App 违法违规收集使用个人信息
监测分析报告

国家计算机网络应急技术处理协调中心

中国网络空间安全协会

2021 年 12 月

App 违法违规收集使用个人信息
监测分析报告

2021 年，国家计算机网络应急技术处理协调中心会同中国网络空间安全协会，发挥网络安全技术力量优势和行业组织特点，有力支撑国家 App 个人信息保护工作。近期，根据 App 违法违规收集使用个人信息技术监测和举报受理数据，对我国 App 收集使用个人信息情况进行了态势分析，具体如下:

一、App 收集使用个人信息总体状况

目前全国主流安卓应用商店在架 App 去重后总数为 112 万款。**从运营者地域分布方面看**，App 运营者主要分布在广东、北京、上海等信息产业发达的地区，占到了总数的一半以上（52.8%），中西部省份分布较少，不足总数的四分之一（21.8%）。**从应用类型分布方面看**，数量最多的三类为网络游戏类（24.0%）、本地生活类（14.6%）、实用工具类（12.4%），大部分类型应用数量较少，全部 39 类常见类型应用中有 21 类应用数量占比不到 1%。**从下载量分布方面看**，下载量在亿级、千万级、百万级的分别有 1127 款（占比 0.1%）、5317 款（占比 0.5%）、1.9 万款（占比 1.7%），其余下载量不到百万的 App 占比 97.7%。

（一）个人信息保护法律法规体系日趋完善，App 违法违规收集使用个人信息治理取得阶段性成果

2021 年 11 月 1 日起,《个人信息保护法》正式颁布实施，标志着我国个人信息保护立法体系进入新的阶段。《个人信息保护法》的出台为个人信息权益保护、信息处理者的义务以及主管机关的职权范围提供了全面的、体系化的法律依据，涵盖个人信息收集、存储、使用、加工、传输、提供、公开、删除等多个环节以及自动化决策、个人信息跨境提供等特定场景，与《民法典》《网络安全法》《数据安全法》等共同构成了我国个人信息保护的法律框架。此外，多项个人信息保护相关法规面向社会公众发布或公开征求意见，我国个人信息保护领域法律法规体系日趋完善。5 月，国家网信办等四部委联合制定的《常见类型移动互联网应用程序必要个人信息范围规定》正式实施，明确 App 不得强制收集非必要个人信息。11 月,国家网信办会同相关部门研究起草的《网络数据安全管理条例》公开征求意见，其中“个人信息保护”章节详细规定了知情同意、最小必要、权利保障、生物特征信息等方面的要求，并明确提出处理一百万人以上个人信息应视为重要数据处理者进行管理。

今年以来，国家网信办持续开展 App 违法违规收集使用个人信息专项治理工作，加大执法监管力度，组织对 39 种常见类型公众大量使用的 1425 款 App 开展了专项检测，已对其中存在严重违法违规问题的 351 款 App 进行了公开通

报，责令限期整改；对未在规定时限内整改的依法采取了相关处罚措施。国家计算机网络应急技术处理协调中心积极运用大数据等新技术手段，建设 App 收集使用个人信息监测平台，实现对国内主流应用商店在架 App 存在的“不给权限不让用、频繁索权干扰用户、启动就索要无关权限、未经用户同意收集个人信息”等 16 项典型违法违规问题的全量快速检测。专项治理有力震慑了违法违规行为，大大提高了 App 运营者对个人信息保护工作的重视程度，取得了良好的治理效果和社会反响。

（二）强制收集非必要个人信息问题明显减少，启动弹窗索要无关权限问题多发

App 打开后强制要求收集个人信息是用户普遍反感的违规行为之一。《常见类型移动互联网应用程序必要个人信息范围规定》明确“App 不得因用户不同意收集非必要个人信息，而拒绝用户使用 App 基本功能服务”。今年以来，App 强制要求用户打开非必要权限、强制要求用户填写非必要个人信息等典型违规行为明显减少，目前检测发现仅有 1%的中小应用残留此问题。然而，很多 App 尽管不再强制收集，仍在首次启动就弹窗索要多个无关权限，用户对此较为反感，由此产生的投诉举报比较集中。目前很多“量大面广”应用已认识到此问题，将启动索要权限改为用户触发特定功能时再索要对应权限，改善了用户体验，如“微信”、“51 Job”等头部应用最新版本启动均不索要存储、设备等无关权限。

但监测显示，在华为、小米、VIVO、OPPO、腾讯应用宝等主流应用商店近三个月新上架应用中，平均每月有近 1000 款存在此问题的应用上架。

（三）超范围收集个人信息行为治理成效初显，但“七类”隐蔽问题仍需紧盯不放

部分 App 出于精准用户画像、推广营销等商业目的，想方设法超出实现功能的必要范围收集更多个人信息。对此，《个人信息保护法》明确规定“处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式，收集个人信息应当限于实现处理目的的最小范围”。

深入技术分析发现，App 超范围收集个人信息的问题目前主要包括七种情形：**一是敏感权限声明超出必要范围。**少量 App 在未提供实际功能的情况下，仍然声明了相关敏感权限，存在热更新后调用和 SDK（软件开发工具包）调用权限的风险。**二是权限索取超出必要范围。**一些 App 超出当前功能需要索取权限，例如某应用的电话拦截功能索要了短信、存储、通讯录等 7 项敏感权限，整改后只保留了功能实现所必需的 3 项敏感权限。**三是收集数据的敏感性超出必要范围。**一些 App 在使用低敏感性数据即可实现功能的情况下，仍然收集高敏感性数据。例如，普通的天气查询功能只需要城市或地区级的粗略位置信息，不应索要精准位置等敏感个人信息。**四是收集数据的具体内容超出必要范围。**一些 App 在仅

