CAICT 中国信通院

移动应用（App）
数据安全与个人信息保护
白皮书
（2019 年）

中国信息通信研究院

安全研究所

2019年12月

（二）政府层面，创新数据安全防护技术手段

一是鼓励企业开放普惠行业的 App 数据安全检测技术能力。鼓励第三方机构固化 App 数据安全及个人信息保护检测流程、规范，开放相关检测工具平台，提升 App 运营者自主发现、主动整改数据安全风险的能力。**二是形成 App 数据安全防护产品集群目录。**联合高校、科研院所和企业等多方力量，合力推进数据资产盘查、数据特征值提取、数据加密、数据匿名化、数据血缘追踪以及数据防泄漏等重点数据安全技术的研究，形成 App 数据安全防护产品集群目录，通过应用试点加速技术成果转化，促进 App 数据安全先进技术创新和产品服务应用推广。**三是推动企业提升 App 数据安全与个人信息保护技术水平。**指导企业加大 App 数据安全技术投入，加快部署网络数据和用户个人信息防窃密、防篡改、防泄漏和数据备份等安全防护措施，提升企业 App 数据安全保障能力。

（三）企业层面，切实落实数据安全主体责任

一是 App 运营者要积极开展数据安全与个人信息保护自评估工作。App 运营者作为责任主体，应建立企业内部的数据安全与个人信息保护机制，严格履行法律法规规定的责任义务，同时依照相关标准，对 App 数据安全与个人信息保护情况进行自评估，积极防范安全隐患。**二是应用商店等平台企业应加强应用上架前数据安全审核。**应用商店等分发平台企业应按照相关制度要求，落实平台管理责任，依托现有应用上架前审核机制，将 App 数据安全与个人信息保护措施作为重点审核内容，对违法违规 App 不予上架。**三是移动智能终端企业应**

严格落实应用软件预置管理要求。移动智能终端企业应按照相关标准，对预置应用软件开展安全评估分级评测，达到相应等级的 App 可通过代码签名的方式进行标识，并拒绝与不符合规范要求的软件提供商合作。严格落实向用户公示预置应用软件相关信息的要求，重点明示应用软件安装及运行所需权限列表，收集、使用用户个人信息的内容、目的、方式和范围等。

（四）行业层面，构建数据安全多方治理生态

一是推动行业组织制定行为准则和指引，提升行业自律水平。依托现有互联网行业自律组织，推动各利益相关方共同制定个人信息收集使用行为准则，签订行业自律公约，对 App 运营者和应用商店进行评估检测和认证，推广宣传企业最佳实践，提升行业整体水平。**二是加大用户宣传教育力度，提升用户防护能力。**用户作为 App 的使用主体，行业组织应着力通过展览、论坛、制作用户安全手册等多种形式，向用户普及安全下载方式、隐私政策阅读要点、索取权限必要性等个人信息安全保护知识，提升用户自身安全防护意识和能力。三**是加强与媒体、社会公众的沟通交流，弥合认知鸿沟。**针对目前少数媒体和公众对于企业业务模式中个人信息收集使用方式和隐私政策存在的误读和误解，包括对隐私条款中的术语、技术处理操作和行业惯例等不理解的情况，应通过普法、普及网络知识等形式对公众进行解读和宣导，积极探索与媒体和公众的对话机制，弥合专业知识和公众认知之间的鸿沟，消除信息不对称导致的隐私焦虑。

五、 移动应用（App）用户安全使用建议

App 个人信息安全事件不断牵动公众神经，用户隐私意识逐渐觉醒。与此同时，大部分用户自身个人信息保护意识和能力仍然不足。因此，除了从管理视角出发对 App 数据安全治理建言献策，报告团队还从用户视角出发，围绕敏感权限索取、隐私政策、用户注销渠道等用户关注热点，梳理出用户安全使用 App 的技巧，提升用户个人信息安全保护能力。

