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

版权声明

前　言

移动应用（以下简称“App”）是数字经济下的重要产品。随着移动网络和智能手机全面覆盖，App 种类和数量增长迅猛。从社交到出行、从网购到外卖，从办公到娱乐，App 已全面渗透用户生活，成为大众生活必需品，并因此汇集大量衣食住行、社交关系等用户个人信息。App 逐渐成为承载网络应用和信息数据的核心载体。

App 在满足用户美好数字生活需要，助力消费升级和经济转型发展方面发挥了不可替代的作用，但也暴露出违法违规收集使用个人信息、用户个人信息泄露与滥用等数据安全问题。App 数据安全关乎个体层面的隐私权利保护，产业层面的健康发展，以及国家层面的全球数字竞争力。欧美等移动互联网发展较早的国家，在移动互联网安全制度构建方面已较为领先。近年来，我国也高度重视 App 数据安全与个人信息保护工作，从法规标准、专项治理、企业自律等方面多管齐下，加大治理力度。

本白皮书在研判 App 发展趋势及社会经济影响的基础上，重点分析目前主流 App 存在的数据安全隐患，系统梳理总结国内外 App 数据安全治理现状，最后从政府、企业、行业三个维度研究提出了我国 App 数据安全与个人信息保护综合治理建议，并从用户视角总结提出了用户安全使用技巧。

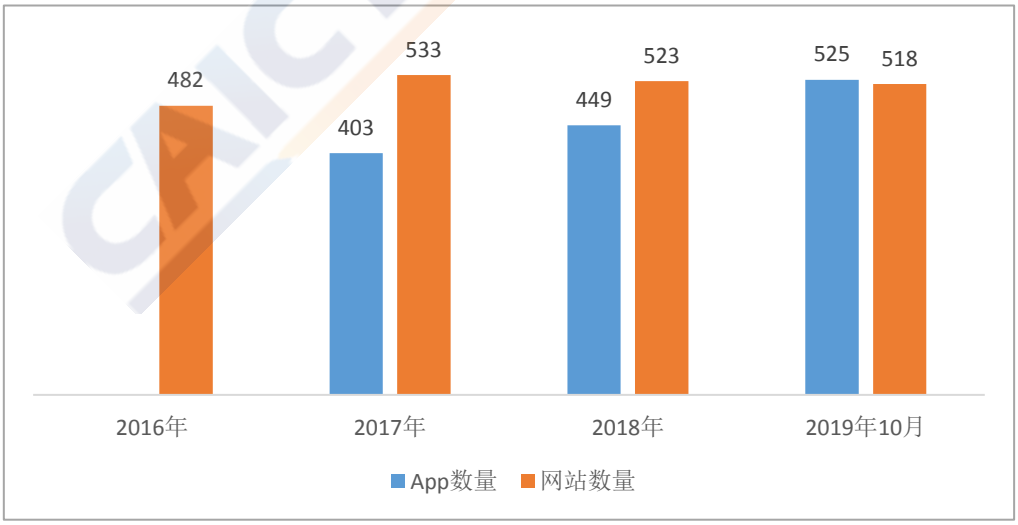
目 录

一、 移动应用（App）发展趋势及影响

（一）移动应用成为互联网服务主要载体

随着移动互联网技术的飞速发展，以智能手机为代表的智能移动终端广泛普及。截至 2019 年 9 月底，三家基础电信企业手机上网用户规模达到 13.04 亿户[1]，普及率超过 90%。移动互联网的持续渗透，直接推动了数字生活的丰富和繁荣，海量用户需求被持续挖掘，移动应用（以下简称“App”）种类和数量持续增长，全面渗透，已成为不可替代的“公共基础软设施”。

从总量上看，App 首次超越网站成为提供互联网服务的主角。近年来，我国 App 数量稳步增长，而网站数量自 2018 年起持续下降。截至 2019 年 10 月，我国本土市场上监测到的 App 在架数量为 525 万款[2]，首次超越我国网站数量 518 万个，传统桌面互联网应用服务已向移动互联网全面迁移。

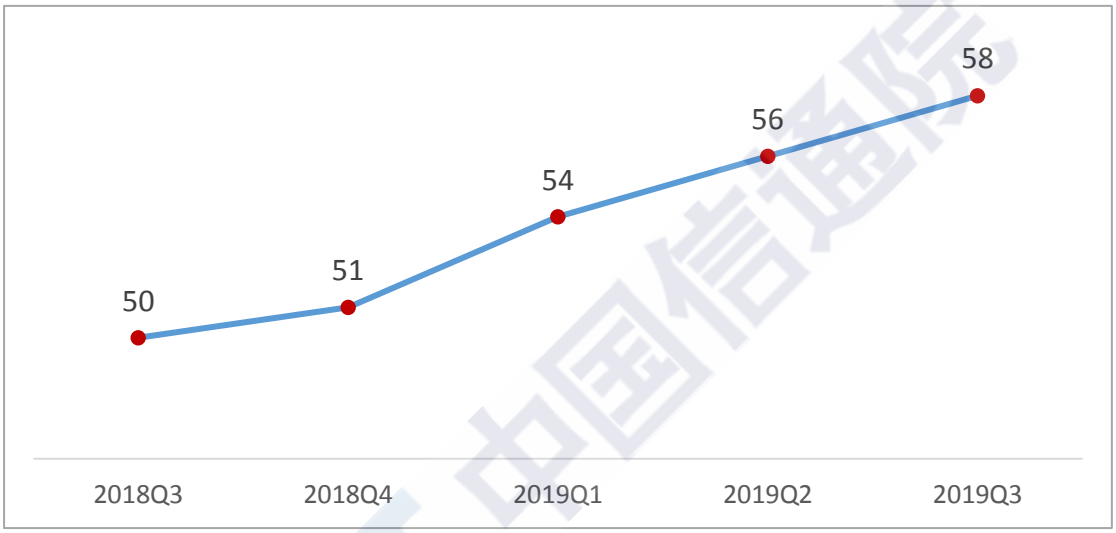


（数据来源：工业和信息化部、CNNIC、爱加密）

图 1 2016-2019 年 App 与网站数量对比

[1] 数据来源：工业和信息化部，《2019 年前三季度通信业经济运行情况》
[2] 数据来源：北京智游网安科技有限公司（爱加密）

从用户使用看，App 成为用户最依赖的互联网入口。用户使用 App 的数量和时长逐年递增，App 成为承载手机用户上网时长的核心。据统计，2018 年我国的 App 下载量将近千亿，其中近 20 款应用下载量过亿[3]，是目前全球 App 下载量最大的国家。2019 年三季度，我国网民人均安装 App 总量增加至 58 款，用户每天花在各类 App 的时间为 4.9 小时[4]，占用户每日上网时长的 81.7%。



（数据来源：极光《2019 年 Q3 移动互联网行业数据研究报告》）

图 2 人均安装 App 的数量增长情况

（二）移动应用引领用户数字生活

网上购物、手机打车、听书、看视频、外卖到家……，App 已经深入渗透进衣食住行等日常生活的方方面面，用户习惯于通过使用 App 解决生活中各类场景需求。在横向覆盖各类功能领域的同时，App 不断深入拓展、发掘不同用户群体的差异化需求，进一步普及数字红利，更好地满足美好数字生活需要。