需部分数据内容即可实现功能的情况下，却实际收集了全部内容。例如，查找好友功能只需匿名化后的手机号码即可实现功能，不应超范围收集通讯录联系人的姓名、邮箱、地址等内容。**五是收集方式超出必要范围。**App 收集个人信息的方式包括单次读取、本地存储、上传云端等，对个人的影响程度依次递增，应在满足功能需求前提下选择影响程度最低的收集方式。例如，只需单次读取或本地存储即可实现功能，不应默认使用上传云端。**六是收集频率超出必要范围。**有的 App 收集每项个人信息的频率明显超出当前功能的必要范围，例如，某运动健身类应用在用户观看视频等无关功能时，每分钟获取位置信息近百次，明显超出必要范围。**七是收集场景超出必要范围。**很多 App 除了在功能必需的合理场景收集信息，还在启动、自启动、后台运行、使用不相关功能等其它场景收集信息，违反了必要原则。例如，某应用除了在共享位置时收集位置信息，还在扫码支付等不相关功能收集位置信息，可用于用户消费行为画像分析，近期已自行整改。

今年国家网信办已通报地图导航、输入法、安全管理、短视频等多类头部应用，针对“七类”超范围收集行为进行了重点整治，包括超范围收集用户通讯录、精确地理位置、短信、通话记录等在内的一大批与人民群众切身利益相关的违法违规问题得到治理。

（四）中小应用“知情同意”问题较多，集中表现为同意前收集、频繁索权等违规行为

知情同意是处理个人信息的基本前提条件之一。《个人信息保护法》进一步细化了“基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出”等要求。根据国家网信办等四部委发布的《App 违法违规收集使用个人信息行为认定方法》，目前常见违反知情同意要求的问题集中表现为以下四类:

一是征得用户同意前收集个人信息。监测发现，2 万中小应用样本在同意隐私政策前将用户安卓 ID 等信息上传至云端服务器，4.4 万中小应用样本没有向用户提供明确的隐私政策拒绝选项。**二是用户拒绝后频繁征求用户同意、干扰用户正常使用。**13 万存量中小应用样本在用户明确拒绝授权后，仍然在使用过程中频繁索取权限，或者用户下次进入应用再次索取权限；且人工抽验显示，在近三个月新上架应用中仍普遍存在频繁索权的问题。**三是诱导用户同意收集个人信息。**例如，以签到、福利等为理由诱导用户提供姓名、手机号、住址，以“绝不收集隐私信息”等欺骗性提示诱导用户安装使用 App 等。**四是个人信息进行定向推送但无法关闭。**有 27 万个应用样本声明会利用个人信息进行定向推送，但人工抽验发现，除了新闻资讯、网络直播、短视频等部分类别外，大多未提供关闭定向推送的选项。此外，部分 App 尽管提供了关闭选项，但还存在为关闭选项强制设定了几个月的有效期，到期后自动恢复定向推送，关闭选项极其隐蔽，普通用户难以发现，关闭定向推送后并不生效等问题。

（五）移动应用无隐私政策问题持续向好，存量问题应用仍需下架清理

隐私政策是用户了解应用处理个人信息目的、规则、方式、范围等信息的重要途径，也是《个人信息保护法》告知同意要求中，最主要的告知手段。监测发现，App 无隐私政策问题呈现下降趋势，问题占比由 2019 年最高的 26%，下降为今年的 6.7%。平台企业公开收集使用规则的意识显著增强，小米、华为等头部应用商店今年已加强无隐私政策问题应用的审核力度，近三个月新上架应用程序此问题已基本清零，并对存在该问题的 8.1 万个存量应用进行了下架处理。但部分中小应用商店审核机制尚未健全，仍有 7.8 万款存量问题需进行下架清理。

（六）明示收集使用个人信息行为日趋重视，未明示敏感数据收集与“一揽子”同意问题突出

《个人信息保护法》规定，在处理个人信息前应当真实、准确、完整地向个人告知收集使用个人信息的目的、方式、范围等内容，从而充分保证用户的知情权。

在敏感数据明示收集方面，监测发现 60.7%的应用收集了安卓 ID 等设备唯一标识信息，55.4%的应用收集了应用列表信息，13.7%的应用收集了剪切板信息，此类信息可用于人物画像、个性化推送等业务，敏感程度较高，App 应向用户明示并取得授权。目前，小米、VIVO 等手机终端企业已开始加强保护措施，将应用列表、剪切板等信息作为敏感权

限进行管控。

在隐私政策明示说明方面，监测数据与人工抽验结果显示，隐私政策存在隐瞒个人信息收集行为、“一揽子”同意等违规问题较为突出。**一是隐瞒敏感个人信息收集行为，**例如，电话、短信拦截功能涉及通话记录和短信等高度敏感权限，隐私政策应清晰告知是否收集用户主叫通话记录和全部短信内容等敏感内容。**二是隐瞒个人信息对外共享行为**，例如，面部特效、私信、客服等功能利用第三方 SDK 实现的，应清晰告知可能将用户人脸信息、私信内容、客服记录等共享至第三方。**三是要求“一揽子”同意隐私政策全部条款甚至不合理条款**，例如，用户未开启个性化推送时，不应要求其同意“要收集设备信息、位置信息、访问记录并共享至第三方进行个性化推送”等条款。目前，头部应用开始重视隐私政策相关问题，部分应用已着手加强收集个人信息和第三方共享个人信息情况的详细告知工作。

