



嘉佑安科
JU Safety

2024年上半年

移动应用隐私安全 观测报告

—
2024年7月



厦门嘉佑安科信息技术有限公司

目 录

第一章 全国移动互联网应用分析.....	4
1.1 全国移动应用地域分布情况.....	4
1.2 全国移动应用厂商地域分布情况.....	5
1.3 全国移动应用分发渠道分布情况.....	6
1.4 全国移动应用类型分布情况.....	7
第二章 2024 年上半年通报 App 分析.....	8
2.1 被通报的移动应用总体分布情况.....	8
2.2 被通报的移动应用违规类型分布情况.....	9
2.3 其他被通报移动应用分布情况.....	10
第三章 移动应用隐私合规风险分析.....	12
3.1 移动应用合规检测类型分布情况.....	12
3.2 移动应用功能类型违规次数分布情况.....	13
3.3 移动应用合规检测违规类型情况.....	14
第四章 移动应用安全风险分析.....	16
4.1 移动应用安全检测类型分布情况.....	16
4.2 移动应用安全检测结果概览.....	17
4.3 移动应用安全检测违规类型情况（高风险）.....	18
4.4 移动应用数据跨境目的地分布情况.....	18
第五章 总结与建议.....	20
第六章 公司及产品介绍.....	21

6.1	公司介绍.....	21
6.2	产品介绍.....	23
6.2.1	观澜●隐私安全检测平台.....	23
6.2.2	观辰●隐私安全探针.....	23
6.2.3	观擎●隐私安全态势分析平台.....	24

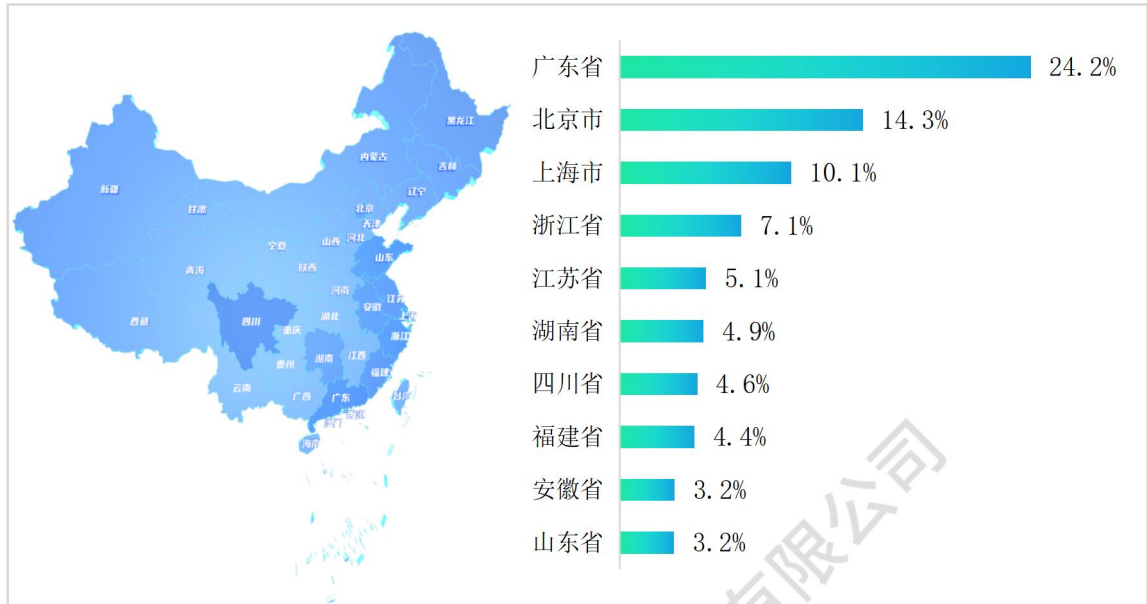
 厦门嘉佑安科信息技术有限公司

第一章 全国移动互联网应用分析

截止 2024 年上半年，厦门嘉佑安科信息技术有限公司收录超 130 万个 App、近 35 万个 App 厂商数据，同时利用观澜•隐私安全检测平台综合对数百个渠道进行实时监测，并基于收录的数据开展深度的数据统计分析。本次观测报告呈现统计分析的结果数据，主要包括移动应用地域分布 Top10 城市、App 厂商集中分布 Top10 城市、App 集中分发渠道排行、App 应用类型分布占比等信息，为监管单位开展 App 隐私合规治理行动提供数据参考，同时让 App 开发者、运营商更清晰产品对社会面影响，加强自身 App 隐私合规意识，提高产品的安全性。

1.1 全国移动应用地域分布情况

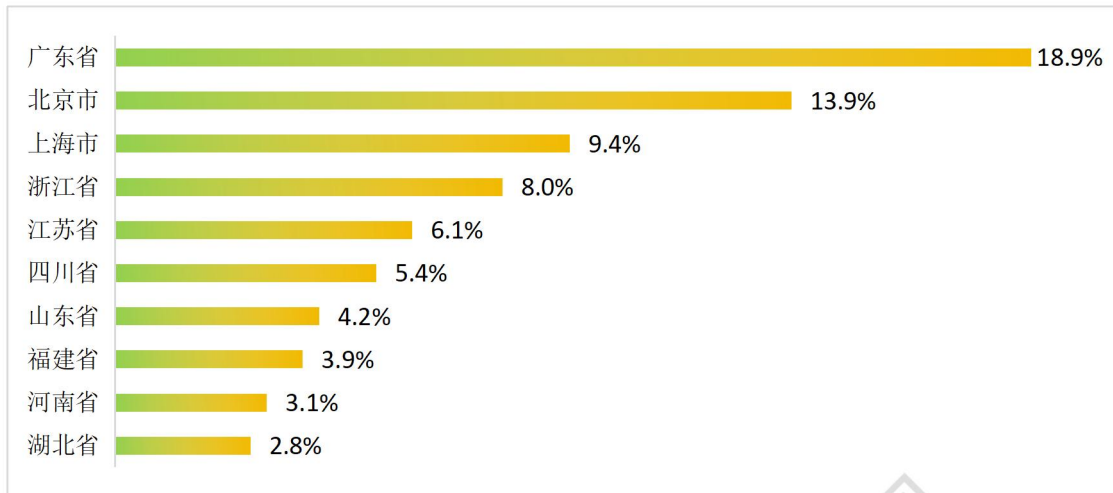
截止 2024 年 06 月 30 日，观澜隐私安全检测平台新收录各类应用超 30 万个。基于收录的应用数据，按照开发商及运营主体进行归属地划分，其中广东省、北京市、上海市所开发的应用数量排在全国的前三，广东省应用数量位居第一，占全国应用总量的 24.2%；其次是北京市，占总量的 14.3%；上海市位列第三，占总量的 10.1%。以下是全国移动应用地域分布 Top10：