（一） 用户授予敏感权限应谨慎

一是下载安装 App 时认真阅读权限提醒，谨慎开启权限。经检测发现，不同类别 App 所申请的敏感权限存在趋同性，反映出部分 App 存在过度索取的倾向。写入及读取外置存储器、读取电话状态（设备 IMSI/IMEI 号）、拍摄、访问粗略定位、访问精准定位、录音、读取通讯录、拨打电话等是 App 常见所申请的收集使用个人信息权限。用户需关注相关权限是否为使用该 App 所必需的权限，下载安装 App 时认真阅读权限提醒，谨慎开启权限，特别是录音、读取通讯录、访问位置等较容易直接泄露个人敏感信息的权限。

二是使用 App 特定功能时再打开相关权限，不使用时及时关闭。经检测发现，为方便及尽可能多地申请权限，App 运营者通常在用户首次打开 App 时即会申请包括核心功能和附加功能所需的所有权限，而非仅在用户需使用相关功能时进行申请。如外卖餐饮类 App 可能会申请录音权限，该权限仅在用户不方便发送文字而使用语音输入转化文字功能与外卖员进行沟通时使用，若首次打开时就申请该权限，可

能涉嫌过度索权。用户应尽可能在未使用特定功能时关闭相关权限，最大可能保障个人信息安全。

三是对于不影响 App 使用的权限，拒绝申请并点击“不再询问”。App 运营者常以频繁申请的方式获取用户敏感权限。用户拒绝授权后，仍会在每次打开时或定时弹窗申请敏感权限，用户往往不堪其扰而同意授权，但这些敏感权限常常是非必要权限。建议用户时刻警惕，不要因为麻烦而给予多余的授权，如果认为该权限与目前使用的功能无直接关联，可先拒绝，并视后续情况决定是否授权。

（二）用户阅读隐私政策宜仔细

一是首先阅读正文中以加粗、下划线的形式突出显示的重点内容。隐私政策的文字冗长且繁琐，用户往往没有耐心打开或完全阅读。但隐私政策中需要特别关注的部分一般会重点显示，例如收集哪些个人敏感信息、如何使用敏感信息等。用户阅读后，可将功能模块与个人敏感信息对应起来，进而判断运营者收集这些个人敏感信息是否必要。一般而言，用户重点阅读这部分内容便可大致了解该 App 收集使用其个人信息的基本情况，以提升阅读隐私政策的效率。

二是重点关注与第三方进行个人信息共享的情况。与第三方共享是用户个人信息脱离原有 App 运营者管理向第三方流转的关键环节，可能陷入原 App 运营者不管、第三方接收者不顾的灰色地带，存在较大的个人信息泄露或滥用的风险。用户可通过这部分内容重点判断其个人信息的流向，并确认其流向是否合理、必要。

三是重点查看隐私政策中赋予的用户权利。重点包括撤回同意的

方法，拒绝接受定向推送信息，停止、退出、关闭相应功能的机制，删除更正个人信息的渠道等。通过这些用户权利，用户可进一步明确自身在个人信息保护中的角色及价值，了解自身享有的权利，从而在必要的时候行使相应权利，有效保护其个人信息。

（三）用户注销个人账号需灵活

一是首先通过隐私政策内的注销渠道了解如何进行账户注销。隐私政策中一般会说明用户的注销渠道，比如主动选择注销、联系人工客服注销等，这是直接指导用户进行账号注销的官方说明，实施起来直接有效。

二是若隐私政策中未详细说明注销渠道，用户可通过一些规律自行查找渠道。一般而言，注销功能多存在于App“我的”“设置”“账号与安全”“安全中心”“客户服务”等栏目内，如果仍未发现，还可联系人工客服进行账号注销。因大部分 App 尚未实现注销处理进度查询功能，用户需在 App 注销模块内或通过询问人工客服确认注销生效时间，并在到期后进一步确认自己的账号状态。

三是使用注销功能需判断相关条件是否合理。App 用户账号注销需要用户账号处于特定状态，比如账号安全、交易结算完毕、解除特定管理员身份、与其他 App 账号或授权登录解绑、不存在进行中的业务、不存在账号纠纷等，这些条件基本是合理的。但是部分 App 会设置过多不合理注销条件，例如用户当时仅用手机号注册，注销时 App 却以验明身份等理由索要用户身份证号、地址、照片等额外的个人敏感信息，用户应予以拒绝。

中国信息通信研究院

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62304839

传真：010-62304980

网址：www.caict.ac.cn