（七）SDK 收集行为普遍存在，处理活动需规范和整治

监测数据表明，一款 App 平均嵌入 10 款以上 SDK，通过 SDK 实现认证登录、消息推送、访问统计等功能，一些自主开发水平较低的中小应用甚至主要功能也完全依靠 SDK 实现。在监测中发现，第三方 SDK 收集行为不规范引发的 App 违规问题日益凸显。**一是同类型中各款 SDK 收集个人信息范围差异较大。**SDK 主要可分为 16 大类，分析发现同类型 SDK 中，各款 SDK 收集的个人信息范围存在较大

差异，缺乏统一标准。例如，目前常见的一键登录 SDK，实现功能相同，但有的收集 IMSI、WIFI 网络信息，有的获取系统设置项等信息，有的则需要 WLAN 状态等权限，App 想要兼容多个登录入口就必须声明获取上述全部信息，增加了 App 过度收集个人信息的风险。**二是 SDK 的权限调用和声明行为不规范。**目前，手机操作系统并未提供单独的 SDK 权限管理机制，而是由 SDK 直接调用 App 的已有权限，部分 SDK 借此强制要求 App 捆绑声明权限，或者调用 App 权限过度收集个人信息。例如，用户为了使用 App“附近”功能授权 App 调用位置权限，技术分析发现，App 内嵌入的广告类、用户画像类等 SDK 也趁机调用位置权限。对于此问题，部分头部企业已开始重视 SDK 权限的管理，增加了 SDK 控制中间件等技术手段，用于管控各类 SDK 对系统权限的滥用。

（八）账号注销功能基本具备，设置不合理条件等违规情形仍需重视

按照《个人信息保护法》第十五条要求，“基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。”监测发现，目前多数 App 已经提供了账号注销功能，但实际使用过程中发现其中不少 App 设置了不合理条件和障碍，导致注销困难。例如，抽样检测发现约 9.7%的 App 存在不同程度的注销困难问题，包括：捆绑注销问题，即申请注销时强制要求将用户在同一运

营者旗下的所有 App 账号全部注销；注销时过度索要个人信息问题，即申请注销时，要求用户提交在注册和正常使用 App 时都未涉及的额外个人信息，否则不予注销；注销周期过长问题，即账号注销响应时间超过《App 违法违规收集使用个人信息行为认定方法》等规定的 15 日期限。

（九）举报受理与宣传教育齐头并进，有效发挥社会监督作用

国家网信办指导中国网络空间安全协会设立 App 违法违规收集使用个人信息行为投诉举报受理平台，及时接收处理群众问题反映。今年以来，已通过微信公众号、邮件等渠道，累计受理个人信息保护投诉举报超过 2 万条，是 2020 年度的两倍以上，涉及 2000 余款 App，其中超范围收集个人信息、强制或频繁索要权限、无法注销账号等问题最为突出，占总举报量的 40%左右。对用户举报的线索、反映的违法违规收集使用个人信息问题进行核验，对实名举报信息逐一沟通核实，及时反馈受理、处理情况。

同时，积极开展科普宣传，通过微信公众号等渠道发布与个人信息保护相关的政策法律法规解读、违规案例、专家解读、知识科普等文章，组织业内专家撰写了《全球个人信息保护报告》《个人信息保护通识读本》等一系列面向各种受众群体的专业论著，及时向公众传递个人信息保护理念，传授个人信息保护知识，提升公众个人信息保护意识与能

力，有效发挥社会监督作用。

二、工作建议

（一）鼓励符合个人信息保护法 App 加强示范应用

现有法律法规和标准规范已提出了较为系统全面的 App 个人信息保护要求。广大 App 运营者应加强自身个人信息保护能力建设，紧密围绕个人信息保护要求，加强研发与应用衔接，积极推出符合个人信息保护法的优秀解决方案，形成示范效应，带动提升 App 个人信息保护整体水平。

（二）持续开展违法违规收集使用个人信息专项治理

随着专项治理工作的开展，App 违法违规收集使用个人信息的技术手段也逐渐升级，隐蔽性不断增强。为持续巩固治理成效，需跟踪 App 违规收集个人信息新技术新手段，围绕隐蔽超范围收集等重点问题，持续提升违法违规活动检测监测、分析取证能力，持续开展 39 类常见类型“量大面广”应用收集使用个人信息专项治理工作，“点面结合”保持对违法违规行为高压态势。

（三）发挥 App 生态关键环节审核把关作用

目前应用商店中超过 95%是下载量不到 100 万的中小应用，虽然每款应用的用户不多，但“长尾效应”累计的用户量仍然较大，而这些中小应用的个人信息保护水平参差不齐，安全隐患较为突出。面对海量中小应用，应用商店、移动智能终端等 App 生态关键环节应充分发挥平台作用，加强应用上架审核、存量应用清理、预装应用审核，完善终端个

人信息保护功能，筑牢用户个人信息安全防线。

（四）加强个人信息保护标准规范体系建设

针对互联网平台及产品服务隐私协议要求、移动智能终端个人信息保护、应用商店 App 个人信息处理规范审核、移动互联网应用程序 SDK 安全指南、利用个人信息自动化决策规范等重点热点领域，加快研究制定相关标准规范，指导 App 运营者提升个人信息保护能力。

