是对于文本的合规工作提出要求，那么“最小必要”原则如同一条紧箍，“实质性”地规范 App 收集使用个人信息的实践。对于 App 运营者而言，在《个人信息保护法》正式生效之前，**要尽快将个人信息保护工作的中心从前端(文本端)转移到后端(实践端)中来**。

要点 4: 敏感个人信息处理要求

《个人信息保护法》为敏感个人信息的保护设定专章，足见监管部门对于保护该等类型个人信息的重视程度。对于 App 运营者而言，《个人信息保护法》下对于“敏感个人信息”的特别保护，将极大地改变 App 各项功能的提供方式。

《个人信息保护法》继承了《个人信息安全规范(2020 版)》对敏感个人信息范围的界定模式，将其定义为“一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息”，除了通常的“生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息”之外，出于加强对于未成年人信息保护的目的，特别将“14 岁以下未成年人的个人信息”亦列入至“敏感个人信息”的范围之内，将对游戏类 App 和二次元类 App 运营者的业务模式产生极大的影响。

根据《个人信息保护法》的规定，处理敏感个人信息，需要满足如下的要求:

- 处理敏感个人信息必须具有**特定的目的和充分的必要性**，并采取严格的**保护措施**

  "特定目的"与**"充分必要"**则实质性地限制了 App 运营者处理敏感个人信息的能力。以 App 通常会收集"位置"信息举例：通常基于风控的原因，App 运营者可能需要收集用户的位置信息，以结合用户所在的位置判断其从事非正当行为(例如刷单、骗取补贴等)的可能性有多高。但是在《个人信息保护法》生效之后，基于风控的原因是否能够被视为满足"充分的必要性"条件，则值得 App 运营者结合自身的业务模式进行分析。

- 处理敏感个人信息需要征得用户的**单独同意**；且应当向**个人告知处理敏感个人信息的必要性**以及对**个人权益的影响**

  例如，App 运营者会基于人脸识别技术，识别或验证用户的身份。根据《个人信息保护法》的该等要求，从现有的实践来看，我们推荐 App 运营者应当制定提供单独的协议(以说明处理的充分必要性，以及拒绝人脸识别后的影响)，并仅在使用场景需要时，向用户推送该等要求，以此征求用户的"单独同意"。

- 个人信息保护影响评估

  "处理敏感个人信息"是《个人信息保护法》第 55 条要求的进行个人信息保护影响评估的法定事由。因此如果 App 将收集敏感个人信息的，App 运营者应当及时进行评估，并做好相应的"留痕"工作。尤其是考虑到《个人信息保护法》下的"合规审计"要求，以及发生个人信息权益损害纠纷时个人信息处理者的"合规自证"要求，开展个人信息保护影响评估不仅仅是履行法定义务，更是个人信息处理者"合法减责"的必备条件。

要点 5：用户权利的实现机制

《个人信息保护法》一再强调对于个人信息主体权益的保护，并将《民法典》下的"查询、复制、异议、更正和删除"个人信息的权利进一步细化，形成专门的"个人在个人信息处理活动中的权利"一章。一改过去立法的"粗略"，《个人信息保护法》在维护个人信息主体的权益"着墨颇多"，对于 App 运营者设计与用户权利相关的页面将产生重大的影响，例如:

- App 是否落实"查询"机制，使得用户可以了解 App 运营者收集个人信息的范围
- App 是否落实"复制"机制，使得用户可以获取个人信息的副本
- App 是否落实"异议"机制，使用用户可以要求更正和补充
- App 是否落实"可撤回同意"机制，使得用户可以自主关闭权限/限缩收集个人信息的范围
- App 是否存在"个人信息删除"机制(例如注销账户机制)
- App 是否存在"自动化决策"(例如 cookies，个性化推荐等)

考虑到上述的合规要求将对 App 的产品逻辑/UI 界面/推送方式等产生重大的影响，我们建议 App 运营者尽快开展相应的调整，以满足《个人信息保护法》下对个人信息主体权益的高保护要求。

写在结尾的话

随着智能手机登上历史舞台，App 作为移动互联网时代业务的主要载体成就了无数中国创业者的梦想。而随着“数据驱动业务”成为商业潮流，App 违法收集个人信息/数据的情况也日益增多，正是这样的背景促使了《个人信息保护法》出台大量直击 App 运营模式的规定。另一方面，在过去的监管实践中，执法部门往往依据位阶低、效力弱的规定进行执法，使得执法者和执法对象往往对于“合规遵从性”判断上产生分歧，而《个人信息保护法》的出台则将执法尺度上升至法律层面，使得 App 运营者不再能够逃避 App 上的个人信息保护问题：**2021 年 8 月 21 日浙江省通信管理局发布的《关于开展互联网行业市场秩序专项整治行动的通知》中就要求 App 运营者提供“合规整改自查报告”。**监管部门的上述动态则表明，对于 App 运营者而言，App 个人信息保护的合规工作已经不再是一道“选择题”。

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	北京市建国门北大街 8 号 华润大厦 4 楼 T: +86 10 8519 2266 F: +86 10 8519 2929	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