全国移动应用地域分布情况 Top10

1.2 全国移动应用厂商地域分布情况

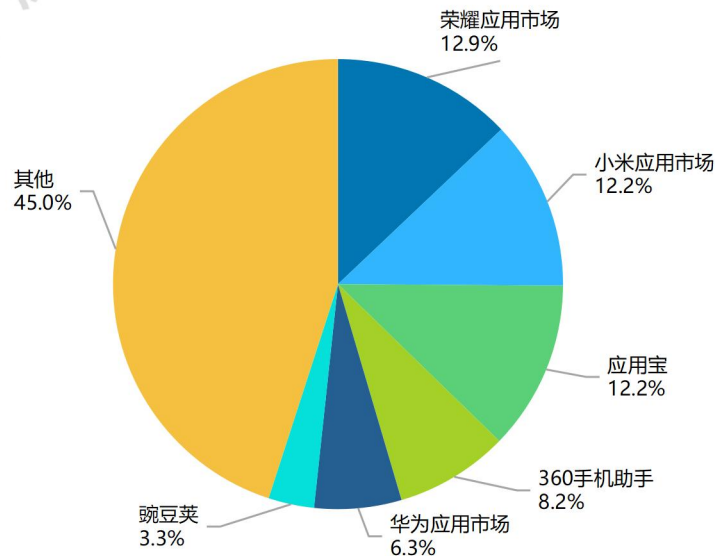
截止 2024 年 06 月 30 日，观澜隐私安全检测平台收录移动应用厂商近 15 万个，其中广东省、北京市、上海市厂商数量排在全国的前三，广东省厂商数量位居第一，占全国厂商总量的 18.9%；其次是北京市，占总量的 13.9%；上海市位列第三，占总量的 9.4%。以下是全国移动应用厂商地域分布 Top10：



全国应用厂商地域分布情况 Top10

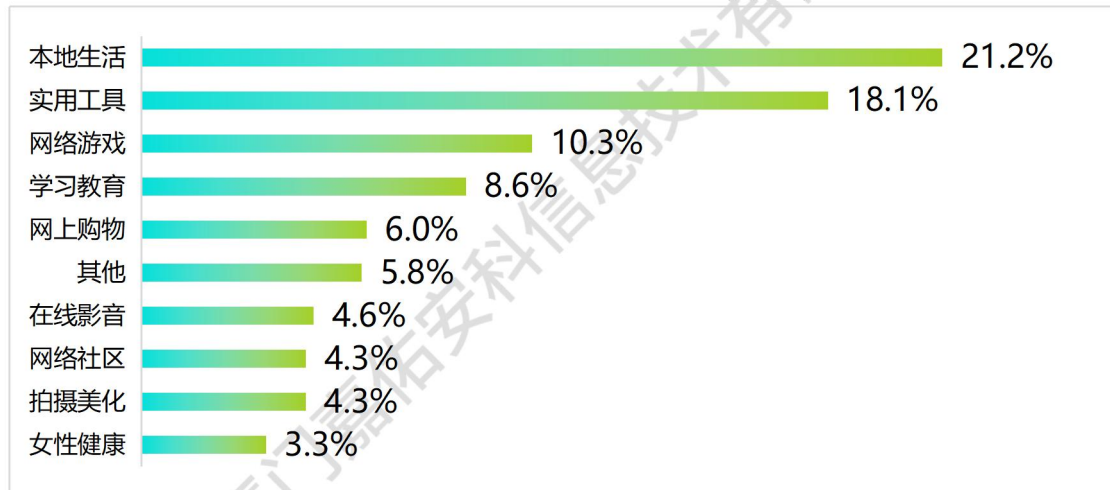
1.3 全国移动应用分发渠道分布情况

截止 2024 年 06 月 30 日，观澜隐私安全检测平台对数百个渠道进行实时监测，从第三方应用市场、手机厂商应用市场、web 下载站等应用市场中收录更新应用的数据，其中应用数量最多的是荣耀应用市场，占应用数量总量的 12.9%；其次是小米应用市场和应用宝，各占总量的 12.2%；360 手机助手位列第三，占总量的 8.2%。以下是全国移动应用分发渠道分布图：



1.4 全国移动应用类型分布情况

截止 2024 年 06 月 30 日，观澜平台按照四部委发布的《常见类型移动互联网应用程序必要个人信息范围规定》对应用进行分类，将应用分为 40 个类型，其中本地生活类应用数量占应用总量的 21.2%，位居第一；实用工具类应用数量占应用总量的 18.1%，位居第二；网络游戏类应用数量占应用总量的 10.3%，位居第三。以下是全国移动应用类型分布 Top10：