（五）完善个人信息保护投诉举报渠道

持续优化完善投诉举报渠道、平台，加强举报投诉受理、分拣、核验、反馈等方面的能力建设，面向社会、企业发布个人信息保护工作满意度、重点痛点问题反馈等方面的调查问卷，广泛听取各方意见，不断提升投诉举报受理处理工作水平。

（六）加大个人信息保护宣传教育力度

加强个人信息保护宣传教育，面向互联网平台、App 运营者、电信运营商、应用商店、移动智能终端设备制造者开展个人信息保护法、数据安全法等互联网法律法规的专题培训，推动上述主体将依法经营、合规管理嵌入业务工作流程全流程、各环节，面向社会公众普及宣传个人信息保护常识，推动个人信息保护法的各项要求和规定在社会生活中得到全面贯彻和实施。

（七）推进个人信息保护行业自律

组织互联网平台、应用商店、智能终端、运营商等主体

起草签署《个人信息保护行业自律公约》，在个人信息处理规范、个人信息安全保障等方面提出落实个人信息保护法的具体要求和倡议，推动行业组织、科研机构、企业、个人等共同参与个人信息保护工作，形成全社会共同维护个人信息安全的良好环境。研究“个人信息保护风险指数”，为网民安全下载使用 App 提供支撑。

附件：

App 违法违规收集使用个人信息监测数据分析

（一）App 基本情况

目前全国主流安卓应用商店在架 App 去重后总数为 112 万款。按照所属地域来看，App 运营者主要分布在信息产业发达地区，排名前三的分别是广东、北京和上海，占比分别是 25.58%、16.98%和 10.22%，如图 1 所示。

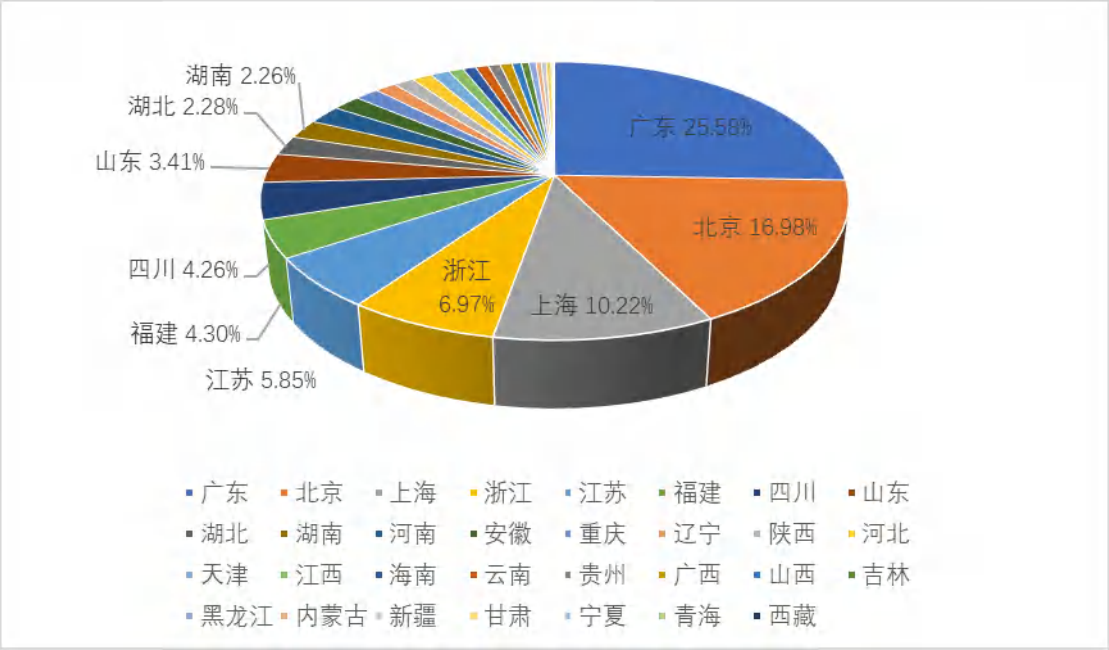

图 1 全国各省 App 运营者分布情况

（二）启动弹窗索要多个无关权限问题情况

主流应用商店 App 启动弹窗索要多个无关权限问题分布情况如图 2 所示。其中，历趣应用市场、西西软件园和绿色资源网数量最多，分别是 2.4 万、2.2 万和 1.7 万。