[3] 数据来源：中国信通院移动应用程序（App）监测平台

[4] 数据来源：QuestMobile《中国移动互联网半年报告》，极光《2019 年 Q3 移动互联网行业数据研究报告》

从应用类型看，App 已实现生活场景全覆盖，形成围绕个人需求的完整消费闭环。截至 2019 年 10 月底，中国信通院安全研究所移动应用程序监测平台上监测到的 App 覆盖 22 种类型，从短视频、游戏、社交为代表的泛娱乐应用拓展到金融理财、旅行交通、健康养生、商务办公、家居服务、教育医疗等生活服务类应用（见表 1），基本实现“一部手机走天下”。社交、搜索、新闻、购物支付等基础应用渗透率都超过 70%[5]，其他细分市场呈现出明显长尾效应。

表 1 App 类型及数量分布

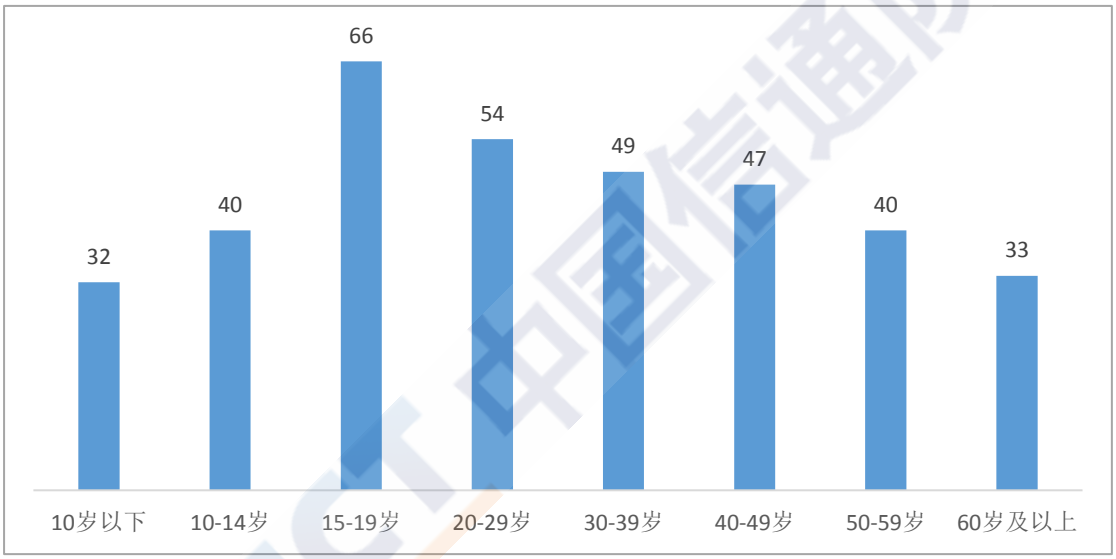
序号	应用类型	App数量（个）	序号	应用类型	App数量（个）
1	游戏	931238	12	健康养生	20077
2	生活服务	137192	13	摄影图像	13963
3	主题美化	78501	14	休闲娱乐	12709
4	影音播放	67638	15	安全保密	8545
5	电子商务	63450	16	手机通信	6913
6	金融理财	47635	17	网络浏览	6554
7	学习帮助	39033	18	文件管理	5808
8	系统工具	38479	19	图形相关	4177
9	网上购物	29274	20	商务办公	531
10	社区交友	26519	21	及时通信	292
11	旅行交通	23517	22	时间日程	66

（数据来源：中国信通院移动应用程序（App）监测平台）

从覆盖人群看，App 基本实现适龄人口全覆盖，并加速向三线及以下城市用户下沉。手机网民年龄分布逐步向两端延伸，14 岁以下青

[5] 数据来源：CNNIC 第 44 次《中国互联网络发展状况统计报告》，极光《2019 年 Q3 移动互联网行业数据研究报告》

少年和 50 岁以上中老年人均手机 App 数量都超过 30 个[6]。除了微信等国民级应用外，中老年人还钟爱理财、购物、广场舞、美颜相机和全民 K 歌等潮流 App。此外，三线及以下市场的潜力和空间正在被发掘，70%左右的三线及以下城市网民刷手机的时间占比都超过一半[7]，娱乐和生活相关的 App 在三线及以下城市发展的新用户更多。阿里巴巴财报显示，截至 2019 年 3 月底，淘宝天猫 1.04 亿移动月活跃新增用户的 77%来自三线城市及以下地区。



（数据来源：CNNIC 第 44 次《中国互联网络发展状况统计报告》，2019.6）

图 3 各年龄段网民人均安装 App 数量

（三）移动应用助推消费提质升级

App 创新活跃、增长迅速、辐射广泛，助推信息消费升级。一方面，App 是拉动流量消费的重要驱动力。App 全场景的使用，大大增强用户粘性，提高用户上网时长，激发了数据流量消费快速攀升。2019 年 1—10 月，通过手机上网的流量达到 995 亿 GB，同比增速仍高达

[6] 数据来源：CNNIC，第 44 次《中国互联网络发展状况统计报告》
[7] 数据来源：企鹅智库，2018 年《中国三四五线城市网民时间&金钱消费数据报告》

85.6%。经测算，2018 年仅微信就带动流量消费 2108 亿元[8]。另一方面，以 App 为载体的信息服务消费规模持续扩大，带动信息消费增长。2019 年前三季度，包括网络音乐和视频、网络游戏、新闻信息、网络阅读等在内的信息服务收入规模达 5660 亿元，同比增长 22.3%，占互联网业务收入比重达 65.8%[9]。

App 作为“连接器”融合线上线下，助力传统消费升级。在信息消费之外，App 覆盖出行、餐饮、购物、酒店、旅游等线下消费场景，传统实体经济的大量商品和服务，通过 App 入口直接与用户对接，提升服务效率，降低交易成本，改善消费体验。在购物领域，据商务部统计，2018 年全国网上零售额突破 9 万亿元，其中实物商品网上零售额 7 万亿元，同比增长 25.4%。在餐饮领域，美团通过 53.1 万日活配送骑手，连接起全国超过 2800 个市县的 3.1 亿年度交易用户和约 440 万年度活跃餐厅。在旅游领域，各大景区或城市与短视频 App 合作打造“网红景点”“网红城市”，带动地方旅游收入增长。

（四）移动应用支撑经济转型发展

App 带动传统产业数字化转型，促进实体经济发展。一方面，以电子商务、数字内容等为代表的大量新应用、新模式、新业态，带动零售、物流配送、文化创意等传统服务业的数字化转型。据国家邮政局统计，2018 年中国快递年业务量突破 500 亿件，自 2014 年开始连续 5 年稳居世界第一。另一方面，App 从消费领域向工业领域快速渗

[8] 数据来源：微信、中国信通院、数字中国研究中心联合发布，《微信就业影响力报告》
[9] 数据来源：工业和信息化部，2019 年前三季度互联网和相关服务业运行情况

透，我国面向工业场景的 App 数量一年增长 7 倍[10]。在工信部印发的《工业互联网 APP 培育工程实施方案(2018—2020 年)》中明确提出，到 2020 年要培育 30 万个面向特定行业、特定场景的工业 App。工业 App 的形成与规模化应用，有利于发挥软件赋能作用，破解企业内部工业技术不足的难题，加速推动制造业转型升级。