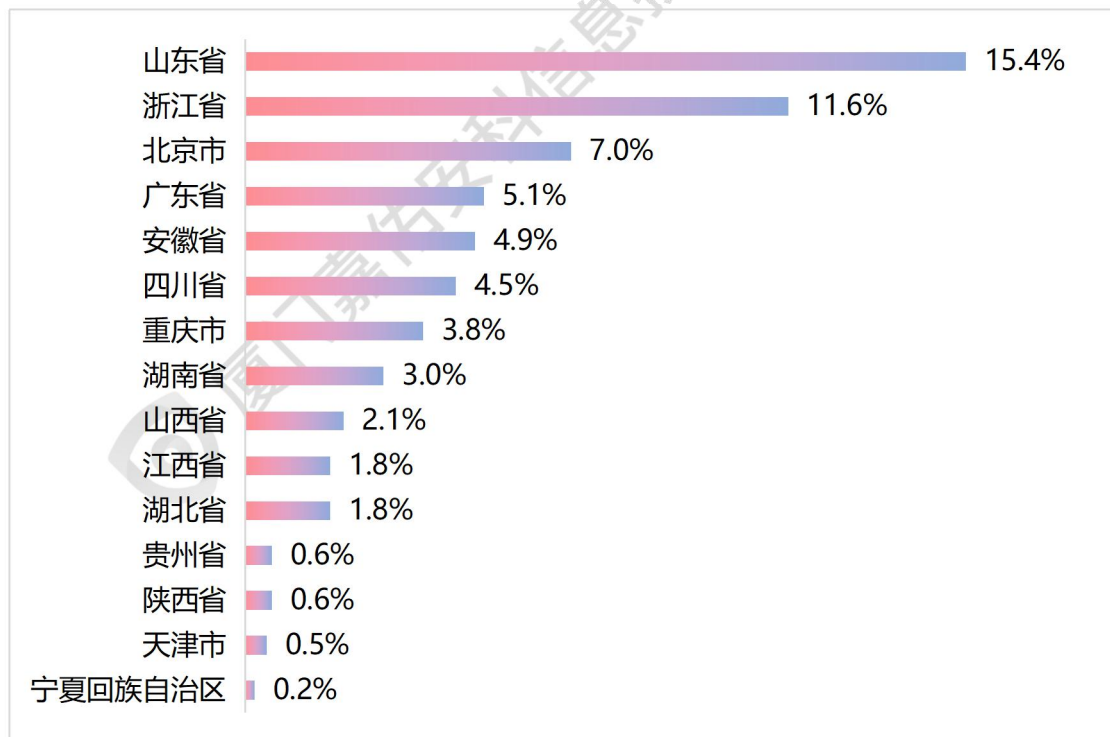


全国移动应用类型分布 Top10

第二章 2024 年上半年通报 App 分析

2.1 被通报的移动应用总体分布情况

2024 年上半年全国监管部门总计通报隐私违规 App 876 款, 其中, 工信部通报 127 款, 占全国工信部通报应用总量的 14.5%; 各地通管局共通报 550 款, 占全国工信部通报应用总量的 62.8%; 其中, 山东省、浙江省、北京市通报应用排在全国工信部通报应用的前三, 分别占全国通报应用的 15.4%、11.6%和 7.0%, 以下是各省份通管局通报应用总量综合情况分布图:



各省份通管局通报应用总量综合情况图

2.2 被通报的移动应用违规类型分布情况

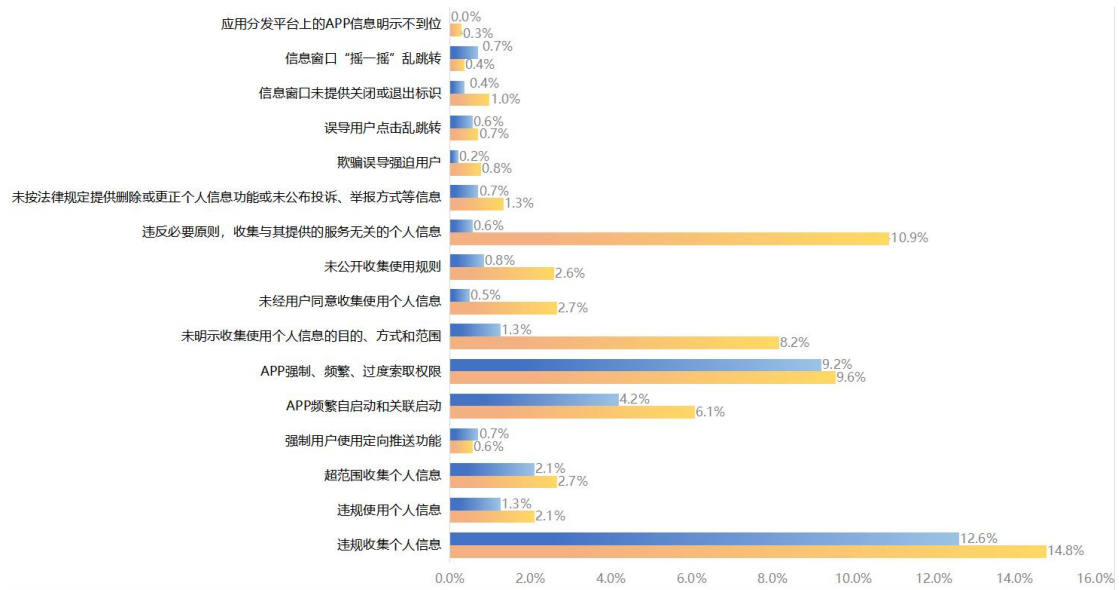
根据 2024 年上半年 2 个季度的问题通报类型占比统计得出如下图所示。

通报类型	Q1占比	Q2占比	趋势
违规收集个人信息	14.8%	12.6%	↓
违规使用个人信息	2.1%	1.3%	↓
超范围收集个人信息	2.7%	2.1%	↓
强制用户使用定向推送功能	0.6%	0.7%	↑
APP频繁自启动和关联启动	6.1%	4.2%	↓
APP强制、频繁、过度索取权限	9.6%	9.2%	↓
未明示收集使用个人信息的目的、方式和范围	8.2%	1.3%	↓
未经用户同意收集使用个人信息	2.7%	0.5%	↓
未公开收集使用规则	2.6%	0.8%	↓
违反必要原则，收集与其提供的服务无关的个人信息	10.9%	0.6%	↓
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	1.3%	0.7%	↓
欺骗误导强迫用户	0.8%	0.2%	↓
误导用户点击乱跳转	0.7%	0.6%	↓
信息窗口未提供关闭或退出标识	1.0%	0.4%	↓
信息窗口“摇一摇”乱跳转	0.4%	0.7%	↑
应用分发平台上的APP信息明示不到位	0.3%	0.0%	↓

