CAICT 中国信通院

南都个人信息安全研究中心

小程序个人信息保护研究报告

（2020 年）

中国信息通信研究院安全研究所·南都个人信息保护研究中心

2020 年 6 月

版权声明

编写团队

编写单位：

中国信息通信研究院安全研究所

南都个人信息保护研究中心

编写组成员：（按姓氏笔画排序）

尤一炜、石莹、闫希敏、张则阳、张媛媛、彭志艺、蒋琳、魏薇

前　言

随着移动互联网的进一步发展，“超级 App+小程序”成为移动互联网时代开发者探索的新模式。以微信、支付宝等移动应用程序（以下简称“App”）为代表的平台在其应用中搭载第三方小程序，丰富向用户提供服务的形式和内容。2020 年新冠肺炎疫情以来，小程序也成为政府机关、医疗机构、企事业单位、社区学校疫情防控的重要工具，进一步推动其快速发展。

目前，小程序作为常用互联网服务入口，已全面渗透用户生活，成为数字化时代不可或缺的一部分。小程序在汇聚大量用户个人信息的同时也暴露一些在用户个人信息收集与使用方面的风险隐患。本报告在研判小程序发展趋势和社会经济影响的基础上，系统梳理总结小程序与 App 以及小程序平台的关系，并通过个人信息安全评测，重点分析目前主流小程序存在的个人信息安全风险隐患，最后从政府、企业、用户三方面研究提出小程序个人信息保护的对策建议。

目 录

一、 研究背景

（一）小程序定义及特点

近年来，受用户红利趋减、市场规模趋于饱和等影响，我国移动互联网用户增速在2019年2月已降至5%以下，2019年2月较2018年12月仅增长700万用户[1]，基于存量市场的流量竞争形势愈发严峻。相较拥有庞大流量的“超级App”，新App的发展情况更加不容乐观，就开发者而言，新App开发推广成本高、周期长、市场生存空间小；就用户而言，大量新App使用流量多、占用手机内存高、学习门槛高。为提升流量资源的分发效率，满足用户多样化需求，进一步挖掘用户价值，“超级App+小程序”成为移动互联网时代开发者探索的新模式。以微信、支付宝等移动互联网应用为代表的平台，开始在其应用中搭载第三方小程序，丰富向用户提供服务的形式和内容。小程序通常具备信息收集、资讯浏览、线上交易等功能，搭载于可承载轻型应用运行、具备流量分发功能、拥有庞大用户量的“超级App”平台（以下简称“小程序平台”或“平台”），利用平台的技术优势和流量资源，在生活服务、政务公益、网络购物、旅游交通等领域提供便捷化服务。

小程序具备以下主要特点：一是功能简单。出于对小程序启动、加载速度的考虑，小程序平台严格限制小程序代码包大小，促使小程序业务逻辑简单，更加关注核心业务、主要功能的实现。二是使用便捷。用户通过搜索、点击、授权即可进入小程序获取服务，不需经历

[1] 数据来源：QuestMobile，《移动互联网全景生态流量洞察报告》

下载、安装、注册、卸载等过程，降低了用户的使用门槛。三是开发成本低。开发者利用小程序平台提供的开发工具，基于小程序平台框架，调用 API 接口，通过组件化编程即可开发具有原生 App 体验的小程序应用，节约开发时间和人力成本。

（二）小程序发展现状

移动互联网的持续渗透推动了数字经济的快速发展，用户的需求呈现多样化趋势，小程序得以快速普及和应用，其数量和用户量持续增长。截至 2019 年 11 月，小程序总量超过 450 万，日活跃用户突破 3.3 亿[2]，已成为人们日常生活中获取互联网服务的主要载体。

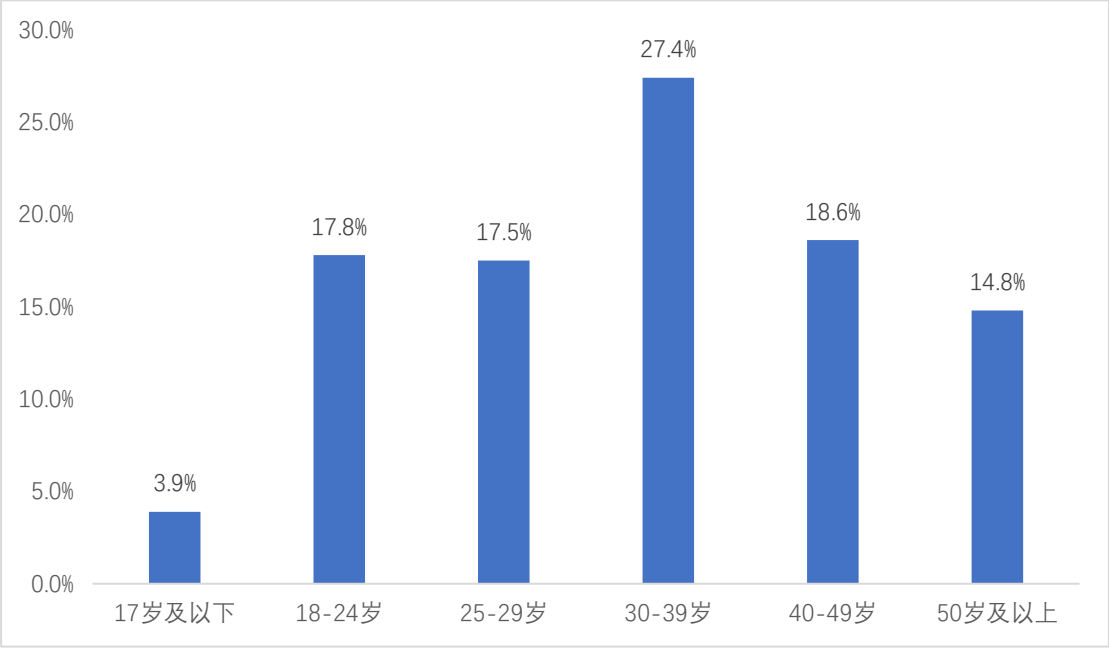
用户粘度提升，小程序成为常用互联网服务入口。2019 年人均使用小程序数量和时长持续增长，用户使用互联网服务的方式已发生转变。据统计，2019 年人均使用小程序数量超过 60，多于同期人均安装 App 个数[2]；支付宝小程序用户次日留存率超过六成，微信小程序次日留存率超过五成[3]，小程序发展初期用户留存难的问题得到改善，用户粘度的提升加深用户对小程序的信任和依赖，小程序成为用户获取互联网服务的常用载体。

