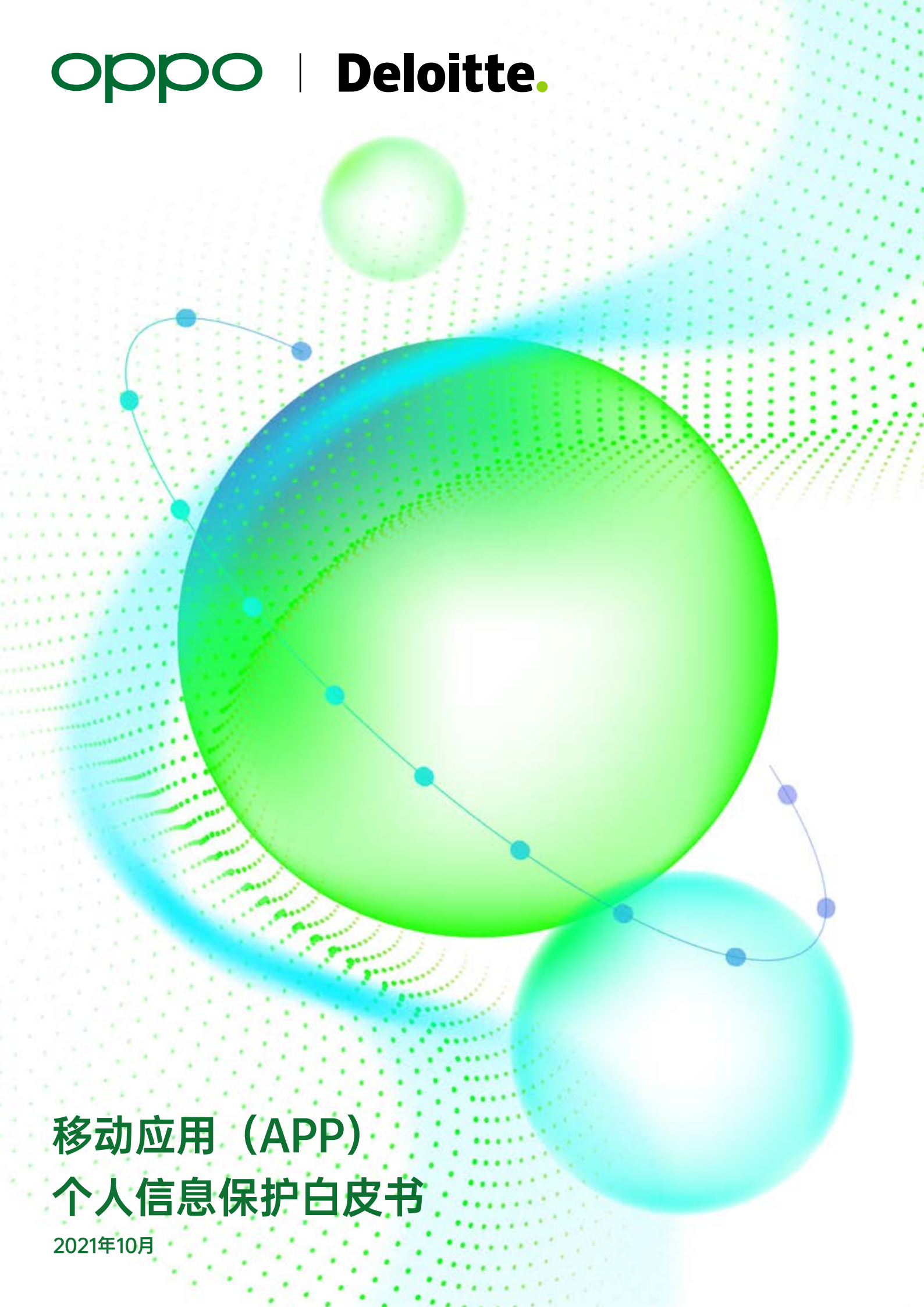


移动应用（APP）个人信息保护白皮书

2021年10月

前言

随着移动通信技术的飞速发展，移动应用已渗透到人们生活、工作的各个领域。从社交到出行，从网购到外卖，从办公到娱乐，移动应用种类和数量呈爆发式增长，是数字经济下的重要产品。尤其在疫情防控过程中，移动应用发挥了重要作用，其在社会经济发展中的基础性作用日益凸显。同时，大数据、云计算、人工智能和物联网相关技术快速发展，企业对数据挖掘技术的利用不断深入，用户数据已成为企业发展的重要战略性资产。移动应用作为用户数据收集的主要入口之一，其用户个人信息保护问题已备受国家和社会重视。

2018年，欧盟《通用数据保护条例》（GDPR）率先发布，引领全球个人信息保护监管趋势。近年来，我国也高度重视移动应用（APP）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，也得到移动应用生态各个环节的积极配合和社会公众关注。最为值得关注的是，2021年我国相继颁布了《数据安全法》、《个人信息保护法》，结合已经施行的《网络安全法》，我国已构筑起数据安全和个人信息保护的监管顶层设计。法律法规的快速完善再次表明了我国对个人信息保护工作的重视，进一步激发消费者、媒体等相关方的关注，对移动应用（APP）个人信息保护合规具有深远影响。