2024 年上半年通报违规类型占比统计图

其中，通报数量前三名是：1、违规收集个人信息，2、App 强制、频繁、过度索取权限，3、未明示收集使用个人信息的目的、方式和范围；同时，对比 2023 年的通报类型情况可知，今年新增了关于欺骗误导、点击乱跳转、“摇一摇”等通报问题点，这说明监管部门今年的重点在这些问题上，因为这些问题会较为严重的侵犯用户个人信息权益，同时我们可以发现这些问题在第二季度相较于第一季度有明显的下降趋势，这说明监管通报效果明显。由此可知，App 运营者仍需要在这几个问题通报类型上深刻分析与修正，尤其是今年新

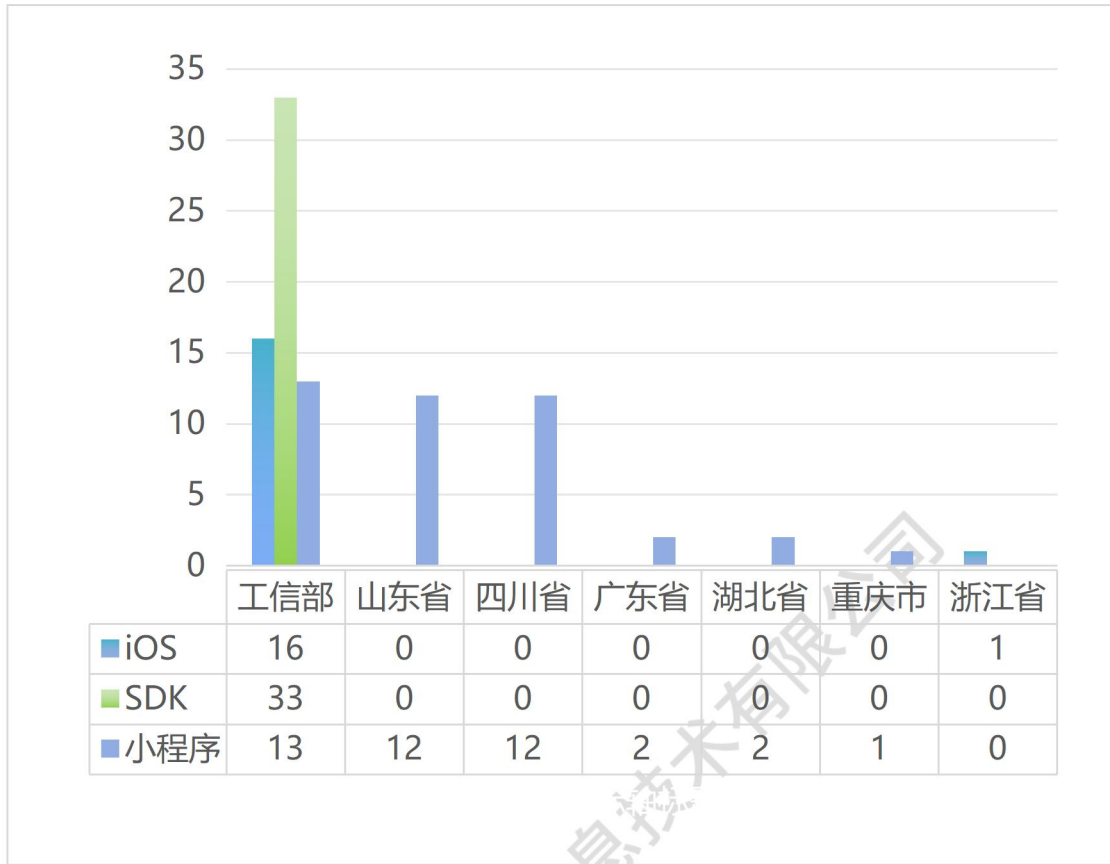
增的问题点。



2024 年上半年通报违规类型占比情况图

2.3 其他被通报移动应用分布情况

2024 年上半年监管部门通报的对象主要是 Android App。除此之外还有不少小程序、快应用等轻量应用和 iOS App 被通报。说明国家监管部门正在不断扩大移动应用隐私合规的监管范围与治理对象。统计情况如下图所示。



除 Android 外通报类型统计



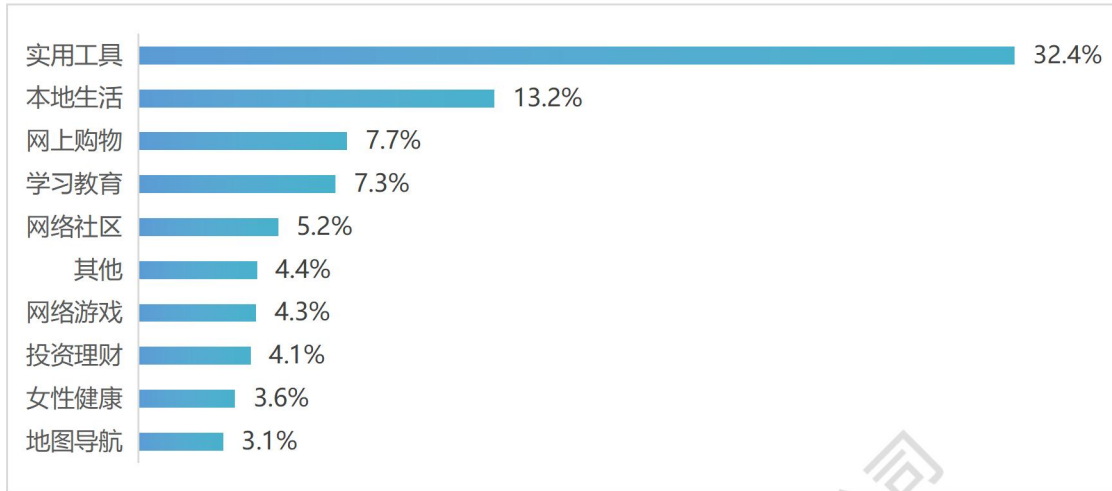
第三章 移动应用隐私合规风险分析

2024 年上半年嘉佑安科采取抽检方式对大量 App 样本开展隐私合规检测，对检测中发现的问题，从 App 合规风险类型、App 功能类型违规次数分布、App 隐私合规违规类型等维度进行统计分析。

