

APP 违法违规 收集使用个人信息 专项治理报告

2019

APP 专项治理工作组

Personal Information Protection Task Force on APPs



序言

2019年1月，中央网信办、工业和信息化部、公安部、市场监管总局四部门联合发布《关于开展APP违法违规收集使用个人信息专项治理的公告》，在全国范围组织开展APP违法违规收集使用个人信息专项治理，并成立APP违法违规收集使用个人信息专项治理工作组（以下简称“APP专项治理工作组”）。一年来，专项治理工作成效显著，《APP违法违规收集使用个人信息行为认定方法》《个人信息安全规范》等标准规范相继出台完善，用户规模大、与生活关系密切、问题反映集中的千余款APP经深度评估后进行了有效整改，无隐私政策、强制索权、无注销渠道等问题明显改善，APP运营者履行个人信息保护责任义务的能力和水平明显提升，全社会关注和重视个人信息安全的氛围基本形成。

本报告介绍了治理工作开展情况，包括技术规范制定、举报信息受理、专业机构检测评估、问题督促整改及处置，以及四部门全面推进深化治理等。报告引用多方数据，客观分析了个人信息保护相关突出问题、企业能力、民众意识、社会影响等方面的发展变化趋势，展示了治理工作成效。最后，在总结2019年治理工作经验的基础上，就持续开展治理工作、培育良好移动互联网生态，提出了具体建议。

● 序言	
● 一、加强 APP 个人信息保护势在必行	01
● 二、2019 年专项治理工作概述	03
(一) 专项治理整体工作思路	03
(二) 四部门多措并举深化治理	05
● 三、2019 年专项治理工作成效分析	07
(一) 评估和举报数据显示, 典型违法违规问题得到遏制	07
(二) 不同时期数据对比显示, 企业个人信息保护能力水平显著提升	11
(三) 媒体报道和问卷调查显示, 专项治理初见成效	14
(四) APP 个人信息保护相关技术文件、科普知识等得到广泛传播	19
● 四、持续开展专项治理工作的建议	22
附件一:《关于开展 APP 违法违规收集使用个人信息专项治理的公告》	26
附件二:关于印发《APP 违法违规收集使用个人信息行为认定方法》的通知	28

一、加强 APP 个人信息保护势在必行

当前，我国已经全面进入移动互联网时代，近 9 亿网民中手机上网比例高达 99.1%，移动互联网服务便捷、即时、普惠的特点在移动互联网应用程序（APP）中得到充分体现。据不完全统计，移动互联网应用商店上架推广的 APP 有近 400 万款，总下载量超万亿次。用户每天在各类 APP 上平均花费时长达 4.9 小时，占用户日均上网时长的 81.7%。APP 的广泛应用，在促进经济社会发展、服务民生等方面发挥着不可替代的作用。但与此同时，APP 强制授权、过度索权、超范围收集个人信息的现象普遍存在，未制定并公开隐私政策、未经用户同意收集个人信息、未提供注销账号功能等不规范行为屡见不鲜，个人信息泄露、滥用等情形时有发生，广大网民对此反映强烈。

中国互联网协会发布的《中国网民权益保护调查报告 2016》显示，2016 年国内 6.88 亿网民因垃圾短信、诈骗信息、个人信息泄露等造成的经济损失估算达 915 亿元。54% 的网民认为个人信息泄露情况严重，84% 的网民曾亲身感受到因个人信息泄露带来的不良影响。南方都市报个人信息保护研究中心于 2017 年发布的《关于收集个人信息“明示同意”的测评报告与建议》显示，被测评的 100 款 APP 中仅有 11% 做到了“明示同意”，在制定了隐私政策的 APP 中，绝大部分也采取“默认勾选”方式。中国消费者协会在 2018 年开展的 APP 个人信息收集与隐私政策测评结果显示，在收集个人信息方面，纳入测评的 100 款 APP 普遍存在涉嫌过度收集个人信息的情况，其中 59 款涉嫌过度收集“位置信息”，28 款涉嫌过度收集“通讯录信息”，23 款涉嫌过度收集“身份信息”，22 款涉嫌过度收集“手机号码”等。

为规范个人信息的收集使用，打击涉个人信息违法犯罪行为，国家相继出台个人信息保护相关法律法规。2012 年《全国人民代表大会常务委员会关于加强网络信息保护的決定》、2014 年实施的《消费者权益保护法》、2017 年实施的《网络安全法》均对收集使用个人信息的法律责任和义务作出规定；《刑法修正案（七）》、《刑法修正案（九）》以及《最高人民法院、最高人民检察院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》中，明确了侵犯公民个人信息犯罪行为的界定和处罚；2017 年实施的《民法总则》强调，自然人的个人信息受法律保护。同时，个人信息保护法已纳入十三届全国人大常委会的立法规划，并已经形成草案稿。

然而，数字时代，数据成为企业竞相争夺的战略资源，个人信息更是最具价值的核心资源，很多企业“跑马圈地”、“野蛮生长”，将获取和利用个人信息作为其核心商业目标，而移动互联网免费服务模式更是加剧了其对个人信息的依赖性，导致个人信息安全问题呈现多样化、复杂化特点。2017 年底，全国人大常委会执法检查组《关于检查〈网络安全法〉、〈全国人民代表大会常务委员会关于加强网络信息保护的決定〉实施情况的报告》中“万人调查”结果显示，部分受访者认为，“一法一决定”中关于用户个人信息保护的多项制度落实得并不理想，举报难、投诉难、立案难现象比较普遍，免费应用程序普遍存在过度收集用户信息、侵犯个人隐私问题。互联网公司和公共服务

部门存储了大量公民个人信息，但安防技术滞后。用户信息泄露呈现渠道多、窃取违法行为成本低、追查难度大等特点，因用户信息泄露引发的“精准诈骗”案件增多，给人民群众财产安全造成严重危害。报告还提出针对上述问题的建议，包括开展监督检查和评估措施、加大打击力度、加强完善投诉受理机制。

近年来，各有关部门高度重视贯彻落实个人信息保护相关法律法规，积极开展工作，完善个人信息保护监督管理机制，打击违法违规收集使用个人信息行为，引导相关企业和公共服务机构强化保护措施，保障公民合法权益。

2017年，为确保《网络安全法》中个人信息保护相关要求有效实施，提升网络运营者个人信息保护水平，中央网信办、工业和信息化部、公安部、国家标准委四部门联合开展隐私条款专项评审工作，对微信、淘宝等十款网络产品和服务的隐私条款进行评审，督促引导其改进完善隐私条款，提升个人信息保护水平。

2019年，《儿童个人信息网络保护规定》发布实施，《数据安全管理办法（征求意见稿）》、《个人信息出境安全评估办法（征求意见稿）》完成向社会公开征求意见，《个人信息安全规范》等国家标准已经发布实施并得到广泛应用。有关部门持续开展了一系列个人信息保护相关监管执法活动，有关社会组织推动社会各界密切关注个人信息保护，引导企业加强合规自律。

二、2019 年专项治理工作概述

2019 年 1 月，中央网信办、工业和信息化部、公安部、市场监管总局四部门联合发布《关于开展 APP 违法违规收集使用个人信息专项治理的公告》（详见附件一），决定自 2019 年 1 月至 12 月，在全国范围内组织开展 APP 违法违规收集使用个人信息专项治理。

（一）专项治理整体工作思路

1. 坚持网络安全靠人民，建立举报平台

专项治理工作建立了专门针对 APP 违法违规收集使用个人信息行为的举报渠道，受理网民投诉举报。截至 2019 年 12 月，微信公众号“APP 个人信息举报”已有超 3 万名用户关注，共收到网民举报信息 12125 条，涉及 2300 余款 APP。其中匿名举报信息 8142 条，占比 67.15%；实名举报信息 3983 条，占比 32.85%。从举报量来看，前五大典型问题分别为：超范围收集与功能无关个人信息、强制或频繁索要无关权限、存在不合理免责条款、无法注销账号、默认捆绑功能并一揽子同意。对于网民举报信息，APP 专项治理工作组逐条进行核验，将问题属实、下载量大、用户常用的 APP 纳入到重点评估范围。

2. 坚持依法治理，明确评估重点

针对广大网民反映强烈的 APP 强制授权、过度索权、超范围收集个人信息等问题，坚持以《网络安全法》等法律法规为准绳，制定发布《APP 违法违规收集使用个人信息行为认定方法》（详见附件二），将 APP 违法违规收集使用个人信息行为概括为“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”、“未经用户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”六类行为，为统一监管执法尺度提供参考。

此外，专项治理工作委托全国信息安全标准化技术委员会组织修订国家标准《个人信息安全规范》，编制国家标准《移动互联网应用程序（APP）收集个人信息基本规范》，明确 APP 收集使用个人信息时应满足的基本要求，以及 30 类大众化 APP 基本业务功能可收集的最小必要信息，细化落实个人信息收集使用的必要性要求。

3. 坚持科学评估，遴选专业评估力量

确保评估工作的科学性、专业性、公正性，专项治理工作综合考虑机构资质背景、人员规模、技术实力、测评经验、管理水平等因素，遴选 14 家专业评估机构对 APP 收集使用个人信息情况进行评估。同时，分批次对评估机构进行培训，由评估机构遵照专项治理工作的技术规范文件和 workflows 开展评估工作。