本白皮书围绕移动应用（APP）个人信息保护工作为读者呈现以下内容：首先，基于近三年来公开的数据，重点分析移动应用（APP）产业现状与趋势、个人信息保护特征和新技术的应用对移动应用（APP）个人信息保护带来挑战和机遇；基于我国个人信息保护法律制度框架逐步形成的背景，对近两年来监管部门开展的移动应用的个人信息保护的专项监督活动和侵犯个人信息的判罚趋势进行分析，并对《个人信息保护法》生效后的监管与司法诉讼的趋势进行研判，呈现我国的个人信息保护治理环境；结合德勤、OPPO和公开的数据，展现我国网民对移动应用（APP）个人信息保护的关注点；重点以OPPO在移动应用（APP）个人信息保护的实践作为蓝本，分享如何开展个人信息保护工作；最后以行业生态视角提出倡议，以及为消费者总结一些实用的个人信息保护建议。

目录

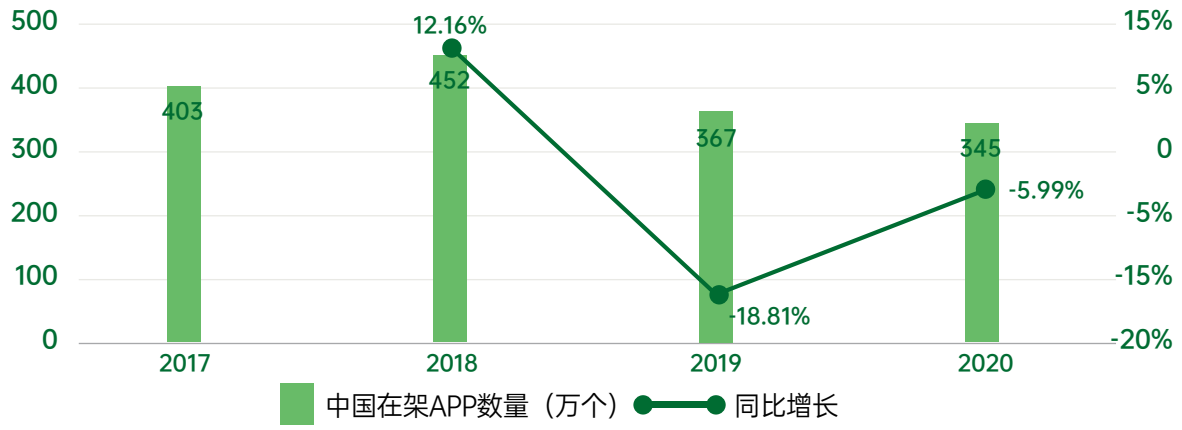
1 移动应用（APP）产业现状、个人信息保护特征和新技术风险分析

1.1 移动应用（APP）产业现状与趋势

1.1.1 近两年移动应用（APP）数量整体呈下降态势，游戏类APP数量仍稳居榜首

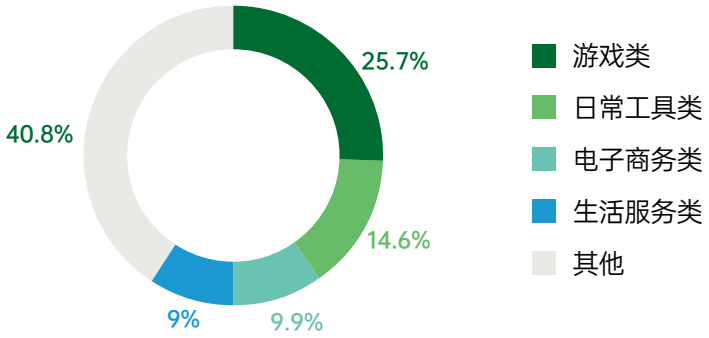
根据工业和信息化部（以下简称"工信部"）的统计数据显示，在2017到2020年期间，我国国内市场监测到的APP数量呈现波动性变化，APP数量缓步增长后呈下降态势。从2018到2020年，约减少107万款，但是应用商店国内在架APP的基数仍然非常庞大。截至2020年12月，国内市场上监测到的APP数量为345万款APP，而数量排在前四位分别为游戏类、日常工具类、电子商务类和生活服务类APP，共占比合计达59.2%。其中，游戏类APP数量达88.7万款，占全部APP数量的比例为25.7%。