在本次监测报告呈现对抽检数据的分析结果值，以抽检数据中的 App 类型占比、集中存在风险点地方、违规采集的情况等维度开展分析，并对分析的结果进行排行统计，更有效的辅助 App 开发者、运营者集中聚焦自身 App 易存在风险项，能够更针对性加强 App 隐私合规保护，同步提高个人信息处理透明度，最大限度地建立用户信任。

3.1 移动应用合规检测类型分布情况

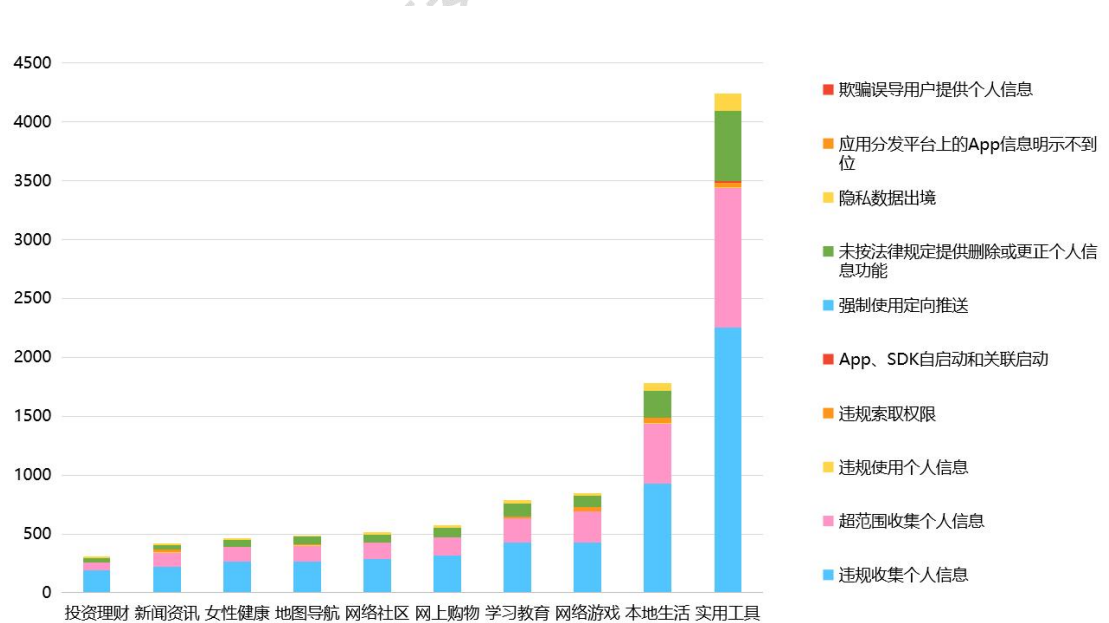
根据抽检移动应用违规的应用类型分布来看，实用工具类应用数量占抽检总量的 32.4%，位居第一；本地生活类应用数量占总量的 13.2%，位居第二；网上购物类应用数量占总量的 7.7%，位居第三。下图为移动应用合规检测类型分布 Top10：



移动应用合规检测类型分布 Top10

3.2 移动应用功能类型违规次数分布情况

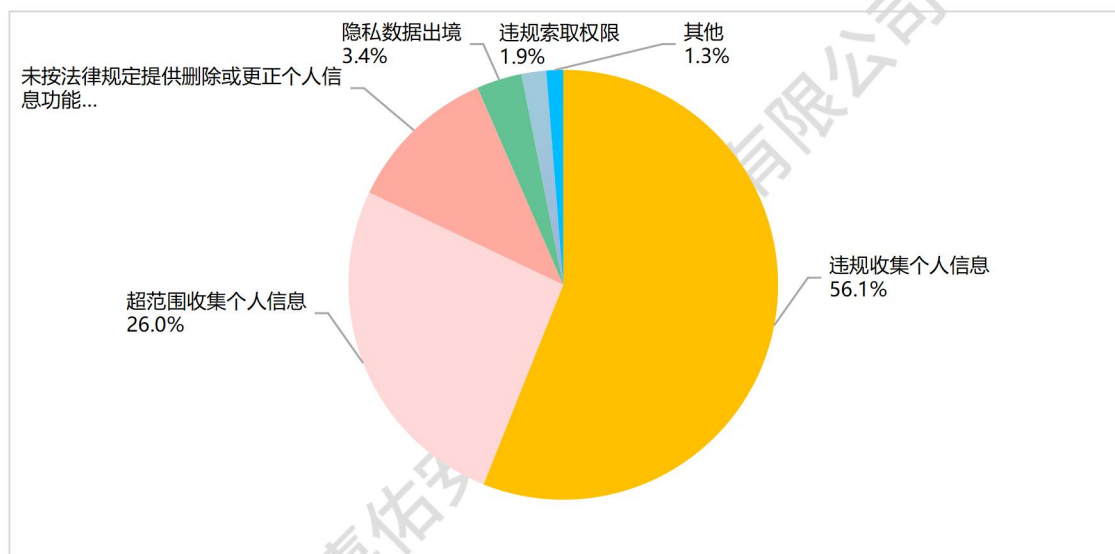
针对抽检的移动应用功能类型进行个人信息违规次数统计，结果显示，实用工具类型违规次数最多；其次是本地生活类型；然后是网络游戏类型。以下是违规应用功能类型次数 Top10：