4. 坚持宣传科普，扩大专项治理效应

坚持网络安全为人民，专项治理工作加大宣传和科普力度，通过广大网民喜闻乐见的渠道和方式推广个人信息保护科普知识，提升网民个人信息保护意识和技能，切实保障人民群众在网络空间的合法权益。一是借助 3·15 晚会、高考等关键时间节点，曝光问题严重的 APP、专题发布典型问题 APP 评估结果，引起全社会的关注和重视，避免广大网民利益受损；二是通过专项治理微信公众号发布科普文章，将个人信息保护知识进行通俗化解读，向网民普及正确的个人信息保护知识；三是联合其他媒体进行 APP 收集使用个人信息情况问卷调查，走群众路线，充分了解民情民意，并以此为基础，持续推进工作开展。

（二）四部门多措并举深化治理

1. 中央网信办、市场监管总局联合推动建立 APP 个人信息安全认证制度



2019年3月15日，中央网信办、市场监管总局联合印发《关于开展APP安全认证工作的公告》，推动建立APP个人信息安全认证制度，按照APP运营者自愿申请的原则，由具备资质的认证机构依据相关国家标准对APP收集、存储、传输、使用个人信息等活动进行评价，符合要求后颁发安全认证证书并允许使用认证标识。通过鼓励搜索引擎和应用商店等明确标识并优先推荐通过认证的APP等方式，引导消费者选用安全的APP产品，利用市场机制的引领作用进一步规范APP运营者的研发和推广行为，形成APP领域个人信息保护的长效机制。目前认证试点工作已经启动，首批试点对象包括15家企业的28款APP。

2. 工业和信息化部开展“电信和互联网行业提升网络数据安全保护能力专项行动” “APP侵害用户权益专项整治工作”

236款
整改

56款
通报

3款
下架

工业和信息化部开展“电信和互联网行业提升网络数据安全保护能力专项行动”，从完善制度标准、开展合规性评估、强化社会监督和行业自律等方面综合施策，加快推动构建行业网络数据安全综合保障体系。推动制定网络数据安全标准体系建设指南、数据分类分级、安全评估等30余项重点行业标准。印发行业网络数据安全合规性评估指

引文件，部署全国基础电信企业、50 余家互联网企业及 400 余款 APP 运营者对标开展合规性评估，及时发现整改数据泄露、滥用及违规对外提供等安全隐患，开展企业合规性评估优秀案例征集遴选和示范推广，促进行业提升数据安全保护水平。充分发挥行业组织作用，设立数据安全和个人信息举报专区，受理大量用户投诉举报。

工业和信息化部开展“APP 侵害用户权益行为专项整治行动”，重点整治违规收集使用用户个人信息等 8 类问题行为，推动多款 APP 完成自查整改，对 236 款 APP 运营者下发整改通知书，公开通报 56 款 APP、下架 3 款 APP。

3. 公安部开展“净网 2019”专项行动



公安部深入开展“净网 2019”专项行动，集中整治 APP 违法违规收集使用个人信息行为，健全完善发现、调查、查处、宣传等工作体系和行政执法规范，继续依法严厉打击侵犯公民个人信息违法犯罪行为，共检测评估 3.1 万余款 APP，累计调查核查相关 APP 违法违规线索 3129 条，依法整改 2090 款 APP，依法查处 1121 款 APP，集中曝光 100 款存在违法违规收集使用个人信息行为的 APP。

4. 市场监管总局开展“守护消费”暨打击侵害消费者个人信息违法行为专项执法行动



市场监管总局开展“守护消费”暨打击侵害消费者个人信息违法行为专项执法行动，共立案查处各类侵害消费者个人信息案件 1474 件，查获涉案信息 369 万余条，罚没款 1946 万余元；组织执法联动 4225 次，开展行政约谈 3536 次。

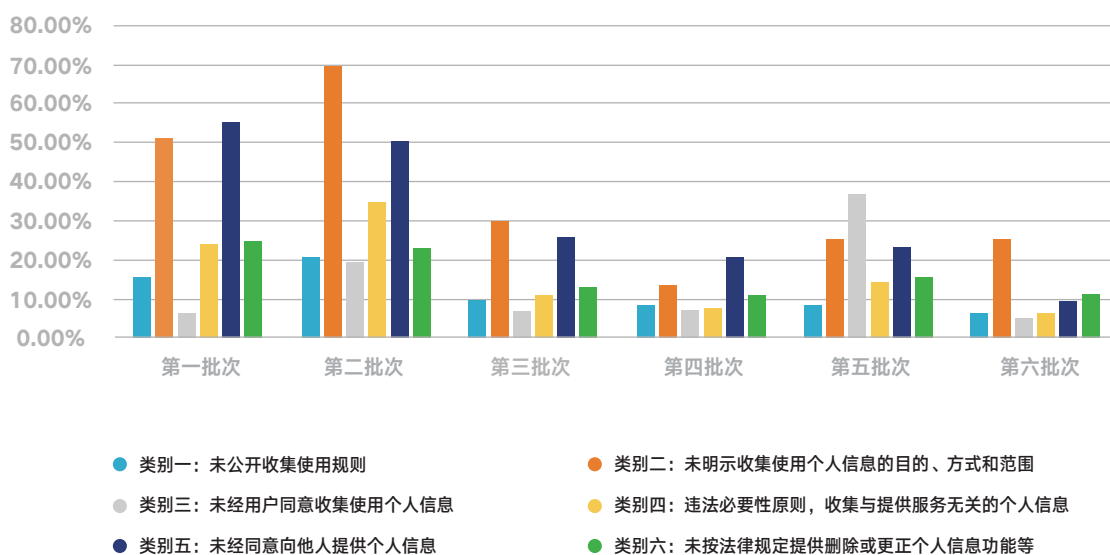
三、2019 年专项治理工作成效分析

（一）评估和举报数据显示，APP 违法违规收集使用个人信息典型问题得到遏制

1. 从千款常用 APP 评估结果看，发现问题比例下降，典型问题整改效果明显

从 2019 年 3 月起，APP 专项治理工作组根据网民举报等情况，分六批次对下载量大、用户常用的千余款 APP 进行了评估。评估发现违法违规收集使用个人信息问题共计 6976 个，向 256 款 APP 的运营者通报问题，督促其完成 1267 个重点问题的整改工作，建议有关监管部门下架未落实整改要求 APP 共 11 款。同时，督促有关 APP 运营者整改的工作还在持续进行。

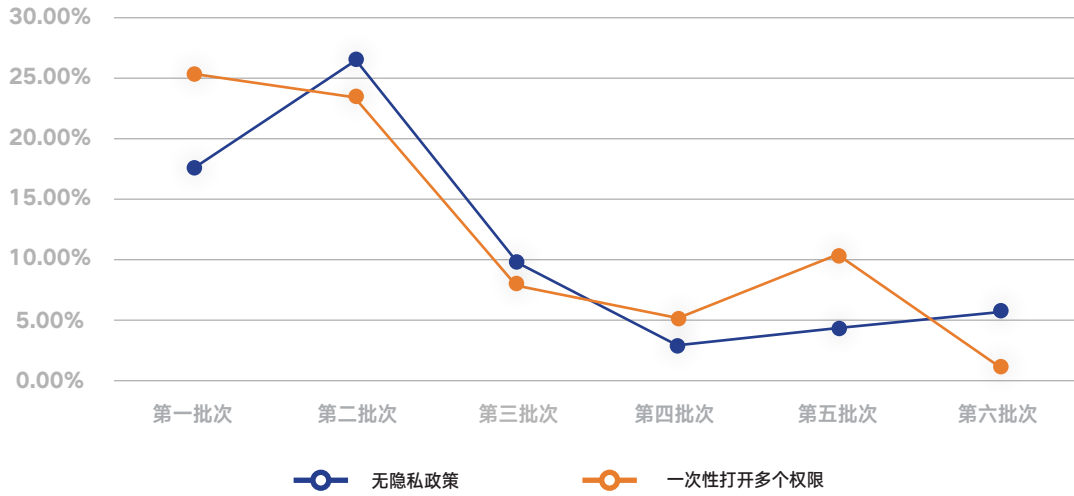
将评估发现的问题分别归入《APP 违法违规收集使用个人信息行为认定方法》中的六类行为，通过六批次评估发现的问题比例总体呈现逐批下降趋势（见图 1）。



▲ 图 1：六批次评估发现问题比例趋势图

随着评估项的进一步细化、评估技术和经验的积累，以及被评估 APP 下载量变化，后两批评估结果显示个别问题的比例有少许增加趋势。因此，为巩固治理成效，还需要继续保持评估、整改力度，防止出现反弹。

针对“无隐私政策”、“一次性打开多个权限”、“收集与业务功能无关的个人信息”、“申请权限未明示目的”四类具体问题，六批次评估中发现的问题趋势如图 2、图 3：



▲ 图 2：“无隐私政策”和“一次性打开多个权限”问题变化趋势



▲ 图 3：“收集与业务功能无关的个人信息”和“申请权限未明示目的”问题变化趋势

从上两张图可以看出，四类具体问题中，“无隐私政策”、“一次性打开多个权限”、“申请权限未明示目的”三类问题降幅明显。下降幅度最大的“一次性打开多个权限”问题是指 APP 将 targetSdkVersion 参数值设置小于 23，进而导致一次性要求用户打开所有申请的可收集个人信息的权限，否则不能安装使用。至 2019 年底，该问题在常用 APP 中已经趋于归零。随着第五批、第六批评估范围的逐步扩大，有个别下载量稍低的 APP 还是存在“无隐私政策”、“申请权限未明示目的”等问题。就“收集与业务功能无关的个人信息”问题来看，由于存在界定“无关”范围的复杂性等问题，该问题目前发现比例较少，且处于波动阶段，应当作为后续治理工作的关注重点。