App 分布地区聚集效应显著，促进区域经济发展。App 地区分布与总体经济繁荣程度密切相关，从接入地分布情况看，App 主要聚集在北上广等一线城市。中国信通院安全研究所移动应用程序监测平台已监测 100 个重点 App 的接入信息，其中在北京接入的 App 最多，接入数量达到 78 个，其次是广东、天津和上海，接入 App 数量分别是 70、56 和 52 个。以上地区综合优势十分明显，北京、上海、天津也是同期全国人均 GDP 排名前三的省市。这一结果说明，App 的发展已广泛渗透到经济社会各个领域，对各地就业拉动、经济发展起到至关重要的带动作用。

二、 移动应用（App）主要数据安全问题

随着 App 的全面渗透，广大用户却面临着享受便捷化泛在化服务与保护个人信息权利之间的两难抉择。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关注度始终居高不下。截至 2019 年 11 月 4 日，报告团队从应用宝、华为应用市场、小米应用商店等 10 个安卓应用市场选择社交通信、餐饮外卖、地图导航、视频直播、网上购物、网约车、医疗教育等 20 个类

[10] 工信部、北京市政府主办的第二十三届中国国际软件博览会展示

别中下载量大、影响范围广、存在典型问题的 200 余款 App 作为检测对象，共计检测出 1265 项数据安全问题。整体来看：

一是 App 个人信息安全整体问题较多且集中。67%的 App 存在 5 个及以上个人信息安全问题，18.5%的 App 存在 10 个及以上个人信息安全问题。超过四成 App 的问题集中在未公开收集使用规则、未明示收集使用目的、超范围收集个人信息等 5 类。具体情况如下图所示。

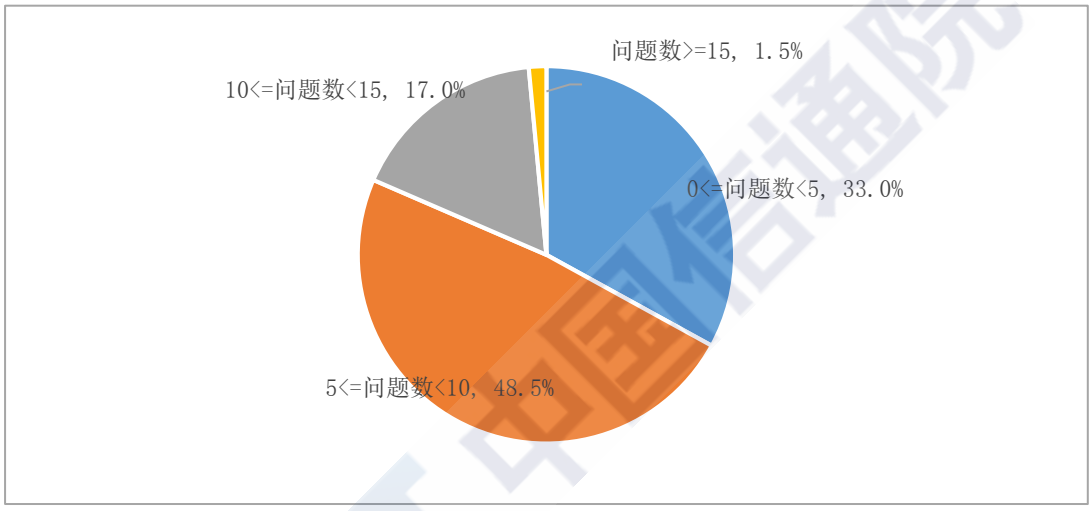


图 4 App 问题数量分布情况

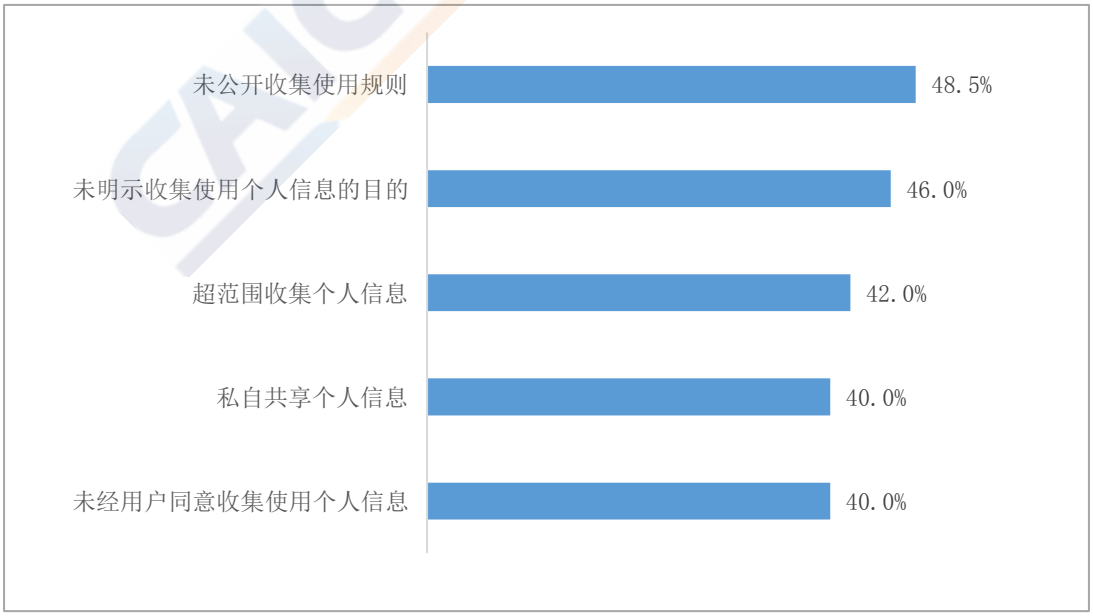


图 5 App 安全检测突出的不合规问题

二是地图导航、医疗健康、安全管理类 App 个人信息安全问题较突出。从业务类别来看，地图导航类 App 个人信息安全问题数量高居首位，平均每款 App 出现 8.4 个问题，医疗健康、安全管理类 App 问题数量位列第二，平均每款 App 出现 8.3 个问题。具体情况如图 6 所示。