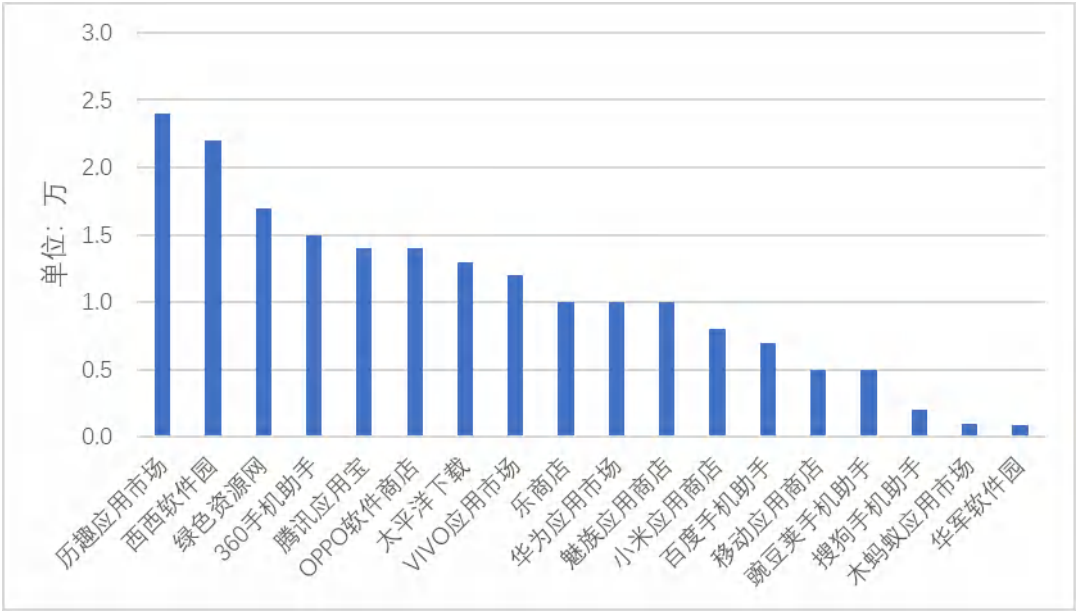

图 2 主流应用商店 App 启动弹窗索要无关权限问题分布情况

（三）超范围收集个人信息问题情况

今年五月以来，国家网信办累计通报的 12 类 351 款 App 中，有 257 款存在“违反必要原则，收集与其提供的服务无关的个人信息”相关问题，具体情况如图 3 所示。其中，网络借贷类、网络直播类和安全管理类存在此类问题的 App 数量最多。