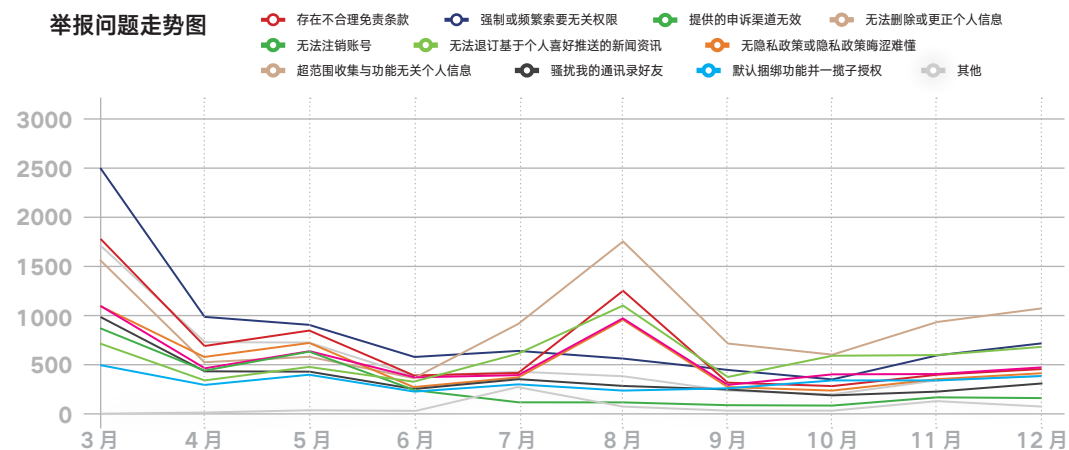
2. 从网民举报内容来看，举报反映问题数量呈现下降趋势

自 2019 年 3 月“APP 个人信息举报”微信公众号开通以来，每月收到有效举报信息数量呈现下降趋势，如图 4：



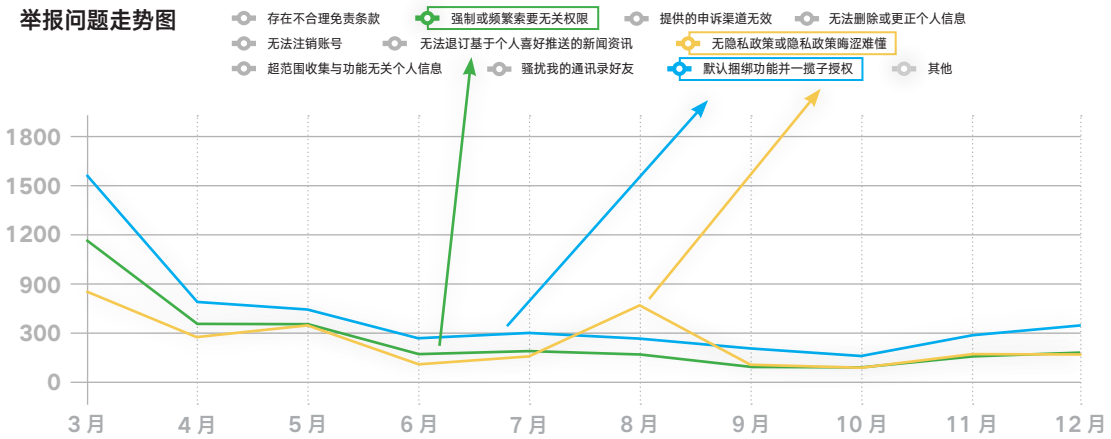
▲ 图 4：“APP 个人信息举报”平台 2019 年月度收到有效举报信息数量走势图

如上图所示，在 5 月、8 月、11 月等涉及通报评估发现问题的时间点，举报数量会出现小幅增长。从举报问题看，2019 年每月收到各类举报问题数量走势如图 5：

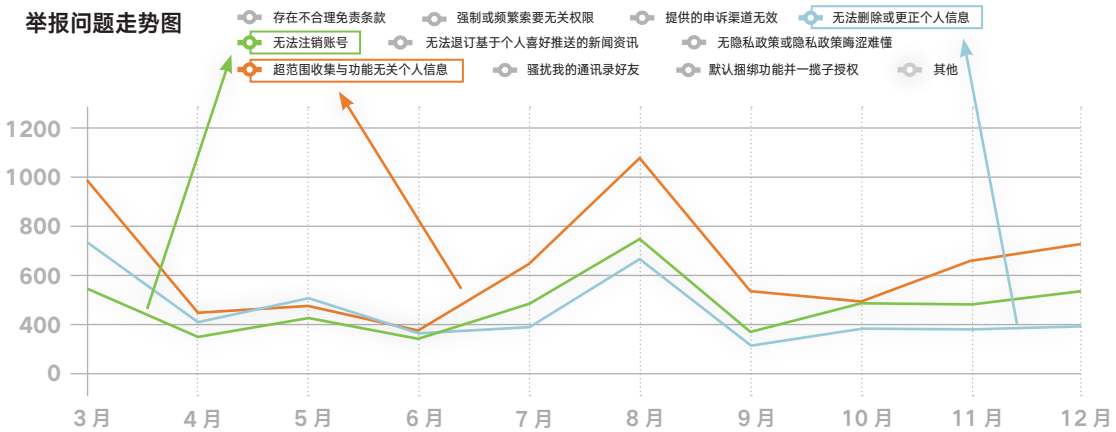


▲ 图 5：不同类型问题举报数量走势图（一）

从举报量较大的“强制或频繁索要无关权限”、“无隐私政策或隐私政策晦涩难懂”、“默认捆绑功能并一揽子授权”、“无法删除或更正个人信息”、“无法注销账号”、“超范围收集与功能无关个人信息”六类举报问题角度，2019年每月举报数量趋势如图6、图7：



▲ 图6：不同类型问题举报数量走势图（二）



▲ 图7：不同类型问题举报数量走势图（三）

从上图可以看出，六类举报问题中，“强制或频繁索要无关权限”、“无隐私政策或隐私政策晦涩难懂”、“默认捆绑功能并一揽子授权”三类问题举报量呈现下降趋势。“无法注销账号”、“无法删除或更正个人信息”、“超范围收集与功能无关个人信息”三类问题举报量呈现波动情形。

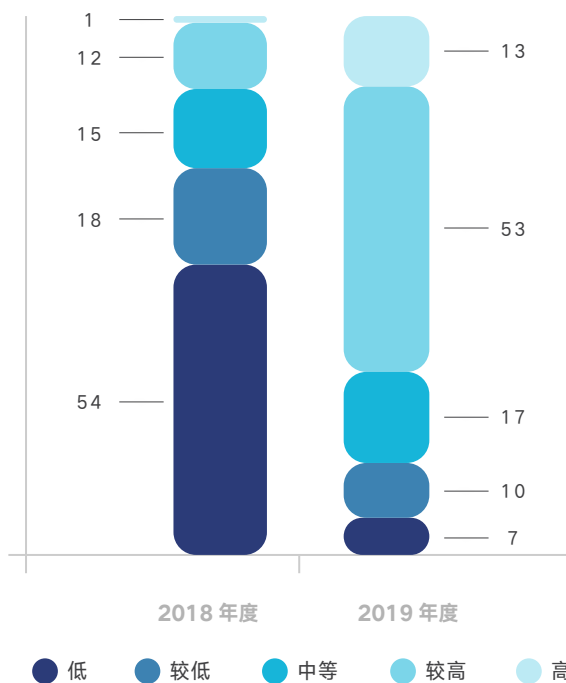
（二）不同时期数据对比显示，企业个人信息保护能力水平显著提升

1. APP 隐私政策透明度数据对比分析

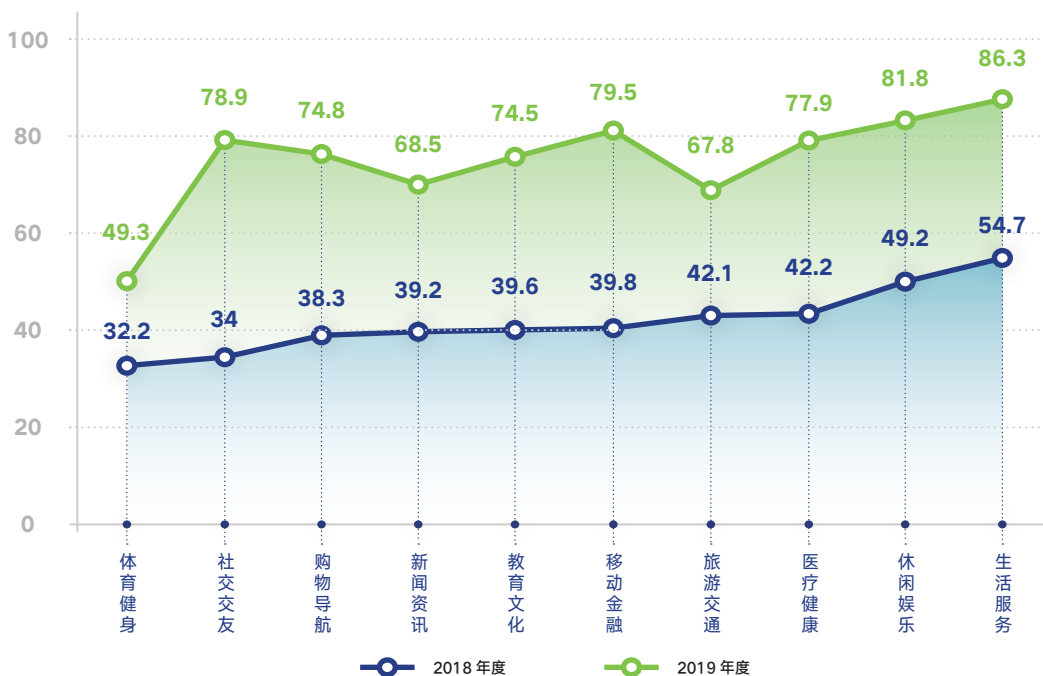
基于研究机构提供的 2018 年、2019 年 100 款 APP 隐私政策透明度评估数据，对比结果如图 8 所示：