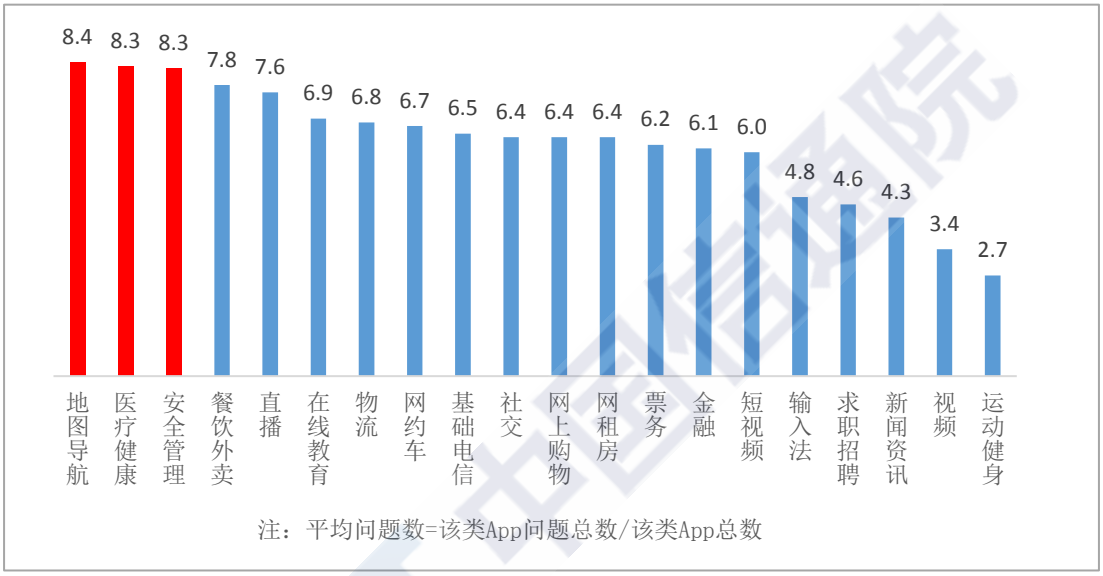


图 6 分业务 App 个人信息安全平均问题数

三是用户数据存储、收集、共享环节安全问题较多。检测工作覆盖用户数据收集、传输、存储、使用、共享、删除等全生命周期关键环节，其中 20.7%的问题属于数据存储环节，20.5%的问题属于数据收集环节，17.1%的问题属于数据共享环节。具体情况如图 7 所示。

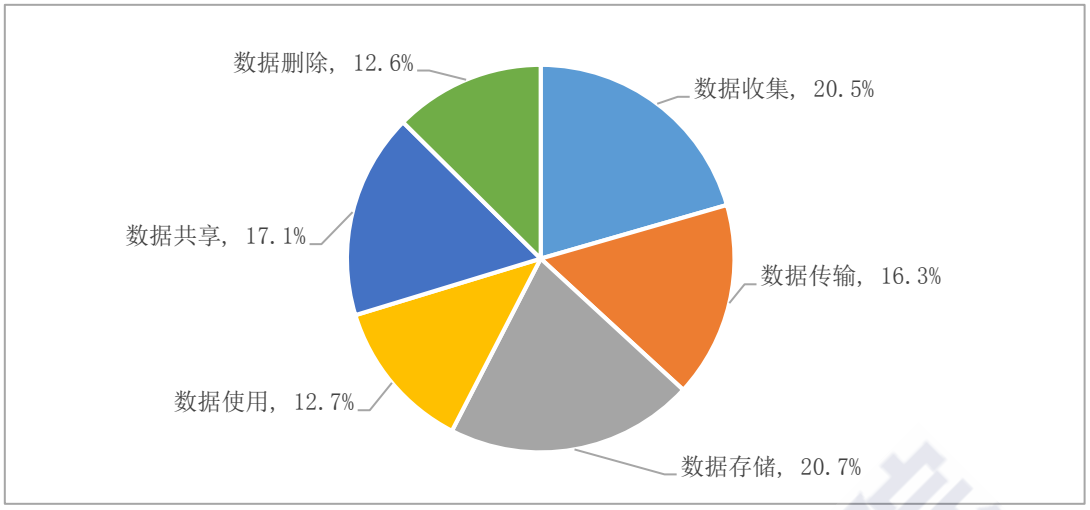


图 7 各环节问题占比情况

基于前述检测和研究，报告团队梳理出当前主流 App 在数据安全与用户个人信息保护方面存在的风险如下：

（一）默示征询个人情况多，存在数据违规收集风险

隐私政策是 App 运营者告知用户个人信息收集规则的主要途径，是保障用户知情权的基础。运营者应在用户首次注册、登录 App 时以弹窗、超链接等明显方式提醒用户阅读隐私政策，以直观的方式告知用户收集使用个人信息的目的、方式、范围，使用户充分了解其个人信息如何被收集、存储、使用、传输、共享、销毁，在知情了解的基础上保护其个人信息安全。

经报告团队检测发现，超过九成的 App 都已具备隐私政策且内容丰富，但是其中超过半数 App 在用户首次登录时向用户默示隐私政策，导致隐私政策难以起到告知作用。63.1%的 App 通过“登录/注册即表示同意隐私政策”的方式强制用户同意，且未提供拒绝选项，用户若想继续使用只能被动同意隐私政策，侵犯了用户自主选择权；

16.9%的 App 在使用过程中仅展示隐私政策但未征询用户同意，违背制定隐私政策的初衷；15.4%的 App 提供了是否同意隐私政策的勾选框，但存在默认勾选问题，在用户不知情的情况下将风险让渡给用户，企图逃避自身责任。具体情况如图 8 所示。

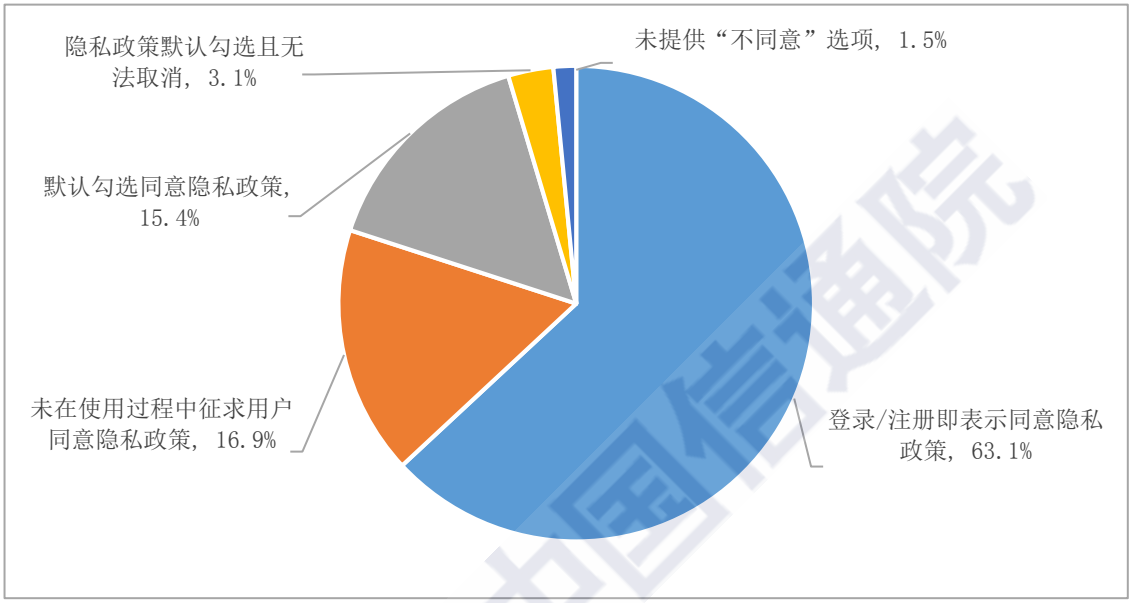


图 8 默示隐私政策各场景占比

与运营者相比，用户在使用 App 时处于信息不对称的弱势地位。若运营者以隐蔽、模糊的方式默示信息收集规则，用户将无法知悉被收集信息的类型、数量以及个人信息的最终流向，失去对其个人信息的知情控制权，大大增加个人信息被违规收集的风险。