违规应用功能类型违规次数 Top10

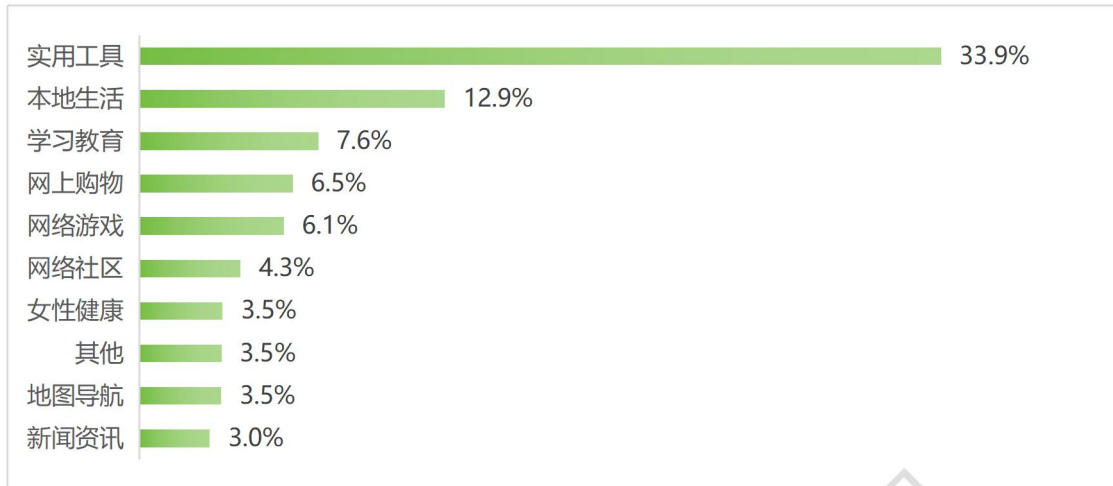
3.3 移动应用合规检测违规类型情况

通过对抽检的移动应用进行检测，并对其存在的违规类型进行统计和分析。其中，发现存在“违规收集个人信息”的占比最多，为 56.1%；其次是“超范围收集个人信息”占比 26.0%，位列第二；位列第三的是“未按法律规定提供删除或更正个人信息功能”，占比为 11.4%。以下是移动应用合规检测违规类型 Top5：



移动应用合规检测违规类型 Top5

再结合相关移动应用的功能类型来看，涉及违规类型占比第一的“违规收集个人信息”的移动应用中，实用工具类应用占该类型检测的总量的 33.9%，排名第一；本地生活类应用占该类型检测总量的 13.6%，排名第二；网上购物类应用占该类型检测总量的 10.8%，排名第三。以下是存在“违规收集个人信息”的功能类型占比 Top10：



存在违规应用功能类型 Top10

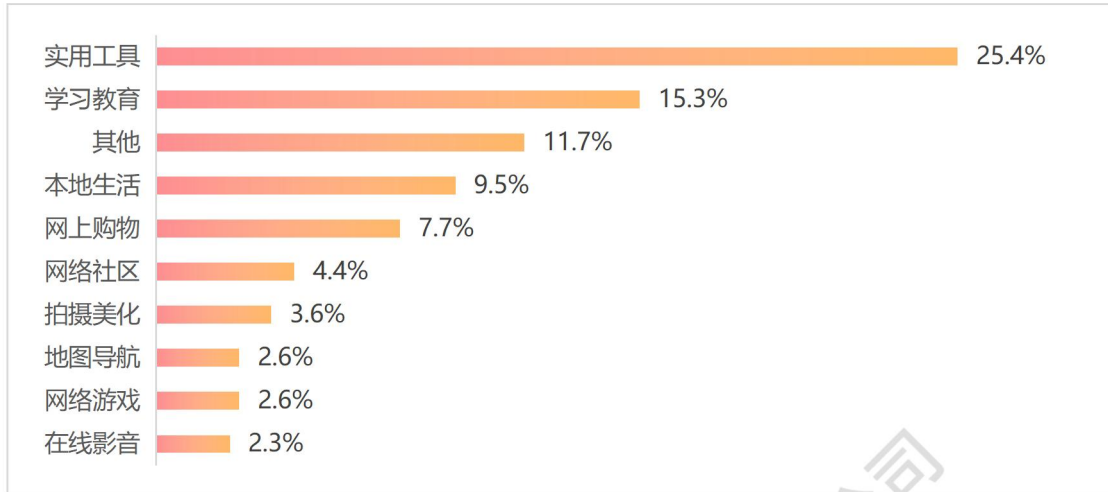
第四章 移动应用安全风险分析

2024 年上半年嘉佑安科采取抽检方式对大量 App 样本开展安全检测，对检测中发现的问题，从 App 安全风险类型、App 功能类型违规分布、App 安全违规类型、数据跨境目的地分布等维度进行统计分析。

在本次监测报告呈现对抽检数据的分析结果值，以抽检数据中的 App 类型占比、集中存在风险点地方、数据跨境地域分布情况等维度开展分析，并对分析的结果进行排行统计，更有效的辅助 App 开发者、运营者集中聚焦自身 App 易存在风险项，能够更针对性加强 App 自身安全防护，提升 App 自身防御能力，保护用户隐私数据安全。

4.1 移动应用安全检测类型分布情况

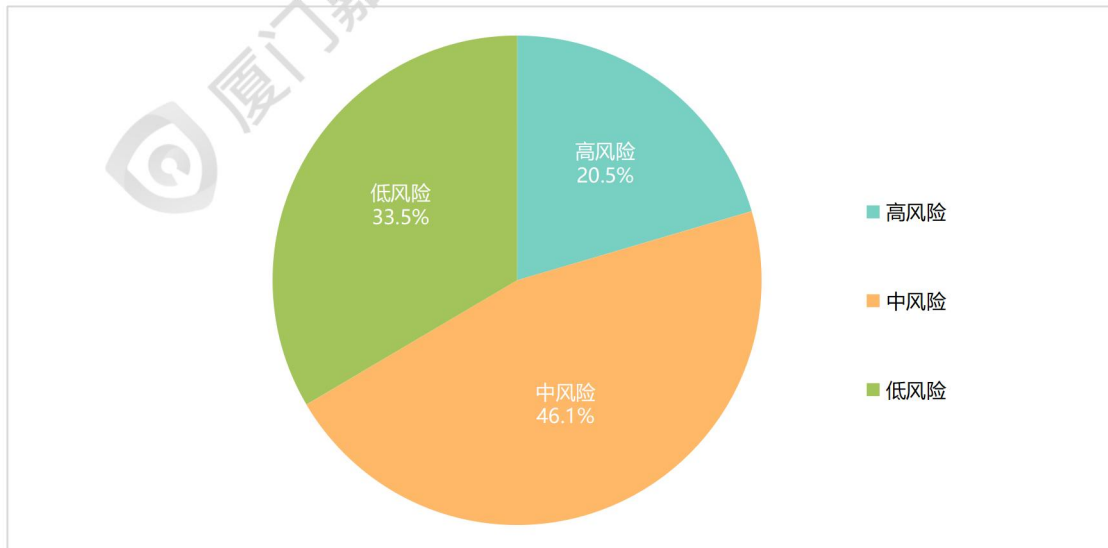
根据存在安全风险的应用类型分布来看，实用工具类应用数量占抽检总量的 25.4%，位居第一；学习教育类应用数量占总量的 15.3%，位居第二；其他类应用数量占总量的 11.7%，位居第三。下图为移动应用安全检测类型分布 Top10：