隐私政策透明度越高说明其对个人信息收集使用等规则阐述更清晰，从上图得知，2019 年度 100 款 App 的隐私政策透明度较 2018 年度有大幅提升，平均分从 41.1 分跃升为 73.93 分，2019 年度隐私政策透明度评分为“高”、“较高”的 APP 占比相比上一年增加了 52.5（根据图 8）百分点。

如图 9 所示，从 100 款 APP 所在的 10 个行业来看，2019 年度隐私政策透明度得分有显著的提高，分差最小的体育健身类也上升了 17.1 分。其中得分显著提高的是社交交友类和移动金融类，均上升了 40 分左右。



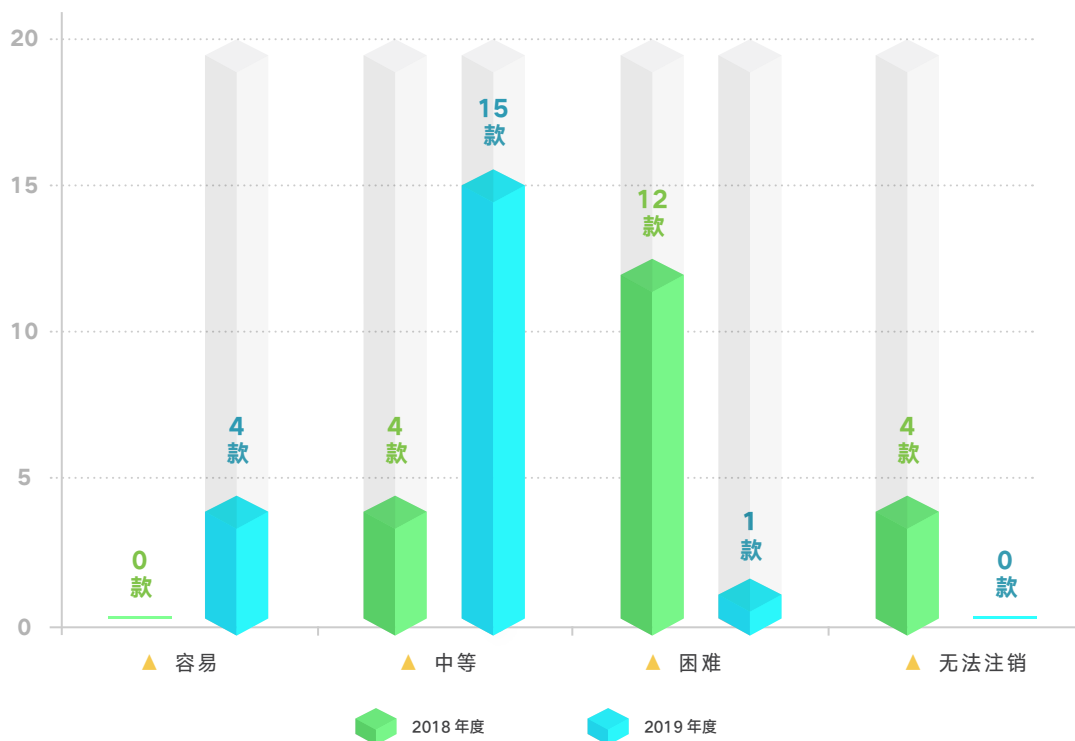
▲ 图 8：2018 年度和 2019 年度 APP 隐私政策透明度分布图



▲ 图 9：2018 年度和 2019 年度十个行业隐私政策平均得分对比图

2. APP 账号注销难易度数据对比分析

基于研究机构提供的 2018 年、2019 年 20 款 APP 账号注销难易度测评数据，对比结果如图 10 所示：

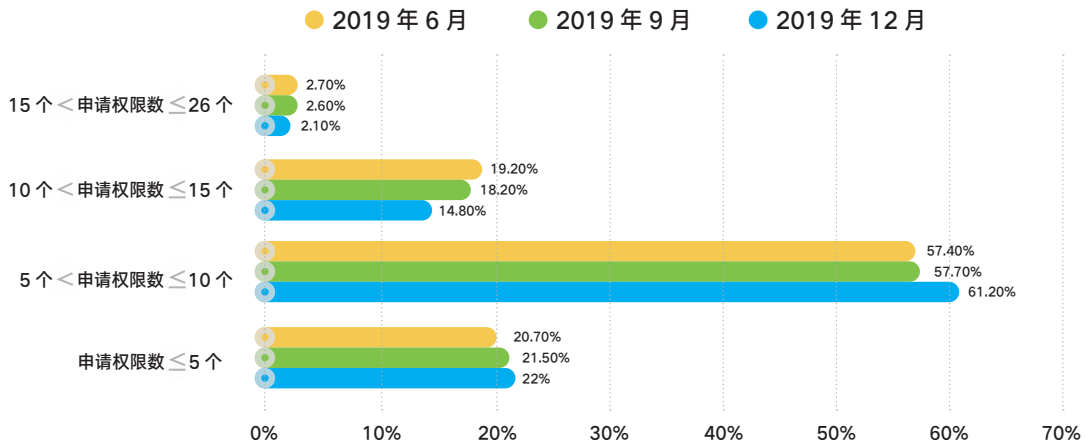


▲ 图 10：2018 年度和 2019 年度 APP 账号注销难易度对比图

从上图可以看出，2018 年，有 16 款 APP 账号注销分布在“困难”和“无法注销”区间，而 2019 年仅有 1 款 App 账号注销为“困难”，其他难易度为“容易”或“中等”。

3. APP 申请可收集个人信息权限数据对比分析

以 26 个可收集个人信息权限为基数，分别在 2019 年 6 月、9 月、12 月对随机抽取的 1000 款 APP 申请可收集个人信息权限数所占比例进行对比（见图 11），发现自 2019 年 6 月至 2019 年 12 月，1000 款 APP 申请的可收集个人信息权限数在不断下降。其中 50 款 APP 申请可收集个人信息权限数从大于 10 个降低到 10 个以内。至 2019 年底，1000 款 APP 中，超过 80% 的 APP 申请权限数少于 10 个。



▲ 图 11：1000 款 APP 申请可收集个人信息权限数量占比对比图

（三）媒体报道和问卷调查反映，专项治理初见成效

1. 主流媒体报道显示，APP专项治理成效显著，网民网络安全感总体提升

新华社在“改陋习、强保护、防隐患——移动互联时代，我们这样打赢个人信息保卫战”报道中提到，《2019 全国网民网络安全感满意度调查统计报告》显示，网民网络安全感总体提升，个人信息保护成热点。法制日报评论“APP 专项治理需要进一步明确细则”中提到，通过半年多的治理，成效明显，但还需相关部门制定科学合理、可操作性强的实施细则确保治理的长效化、制度化。科技日报“APP 这些越线行为现在管得更严了”一文中提到，目前下载量大的主流 APP 强制索取通讯录权限的情况已经基本消失，治理已见成效，网民个人信息的有效举报数量下降，但用户安全意识仍较淡薄。经济日报“《个人信息安全年度报告（2019）》显示：APP 专项治理成效明显”报道中提到，开展 APP 违法违规收集使用个人信息专项治理以来，APP 注销难、强制索权等问题得到明显改善。