（二）过度索取个人权限多，存在数据恶意滥用风险

权限是移动终端操作系统对于 App 运营者收集使用用户个人信息的限制，运营者可通过申请权限的方式获取用户个人信息。为保障用户数据的安全，安卓系统的 App 在默认情况下不拥有任何系统权限。如果 App 运营者因业务功能需要申请权限，应当遵循最小够用原

则，仅收集使用业务功能必需的最少类型和数量的个人信息。App 违法违规收集使用个人信息专项治理工作组于 2019 年 5 月发布的研究报告《App 申请安卓系统权限机制分析与建议》称，绝大部分 App 申请 10 个（含）以下与收集个人信息相关的权限即可满足需要。

经报告团队检测发现，近三成的 App 申请的与收集个人信息相关的权限数量大于 10 个，部分金融类 App 申请权限多达 14-16 个，所收集的个人信息远远超出全国信息安全标准化技术委员会发布的《网络安全实践指南——移动互联网应用基本业务功能必要信息范围》中规定的金融行业 App 的 7 项必要信息，涉嫌超范围获取权限。检测发现“写入外置存储器”权限、“读取电话状态”权限被申请的百分比大于 85%，二者均属于安卓系统中的危险级别权限。拥有“写入外置存储器”权限的移动 App 可以修改和删除设备存储卡中的数据，可能导致用户设备被植入恶意程序；拥有“读取电话状态”权限的移动 App 可以获取设备唯一标识信息和手机通话状态，设备唯一标识信息可关联用户的生活习惯和消费行为，为实施精准诈骗等恶意行为提供数据支持。此外，“拍摄”、“访问粗略定位”、“访问精确定位”、“读取外置存储器”、“录音”等危险权限的申请比例也超过七成。

App 过度索权现象成常态，用户缺少自主选择权，处于要么放弃使用、要么授权的被动地位。过度索取危险权限为违规收集用户个人信息提供了渠道，一旦这些个人信息被不法分子获取滥用，将严重危害用户权益。

（三）明文存储个人信息多，存在数据非法获取风险

数据存储是App运营过程中的关键环节，也是网络黑客攻击窃取数据的切入点，可靠的数据存储为用户个人信息的正常使用提供重要保障。App运营者应在不影响用户终端和服务正常使用的情况下，优先在用户个人终端内存储所收集的个人信息，并采取加密等技术措施确保用户数据即使泄露也难以被破解。

经报告团队检测发现，超过九成的App会在用户终端内存储运行日志、设备信息、用户信息等数据，但其中25%的App存在明文存储用户个人信息的问题。从明文存储的个人信息类型来看，网络身份标识信息占比35.1%，其中主要包括个人信息主体账号以及密码；个人基本资料占比38.6%，主要包括用户手机号、邮箱、生日等信息；精确定位信息占比15.8%，主要包括用户所在位置的经纬度信息。网络身份标识信息被不法分子获取后可直接窃取账号内的全部数据；个人基本资料和精确定位信息被非法获取后，将成为利用人工智能挖掘分析形成用户画像的基础数据，为“大数据杀熟”提供数据支撑，甚至

为恶意欺诈行为推波助澜。具体情况如图 9 所示。

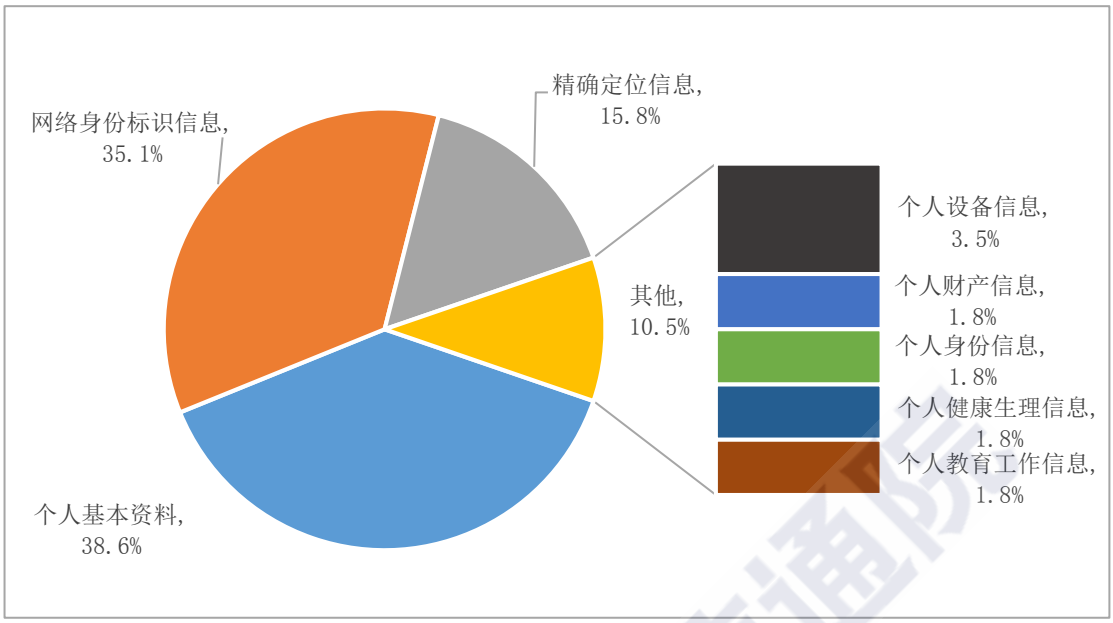


图 9 本地明文存储数据类型占比

运营者本地存储用户个人信息的行为通常在用户不知情的情况下发生，存储的数据往往是使用 App 过程中常用的重要信息。发生数据泄露事件时，若未对存储的数据采取加密等保护措施，用户个人信息将直接被识别利用，降低了不法分子的犯罪难度，极大地增加了用户数据被非法获取利用的风险。

（四）私自共享用户数据多，存在数据恶意散播风险

私自共享是指 App 运营者未经用户同意与第三方共享用户个人信息的行为。运营者应在用户跳转至第三方应用前明示用户其个人信息是否被共享及共享后个人信息的传播路径，同时还应根据共享的个人信息私密程度、安全系数的不同，为用户提供是否同意信息共享及信息共享路径的选择权。

经报告团队检测发现，四成 App 存在跳转第三方应用时，未提醒

用户关注第三方收集使用个人信息规则问题。跳转的第三方应用以金融类和网上购物类为主，占比均为 31%。金融类第三方应用易受病毒感染，恶意仿冒、窃取隐私现象频发，容易导致用户个人敏感信息泄露，甚至造成经济损失；网上购物类第三方应用存在过度使用用户个人信息、追踪用户行为、恶意窃取交易信息等现象，由此引发的骚扰电话、推销广告等行为将严重干扰用户的正常工作生活，甚至影响用户人身和财产安全。具体情况如图 10 所示。