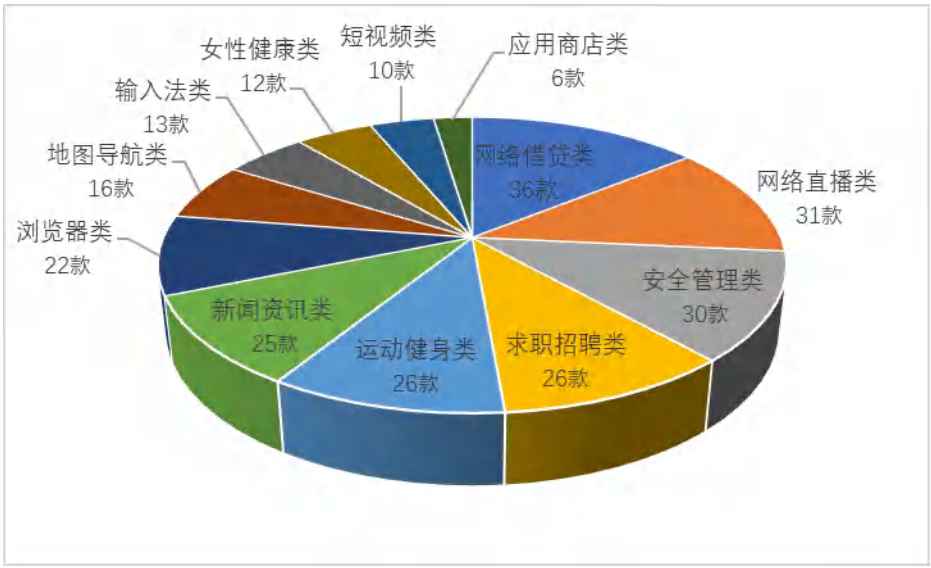

图 3 已通报类别 App 超范围收集情况

（四）强制收集个人信息问题情况

应用强制用户授予非必要权限或同意收集非必要个人信息，否则无法使用基本功能。主流应用商店 App 强制收集个人信息问题分布情况如图 4 所示。

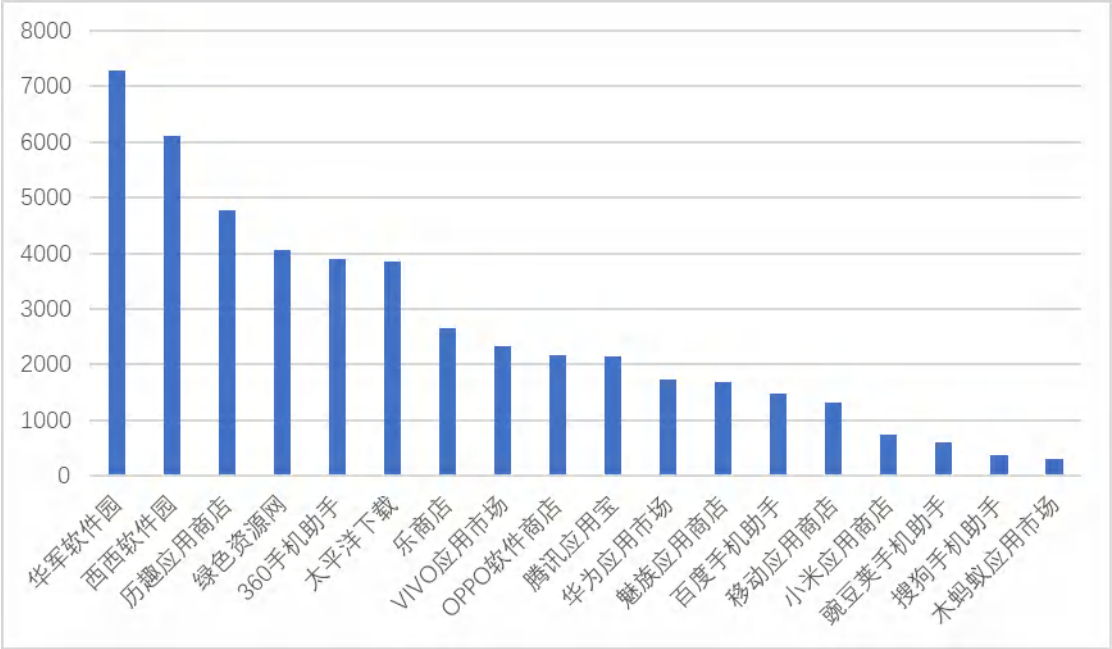

图 4 主流应用商店 App 强制收集个人信息问题分布情况

（五）违反“知情同意”要求问题情况

1.频繁索权问题情况

应用使用过程中频繁索要无关权限，严重干扰用户使用。主流应用商店 App 在用户使用过程中频繁索权问题分布情况如图 5 所示。其中，西西软件园排名第一，绿色资源网和历趣应用商店排名第二和第三。