疫情期间小程序发展迅速，助力疫情防控工作。2020 年新冠肺炎疫情的爆发推动了小程序的发展，截至 2020 年 3 月，月活跃用户数大于五百万的微信小程序数量升至 317 个，较 2019 年 12 月提升 61.7%[4]。小程序成为政府机关、医疗机构、企事业单位、社区学校疫

[2] 数据来源：阿拉丁研究院，《2019 年小程序互联网发展白皮书》
[3] 数据来源：即速应用，《小程序 2019 行业年中增长研究报告》
[4] 数据来源：QuestMobile，《中国移动互联网春季大报告》

情防控的重要工具，借助于小程序的疫情防控数据填报、疫情新闻传递、疫情信息查询、在线医疗问诊、健康码申报管理等功能，有效推动疫情防控管理工作，提升在线医疗服务效率，保障线上复工复产。

小程序实现生活场景和适龄人口全覆盖，融入用户日常生活。截至 2020 年 4 月，各平台内小程序覆盖 11 大类型，从小游戏、视频影音为代表的娱乐类应用到教育文化、旅游交通、日常工具、生活服务、体育健身、网络购物、新闻资讯、医疗健康、政务公益等服务类应用，涵盖民众日常生活中的常见场景。小程序的用户群覆盖各个年龄区间，其中 30-39 岁用户占比最多达到 27.4%，生活服务、网络购物、日常工具、视频影音类小程序在不同年龄段用户群体中使用频率较高。



数据来源：阿拉丁研究院《2019 年小程序互联网发展白皮书》

图 1　2019 年小程序用户年龄分布

小程序连接线上线下场景，助推消费提质升级。以小程序为载体

的互联网零售业消费规模进一步加大，2019 年小程序交易金额超过 12000 亿，同比增长超过 100%[5]。2019 年 4 月，同程旅游 97.2%的流量来自于微信小程序，淘票票 79.5%流量来自于支付宝小程序[6]。新冠肺炎疫情期间，线下服务行业业务受阻，小程序在迅速崛起的新型“宅经济”中扮演重要角色，数据显示，2020 年 3 月上旬，小程序点餐相比 2 月上旬增长 322%。小程序凭借其线上线下枢纽功能，持续赋能“无接触”商业模式，有效提升用户消费体验和商家服务效率。

小程序初步建立生态体系，平台各有所长、特点鲜明。2019 上半年，小程序平台从 2018 年的 2 家扩充至 8 家，腾讯、阿里、百度、字节跳动等多家头部互联网企业开始小程序布局。微信小程序平台利用其社交属性，涉及小程序种类广泛，先发优势明显；支付宝小程序平台着重消费与金融场景，以生活服务、商业服务类型为主；百度小程序平台以搜索、信息流形式结合人工智能实现小程序智能推荐；今日头条小程序平台为小程序提供多种流量入口，利用资讯浏览业务形态优势，通过信息流推荐小程序。

（三）小程序管理现状

近年来，我国高度重视移动应用程序（App）数据安全和个人信息安全工作，从法规标准、专项治理等多方面开展安全治理工作。目前的监督管理基本集中于 App，鲜少涉及小程序。

在国家法律层面，《网络安全法》明确了我国个人信息保护的基本原则，规定网络运营者的保护义务和责任。在政策法规层面，相关

[5] 数据来源：阿拉丁研究院，《2019 年小程序互联网发展白皮书》
[6] 数据来源：QuestMobile，《移动互联网全景生态流量洞察报告》

部门针对 App 业务特点制定细化规章落实国家法律。2013 年 7 月，工业和信息化部公布《电信和互联网用户个人信息保护规定》，明确了行业内个人信息的保护范围、个人信息收集使用原则等内容。2016 年 6 月，国家互联网信息办公室发布《移动互联网应用程序信息服务管理规定》，要求移动互联网应用程序提供者保护用户信息安全，依法履行相关义务。2019 年 12 月，国家互联网信息办公室、工业和信息化部、公安部、市场监管总局联合印发《App 违法违规收集使用个人信息行为认定方法》，明确细化了 App 违法违规收集使用个人信息行为标准。小程序的业务形态和用户数量迅速发展，其个人信息收集使用愈加频繁，对其开展安全管理的必要性急剧上升。不少平台运营者出于管理的需求，参考 App 个人信息保护相关工作，对平台内小程序进行安全管理。