移动应用安全检测类型分布 Top10

4.2 移动应用安全检测结果概览

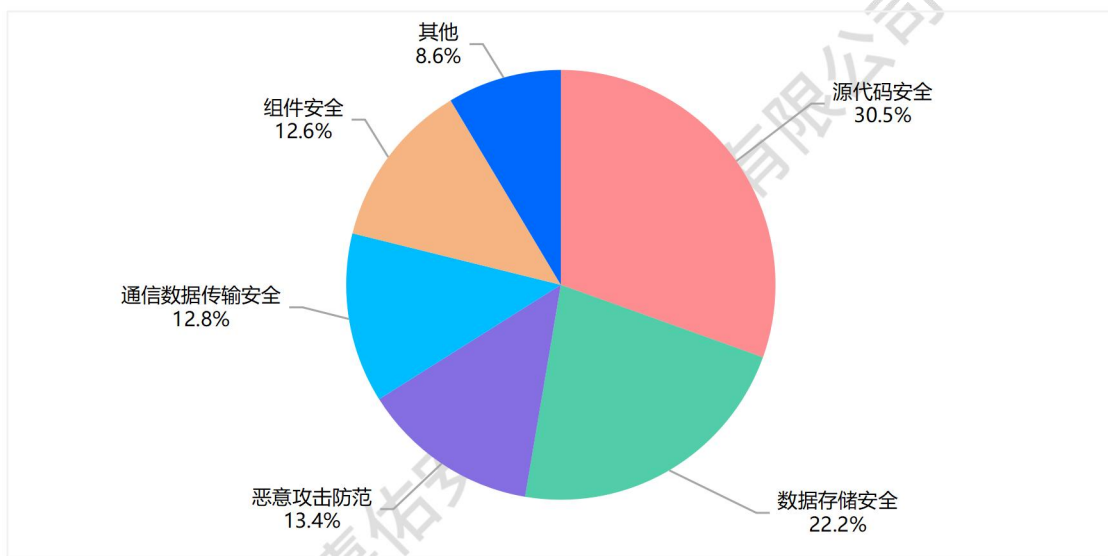
针对抽检的移动应用进行安全检测，并对检测结果进行统计，其中，主要有存在高风险的应用，占比 20.5%；其次是存在中风险的应用，占比 46.1%；排名第三的是存在低风险的应用，占比 33.5%；以下是移动应用安全检测结果概览图：



移动应用安全检测结果概览图

4.3 移动应用安全检测违规类型情况（高风险）

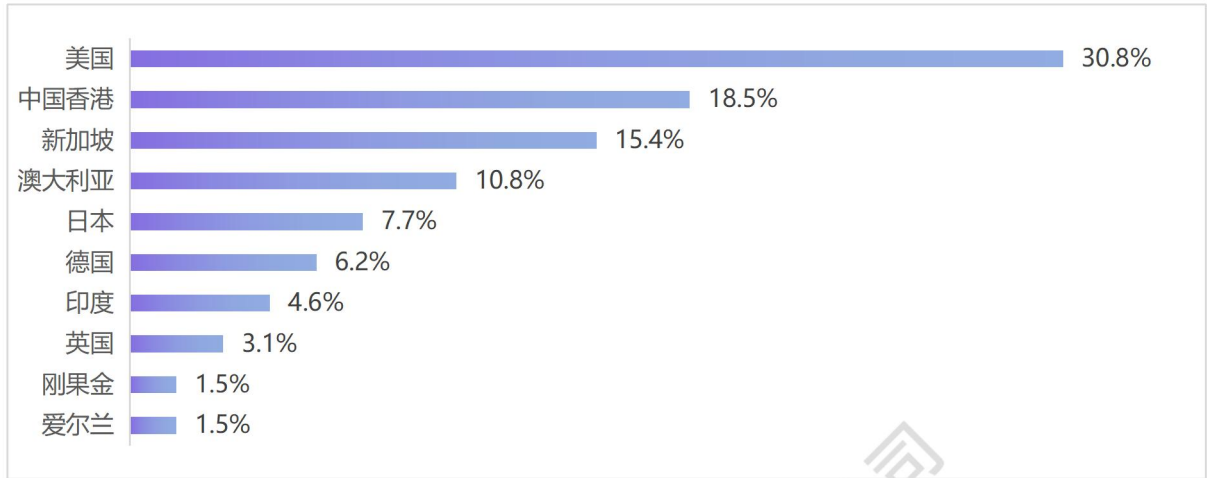
在涉及安全检测违规类型占比第一的高风险的移动应用中，嘉佑安科安全专家团队通过检测结果发现其中存在安全问题最多的是：“源代码安全”，占比 30.5%；其次是“数据存储安全”，占比 22.2%；排名第三的是“恶意攻击防范”，占比 13.4%；以下是移动应用安全检测违规类型情况 Top5：



移动应用安全检测违规类型情况 Top5（高风险）

4.4 移动应用数据跨境目的地分布情况

针对抽检的移动应用的数据跨境传输行为进行分析，发现数据流向多个国家和地区。具体来看，数据跨境传输排名第一的目的地是美国，占比 30.8%；排名第二的是中国香港，占比 18.5%；排名第三的是新加坡，占比 15.4%。具体情况可见移动应用数据跨境目的地分布图：