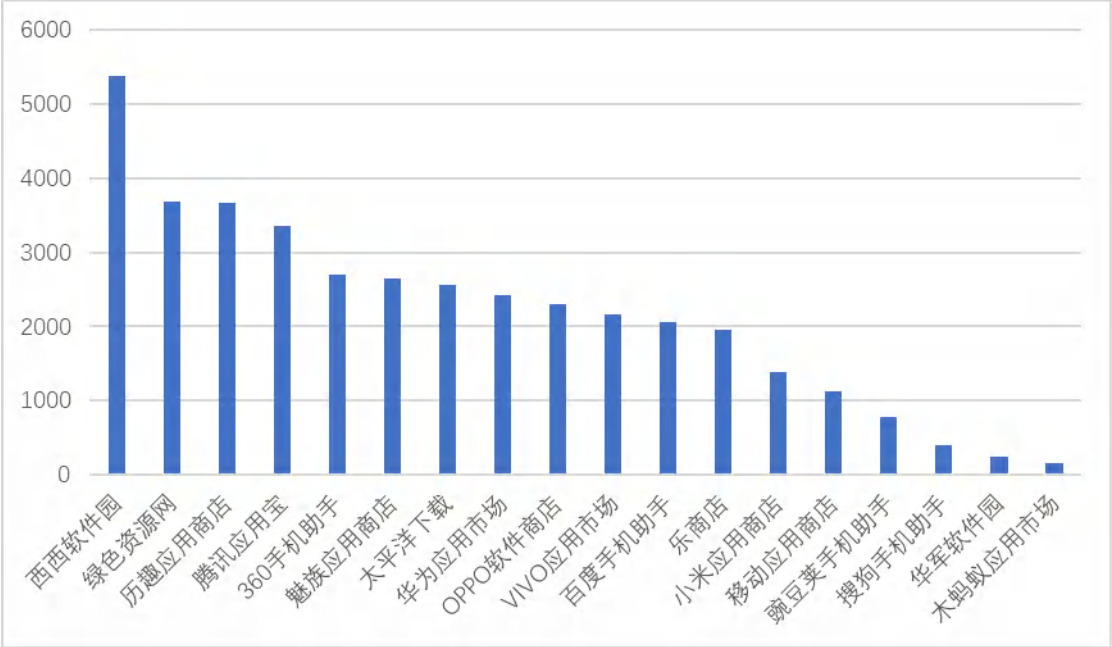

图 5 主流应用商店 App 使用过程中频繁索权问题分布情况

部分 App 只要用户不开启权限，每次重启就会反复索要，直到用户不堪打扰而开启权限。主流应用商店应用重启后频繁索权问题分布情况如图 6 所示。

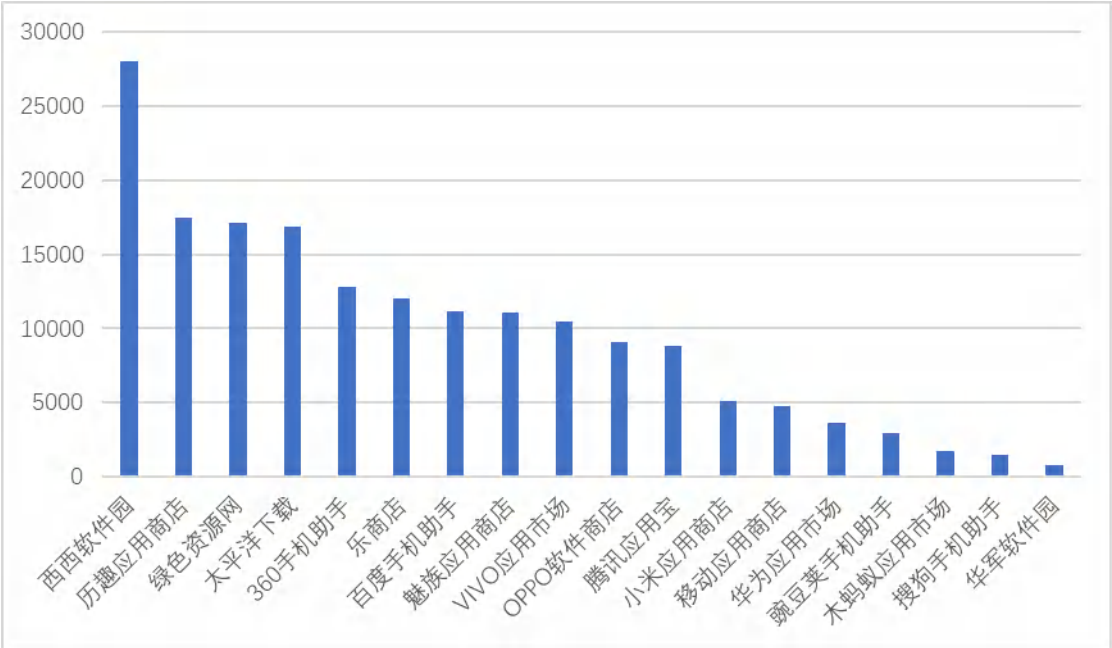

图 6 主流应用商店 App 重启频繁索权问题分布情况

2.同意隐私政策前收集个人信息问题分布情况

部分应用同意隐私政策前会上传 Android ID、设备序列

号等个人信息到云端服务器。主流应用商店该问题分布情况如图 7 所示。

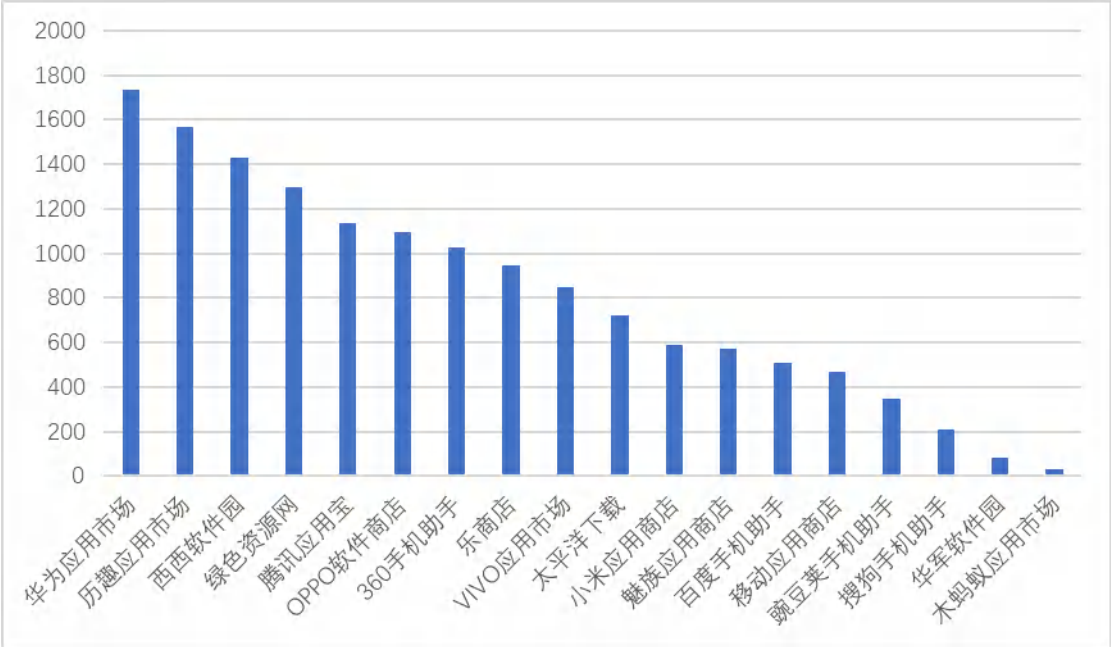

图 7 主流应用商店 App 同意隐私政策前收集个人信息问题分布情况

3.无法关闭定推问题类型分布情况

无法关闭定推问题主要体现在以下几方面，如图 8 所示：一是利用个人信息进行定向推送，但应用内未提供关闭选项，该类问题占比超过六成；二是关闭定推只能关闭有限期限，例如 3 个月之后自动恢复开启状态，无法彻底关闭；三是关闭定推按钮比较隐蔽，例如隐藏在隐私政策中，普通用户很难快速发现关闭按钮；四是关闭定推无法立即生效，例如有的应用声称在用户关闭 48 小时后才能生效；五是用户未注册登录（仅浏览）时就有定推内容，但关闭定推需强制用户先注册登录，否则无法完成操作。