▲ 图 12：媒体部分报道页面

2. 万份问卷调查显示，过半受访者认为 APP 个人信息安全状况有所好转

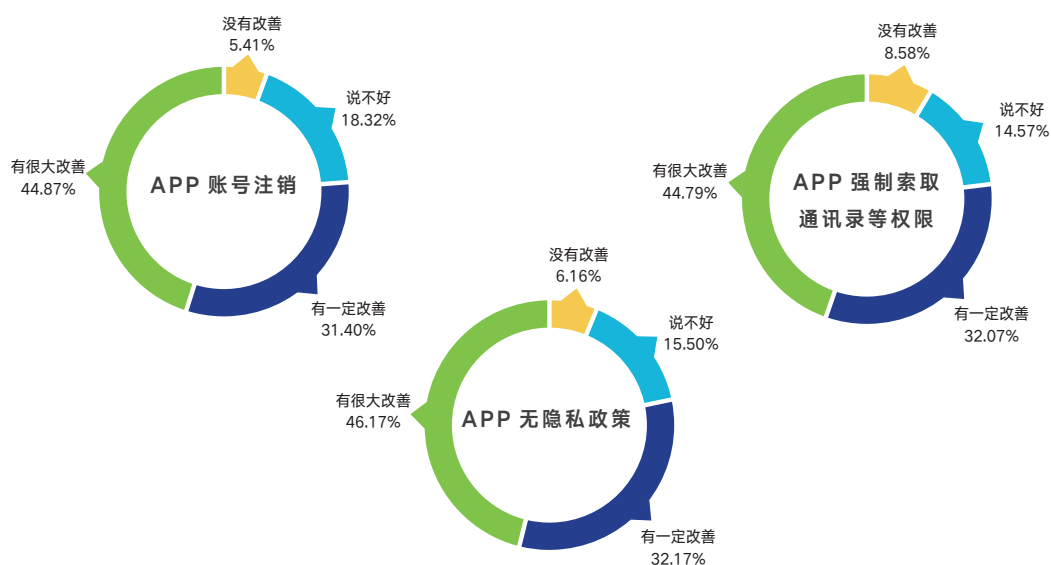
万份问卷调查显示，过半数（50.19%）的受访者认为 APP 违法违规收集个人信息情况有所好转，32.83% 的受访者认为 APP 个人信息收集问题得到了普遍重视和关注，16.98% 的受访者认为 APP 个人信息收集的状况变化不大（见图 13）。



▲ 图 13：万份问卷调查结果（一）

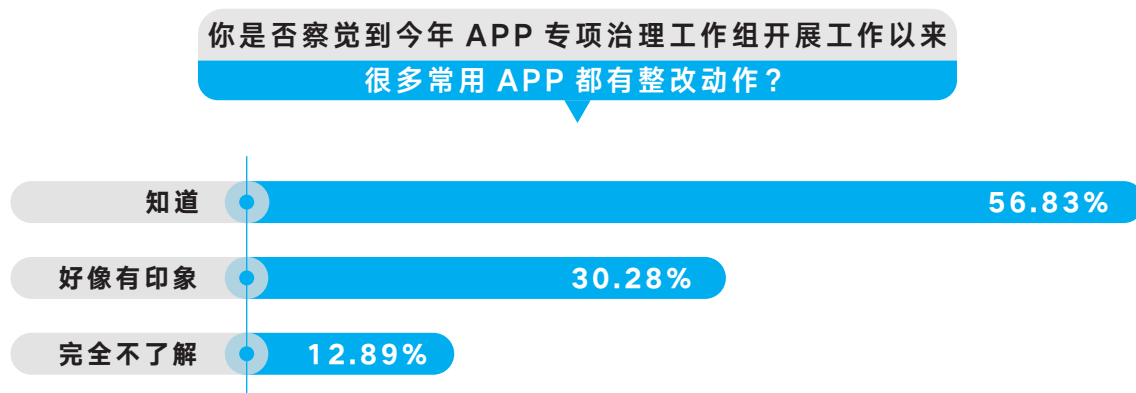
具体到一些典型个人信息保护问题，超七成受访者认为，2019 年以来 APP 账号注销问题（76.27%）、强制索取通讯录等权限问题（76.86%）、无隐私政策问题（78.34%）均有所改善（见图 14）。

【你认为今年以来，以下问题有所改善吗？】



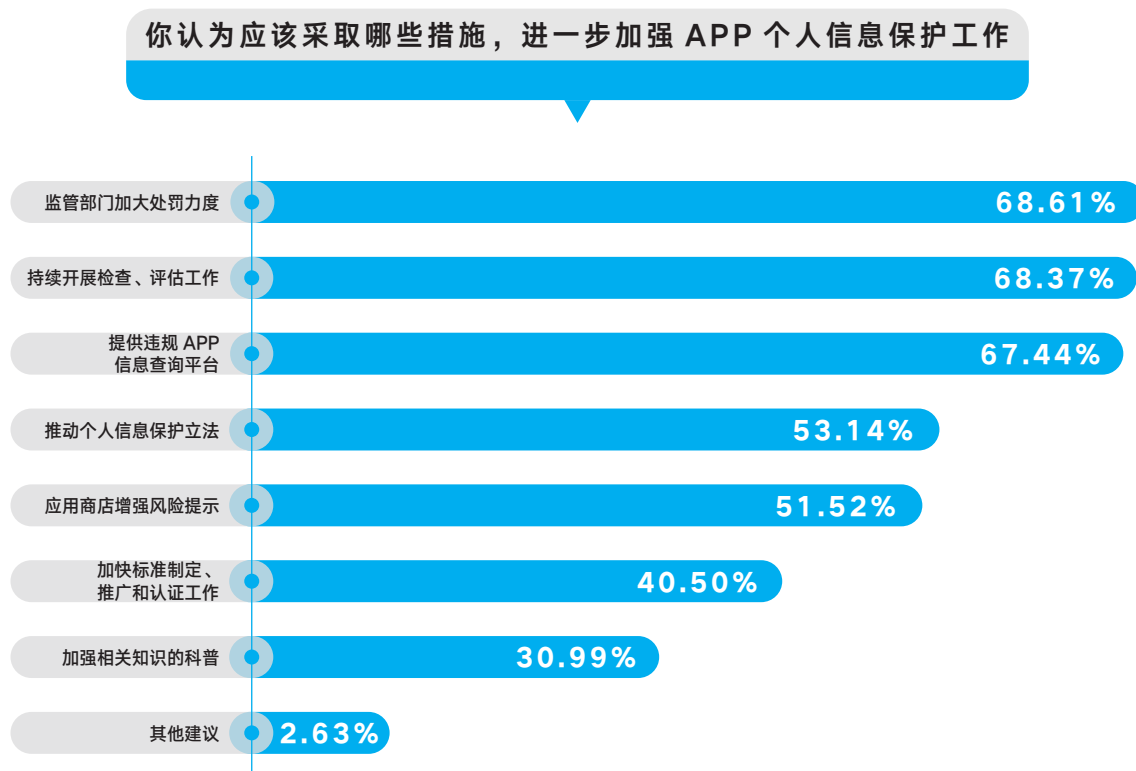
▲ 图 14：万份问卷调查结果（二）

在谈及切身体验时，超八成受访者表示察觉到 2019 年以来，常用 APP 都有整改动作（见图 15）。



▲ 图 15：万份问卷调查结果（三）

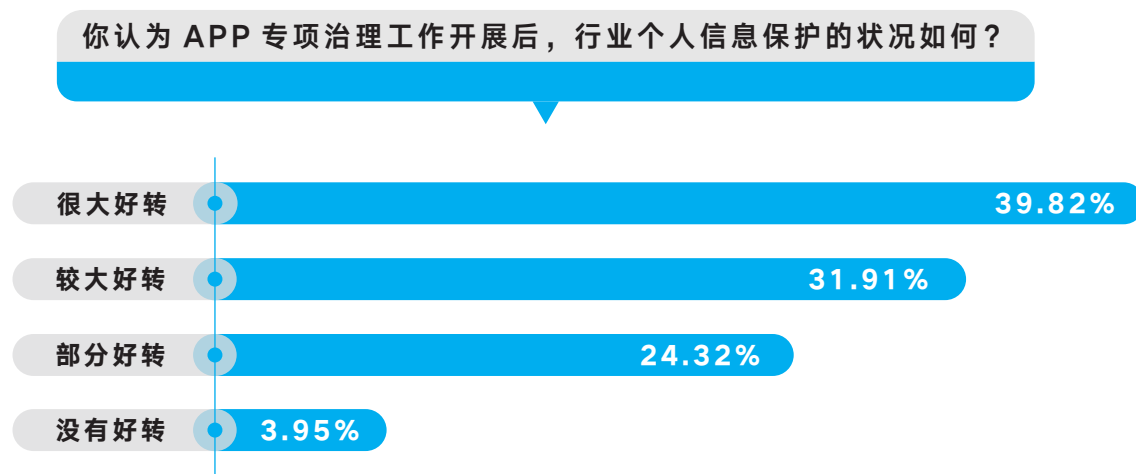
在谈及对加强 APP 个人信息保护的建议时，受访者普遍支持采取措施加强监管，包括监管部门加大处罚力度（68.61%），持续开展检查、评估工作（68.37%），提供违规 App 信息查询平台（67.44%），推动个人信息保护立法（53.14%），应用商店增强风险提示（51.52%），加快标准制定、推广和认证工作（40.50%）等。调查结果如图 16 所示：