随着小程序与民众日常生活进一步融合，为提供更加个性化的服务，小程序在开展业务的过程中难免会涉及更多的用户个人敏感信息，用户在享受便捷化服务的同时将面临潜在安全隐患，亟需梳理分析小程序目前存在的数据安全和个人信息安全风险，针对性提出对策建议，推动提升小程序安全保障能力，促进小程序健康有序发展。

二、 小程序与 App 和小程序平台的关系

（一）小程序和 App 的差异

小程序的开发以及运行均基于小程序平台，这使得小程序具备无需安装、使用便捷等优点的同时，在接口调用、权限获取和管理、消息推送等方面受限于小程序平台，与 App 相比相关能力较为简单。

一是小程序有权调用的 API[7]少于 App。小程序无法绕过小程序平台直接调用手机系统 API 并和系统互动; App 则可调用所有手机系统 API，直接与系统对话，实现修改手机系统音量、网络连接等功能。

二是小程序可获取的权限少于 App。小程序只能获取小程序平台已经从手机系统获取的权限，通常仅限于用户信息、地理位置、后台定位、相册、通讯地址、发票、录音、摄像头、运动步数; 而 App 能够获取的手机系统权限多达一百余项，其中不乏日历、通讯录、麦克风、短信等敏感权限。

三是小程序的权限管理方式异于 App。小程序的权限管理通常是从小程序平台“设置”中选择“允许”或“拒绝”某项权限，且一次只能进行一款小程序的权限设置; App 的权限管理则可在手机系统设置中完成，且可实现集中管理，即可一次性针对多款 App 的权限情况进行修改。

四是小程序推送消息的渠道少于 App。小程序只能发送模板消息，或在被用户主动订阅后进行推送，App 则可以随时随地为用户推送消息。

（二）小程序和小程序平台的关系

目前所有小程序必须依托小程序平台搭建的入口进入，因此小程序能够获取的信息范围受限于平台规则。**二者的关系主要体现在两个方面：小程序通过平台获取信息，以及平台为保护个人信息对小程序提出要求。**

[7] 应用程序编程接口，用于提供应用程序与开发人员基于某软件或硬件得以访问一组例程的能力，而又无需访问原码，或理解内部工作机制的细节

小程序可从小程序平台获取以下信息：一是用户信息。小程序在获得用户授权后，可获取用户的平台昵称、头像、性别、所在地区、语言、手机号、身份证号等个人信息，人脸、指纹等个人生物信息，以及通过权限申请获取的地理位置、通讯地址等信息。除此之外，小程序还可从具备资金管理能力和实人认证能力的平台获取财产信息相关认证结果。二是设备信息。小程序可获取的设备信息分为网络状态、Wi-Fi、加速度传感器、罗盘、剪贴板、系统信息、屏幕等多个类型，其中系统相关信息包括操作系统版本、操作系统类型、手机品牌、手机型号、平台版本号、平台名称、屏幕宽度、屏幕高度、设备像素比等，屏幕相关的设备信息包括屏幕是否常亮、用户是否截屏等，有些平台还支持小程序添加手机通讯录联系人、获取设备电量、添加和删除日历活动等功能。三是统计信息。大量用户使用小程序的行为可汇聚形成统计数据，小程序运营者借此了解小程序的运营状况，分析小程序的用户来源、用户构成、用户增长趋势、用户留存与转化、用户使用行为习惯等，帮助小程序迭代优化和运营。除了常规的数据分析，例如通过用户访问规模、来源、频次、时长、深度、留存来判断产品使用粘性，通过用户年龄、性别、地区、终端及机型分布刻画用户画像，通过展示各个页面的访次、停留时间、退出率等体现页面受欢迎的程度等之外，小程序还可在小程序平台内自定义分析用户实时行为，对其行为做精细化跟踪，满足页面访问等标准统计以外的个性化分析需求。

涉及到用户个人信息保护时，平台通常从数据收集和存储与授权、

数据使用规范、数据安全、地理位置四个方面对小程序提出要求。

数据收集、存储与授权方面，小程序采集用户数据之前，必须确保经过用户同意，并向用户如实披露采集数据内容、数据用途、使用范围等相关信息；小程序不得非法收集或窃取用户密码或其他个人数据，不得强迫用户输入个人信息或收集用户密码；若用户要求，小程序运营者应删除接收的所有关于该用户的数据，除非依据法律、法规有权要求保留这些数据；用户拒绝授权后，小程序运营者有义务清除并不再继续使用该用户的平台头像、昵称等数据；若小程序运营者终止使用小程序，应立即删除从平台和小程序接收的所有用户数据。