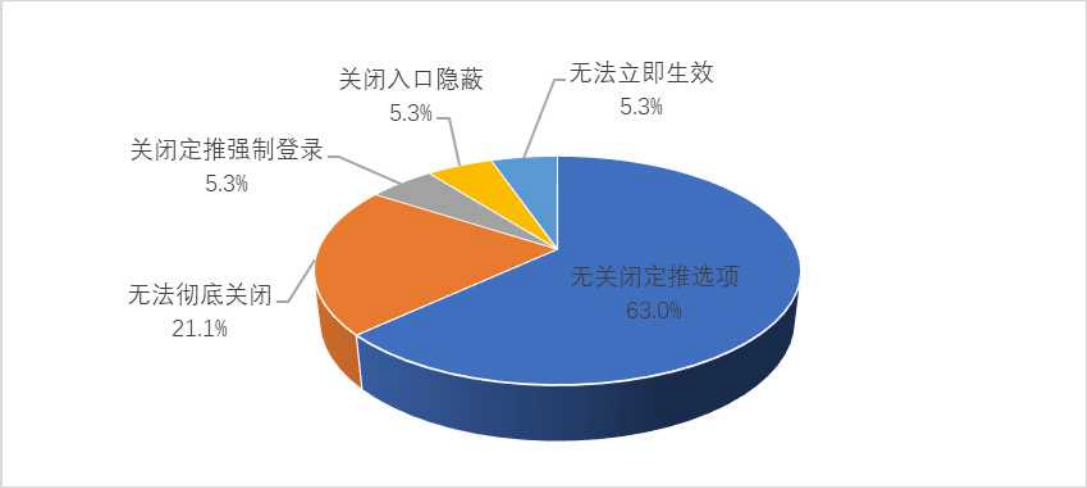

图 8 关闭定推各类型问题分布情况

（六）应用商店在架 App 隐私政策违规情况

主流应用商店在架 App 无隐私政策或隐私政策难以访问等问题分布情况如图 9 所示。其中，360 手机助手、太平洋下载、西西软件园该问题应用数量较多。

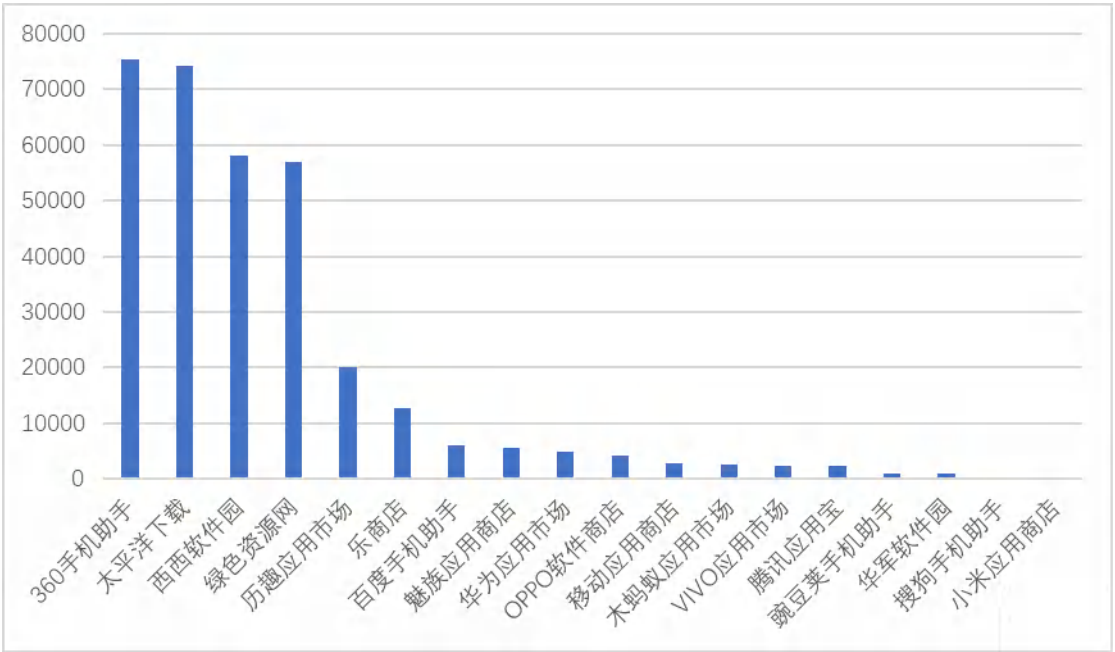

图 9 主流应用商店 App 无隐私政策、隐私政策难访问问题分布情况

（七）App 个人信息保护举报投诉受理情况

中国网络空间安全协会近三年来受理的个人信息保护投诉举报事件逐年攀升，2019 年、2020 年、2021 年 1 至 10

月分别受理各类投诉举报事件 3000 条、7800 条和 20000 余条。其中，超范围收集无关个人信息、强制或频繁索要无关权限、无法注销账号等问题数量较多，如图 10 所示。

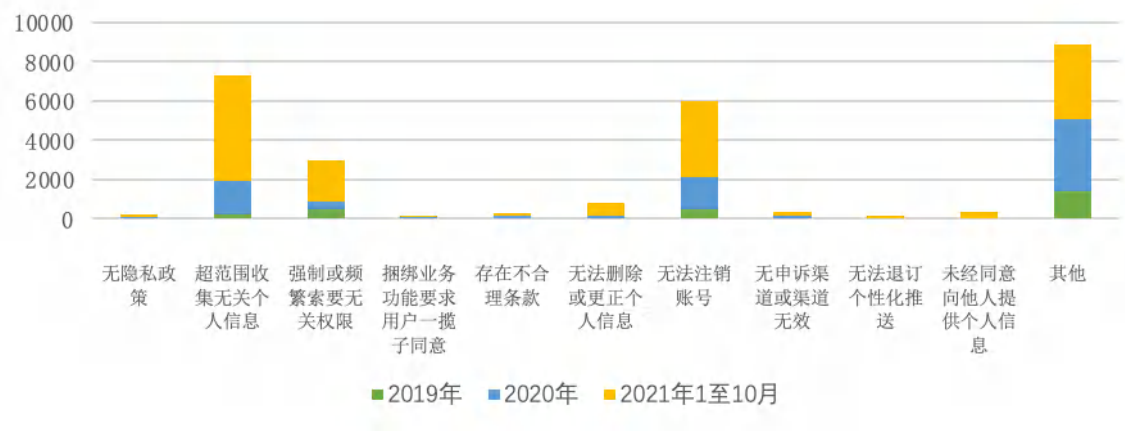

图 10　App 个人信息保护举报投诉受理情况