2017年-2020年国内市场监测到的APP数量变化情况（单位：万个）



数据来源：工业和信息化部公开数据

截止2020.12国内市场监测到的APP按类型分布

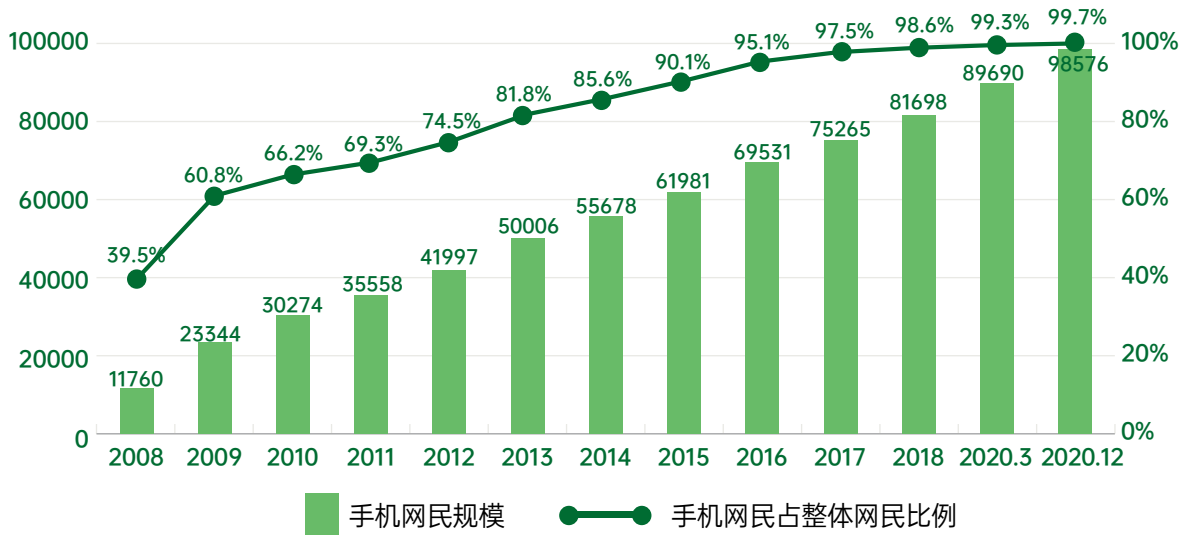


数据来源：工业和信息化部公开数据

1.1.2 中国手机网民规模接近10亿且保持稳步增长，移动应用将涉及更高量级的个人信息收集和使用

根据中国互联网络信息中心（CNNIC）统计数据显示，截止2020年底，中国手机网民规模已达9.86亿，从近十年的增长趋势看，手机网民规模保持稳步增长。结合中国2020年第七次人口普查结果全国人口总量计算，中国手机网民在全体国民的渗透率约达69.8%，该数值与欧美发达国家72%-90%的渗透率相比较，仍有一定的增长空间，但增长速度放缓，预计开发者会致力于提升应用使用频次，增加应用使用黏性，同时，单个APP收集和使用个人信息的量级将会进一步增长。

手机网民规模及其占整体网民比例



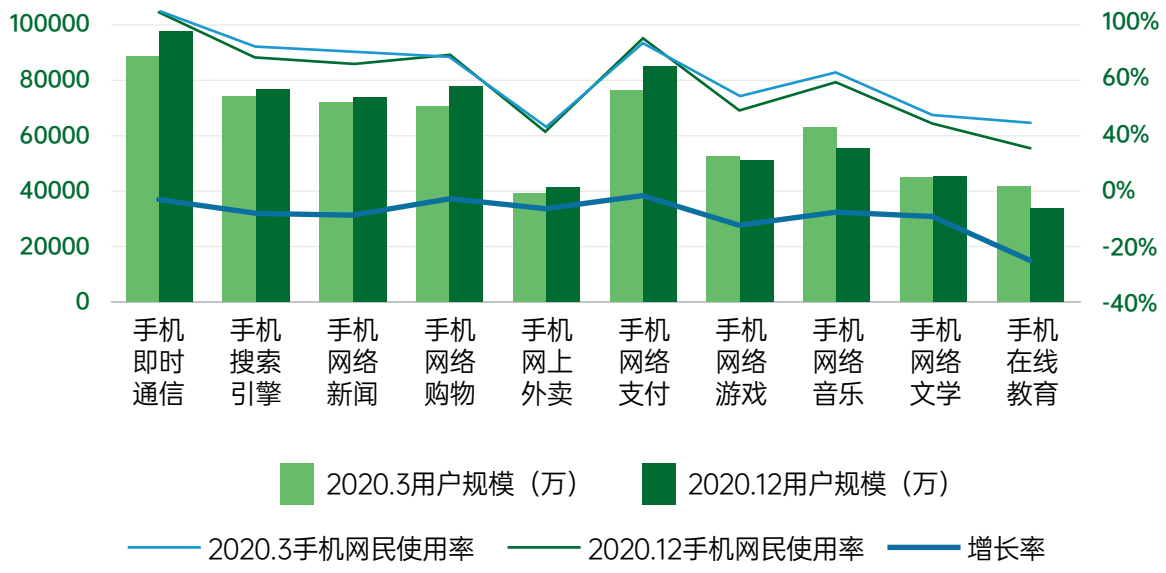
数据来源：CNNIC《第47次中国互联网络发展状况统计报告》

1.1.3 疫情后的新常态下，手机即时通讯获得更深层次的发展和更广泛的市场普及，远程办公、在线娱乐和直播购物类成为移动应用增长点，用户行为全面"数字化"进程将进一步加深