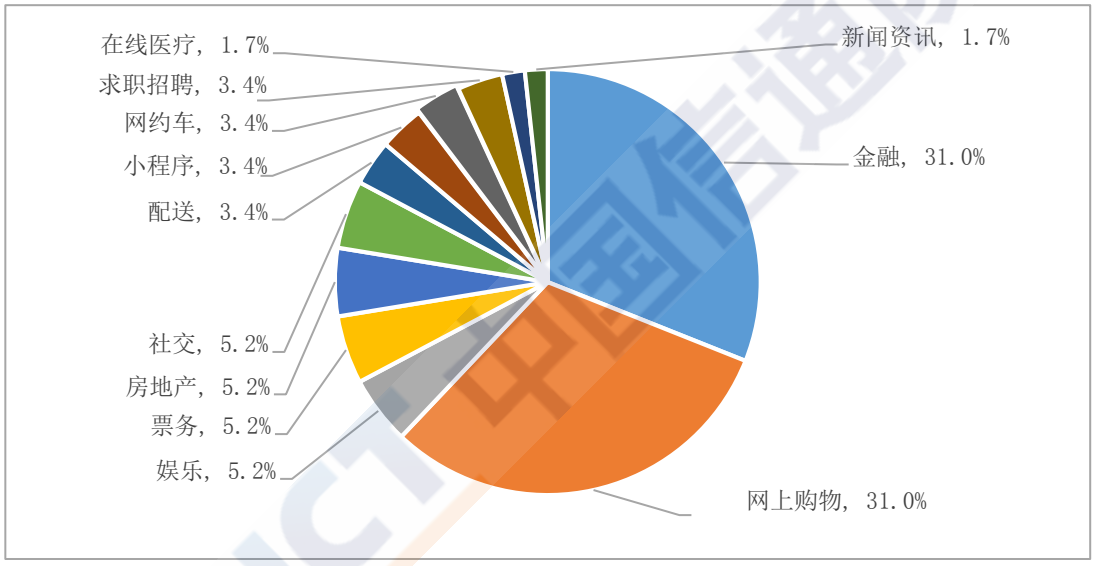


图 10 跳转的第三方应用类型占比

在 App 使用过程中，跳转至第三方应用，在用户毫不知情的情况下使其个人信息被第三方获取，将导致用户无法掌握并控制个人信息的传播路径、使用范围及风险系数，极大增加了用户数据被恶意散播的风险。

（五）设置注销限制条件多，存在数据过度留存风险

账号注销功能是用户自主注销权的重要保障，也是民众关注的热点，中国青年报社调查数据显示，80.2%的受访者存在注销 App 账号

的意愿和需求[11]。《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》等制度标准中明确要求运营者提供注销账户功能。App 运营者应在积极为新用户推广业务的同时，为老用户提供终止业务的便捷途径，避免“注册容易注销难”的现象发生。

经报告团队检测发现，20.5%的 App 未提供注销功能。App 账号常与用户银行卡、身份证等敏感信息相关联，若账号无法注销将导致用户个人敏感信息长期被运营者留存，增大数据泄露风险。26.9%的 App 虽然提供了注销功能，但注销耗时长、流程繁琐，还需比注册时多提交额外非必要的个人敏感信息，如用户真实姓名、住址、邮箱、身份证照片等，且 App 运营者并未明确额外信息在注销后是否会删除。相比简单的注册流程，为用户注销账号设置了大量不合理条件，阻碍用户行使注销权。

用户量是 App 商业价值的重要衡量标准，但由此导致的 App 运营者为提升其市场竞争力而限制用户注销账户的行为，侵犯了用户的选择权、隐私权和平等交易权等权益。无法注销账户或者为完成注销流程需要用户额外提交个人信息的行为，均存在数据过度留存风险。

三、 国内外移动应用（App）数据安全管理现状

（一） 国外移动应用数据安全管理现状

移动互联网应用服务领域的安全问题已经成为了国际社会面临的重大挑战。欧美等移动互联网发展较早的国家，在移动互联网安全制度构建方面也较为领先，已从制度构建阶段步入到深化拓展阶段。

[11] 中国青年报，《75.9%受访者遭遇过 App 账号注销难》

整体来看，欧美等主要国家均通过基础性立法、针对性指导文件、安全审查、行业自律等综合性举措，以个人隐私保护为重点，逐渐加强对 App 的治理和指引。

1、管理制度：完备的基础性数据安全立法奠定监管基础

一是世界主要国家和地区以个人信息保护为切入点，抓紧出台和完善数据安全基础性和行业性法律。截至 2018 年年底，全球近 120 个国家和独立的司法管辖区已采用全面的数据保护或隐私法律来保护个人数据。现有法律法规主要是一般性规定，其中对网络运营者的数据安全保护义务和责任同样适用于 App 服务提供者。如欧盟《一般数据保护条例》(GDPR)，英国《数据保护法案》(Data Protection Act)、瑞典《瑞典数据法案》(Swedish Data Act)、爱尔兰《2018 数据保护法案》、美国加利福尼亚州颁布《加州消费者隐私保护法案》（CCPA）等，都围绕个人数据的收集、使用、保存、分享、转移等，对数据控制者和处理者、数据主体的权利义务进行了全面规定。

二是在移动互联网应用安全专门法规方面，美国也有一些成功探索。2016 年美国发布《应用程序隐私保护和安全法案》，这是第一部全国性的专门规范 App 收集使用用户隐私信息的法案，试图实现用户隐私保护与 App 功能正常之间的动态平衡。法案的内容并没有新颖之处，但是它将专门针对 App 的个人信息保护原则上升到法律的高度，且明确一个强有力的执行机构，能够使该法案的相关规定得到切实执行。

三是通过高压执法、强力处罚推动企业落实法律法规要求。美、

欧等国保护消费者隐私和个人信息最主要的手段就是采取强制执法措施来制止违法行为，并要求企业采取积极整改措施。美国联邦贸易委员会（FTC）已建立两年一次的独立专家评估制度，并针对一系列移动互联网应用隐私问题开展执法行动，通过高罚款、禁止销售运营等强力处罚手段，震慑移动应用提供者。2019 年 7 月，FTC 认为 Facebook 多次使用欺骗性的披露和设置来破坏用户的隐私偏好，且对违反其平台政策的第三方应用程序采取的措施不足，对其处以 50 亿美元罚款。2019 年 10 月，FTC 认为三款 App 未经移动设备用户的知情或同意，监控 App 使用者的移动设备地理位置，损害了消费者的隐私权以及移动设备的安全性，现已禁止其继续推广和销售。

2、管理思路：重视产业链各环节主体的责任落实和协作

针对 App 的独特性，加拿大、美国、欧盟等国家和地区纷纷发布 App 个人隐私保护的指导意见，对 App 产业链上的开发者、应用商店、终端制造商等相关主体提出细化要求。

一是在移动应用开发设计环节即纳入隐私保护要求。2012 年 10 月，加拿大隐私专员办公室发布《移动 App 开发隐私指南》，该指南指出开发者在 App 设计和开发过程中，应如何加强个人隐私数据安全保障。2014 年 9 月澳大利亚信息专员办公室（OAIC）制定《移动隐私：面向移动应用开发者的更好的实践指南》，要求 App 开发公司设置隐私事项专员，在应用的规划设计阶段应进行隐私影响评估(PIA)，并需要有适当的控制措施（例如合同），确保第三方应用合法合规处理个人信息。