数据使用规范方面，小程序不得向其他用户或任何第三方显示用户个人信息[8]或用于任何未经用户及平台授权的用途；小程序不得进行反射查找、跟踪、关联、挖掘、获取或利用用户个人信息从事与小程序所公示身份无关的行为；小程序不得在未经用户明确同意、未向用户如实披露数据用途、使用范围等场景下复制、存储、使用或传输用户数据；未经平台授权或允许，不得使用从平台和小程序接收的数据用于做出有关资格的决定；若小程序运营者的主体被第三方收购或合并，则小程序运营者从平台和小程序接收的数据仅能在小程序内继续使用；在检测到相关小程序遭到非法攻击产生的异常状况或数据泄露后，平台有权对相关接口进行保护，包括但不限于临时关闭，限制流量，限制频次等方式阻断恶意攻击；小程序不得明文传输用户隐私数据。

[8] 包括但不限于平台账号、名称、手机号、电子邮箱地址等信息

数据安全方面，平台要求小程序谨慎保管所使用的账号、密码和密钥，保护用户授权的隐私信息与数据；若使用第三方合作伙伴服务，小程序应同合作伙伴签署合同，限制其对这些信息的使用并保持信息的保密性；小程序不得要求用户降低手机操作系统安全性后才能使用相关功能；一旦小程序运营者停止使用相关服务，或平台基于任何原因终止小程序运营者使用相关服务，小程序必须立即删除全部因使用该服务获得的数据及备份，且不得再以任何方式继续使用；当出现数据泄露，小程序运营者有义务通知平台，平台有义务配合进行紧急安全处理与相关调查；小程序所有展示的用户个人隐私信息[9]，必须进行脱敏。

地理位置方面，平台要求，只有在服务过程中确有实际需要的，小程序才能向用户申请获取实时位置信息；在采集、传送或使用地理位置数据之前必须获得用户同意；地理位置数据只能用于小程序提供的直接相关功能或服务；小程序在申请地理位置接口时，应同时说明申请理由；如用户拒绝共享实时地理位置，小程序应当允许用户手动选择位置，不能因此不向用户提供服务。

（三）小程序和小程序平台的责任划分

基于前述特性，小程序属于国家标准《信息安全技术 个人信息安全规范》中定义的“具备收集个人信息功能的第三方产品或服务”，该规范针对平台应尽到的安全管理责任，从建立安全评估机制、签订合同、征得个人信息主体授权等方面提出了详细要求。2019 年 5 月，

[9] 包括但不限于姓名、手机号、身份证号

国家互联网信息办公室公开《数据管理办法（征求意见稿）》，规定网络运营者应对接入其平台的第三方应用明确数据安全要求和责任，督促监督第三方应用运营者加强数据安全管理；第三方应用发生数据安全事件对用户造成损失的，网络运营者应当承担部分或全部责任，除非网络运营者能够证明无过错。

当小程序出现个人信息安全问题时，平台是否需要承担责任，需综合考量小程序收集用户信息的路径，以及小程序和平台的安全技术水平。

小程序收集用户个人信息的方式分为两种：直接收集和间接收集。**直接收集**是指用户手动输入信息交给小程序，比如使用提供快递服务的小程序时，用户需输入收货者的姓名、地址、联系方式等信息。这种情形下，责任由小程序运营者独立承担。**间接收集**是指用户使用平台账号登录小程序，“一键授权”账号、密码。小程序通过平台获取用户信息需经过“三方”授权的操作，即小程序向平台发起申请，平台再询问用户意见，最终由用户决定是否将信息交给小程序。此时，平台相当于用户信息的存放者，不会主动将信息分享给小程序，与直接收集时一样，用户享有最终决定权。这种情形下，平台需要尽到中转告知和管理的责任。如果平台尽到责任，小程序仍然未经用户授权收集信息或骗取用户信息，则属于违规行为，小程序后续处理信息的一系列操作也将缺少合法前提。如果平台明知小程序侵害用户权益，却存在怠于处置的情况，平台应对处理不及时导致的用户损失扩大承担连带责任。

如果平台存在漏洞，导致小程序可未经授权获取用户信息，则小程序属于不法获得用户信息。一旦造成用户信息泄露，平台和小程序需分别承担相应责任。2018 年“剑桥分析”事件属于平台与其搭载的第三方应用均存在过错的情形，可对小程序和平台的责任划分提供参考。由于 Facebook 平台存在管理漏洞，第三方应用可在未经用户充分授权的情况下获取用户的好友信息，而 Facebook 没有将此情况告知受影响的用户，最终导致 8700 万用户信息泄露。为此，Facebook 与美国联邦贸易委员会达成和解，赔偿 50 亿美元，并遭到全球多国处罚。