截止2020年12月，根据CNNIC数据显示，手机即时通讯用户规模达9.78亿，是所有手机应用类别之首。新冠疫情期间，即时通讯应用获得飞跃性的发展，一是即时通讯的公众号、小程序成为信息发布的重要渠道；二是大型科技公司入局企业即时通信业务，即时通讯应用与云服务开始融合，大力推动各地复工复产复学，为在线娱乐、远程办公和远程医疗提供技术保障。

疫情后的新常态下，用户移动应用使用习惯发生转变，优先考虑"无接触服务"，并强化在线服务的使用习惯。同时，该习惯影响产业服务远程化和在线化，远程办公、网络支付、外卖跑腿和在线医疗成为移动应用场景分布的新增长点。用户的衣食住行，生活和工作方面将进一步与移动应用"绑定"加深，用户的行为和生存轨迹更容易通过数字化形式进行呈现。

2020.3-2020.12 手机网民各类互联网应用用户规模和使用率



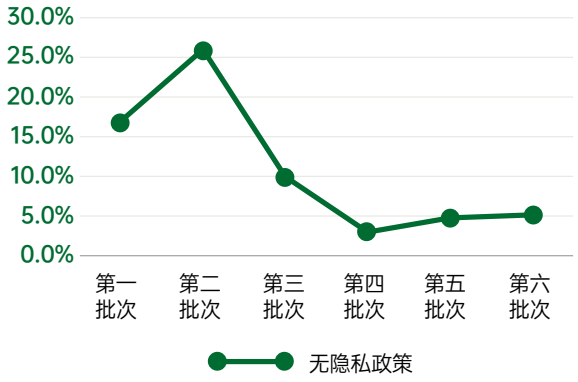
数据来源：CNNIC《第47次中国互联网络发展状况统计报告》

1.2 移动应用（APP）个人信息保护特征分析

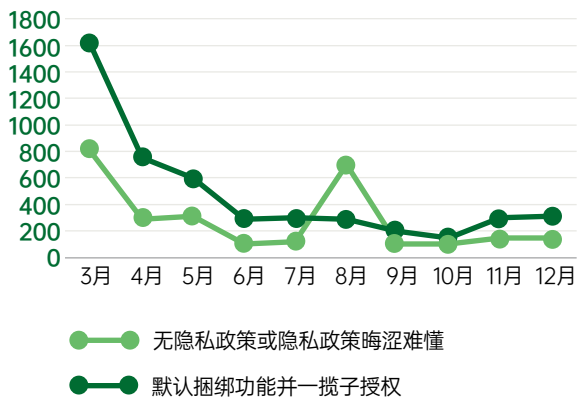
1.2.1 无隐私政策或隐私政策晦涩难懂情况得到较大改善，企业个人信息保护合规水平明显提升；但APP违规收集和使用个人信息依然是当前APP违规的主要问题

根据由中央网信办、工信部、公安部、国家市场监督管理总局（以下简称"四部委"）成立的"APP专项治理工作组"2019年的工作报告，从2019年3月起，APP专项治理工作组分6个批次对千余款APP进行了评估，发现APP"无隐私政策"问题下降幅度相对明显。从用户举报量显示，"无隐私政策或隐私政策晦涩难懂"问题也呈现下降趋势，APP隐私政策透明度明显提高，企业对其个人信息收集规则阐述更加清晰。基于APP专项治理工作组提供的研究数据，从10个行业抽取的100款APP来看，相比2018年，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。其中得分提高最为显著的是社交交友类和移动金融类，上升了40分左右。