二是对于智能终端预置应用数据安全性提出监管要求。2013 年美国加利福尼亚州司法部长发布《手机 App 隐私保护规范》，要求操作系统开发商提供全球性的隐私设置，使手机用户能够控制访问 App 的数据和硬件配置特征，并向 App 开发商提供工具，使其能够综合评价隐私信息的收集、使用和传输情况。韩国未来创造部于 2014 年 1 月发布《关于智能手机预置应用准则》，该准则规定上市的智能手机应保证用户对于预置应用的选择权以及向用户公开预置应用的相关信息。

三是推动移动应用商店加强应用上架前数据安全审核管理。美国《手机 App 隐私保护规范》中明确要求 App 分发平台建立健全审核机制以及投诉举报制度。苹果应用程序商店（App Store）随着 iOS 版本更新和终端类型的增加，持续完善事前审核规则，实行对开发者资质和 App 安全性的双重审核，且审核内容逐步扩大，包括程序中是否使用非公开 API、是否安装或运行其他可执行代码、是否隐蔽调用位置信息及传输用户相关数据等。

3、管理方式：行业组织多管齐下引导行业自律成共识

各国在监管实践中均重视多方治理，通过“政府主导+行业自律”混合模式，充分发挥行业协会、第三方机构和社会公众的作用。目前典型的做法主要有以下几种：

一是通过制定标准指导企业开展自评估。2014 年，美国国家信息安全保障合作组织（NIAP）和美国标准与技术研究院（NIST）分别制定《移动互联网相关保护轮廓》和《移动应用安全审查》，为各行各

业(包括医疗保健)明确了移动应用隐私风险等安全评估审查方法和流程。评估审查主要包括应用测试和应用批准/拒绝两个步骤：应用测试是指利用自动化工具和人员测试软件漏洞，形成漏洞报告和风险评估；应用批准/拒绝是指根据评估报告决定该应用软件是否可用于移动设备。其他国家也同样制定了类似移动应用安全审查验证的标准，比如欧洲网络与信息安全局（ENISA）发布的《智能手机开发者安全开发指引》、日本智能终端安全社（JSSEC）发布的《Android 应用安全设计/安全代码指导》。

二是通过认证或资金奖励鼓励企业加强数据保护。美国建立网络隐私认证计划，通过权威的第三方机构对遵守信息收集规则并服从监督管理的企业颁发认证标志，如果企业违反相关规定侵害用户隐私，将被取消认证，以此督促企业加强对个人信息的保护。美国国内存在多个网络隐私认证组织，其中最有名的是加州个人隐私认证机构“TRUSTe”，目前已为雅虎、微软、苹果等 3500 多家企业网站及 App 提供认证。美国健康信息技术全国协调员办公室（ONC）还用资金奖励的方式鼓励企业对数据保密性进行防护。比如，为了达到 ONC 的数据认证要求并满足特定的政府补助规定，医疗设备制造商必须证明自己能够充分适当地处理用户隐私数据。

二是为用户提供技术软件保护用户个人信息。英国为用户提供先进的个人信息保护软件，让用户掌握保护个人隐私的主动权。当 App 需要收集用户隐私时，该技术保护软件就会主动提示用户并识别即将收集的个人信息类型和内容。用户可评估被收集信息的敏感程度以及

泄露后果的风险，自行决定是否继续使用该 App 的服务。同时，该技术软件还提供设定权限的功能，即允许设置哪些隐私可被收集，以及绝不允许哪些隐私被收集。

三是发布指引引导企业自律，提高用户保护意识。2013 年美国电信和信息管理局（NTIA）发布《关于移动 App 行为准则的倡议》，要求 App 收集和使用用户数据必须向用户明示，以增强 App 的透明性。2013 年美国联邦贸易委员会（FTC）发布报告《手机隐私披露:通过透明度建立信任》，对 App 产业链各主体提出相应建议，并提出行业协会应促进 App 隐私保护政策统一和标准化，并制定标准化图标插入在 App 程序内部，通过该图标用户可以了解隐私政策和保护实践。美国健康信息技术全国协调员办公室（ONC）针对消费者和设备制造商发布了一系列用于移动健康数据保密的资源，包括为移动健康应用设备使用者准备的安装指南，为消费者准备的数据管理软件和为开发者准备的新款升级更新。

（二）国内移动应用数据安全管理现状

数字经济时代，以 App 安全为代表的数据安全关系到个体层面的隐私保护，产业层面的科技竞争、创新和发展，以及国家层面的数据安全和全球数字竞争力。我国高度重视 App 数据安全，已形成以个人信息保护为核心的法律制度框架，各监管部门基于自身职能，以专项行动为牵引，着力开展 App 数据安全管理实践，对企业监督执法力度持续加强。

1、基本建立 App 数据安全和个人信息保护制度体系

一是我国已形成以法律为统领，行政法规、部门规章为支撑的多层级规范体系，适用于包括 App 在内的所有网络运营者。在法律层面，我国有关个人信息的保护要求均纳入刑事、民事、行政三大部门法之中。《网络安全法》以网络空间基本法的形式进一步明确了我国个人信息保护的基本原则和框架，强化网络运营者的保护义务与责任。在法规制度层面，相关部门积极制定细化的规章配合法律落地实施。工信部专门制定《电信和互联网用户个人信息保护规定》，明确细化了行业内电信和互联网用户个人信息的保护范围、用户个人信息收集和使用原则和规则、安全保障措施、监督检查制度等内容。网信办今年 5 月发布《数据安全管理办法（征求意见稿）》，办法中明令禁止 App 强迫授权或默认勾选，要求 App 运营者保障用户注销账号和删除个人信息的权利，对接入 App 的第三方应用应加强数据安全管理。

二是相关部门陆续加强 App 专项管理政策制定。网信办 2016 年 6 月发布《移动互联网应用程序信息服务管理规定》，明确要求移动互联网应用程序提供者应当建立健全用户信息安全保护机制，未向用户明示并经用户同意，不得开启收集地理位置、读取通讯录、使用摄像头、启用录音等功能，不得开启与服务无关的功能，不得捆绑安装无关应用程序。互联网应用商店服务提供者应当对应用程序提供者履行四项管理责任。工信部 2016 年 12 月发布《移动智能终端应用软件预置和分发管理暂行规定》，重点对移动智能终端应用软件预置行为，以及互联网信息服务提供者提供的移动智能终端应用软件分发服务进行规范。今年 9 月，教育部等八部门联合发布《关于引导规范教育

移动互联网应用有序健康发展的意见》，要求教育 App 提供者建立覆盖个人信息收集、储存、传输、使用等环节的数据保障机制，收集使用未成年人信息应当取得监护人同意、授权，不得变相强迫用户授权和过度收集个人信息。