当小程序和平台同时掌握用户信息且发生数据泄露事件时，如果难以确认责任主体，双方应共同承担责任。在 2017 年庞某鹏诉中国东方航空股份有限公司（下称“东航公司”）、北京趣拿信息技术有限公司（下称“趣拿公司”）隐私权纠纷[10]事件中，庞某鹏委托其助理通过趣拿公司运营的去哪儿网购买东航公司机票，其后收到诈骗短信，短信内容含有庞某鹏所乘航班的起飞时间、降落时间、机场名称、航班号。法院在本案中认定，被告东航公司和趣拿公司掌握了庞某鹏的身份证号、手机号和航程信息，其后，相关信息又在合理时间内发生泄露，根据高度盖然性的证明标准，足以认定信息泄露系被告导致，故二被告构成对庞某鹏隐私权的侵犯，应当承担侵权责任。以上案例中的信息承载主体虽非小程序和平台，但对于责任主体无法辨别情境下由小程序和平台共同承担责任这一划分方式提供了参考。

[10] https://www.bjinternetcourt.gov.cn/cac/zw/1536234373997.html

三、 小程序个人信息安全风险

小程序因其便捷性已经深入经济社会的各个领域，不时暴露出违法违规收集使用个人信息的风险。不法分子利用小程序开发、上线流程简易快速和可利用小程序平台引流等特点，以领取红包、参与抽奖等名义，通过设置登录授权或诱导用户填写的方式，套取用户个人信息，存在个人信息安全隐患。疫情期间，个人健康信息上报、健康码获取等疫情防控工作大多借助小程序开展，涉及大量个人信息的收集使用，存在个人信息泄露、滥用、窃取风险，其数据安全性引起广泛关注。

报告团队于2020年4月7日-4月26日[11]，从微信、支付宝、今日头条、百度四大主流小程序平台中，选择新闻资讯、生活服务、视频影音、网络购物、医疗健康、教育文化、政务公益、旅游交通、体育健身、日常工具等10大类中知名度高、影响范围广、涉及较多个人信息的52款小程序作为个人信息安全评测对象。评测包括两大部分：**一是**隐私政策评测，考察小程序的隐私政策中关于小程序运营者收集、使用、存储和保护个人信息的描述是否清晰和全面。**二是**数据安全检测，检测小程序在收集、传输、共享、删除等重点环节中的个人信息安全风险。

（一）隐私政策评测

隐私政策评测发现，只有38.5%的小程序提供了独立的隐私政策，且各平台的小程序情况相差较大，提供了隐私政策的小程序在各

[11] 上述取证时间之外的修改不计入本次评测结果。

平台占比从 23.1%到 76.9%不等，其中政务公益、日常工具、体育健身、医疗健康类小程序的问题较为严重，集中在小程序无隐私政策、使用与 App 不一致的隐私政策，以及默认勾选隐私政策等方面。

1.未提供有效的隐私政策，侵害用户的知情权

小程序的登录方式通常分为三种：一是自行注册小程序账号，二是直接使用小程序所在平台账号，三是使用第三方平台账号。报告团队发现，如果小程序仅提供第二种方式，常常会出现小程序不提供隐私政策，而是由平台代为提供相关协议的情况。例如某共享单车小程序在首次打开时，会申请获取用户昵称、头像等基本信息，姓名、手机号、证件号码、用户的信用评估结果等个人信息，但提供的四份相关协议均为所在平台提供的标准协议，小程序运营者本身并未提供任何隐私政策或对收集上述信息的场景、用途、目的做出说明。某在线购票小程序可以从平台获得用户信息，还可以获取用户的地理位置信息，但注册时跳转的是平台的注册登录页面，用户只能看到平台提供的用户协议和隐私政策。

即使提供了隐私政策，少数小程序也存在链接无效的情况，用户同样无法得知个人信息收集使用规则。例如某在线购物小程序的《隐私保护声明》为空白页面。某工具类小程序和某视频类小程序提供的相关协议则都显示打开失败。

此次选取的 52 个小程序均具备收集和使用用户个人信息的能力。根据相关法律法规要求，作为个人信息控制者，小程序有义务向用户详细告知收集和使用的目的、范围，如何存储，以及如何保障用

户信息安全等问题，而不是仅由所在平台提供协议，不提供或提供无效的隐私政策，否则将侵害用户的知情权。

2. 未采取主动选择同意的形式，侵害用户的选择权

在用户注册或登录时，小程序通常会在上述页面提供隐私政策等相关协议，以告知收集、使用个人信息的目的、方式和范围。但报告团队发现，在 21 个提供了隐私政策的小程序中，绝大多数采用的都是“登录即同意”的方式征得用户同意，只有极少数需要用户主动勾选同意隐私政策。

根据《信息安全技术 个人信息安全规范》要求，收集个人信息需获得个人信息主体的授权同意；收集个人敏感信息前应征得个人信息主体的明示同意，并应确保个人信息主体的明示同意是其在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示。

因此，小程序应在提供隐私政策链接的同时，赋予用户主动选择同意的权利，征得用户的明示同意，否则将侵害用户的选择权。

3.隐私政策与 App 不同，带来数据收集使用规则混淆风险

如前所述，小程序收集的个人信息受制于平台，是包含于或等于对应 App[12]能够收集的个人信息的，一般与 App 共享一套数据处理流程。因此，小程序和 App 提供的隐私政策应保持一致。但报告团队发现，绝大多数小程序对应的 App 都有隐私政策，但近半小程序无隐私政策或使用的是与 App 不同版本的隐私政策。例如某旅游类小程