2019年度"无隐私政策"问题变化趋势

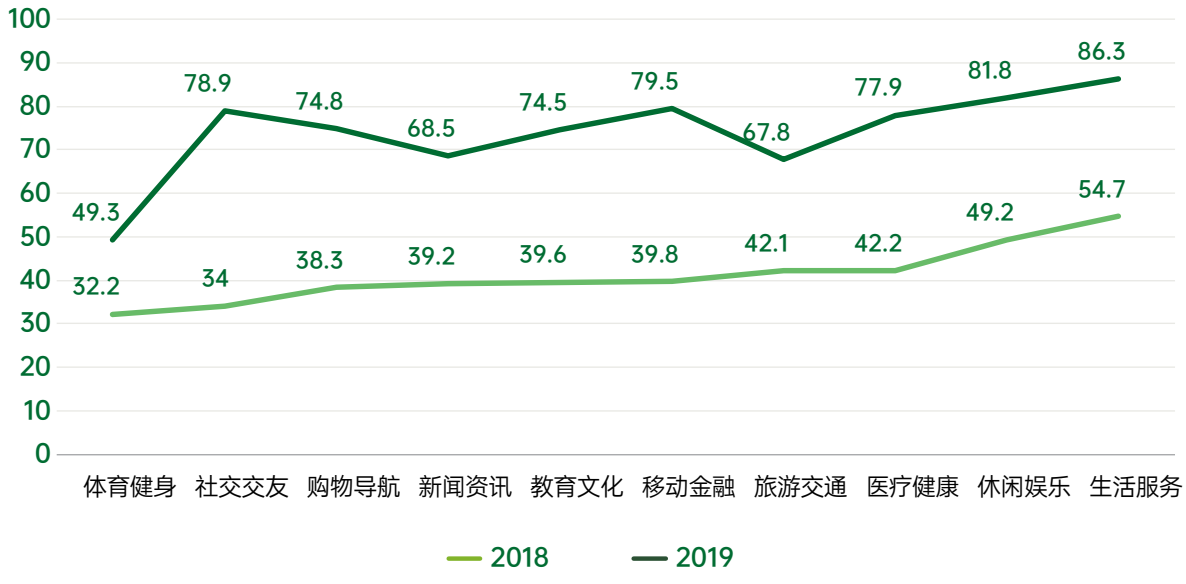


2019年度不同类型问题举报数量趋势



数据来源：《APP违法违规收集使用个人信息专项治理报告（2019）》

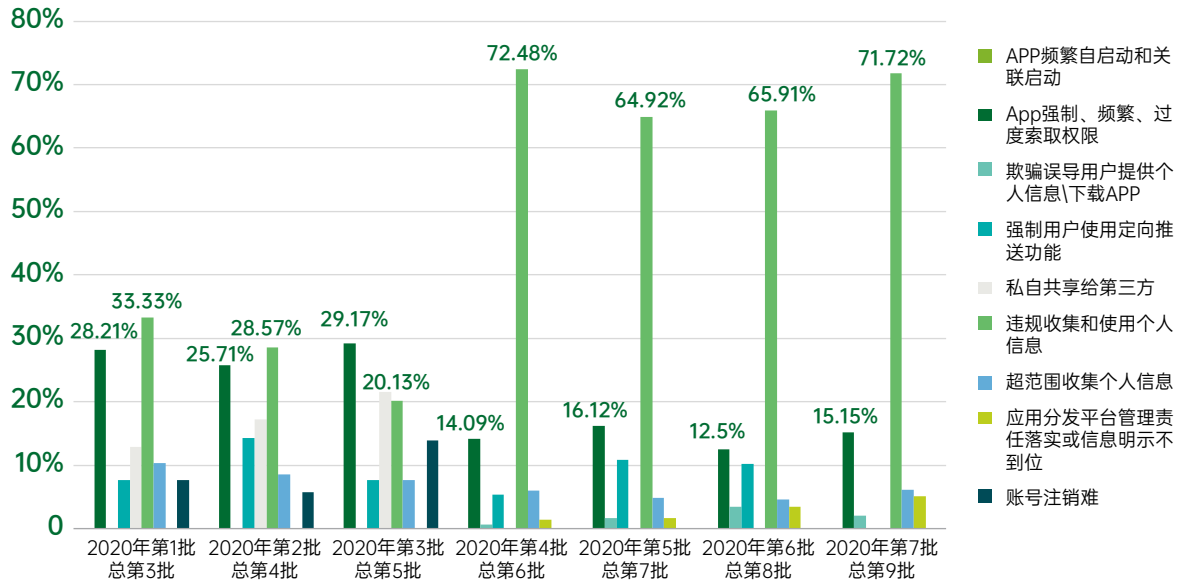
2018年度和2019年度十个行业隐私政策平均得分对比



数据来源：《APP违法违规收集使用个人信息专项治理报告（2019）》

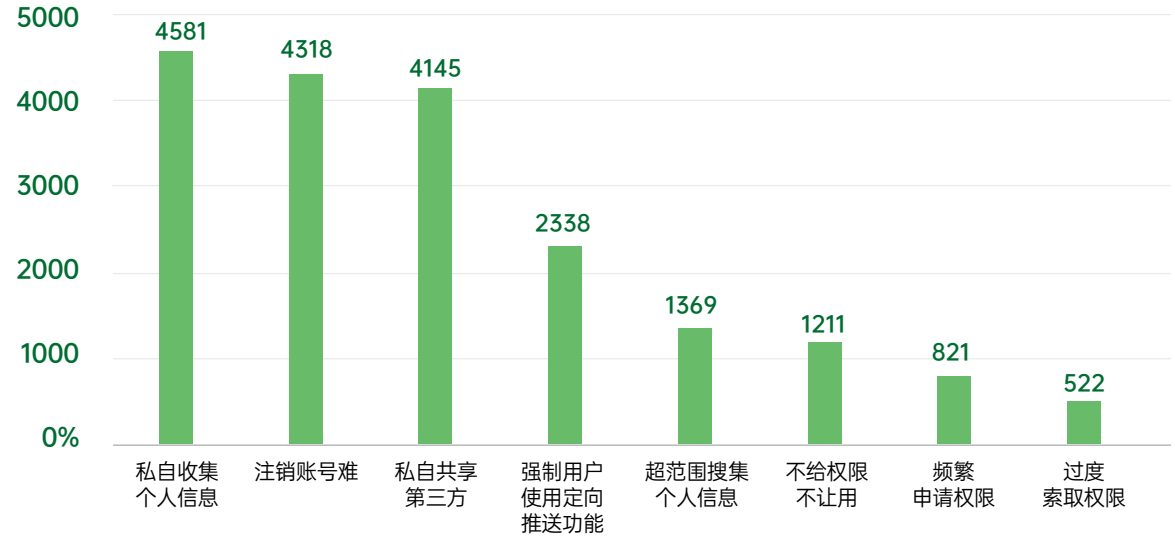
根据工信部关于侵害用户权益行为的APP通报数据显示（从2020年第1批—2021年第9批），共1353起APP违反最小必要原则和相关规定，收集和使用与其提供的服务无关个人信息，我们发现在2020年总计7个批次的通报中，该问题在其中6个批次是出现频率最高的。而在2021年已通报的9个批次中，该问题依然占据榜首且比例远高于其它类型问题。对此，我们也从广东省通信管理局APP监管平台发布的数据中得到验证。该APP监管平台共收录597万个版本，242.12万款APP，其在2020年1月至12月期间共发现11835个疑似违规问题APP，其中有4581个APP存在私自收集个人信息的问题。同一时期，四部委联合发布《常见类型移动互联网应用程序必要个人信息范围规定》作为最小必要原则的执行准据，该规定于2021年5月1日起正式施行，可见该问题持续引起监管部门的重视，企业在个人信息保护实践中需重点关注。另外，APP强制索权、频繁索权以及过度索权的问题也是监管通报中第二大常见问题，也是开发者在APP开发过程中需重点关注的问题。