移动应用数据跨境目的地分布图

厦门嘉佑安科信息技术有限公司

第五章 总结与建议

随着移动互联网的普及和深入，移动应用带来的安全风险和隐私违规风险也愈发凸显，恶意软件、网络钓鱼、数据泄露等安全威胁层出不穷。加上网络环境的复杂性和技术手段的局限性，个人信息泄露的风险始终存在。一旦个人信息数据泄露，将面临泄露的个人信息存在被不法分子用于电信诈骗、网络钓鱼等违法犯罪活动，给用户带来财产损失和精神压力；同时泄露的个人信息还可能被用于精准营销、恶意推送等商业活动，干扰用户的正常生活。更为严重的是，一些敏感信息的泄露还可能威胁到国家安全和社会稳定。

因此，加强移动应用的安全和隐私防护，构建全方位的移动安全体系，已成为当务之急。其中在移动安全体系的构建中，除了基础的防护措施如数据加密、访问控制等，还需要特别关注移动应用的身份认证机制。传统的用户名密码认证方式已无法满足现代移动应用对安全性的要求，因此，多因素认证、生物识别技术等新型身份认证手段逐渐得到广泛应用。这些技术不仅能提高认证的安全性，还能提升用户体验，减少因忘记密码等问题带来的不便。

另外建议 App 开发者、运营者在 App 上架前把好第一道隐私合规关卡，确保 App 上架合规，避免因 App 存在违规收集个人信息、超范围收集个人信息、违规使用个人信息等问题，面临被监管通报下架的风险，同时对保障用户个人隐私数据安全，建立用户信任渠道，提升用户安全感、促进 App 市场健康良性发展具有重要意义。

第六章 公司及产品介绍

6.1 公司介绍

(一) 公司概况

厦门嘉佑安科信息技术有限公司（下称：嘉佑安科）位于海上花园城市—厦门，注册资金人民币 1000 万元。是一家致力于打造完善的隐私安全合规产品，集自主研发、技术运营为一体，保护公民个人信息安全的服务商。嘉佑安科母公司---厦门铠甲网络股份有限公司荣获国家高新技术企业、福建省重点上市后备企业、福建省数字经济核心产业领域未来独角兽企业、福建省科技小巨人领军企业、福建省互联网最具成长型企业、厦门十大科创板潜力企业、厦门市重点软件和信息服务企业等资质和荣誉，现拥有 150 项软著和专利。

(二) 愿景使命

公司坚守以“成为人民隐私安全的忠诚守护者”为企业愿景，勇担“保护人民合法权益，保护国家安全、社会和谐稳定”的企业使命，发展规划始终以人民根本利益为中心，通过发挥技术优势、专业的安全服务，为用户、政府、企业、开发者和消费者打造安全、稳固、可信的网络空间生态环境。

(三) 联系方式

官网地址：www.jusafety.com

联系电话：0592-5837215 / 0592-5837310

企业邮箱：jy@kaijia.com

公司地址：厦门市软件园二期观日路 26 号之二 202A

企业公众号：

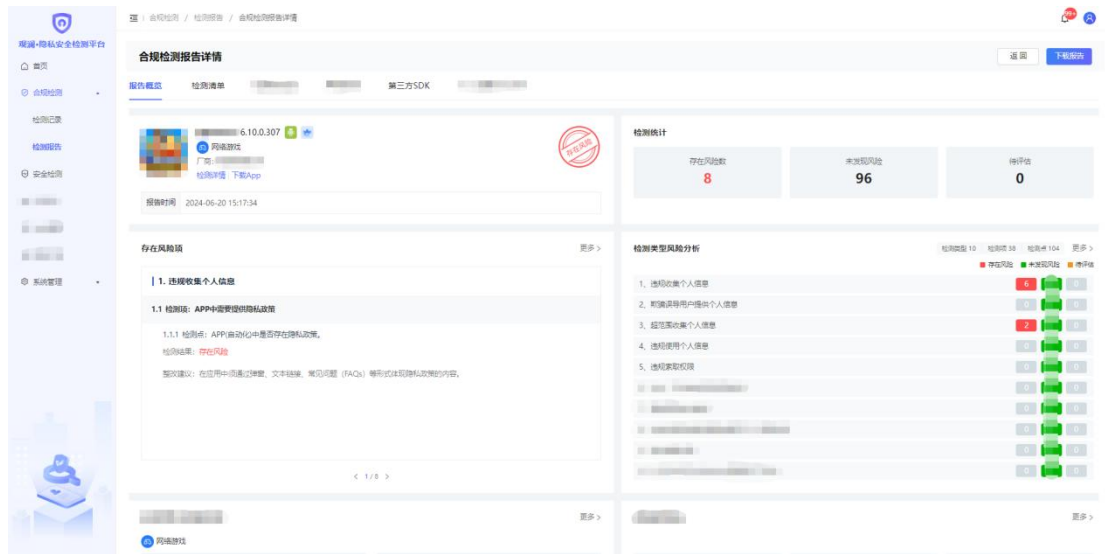


 厦门嘉佑安科信息技术有限公司

6.2 产品介绍

6.2.1 观澜•隐私安全检测平台

通过自动化检测+专家级人工检测的方式，面向 App 运营者或开发者、应用市场和监管部门，提供专业、规范、精确、高效的隐私合规检测服务。



观澜-隐私合规检测平台图

6.2.2 观辰•隐私安全探针

在 App 中接入观辰隐私安全探针（SDK），有利于应用更好的保护用户个人信息安全，帮助 App 运营者主动发现潜在的违规风险，降低隐私安全违规问题发生的可能性与危害程度，将隐私安全标准落实到 App 日常运营中。

6.2.3 观擎•隐私安全态势分析平台

通过对隐私合规检测结果数据的系统化分析，同时对 App 隐私行为进行识别，结合大数据清洗、建模分析、机器学习等技术，实时监测 App 隐私合规风险，构建 App 隐私安全监控和运行监测的态势分析平台。



观擎-隐私安全态势图