▲ 图 16：万份问卷调查结果（四）

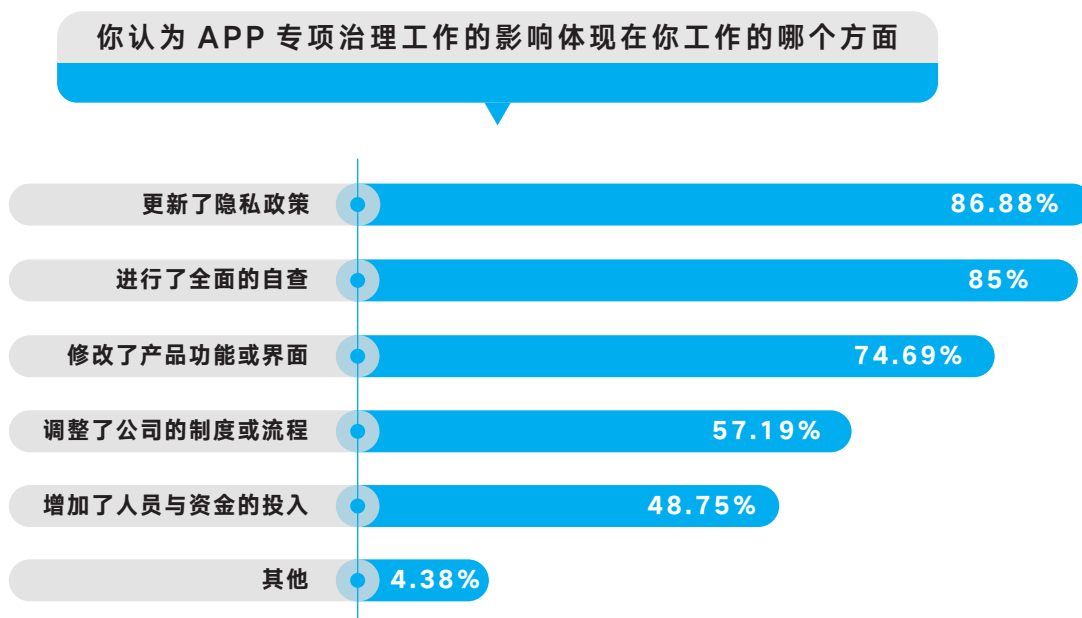
3. 对 APP 运营企业和相关机构调研发现，APP 专项治理工作受到积极关注和响应

调研结果(见图 17)显示,逾九成受访企业和机构表示行业个人信息保护状况有好转。



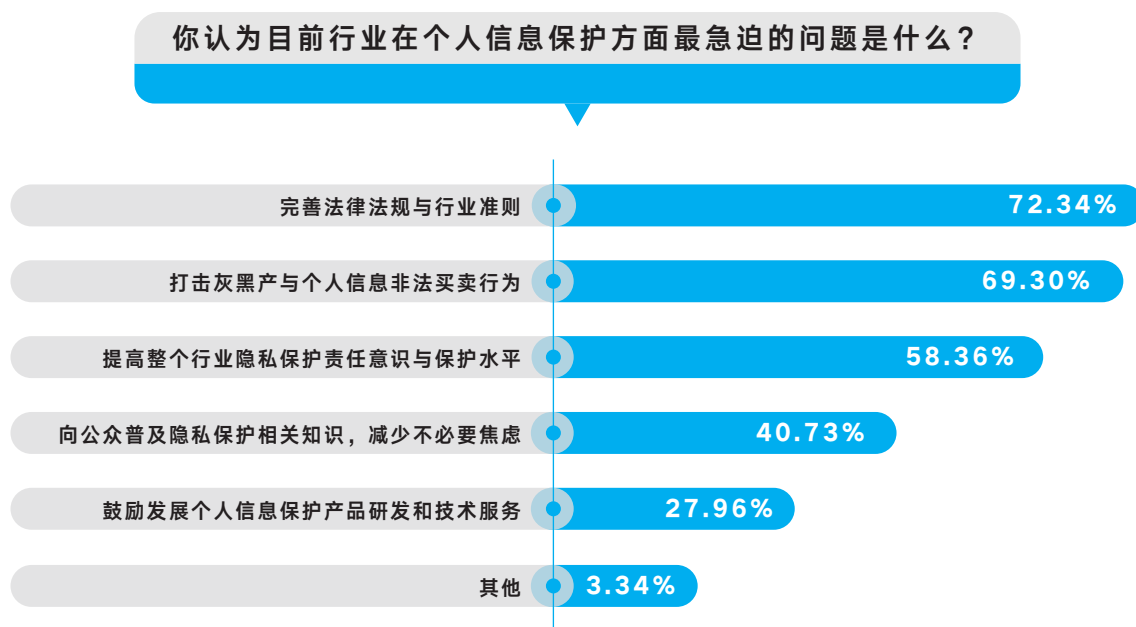
▲ 图 17：代表性 APP 运营企业和机构调研结果（一）

就 APP 专项治理工作响应来看，逾八成受访企业和机构表示更新了隐私政策，并根据专项治理工作发布的技术文件进行了全面的自查。调研结果如图 18 所示：



▲ 图 18：代表性 APP 运营企业和机构调研结果（二）

同时，逾八成受访企业和机构表示 APP 专项治理工作发布的技术文件指导性强，对工作帮助较大。逾七成受访企业和机构表示最急迫的问题是完善法律法规与行业准则，打击灰黑产与个人信息非法买卖行为次之，接近六成受访企业认为整个行业亟待提升个人信息保护责任意识与保护水平。调研结果如图 19 所示：

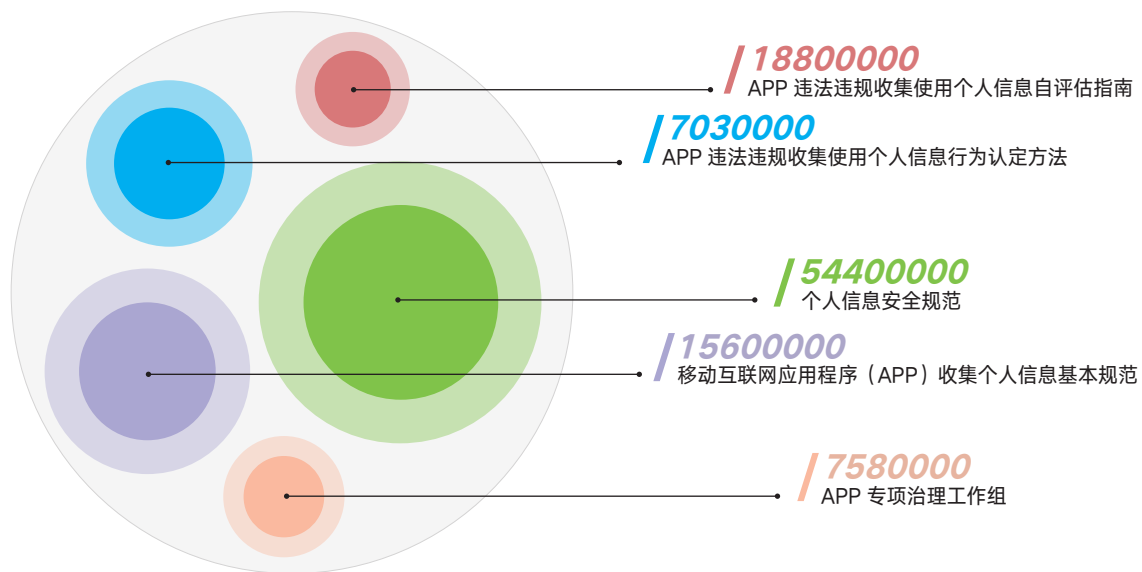


▲ 图 19：代表性 APP 运营企业和机构调研结果（三）

（四）APP 个人信息保护相关技术文件、科普知识等得到广泛传播，全社会关注和重视的氛围已基本形成

1. APP 专项治理工作发布的相关技术文件，被多方广泛应用

以“APP 专项治理”相关关键词进行搜索发现，包含“APP 专项治理工作组”关键词的网页约 758 万个，资讯页面约 19.8 万个；《APP 违法违规收集使用个人信息行为认定方法》相关结果约 703 万个，相关资讯约 37.1 万篇；《移动互联网应用程序 (APP) 收集个人信息基本规范（征求意见稿）》相关结果约 1560 万个，相关资讯约 56.7 万篇；《APP 违法违规收集使用个人信息自评估指南》相关结果约 1880 万个，相关资讯约 16.7 万篇；《个人信息安全规范》相关结果约 5440 万个，相关资讯约 104 万篇。



▲ 图 20：APP 专项治理工作技术文件等关键词搜索结果

自专项治理工作开展以来，网信、工信、公安、市场监管等多个部门在开展个人信息保护相关监管执法行动中也参考了专项治理工作发布的各类技术文件；消费者协会、互联网协会、网络空间安全协会、互联网金融协会、网络文化协会等多类社会组织，以及各大应用商店、平台型应用厂商等均在相关工作中引用、参考相关技术文件；专项治理工作发布的各类技术文件已经逐步成为各行业、各领域开展 APP 个人信息保护工作的“统一标尺”。

2. 专项治理工作频繁推出技术研究报告，广泛传播个人信息保护科普知识，受到多方点赞

专项治理工作通过微信公众号“APP个人信息举报”发布APP个人信息保护相关研究报告、科普文章、专题调研等，向APP运营企业和机构解读个人信息保护合规要点，向公众普及正确的个人信息保护知识，提升网民个人信息保护意识及防范技能。截至2019年12月，“APP个人信息举报”公众号共发布文章70余篇，总计阅读量达30万，与40余家微信公众号进行合作，文章被其它微信公众号转载达500余次。