2020年度关于侵害用户权益行为的APP通报统计



数据来源：工业和信息化部公开数据

2020年度APP个人信息违规问题分类统计



数据来源：广东省通信管理局 《广东省移动智能终端应用程序（APP）2020安全白皮书》

1.2.2 SDK广泛应用带来的违规收集和使用个人信息的问题已成为移动应用生态治理的难点和痛点，监管部门逐步加强监管并完善标准规范

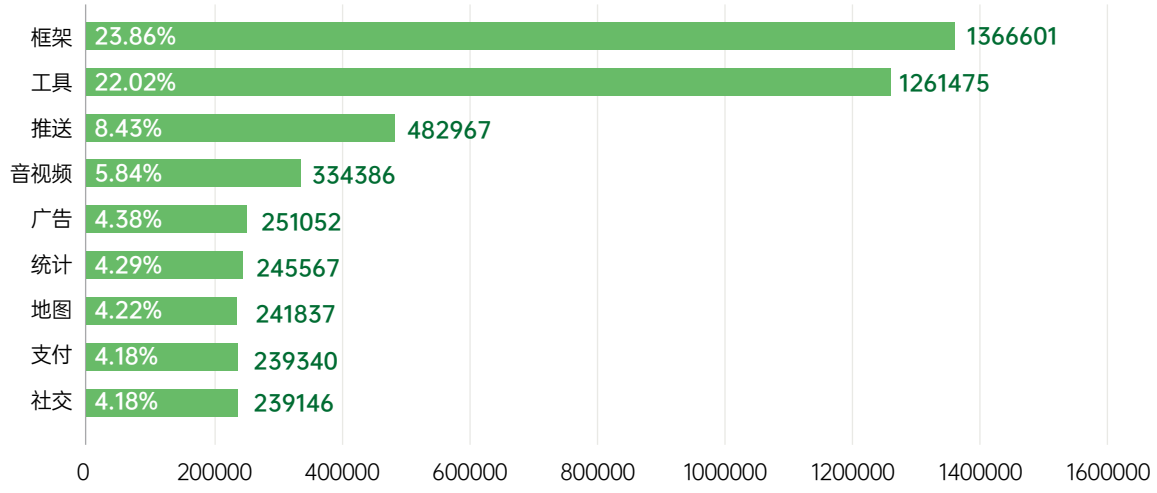
根据第三方机构2021Q1的全国移动互联网观测报告，全国的移动应用APP平均集成SDK（Software Development Kit，软件开发工具包）已达8.9个。在2021Q2的报告中显示，集成频率最高的SDK类型是框架类SDK，占比23.86%，其次是工具类SDK，占比22.02%；值得注意的是，推送类SDK已成为集成频率仅此于工具类的第三大类型。

早在2019年，APP治理工作专项报告明确指出"第三方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……建议将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"。其后在2020年3月疫情期间某视频会议软件的SDK个人信息泄露事件被曝光，以及2020年7月"3.15"晚会曝光某SDK未经用户许可窃取个人信息问题，引起社会舆论对第三方SDK个人信息保护问题的关注。