[12] 由同一运营者开发，与小程序所对应的 App。

序没有提供隐私政策，但其对应的 App 却有十分详尽的隐私政策。某外卖小程序使用的隐私政策的更新日期早于对应 App 版本的隐私政策，即小程序使用的是旧版本的隐私政策。

尽管小程序和 App 在前端的表现形式不同，但后台的服务器、数据库通常是共用的，且小程序的功能并无超出 App 之处。因此二者收集和使用用户个人信息也应该适用同一套规则，不应在隐私政策文本上有所差别。若小程序在隐私政策更新的及时性方面不如 App，极易造成数据收集使用规则混淆风险。

（二）数据安全检测

数据安全检测发现，每款小程序平均约存在 3 个问题，其中教育文化、旅游交通、新闻资讯、生活服务类小程序个人信息保护问题较为突出（见图 2），主要问题集中在收集、删除、传输等环节（见图 3）。

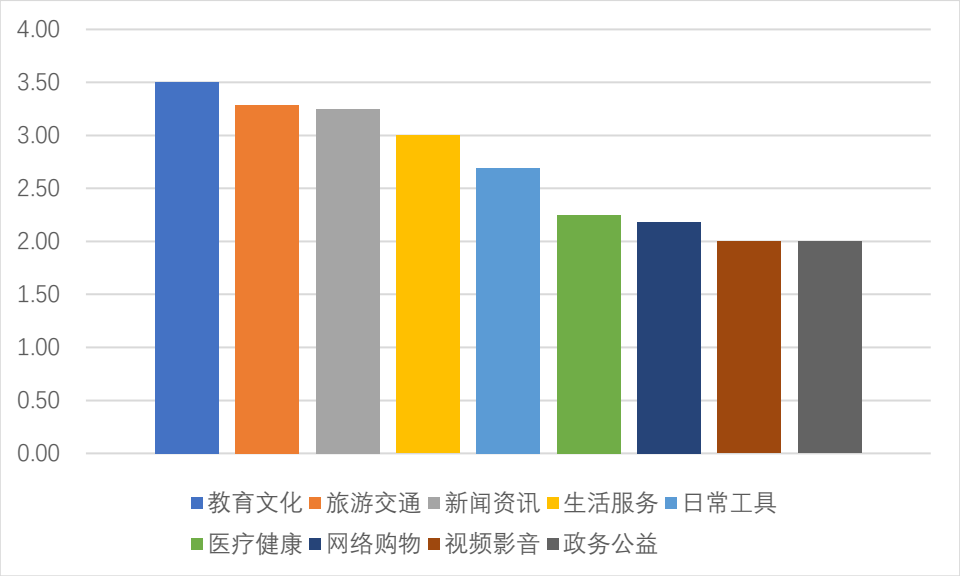


图 2　各类别小程序平均问题数量

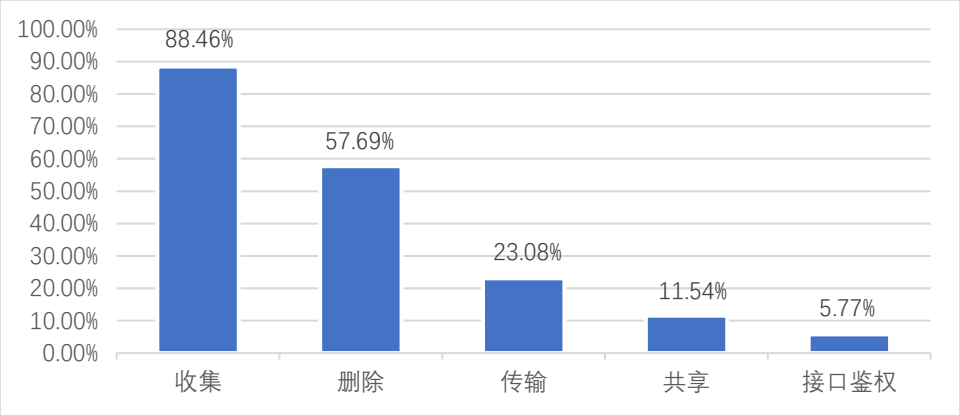


图 3　小程序在各环节出现问题占比

基于检测结果，报告团队梳理出当前小程序存在的用户个人信息方面的典型安全问题。一方面，小程序可视为类似 App 的简易版应用，其用户个人信息方面的问题与 App 存在类似之处；另一方面，因小程序在功能数量、搭载平台、使用场景、个人信息流转环节等方面与 App 存在诸多差异，其用户个人信息方面的问题也具备特殊性。

1.超范围收集个人信息，带来数据违规收集风险

用户在使用小程序体验相关服务时，需要在特定功能触发时让渡一些必要的个人信息以提升服务的精确性。例如在线租房类小程序需获得用户地理位置以提升附近房源推荐的准确性。但报告团队发现，某些小程序存在收集与当前场景无关个人信息的行为。例如某健身类小程序申请获得个人真实姓名和电话号码，而相关个人信息与观看健身视频、健身打卡等功能没有直接关系。某购物类小程序申请获取用户蓝牙权限，与线上购物这一行为相比，这些信息收集的合理性存疑。某防疫类小程序除获取个人姓名、身份证号等敏感信息外，还需进行人脸识别，获取大量人脸信息。用户通过姓名、身份证号以及二者的