2、加快完善 App 数据安全和个人信息保护配套标准

一是制定多项安全保护技术标准，作为法律法规的重要补充和配套。在国家标准层面，我国信息安全标准化技术委员会（TC260）下已有 22 项数据安全国家标准项目，涵盖安全要求（7 项）、实施指南（8 项）、监测评估（4 项）、基础框架（3 项）等四大类别。其中国家推荐性标准《信息安全技术：个人信息安全规范》已于 2018 年 5 月 1 日正式实施，对个人信息收集、保存、使用、流转等环节提出要求，填补了国内个人信息保护在实践标准上的空白。在行业标准层面，中国通信标准化协会（CCSA）TC8 和 TC11 已陆续发布实施《移动互联网联网应用安全防护要求》、《移动互联网应用商店安全防护要求》、《移动应用软件安全评估方法》等标准，涵盖访问控制、加密存储等部分数据安全保护要求。CCSA TC543“用户个人信息保护标准工作组”发布《电信和互联网服务用户个人信息保护定义及分类》、《电信和互联网服务 用户个人信息保护技术要求 移动应用商店》等系列行业标准，明确 App 用户个人信息保护技术要求。此外，2019 年，CCSA TC8 下成立“数据安全标准特设项目组”，重点推进数据安全行业标准的研制工作。

二是聚焦个人信息保护，App 数据安全标准起草制定工作进入快

车道。2019 年 5 月发布的《信息安全技术网络安全等级保护基本要求》中首次提出了 App 等级保护要求。2019 年 6 月发布的《移动互联网应用基本业务功能必要信息规范》，针对地图导航、网络约车、即时通讯社交、网络支付、新闻资讯、网上购物、短视频等 16 类常用 App 的基本业务功能，清晰界定了保障其正常运行的必要个人信息范围，为其收集个人信息提供实践指引。2019 年 8 月发布的《信息安全技术技术 移动互联网应用(App)收集个人信息基本规范(草案)》，针对 App 收集个人信息方面提出了更加细化的管理和技术要求。相关标准文件的出台，规范了 App 收集、使用、存储、传输、销毁个人信息等数据的各类行为，也为相关机构提供了评估标准和依据。

3、持续强化 App 个人信息保护监督执法力度

一是指导行业机构开展网络产品和服务隐私条款专项评审工作。2017 年，中央网信办与工信部等三部委联合开展个人信息保护提升行动之隐私条款专项工作，指导相关行业机构对微信、微博、淘宝、京东商城、支付宝、高德地图等十余款网络产品和服务的隐私条款进行评审。通过评审和宣传形成社会示范效应，带动行业整体个人信息保护水平的提升。从评审结果来看，十款产品在隐私政策方面均有不同程度提升，做到了明示收集、使用个人信息的规则，并征求用户明确授权，其中个别产品还做到了向用户主动明示并提供更多选择权。

二是四部委联合开展 App 违法违规收集使用个人信息治理专项行动。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组织开展 App 违法违规收集使用个人信息专项治理。目

前专项治理工作取得了阶段性成效，通过对百余款用户投诉量大、社会关注度高的App进行检查评估，发现存在强制授权、过度索权、未经同意收集个人信息和对外提供个人信息等典型问题，并督促企业及时整改。App专项治理工作组陆续发布《App违法违规收集使用个人信息自评估指南》、《App违法违规收集使用个人信息行为认定方法(征求意见稿)》，为App运营者提供自查自纠提供参考。

三是相关部门依法履职开展各类专项行动，强化重点问题整治。2019年7月，工信部印发《电信和互联网行业提升网络数据安全保护能力专项行动方案》，重点任务之一就是组织第三方评测机构开展App数据安全风险滚动式评测，对在网络数据安全和用户信息保护方面存在违法违规行为的App及时进行下架和公开曝光。2019年10月，工信部结合2019年信息通信行业行风建设暨纠风工作安排，开展为期两个月的App侵害用户权益专项整治工作，重点对用户关心的违规收集和使用用户个人信息、不合理索取用户权限、为用户账号注销设置障碍等八类问题进行监督检查和规范整治。公安部组织开展“净网2019”专项行动，组织开展App违法违规采集个人信息集中整治，已依法查处违法违规采集个人信息的App共683款。

4、积极探索App个人信息保护多方共治模式

一是鼓励企业开展自愿性App个人信息安全认证工作。2019年3月，中央网信办、市场监管总局正式发布《移动互联网应用程序(App)安全认证实施规则》，明确认证依据、认证模式、认证流程、认证规则、时限等要求。认证需按照App运营商自愿申请的原则，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、处理、使用个人信息等活动进行评估，符合要求后颁发安全认证证书并允许认证标识。通过鼓励搜索引擎和应用商店优先推荐获证 App 等方式，引导消费者选用安全的 App 产品，提升个人信息保护意识和能力。

二是第三方机构、安全企业探索 App 检测评估服务。中国信息通信研究院等单位积极开展 App 数据安全与个人信息保护检测能力建设。中国信息通信研究院已建设移动应用程序监测平台，实现应用商店及 App 市场发展和接入情况监测、数据安全和诱骗欺诈风险检测，强化对应用商店及 App 巡查监测能力，为行业主管部门开展 App 数据安全监管提供技术支撑。部分安全服务企业也建立 App 测试平台，通过静态检测、动态检测、源码扫描等技术，为企业提供本地数据存储、数据传输、加密安全、第三方 SDK 等方面的安全检测服务。

三是重点地区和业务领域发布 App 行业自律公约。2014 年，为规范 App 发布虚假信息、窃取用户隐私、非法营销等行为，促进行业健康有序发展，北京市互联网协会组织新浪、网易、搜狗、今日头条等 50 余家互联网企业签署《北京市移动互联网应用程序公众信息服务自律公约》，这是国内首个移动互联网应用行业自律公约。2019 年，一起教育科技、科大讯飞、极课大数据、思骏科技等企业共同签署学习类 App 行业自律倡议，在内容审核、商业模式、学生信息安全等方面明确了行业准则，承诺不断提升技术防护能力，及时总结推广成功经验，逐步建立学习类 App 使用管理的长效机制。

四、 移动应用（App）数据安全治理建议

面对当前 App 数据安全治理的严峻形势和用户个人信息保护的强烈需求，我国需要从实际出发，不断完善标准指引，积极研发安全技术，政府、企业、行业组织等多方协同，多管齐下，持续完善以法律法规为准绳、制度指引为方向、监管机制为保障、技术手段为依托、标准评估为支撑的全方位 App 数据安全治理体系。

（一） 政府层面，加快完善数据安全监管体系

一是完善 App 数据安全和个人信息保护制度建设。加快推动《数据安全法》、《个人信息保护法》等相关法律出台，通过立法进一步细化包含 App 运营者在内的企业收集使用用户个人信息的规范。持续推进 App 数据安全和个人信息保护相关标准研制，聚焦工业 App 等新型应用和问题集中的位置导航、外卖等重点应用，结合业务属性和应用特点，制定数据安全技术标准和配套的检测标准。**二是强化跨部门 App 数据安全联动管理。**在前期 App 个人信息专项治理工作基础上，完善行业分管、协同联动的管理模式，对于各行业内 App 数据安全保护工作由行业主管部门负责牵头实施，对于融合领域 App 数据安全保护工作要加强检测实施、通报处置等环节的沟通协同。**三是建立 App 数据安全长效监管机制。**建立 App 数据安全检测和通报常态化机制，及时发现安全隐患，督促整改。进一步扩大监督检查范围，定期开展针对重点移动应用商店和智能终端企业的监督检查，以查促管，督促企业落实平台审核责任。基于隐患整改和投诉举报信息，建立信用监管机制，对存在不良信用记录的 App 重点监管。

（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