由于第三方SDK一般不独立面向用户提供服务，而依赖于APP接入，即使第三方SDK直接收集个人信息，用户在使用APP过程中对其行为也处于无感知状态或者弱感知状态；另外，多数情况下第三方SDK的个人信息处理活动对于APP开发者较不透明，对APP开发者而言，很难进行管控。虽然SDK作为个人信息保护的关键一环，但相关标准和行业实践经验都相对较少。近年来，考虑到用户对个人信息保护的诉求，APP开发者及运营者联合第三方SDK提供者，采用APP逐一列出所接入第三方SDK收集用户个人信息情况并征得用户同意等措施，以提升第三方SDK收集个人信息的透明度，以保证用户知情权。我们也可以看到，全国信安标委已在2020年12月发布了《网络安全标准实践指南—移动互联网应用程序（APP）使用软件开发工具包（SDK）安全指引》，并在2021年4月开始对《信息安全技术移动互联网应用程序（APP）SDK安全指南征求意见稿》公开征求意见。该指南征求意见稿当中提到SDK的安全风险：SDK在开发时聚焦于功能实现而忽视了安全性，可能导致SDK本身存在安全漏洞；SDK典型恶意行为如广告刷量、隐私窃取、远程控制等；SDK收集使用个人信息安全存在问题。同时，该征求意见稿针对SDK生命周期安全、个人信息安全和APP联动三方面提出了不同要求，也给企业SDK治理工作提供了指引。

即便如此，由于第三方SDK的广泛应用和不透明性，其违规收集和使用个人信息已成为移动应用生态治理的难点和痛点，亟需监管、企业和相关方共同探索最佳实践并完善标准规范。

不同类型SDK对应的APP分布情况



数据来源：《全国移动App第二季度安全研究报告》2021

1.2.3 移动应用商店进一步完善APP上架审核和在架监测机制，携手监管和开发者，共同维护用户权益和个人信息安全

移动应用分发平台是重要的流量入口，是各大手机厂商和互联网企业的必争之地，在这一领域企业相互竞争的过程中，用户处于弱势和被动的地位，大部分消费者因无法准确甄别APP个人信息安全的保护能力，而依赖移动应用分发平台获取其所需的APP。

移动应用商店作为APP主要分发渠道，已针对当前用户面临的痛点和难点，持续完善APP上架审核和在架监测机制，积极参与到个人信息保护治理工作中，督促开发者整改，及时下架违法违规APP，并为开发者整改提供指引和建议，共同维护用户权益和个人信息安全。

我们也可以看到，工信部于2021年4月，公开征求对《移动互联网应用程序个人信息保护管理暂行规定（征求意见稿）》的意见，其中提到APP分发平台需履行的个人信息保护义务：开发者实名登记、APP上架基本信息公示、APP安全上架审核及跟踪管理、公开投诉举报方式并受理公众举报等。作为移动应用分发平台的企业须肩负起移动应用生态个人信息保护的职责，在盈利的同时实践企业的社会责任。

1.3 新技术的应用对移动应用（APP）个人信息保护带来挑战和机遇

1.3.1 生物特征识别技术的应用为个人信息保护带来了新的挑战，国家监管治理体系逐步探索和完善

近年来，随着信息技术飞速发展，生物特征识别逐步渗透到人们生活的方方面面。指纹、声纹、虹膜特征解锁在安防领域广泛应用，语音助理功能几乎成为智能手机标准配置。人脸识别技术更是在国境边防、智慧城市、公共交通、城市治安、疫情防控，以及手机客户端登录解锁、支付等诸多领域大放异彩。根据全球第二大市场研究机构Markets and Markets发布的预测，2019年全球人脸识别市场规模预计为32亿美元，五年后将达79亿美元。然而，生物特征识别技术在蓬勃发展的同时，也带来了诸多安全挑战。个人生物特征数据泄漏、技术滥用等造成的问题亟待解决。

生物特征识别信息收集的必要性欠缺、技术和数据的滥用是首要及核心问题，人脸数据的使用问题尤为突出。2019年，瑞典北部斯盖乐夫提市的一所高中因使用面部识别技术来监控学生的出勤情况，被瑞典数据监管机构处以20万瑞典克朗（人民币14.8万元）的罚款，是GDPR生效以来首例针对人脸识别问题的罚款。在我国，2021年的3·15晚会曝光某连锁家具门店使用“无感式”人脸识别技术，在用户无感知的情况下，未经同意擅自收集消费者人脸数据，并进行持续分析，获取消费者的性别、年龄、心情等数据，进而采取针对性的策略。而且，这些人脸和用户画像数据不仅被商家持有，还被分享给了该分析技术的提供方。由此，人脸识别技术隐患已经显露端倪。而且，目前法律对于人脸数据提供、使用主体之间权利和义务划分不够清晰，各主体在人脸数据生命周期各环节中应采取的安全合规措施缺失。

为了解决上述问题，在立法及执法层面，我国已经开启了对人脸识别技术应用进行重点监管的进程。《民法典》、《个人信息保护法》等基础性法律奠定了人脸数据保护的基础，同时，各地也在上位法精神的指导下，颁布配套实施细则，例如：《天津市社会信用条例》要求市场信用信息提供单位不得收集自然人的宗教信仰、血型、疾病和病史、生物识别信息以及法律、行政法规规定禁止收集的其他个人信息；《深圳经济特区数据条例》，该条例对处理生物识别数据作出了更加严格的规定，要求处理生物识别数据时，除该生物识别数据为处理个人信息目的所必需，且不能为其他非生物识别数据所替代的情形外，应当同时提供处理其他非生物识别数据的替代方案等。同时，在执法层面，最高人民法院发布了《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》并于2021年8月1日施行，该规定以保护当事人合法权益，促进数字经济健康发展为宗旨，对滥用人脸识别问题作出统一规定。同时，我国人脸识别第一案也于今年4月份二审宣判。