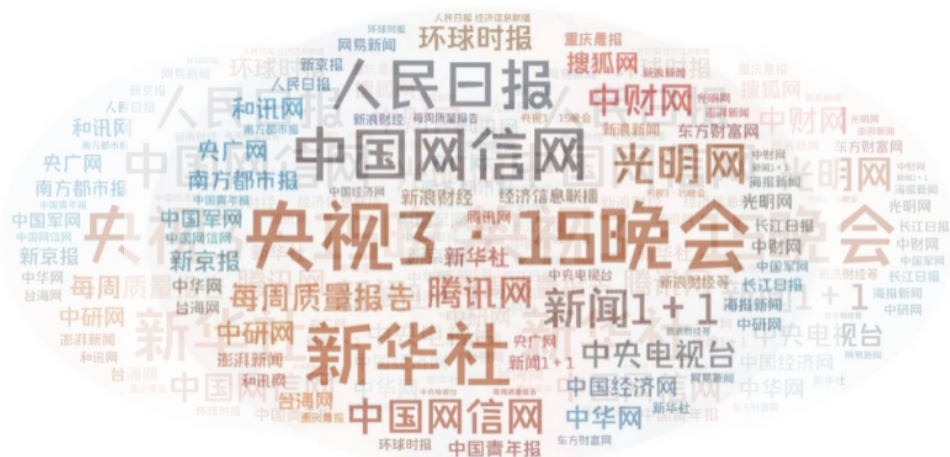
2019年9月，国家网络安全宣传周网络安全博览会在天津梅江会展中心举办。由APP专项治理工作组主办的“APP个人信息保护展”首次亮相国家网络安全宣传周，展会期间，工作人员与广大观众进行科普互动，良好的互动成效成为本次展览的一大亮点。



▲ 图 21：“APP个人信息保护展”亮相国家网络安全宣传周

3. 媒体普遍关注专项治理工作，个人信息保护成为全民热议话题

APP 专项治理工作组配合央视在“3·15”晚会上曝光“社保掌上通”APP 违法违规收集个人信息行为后，国内主流应用商店及时下架该款 APP，有效震慑了违法违规行为。APP 专项治理工作组多次配合新华社、人民日报、中央电视台、环球时报等主流媒体解析 APP 个人信息保护问题和工作进展；光明网采访了 APP 专项治理工作组相关负责人，负责人就开展 APP 违法违规收集使用个人信息评估工作答记者问，中国经济网、澎湃新闻、新浪财经等二十余家媒体进行转载报道；南方都市报、新京报记者就民众关心的隐私泄露隐患等问题对话 APP 专项治理工作组专家，新浪新闻、搜狐网、网易新闻、腾讯网等十余家网站进行转载报道；除此之外，央广网、中华网、中研网、中财网、中国青年报等几十家网站和媒体都对 APP 专项治理相关情况进行了报道。治理工作期间发布的公告、通报名单、问题清单等多次进入微博等媒体热搜榜，阅读量超过亿次。



▲ 图 22：专项治理工作受到媒体广泛关注

四、持续开展专项治理工作的建议

APP 专项治理工作取得了一定成效，在治理过程中，通过开展技术文件制定、检测评估等工作摸清了个人信息收集使用现状，加深了对问题成因的了解。就当下个人信息保护工作面临的挑战，以及下一步如何持续开展专项治理工作，提出以下简要分析和建议，供各方参考。

1. 举报受理和检测评估工作有待持续开展

从专项治理举报受理和检测评估工作发现问题规律来看，问题下降趋势有减缓和波动的迹象。究其原因，一是评估工作对象逐步从头部企业 APP 向中小型企业 APP 扩展，中小型企业个人信息保护方面整改力度不足；二是典型问题经过曝光、整改后，剩余问题成为治理工作“深水区”，在问题识别、评估、判定等方面的研究和积累还需进一步加强。因此，持续开展评估将是巩固治理工作成效，推动广大 APP 运营者持续重视个人信息保护工作，切实提升个人信息保护水平的有效措施。同时，针对一些新业态、新模式、新问题，还有必要通过评估的方式及时发现隐患，督促 APP 运营者进行整改完善。

持续开展评估工作，首先需要成熟的体系文档作为支撑。从完善技术规范体系角度看，在《APP 违法违规收集使用个人信息行为认定方法》基础上，可进一步制定对典型、难点问题的评估认定相关内容进行细化解读的技术文件；从指导评估实施角度看，制定评估操作指南、实施细则等文件将有助于规范评估过程；从评估机构管理角度看，制定评估机构技术能力评价、评估人员能力评价等文件将有助于提升评估质量。

其次，持续开展评估工作，离不开专业的评估技术团队。调研发现，由于个人信息检测评估工作开展时间比较短，现阶段具备足够技术能力的评估技术力量远远达不到当前数百万量级 APP 检测评估的需求。建议一方面，鼓励从事网络安全服务的组织机构开展 APP 收集使用个人信息相关的检测评估技术研究和社会化服务，壮大产业生态；另一方面，加强相关国家标准、技术规范等的宣贯工作，加强对从事 APP 检测评估工作机构、人员的管理和能力认定。尤其是当下，可借助贯彻落实《APP 违法违规收集使用个人信息行为认定方法》的契机，广泛开展交流、沟通、培训等工作。

2. 治理关注范围有待扩展至移动全生态

治理工作中发现，APP 个人信息保护问题不仅与 APP 自身有关，还涉及移动设备生产商（手机厂商）、APP 分发平台（应用商店）、第三方（第三方 SDK、合作伙伴）等多方主体，是一个复杂的移动生态问题。

一是从 APP 的运行机制来看，APP 要运行于特定的移动设备之上，而 APP 开发的设计理念、权限分组分级、权限申请机制等受制于移动设备操作系统。其中，Android 操作系统可由各移动设备生产商在 Android 开源项目基础上进行自身硬件设备的优化开发。就硬件设备操作系统层面，建议倡导国内硬件设备生产商在对 Android 系统进行优化时，依照国内法律法规要求，参考国家标准等技术规范，贯彻隐私设计理念，开发用户隐私保护友好型移动设备操作系统。

二是从 APP 的开发过程来看，APP 开发时嵌入第三方封装的软件开发工具包（SDK），可迅速获得第三方提供的广告、支付、统计、推送、社交网络、地图、定位等方面的功能，以满足相互协作、能力共享、信息互通的需求，不用“重复制造轮子”，大幅度提高开发效率，降低开发成本，因此，使用第三方 SDK 已经成为移动生态的重要组成部分。但同时，SDK 自身的安全性，以及其收集使用个人信息行为，也成为移动生态中个人信息保护的风险点。专项治理在对 APP 评估过程中，发现第三方 SDK 存在收集使用个人信息规则不明、涉嫌超范围收集个人信息等诸多问题。建议加快研究制定我国 SDK 个人信息保护标准和指南，将 SDK 收集使用个人信息行为纳入专项治理范围，以促进 SDK 行业加强数据收集使用规范性。

三是 APP 上线前通常需要通过 APP 分发平台（应用商店）的上线审核，但调研发现，目前国内尚缺乏应用商店对 APP 个人信息安全方面审核的统一要求和标准。根据现有法律法规等相关要求，应用商店对其上架的 APP 应建立审核管理机制，对 APP 进行安全、内容、服务等方面的审核。但由于应用商店之间存在激烈的市场竞争关系，在没有法律法规、国家标准等对应用商店上架的 APP 的审核提出详细、一致标准的情况下，应用商店出于竞争考虑，对 APP 的审核尺度不一，导致无法保证上架的 APP 在个人信息保护方面均达到一致的安全水平。建议通过研究制定应用商店在个人信息保护方面的 APP 上线审核、管理标准，强化对问题 APP 的筛查，避免问题 APP 被下载使用。同时，专项治理工作还可探索与应用商店进行联动的方法，如在投诉举报、问题评估、督促整改等方面形成高效反馈机制。

综上，从移动全生态视角开展治理工作，将进一步巩固和提升治理工作成效，同时，形成良性的淘汰机制提升 APP 整体安全水平。

3. 持续监督技术能力有待进一步加强

构建切实有效的持续技术监督能力是长期巩固治理效果，培育良好移动生态，推动安全与发展相统一，切实维护民众利益的重要举措。尤其是随着技术的快速发展，没有扎实的技术手段作为辅助，监督效果可能会大打折扣。

一方面，从检测评估情况来看，有的 APP 在过度收集个人信息时使用加密数据包，有的 APP 对测试环境进行识别，以规避检测工具发现其异常传输行为，还有的 APP 绕过移动设备操作系统权限控制机制，采用读取外部存储区方式获取设备唯一标识符。当 APP 使用上述方式，现有检测手段发现超范围收集个人信息问题和举证的难度会加大不少。因此，进一步加强深度检测技术研究，才可能在后续持续监督的过程中占据主动权，有效震慑违法违规行。同时，建议加强与该领域研究能力突出的高校、科研院所、企事业单位的合作，形成科研成果，并在相关检测工作过程中予以转化，提升检测效率和质量。

另一方面，建议结合已有评估工作经验，归纳 APP 违法违规收集个人信息的行为特征，研究权限申请使用、收集个人信息频率、数据包流量、数据包涉及的 IP 地址数量、嵌入第三方插件数量等自动化监测指标，建立监测技术手段迅速定位存在涉嫌违法违规收集使用个人信息行为的 APP，以便于进一步开展检测评估和监管执法。建议充分利用产业力量，加大 APP 个人信息保护技术手段研究，推动建立 APP 技术检测平台，提升自动化检测水平，为 APP 监测、监督检查、溯源取证和违法处置等工作提供有效支撑。同时，还可研究监测技术平台与应用商店等的联动机制，在 APP 上线、更新、使用等阶段高效、动态监测 APP 是否存在“可疑”行为，通过警示、阻断等方式，防止“可疑”APP 被用户下载使用，预防个人信息被过度收集、滥用等风险，有效保障个人权益。