对应关系，在实际线下防疫工作中再配合真人及身份证查验，在不获取人脸信息的情况下可保证信息的准确性，收集使用人脸信息这一极敏感的生物特征信息的必要性有待商榷。

与运营者相比，用户在使用小程序时处于弱势地位。若运营者存在不单纯的收集目的，超范围收集非必要用户个人信息，用户处于放弃使用或被动提供信息的两难选择，一旦相关个人信息被不法分子获取滥用，极易造成用户权益损害。

2.明文传输个人信息，带来数据非法获取风险

数据传输安全是保障数据安全的关键环节，网络黑客可能攻击截获传输的数据包，进行数据窃听、数据篡改、身份伪造等，可靠安全的数据传输是使用小程序的重要保障。小程序运营者应采取加密等技术措施，确保数据即使被恶意泄露或截获也难以被破解。经报告团队技术检测，有约 1/4 的被测小程序明文传输个人信息甚至个人敏感信息。例如某共享单车小程序和某外卖小程序明文传输用户精确定位位置（经度、纬度）；某酒店机票预订小程序明文传输订单信息（订单号、机票起终点机场、航空公司、机票日期）；某电子商务小程序明文传输用户收货地址；某教育类小程序明文传输学生姓名、年级、学校和家长电话；某医疗健康小程序明文传输用户健康档案信息（用户和档案人关系、姓名、性别、身高、体重、出生日期、药物过敏史）。

这些明文的个人信息一旦在传输中被截获，无需破解即可被直接识别利用，降低了不法分子的犯罪门槛，可能为用户带来骚扰诈骗风险甚至经济财产损失。

3.未告知用户关闭权限路径，带来权限持续开放风险

权限是小程序平台对于小程序运营者收集使用用户个人信息的限制，运营者可通过向用户申请权限后获取用户个人信息。目前各大小程序平台均为用户提供了关闭小程序的已授权权限功能，但鲜少有小程序对用户进行告知，用户难以了解该功能使用路径。

经报告团队检测发现，94%被测小程序未向用户告知如何关闭已授权权限路径，这可能导致用户在使用完小程序后仍将一些权限开放给小程序。例如某生活服务类小程序，申请获取用户信息和地理位置权限，用户使用完后若不关闭相关权限，则相关权限一直开放给小程序，意味着小程序可较长时间留存用户的个人信息或在下次被使用时不需再次向用户询问申请获取相关权限，可能存在个人信息在用户未知情况下被使用的风险。

4.关闭授权后仍使用之前授权信息，带来数据滥用风险

小程序搭载在小程序平台之上，用户授权小程序后可直接使用小程序平台账号登录使用。用户需要仅注销某小程序中的账号而不是注销自己的小程序平台账号时，关闭对于小程序的“用户信息”授权即可。其他授权同样适用这一功能。该功能的设计使得用户能及时停止授权给某小程序的用户信息（一般包括用户名（某些实名制小程序平台为用户真实姓名）、头像、手机号、身份证号）和地理位置等。小程序平台一般规定用户拒绝授权后，小程序运营者有义务清除并不再继续使用该用户的平台头像、昵称等数据。但经报告团队检测发现，约 1/4 的小程序在用户关闭“用户信息”授权后再次进入，仍显示上次授权时

的个人信息，如姓名、手机号等。用户关闭某具备求职功能的生活服务类小程序“地理位置”权限后，间隔一段时间重新使用小程序，求职区域仍显示用户当前所在城市区域。这表明用户取消授权后，相关小程序并未及时对用户授权情况进行更新，甚至可能在用户已经解除授权的情况下仍在收集使用用户个人信息，存在用户个人信息滥用风险。

5.默认共享用户个人信息，带来数据脱离控制风险

小程序中包含两类较为特殊的小程序，一类小程序为小程序平台运营的平台小程序，一类小程序为同一公司运营的多个关联小程序，它们的共同特点是由同一公司运营。经报告团队检测发现，在未进行权限申请的情况下，某些平台小程序默认获取并使用了用户在平台内的信息，或者某些小程序默认获取并使用了其关联小程序的用户信息，包括账号信息、收货地址等。同时，因这类小程序跳过权限申请这一步骤，设置中的已授权权限为空，导致用户无法关闭相关用户信息授权。

在这一情况下，运营者告知不足，用户不了解具体情况，并未自主同意被同一公司旗下的所有小程序共享使用其个人信息，这可能导致用户无法完全掌握控制其个人信息的传播路径、使用范围及使用风险。

6.未提供删除个人信息渠道，带来数据过度留存风险

App 提供账号注销功能保障用户自主删除个人信息权利，小程序功能简单，绝大多数基于小程序平台账号进行服务，可能无法提供单独的注销账号服务，但这并非是小程序运营者不提供删除个人信息渠

道的理由。小程序运营者宜按照《电信和互联网用户个人信息保护规定》《信息安全技术 个人信息安全规范》等制度标准要求，为用户提供个人信息删除渠道并在后台实际删除，如删除收货地址、运动轨迹、人脸信息等。