4. 治理工作模式有待创新和发展

据统计，主流应用市场有近 400 万款 APP，虽然专项治理工作已经对下载量大、用户常用的 APP 进行评估和督促整改，但与 APP 总量相比差距很大，现有评估力量难以应对；且 APP 更新频繁、可更新热补丁等特点导致传统监管手段存在滞后性，创新治理工作模式成为迫切需求。

一是建立众测机制和队伍，壮大社会监督力量。APP 数量大、更新快等特点为开展监督管理工作带来了困难，广泛调动社会监督力量可以有效弥补不足，推动 APP 运营者自律，促进移动生态良性发展。首先，可结合其他领域众测和已有检测评估经验，研究建立 APP 违法违规收集使用个人信息行为的众测技术方法、管理方式、运营模式和系统平台。其次，可结合人才培养、技能培训等需求，优先动员网络安全一流学院、优秀网络安全企业参与众测等工作，持续打造专业人才梯队，推进社会化服务体系建设，引导个人信息保护技术创新发展。

二是打造权威发布渠道，广泛传播专业声音。APP 个人信息安全相关事件频发且造成不良影响，受到媒体和公众强烈关注。但此类事件发酵过程中缺少专业角度的解读、评论，因此出现了一些片面、误读的声音，既对监管部门依法有序处理相关安全事件带来干扰，也不利于向用户传递正确的个人信息保护观念、知识、技能。因此，打造权威、专业的个人信息保护方面的发布渠道，通过对热点事件的分析，迅速形成科学、理性的解读、评论，及时响应网民和社会关切，将对协助监管部门开展后续监管活动，指导企业及时改进，降低事件影响，有效保护个人权益起到积极推动作用。

附件一

《关于开展 APP 违法违规 收集使用个人信息专项治理的公告》

近年来，移动互联网应用程序（APP）得到广泛应用，在促进经济社会发展、服务民生等方面发挥了不可替代的作用。同时，APP 强制授权、过度索权、超范围收集个人信息的现象大量存在，违法违规使用个人信息的问题十分突出，广大网民对此反映强烈。落实《网络安全法》《消费者权益保护法》的要求，为保障个人信息安全，维护广大网民合法权益，中央网信办、工业和信息化部、公安部、市场监管总局决定，自 2019 年 1 月至 12 月，在全国范围组织开展 APP 违法违规收集使用个人信息专项治理。现将有关事项公告如下：

一、APP 运营者收集使用个人信息时要严格履行《网络安全法》规定的责任义务，对获取的个人信息安全负责，采取有效措施加强个人信息保护。遵循合法、正当、必要的原则，不收集与所提供无关的个人信息；收集个人信息时要以通俗易懂、简单明了的方式展示个人信息收集使用规则，并经个人信息主体自主选择同意；不以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得违反法律法规和与用户的约定收集使用个人信息。倡导 APP 运营者在定向推送新闻、时政、广告时，为用户提供拒绝接收定向推送的选项。

二、全国信息安全标准化技术委员会、中国消费者协会、中国互联网协会、中国网络空间安全协会，依据法律法规和国家相关标准，编制大众化应用基本业务功能及必要信息规范、APP 违法违规收集使用个人信息治理评估要点，组织相关专业机构，对用户数量大、与民众生活密切相关的 APP 隐私政策和个人信息收集使用情况进行评估。

三、有关主管部门加强对违法违规收集使用个人信息行为的监管和处罚，对强制、过度收集个人信息，未经消费者同意、违反法律法规规定和双方约定收集、使用个人信息，发生或可能发生信息泄露、丢失而未采取补救措施，非法出售、非法向他人提供个人信息等行为，按照《网络安全法》《消费者权益保护法》等依法予以处罚，包括责令 APP 运营者限期整改；逾期不改的，公开曝光；情节严重的，依法暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。

四、公安机关开展打击整治网络侵犯公民个人信息违法犯罪专项工作，依法严厉打击针对和利用个人信息的违法犯罪行为。

五、开展 APP 个人信息安全认证，鼓励 APP 运营者自愿通过 APP 个人信息安全认证，鼓励搜索引擎、应用商店等明确标识并优先推荐通过认证的 APP。特此公告。

中央网信办
工业和信息化部
公安部
市场监管总局
2019 年 1 月 23 日

— | 附件二 | —

关于印发《APP 违法违规 收集使用个人信息行为认定方法》的通知

各省、自治区、直辖市及新疆生产建设兵团网信办、通信管理局、公安厅（局）、市场监管局（厅、委））：

根据《关于开展 APP 违法违规收集使用个人信息专项治理的公告》，为认定 APP 违法违规收集使用个人信息行为提供参考，落实《网络安全法》等法律法规，国家互联网信息办公室、工业和信息化部、公安部、市场监管总局联合制定了《APP 违法违规收集使用个人信息行为认定方法》。现印发你们，请结合监管和执法工作实际参考执行。

国家互联网信息办公室秘书局

工业和信息化部办公厅

公安部办公厅

市场监管总局办公厅

2019 年 11 月 28 日

《APP 违法违规收集使用个人信息行为认定方法》

根据《关于开展 APP 违法违规收集使用个人信息专项治理的公告》，为监督管理部门认定 APP 违法违规收集使用个人信息行为提供参考，为 APP 运营者自查自纠和网民社会监督提供指引，落实《网络安全法》等法律法规，制定本方法。

（一）以下行为可被认定为“未公开收集使用规则”

- ① . 在 APP 中没有隐私政策，或者隐私政策中没有收集使用个人信息规则；
- ② . 在 APP 首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；
- ③ . 隐私政策等收集使用规则难以访问，如进入 APP 主界面后，需多于 4 次点击等操作才能访问到；
- ④ . 隐私政策等收集使用规则难以阅读，如文字过小过密、颜色过淡、模糊不清，或未提供简体中文版等。

（二）以下行为可被认定为“未明示收集使用个人信息的目的、方式和范围”

- ① . 未逐一列出 APP（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式、范围等；
- ② . 收集使用个人信息的目的、方式、范围发生变化时，未以适当方式通知用户，适当方式包括更新隐私政策等收集使用规则并提醒用户阅读等；
- ③ . 在申请打开可收集个人信息的权限，或申请收集用户身份证号、银行账号、行踪轨迹等个人敏感信息时，未同步告知用户其目的，或者目的不明确、难以理解；
- ④ . 有关收集使用规则的内容晦涩难懂、冗长繁琐，用户难以理解，如使用大量专业术语等。

（三）以下行为可被认定为“未经用户同意收集使用个人信息”

- ① . 征得用户同意前就开始收集个人信息或打开可收集个人信息的权限；
- ② . 用户明确表示不同意后，仍收集个人信息或打开可收集个人信息的权限，或频繁征求用户同意、干扰用户正常使用；
- ③ . 实际收集的个人信息或打开的可收集个人信息权限超出用户授权范围；
- ④ . 以默认选择同意隐私政策等非明示方式征求用户同意；
- ⑤ . 未经用户同意更改其设置的可收集个人信息权限状态，如 APP 更新时自动将用户设置的权限恢复到默认状态；
- ⑥ . 利用用户个人信息和算法定向推送信息，未提供非定向推送信息的选项；
- ⑦ . 以欺诈、诱骗等不正当方式误导用户同意收集个人信息或打开可收集个人信息的权限，如故意欺瞒、掩饰收集使用个人信息的真实目的；
- ⑧ . 未向用户提供撤回同意收集个人信息的途径、方式；
- ⑨ . 违反其所声明的收集使用规则，收集使用个人信息。

（四）以下行为可被认定为“违反必要原则，收集与其提供的服务无关的个人信息”

- ① . 收集的个人信息类型或打开的可收集个人信息权限与现有业务功能无关；
- ② . 因用户不同意收集非必要个人信息或打开非必要权限，拒绝提供业务功能；
- ③ . APP 新增业务功能申请收集的个人信息超出用户原有同意范围，若用户不同意，则拒绝提供原有业务功能，新增业务功能取代原有业务功能的除外；
- ④ . 收集个人信息的频度等超出业务功能实际需要；
- ⑤ . 仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，强制要求用户同意收集个人信息；
- ⑥ . 要求用户一次性同意打开多个可收集个人信息的权限，用户不同意则无法使用。

(五) 以下行为可被认定为“未经同意向他人提供个人信息”

- ① . 既未经用户同意，也未做匿名化处理，APP 客户端直接向第三方提供个人信息，包括通过客户端嵌入的第三方代码、插件等方式向第三方提供个人信息；
- ② . 既未经用户同意，也未做匿名化处理，数据传输至 APP 后台服务器后，向第三方提供其收集的个人信息；
- ③ . APP 接入第三方应用，未经用户同意，向第三方应用提供个人信息。

(六) 以下行为可被认定为“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”

- ① . 未提供有效的更正、删除个人信息及注销用户账号功能；
- ② . 为更正、删除个人信息或注销用户账号设置不必要或不合理条件；
- ③ . 虽提供了更正、删除个人信息及注销用户账号功能，但未及时响应用户相应操作，需人工处理的，未在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）完成核查和处理；
- ④ . 更正、删除个人信息或注销用户账号等用户操作已执行完毕，但 APP 后台并未完成的；
- ⑤ . 未建立并公布个人信息安全投诉、举报渠道，或未在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）受理并处理的。



扫一扫关注公众号 举报违法违规行 了解更多实用讯息