经报告团队进行检测，超过一半的小程序未提供删除个人信息渠道。某些生活服务类、医疗健康、旅游交通、政务公益类小程序收集大量个人敏感信息，如精确地理位置、真实姓名、身份证号、健康信息、人脸信息及这些敏感信息的对应关系，用户填写上述信息后，小程序并未对相关个人敏感信息的后续处理提供说明，或者为用户提供删除或匿名化个人信息渠道。用户难以了解、更难以控制这些个人信息的留存情况与最终去向，可能带来个人信息过度留存的风险。

四、 对策建议

面对当前小程序发展的如火如荼和小程序个人信息保护需求的急剧攀升，需加强政府、企业、用户的多方协同，形成小程序个人信息保护管理体系。

（一）规范层面，建议将小程序纳入个人信息保护管理范畴

我国高度重视 App 个人信息保护工作，从法规标准、专项治理等多方面开展安全治理。但小程序的管理依据、责任划分、收集使用个人信息标准等处于模糊地带。随着业务形态和用户数量的迅速发展，小程序预计成为发展态势和使用场景比肩 App 的应用，建议将小程序这一新兴业态纳入个人信息保护管理范畴，参照 App 安全治理模

式，针对小程序特点，研究制定个人信息安全保护指南规范，明确小程序与小程序平台之间的主体责任划分等，鼓励指导小程序运营者和平台运营者强化用户个人信息安全保护。

（二）企业层面，切实落实个人信息保护主体责任

一是小程序运营者主动开展数据安全及个人信息保护自评估工作。及时发现其运营应用存在的个人信息保护风险，配备与业务功能相适应的个人信息保护管理制度要求和技术手段能力，降低违规收集、使用、传输、共享个人信息的风险。二是小程序平台运营者进一步加强对搭载于其平台内小程序的管理工作。将小程序的个人信息保护情况纳入审核重点内容，并对小程序的运营加强监督巡查，接受用户举报，发现小程序存在个人信息安全方面问题时及时进行处理。

（三）用户层面，提升使用小程序的个人信息保护意识和能力

随着 App 专项治理行动的广泛开展和相关宣传工作的有力支持，用户对于其在使用 App 时的隐私保护意识和能力逐渐提升。但对于小程序，大部分用户自身个人信息保护意识和能力仍然不足，为使用相关服务而被动提供个人敏感信息的情况屡见不鲜。亟需通过科普讲座、社区宣传等丰富形式，对用户进行解读和宣导，使其明确个体作为其个人信息控制者的权利，提升保护个人信息的意识和能力。在保护用户个人信息免受侵害的同时，鼓励用户积极举报违规行为，发动社会力量，推动小程序规范健康发展。

附 录

从隐私政策和数据安全两大方面对小程序进行评测，督促小程序运营者在开展收集、使用、传输、共享、删除等个人信息处理活动时，遵守国家相关法律法规、政策标准的要求，保障个人信息安全且不侵犯个人信息主体权益。

法律依据如下:

- 《中华人民共和国网络安全法》
- 《电信和互联网用户个人信息保护规定》
- 《移动互联网应用程序信息服务管理规定》
- 《App 违法违规收集使用个人信息行为认定方法》
- 《数据安全管理办法（征求意见稿）》

其他参考的规范、标准、指南有:

- 国家标准 GB/T 35273-2020 《信息安全技术 个人信息安全规范》

本次个人信息安全评测项目[13]如下:

隐私政策评测项目包括: 是否提供了隐私政策，隐私政策的规范性和实用性，履行必要的告知和警示义务，收集、存储、使用用户个人信息的规则，关于定向推送的说明，用户的选择权和同意权，用户的访问权、更正权、删除权、撤回同意及注销权，披露开发者相关信息，向第三方披露用户个人信息的说明，安全承诺，在个人信息泄露事件中的救济机制，特殊情形下对用户个人信息的处理原则，对于使

[13] 本评测所采用的标准仅代表第三方机构观点，旨在提供合规建议，小程序运营者并非必须按照这一标准进行隐私合规。

用 cookie、clickstream 和 web beacon 等技术的专门声明，对链接到第三方网站的免责说明等共 14 项评测项。

数据安全检测项目包括：是否明示收集使用个人信息的目的、方式、范围；是否经用户同意收集使用个人信息；收集使用个人信息是否遵循必要原则；个人信息传输安全性；删除更正个人信息渠道；敏感权限与业务功能的对应关系；权限申请使用情况；用户身份鉴别等 8 大类 15 项检测项。

免责声明

本报告内容供相关单位参考，酌情使用。若本报告内容与其他机构研究结果有差异，请使用方自行辨别，中国信息通信研究院安全研究所和南都个人信息保护研究中心不承担与此相关的一切法律责任。因研究团队能力有限，报告内容多有不足之处，欢迎各领导专家批评指正，我们持续改进。

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62305670

传真：010-62300264

网址：www.caict.ac.cn

南都个人信息保护研究中心

地址：北京市朝阳区时间国际 8 号楼

邮政编码：100028

传真：010-59540277

联系邮箱：ppa_nandu01@163.com

网址 http://research.nandu.com/piprc/#