1.3.2 个人信息和重要数据保护成为国家对智能网联车监管的重点之一

智能汽车是指通过搭载先进传感器等装置，运用人工智能等新技术，具有自动驾驶功能，逐步成为智能移动空间和应用终端的新一代汽车。智能汽车通常又称为智能网联汽车、自动驾驶汽车等。随着智能汽车在中国市场的逐渐增长，消费者在接触的过程中遇到驾驶体验、维权事件和事故调查，也同时衍生出的智能汽车的数据安全问题，比如：自动驾驶数据的安全及合规问题如何监管，如何保障车辆数据的真实性和防篡改性，以及自动驾驶数据如何进行披露和数据公布。针对这不断暴露出智能汽车产业发展痛点，国家层面相当重视，自2021年以来，国家有关部门先后出台了多份规范性文件，包括：4月底全国信安标委发布的《信息安全技术网联汽车采集数据的安全要求（草案）》、8月中旬国家互联网信息办公室发布的《汽车数据安全管理若干规定（试行）》，以及在9月中旬工信部发布的《关于加强车联网网络安全和数据安全工作的通知》。上述规范性文件要求企业加强个人信息和重要数据保护，规范汽车数据处理活动，同时，也明确了车联网个人信息与重要数据的本地化存储要求。

1.3.3 大数据和人工智能算法广泛引用所衍生的个人信息保护问题引起国家监管关注，“大数据杀熟”成为监管重点

近年来大数据时代下，部分互联网企业利用已收集的海量消费者数据进行大数据分析，为消费者提供“精准推荐”及“个性化广告”。这类服务一定程度上为消费者带来便利，但随着技术发展，这种便利也成为困扰，某些企业采用“大数据杀熟”的行为更是严重侵害消费者利益。“杀熟”的形式，主要有三种表现，1）根据用户使用的设备不同而差别定价，比如针对iOS系统用户与安卓系统用户制定不同的价格；2）根据用户消费时所处的场所不同而差别定价，比如对距离商场远的用户制定的价格更高；3）三是根据用户消费频率的不同而差别定价，一般来说，消费频率越高的用户对价格承受能力也越强。在GDPR中7大数据主体权利中明确有反自动化决策权，自动化决策所依靠的数据可能本身就包含个人或社会成见，导致基于偏见数据所做出的自动化决策结果不公平地歧视个人或群体，干扰个人权利，导致人们被排除在社会生活的某个领域之外，使个人无法享受某些服务或福利待遇。值得关注的是，我国在2021年11月1日施行的《中华人民共和国个人信息保护法》对大数据杀熟有比GDPR更明确的规定，其要求“个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇”。基于此，国家互联网信息办公室，在个人信息保护法宣布通过后的当月（2021年8月份），也发布了《互联网信息服务算法推荐管理规定（征求意见稿）》，该征求意见稿第十条提出“不得设置歧视性或者偏见性用户标签”，直接对用户模型和用户标签管理提出要求。

1.3.4 隐私保护技术的发展为平衡个人信息保护合规要求和数据使用需求提供了可能

个人信息保护毫无疑问是企业发展的合规红线。但随着数字化应用高速发展，各行各业对于数据共享的需求也不能忽视。国务院2020年5月发布的《关于构建更加完善的要素市场化配置体制机制的意见》中，首次将数据作为生产要素纳入进来。在现已生效的《数据安全法》中也提倡数据安全与发展平衡。数据需要通过开放、流动和共享才能产生价值，而无序的管控和无技术的保障将会产生数据泄露等安全合规风险，也会与目前个人信息保护的趋势产生冲突。如何平衡个人信息保护和数据流通使用的矛盾和冲突，成为隐私保护技术研究的重点。

其中，隐私计算技术能在数据提供方不泄露敏感数据的前提下，对数据进行计算并能验证计算结果，迎来产业和市场的巨大关注。使用隐私计算技术可以很好地缓解用户隐私焦虑，确保用户真实数据只保留在用户信任的终端进行计算，并且不会传输用户个人信息至云端。隐私计算技术并不能简单归属于某一个学科领域，而是一套融合了密码学、安全硬件、数据科学、人工智能、计算机工程等众多领域的跨学科技术体系。从应用前景来看，一方面隐私计算可以增强数据流通过程中安全性以及对个人信息安全的保护；另一方面隐私计算也为数据的融合应用和价值释放提供了新思路。目前，隐私计算技术中的多方安全计算、可信执行环境和联邦学习三大方向广受关注。在具体实践上还会结合同态加密、零知识证明和差分隐私技术的支持，以及联合区块链技术进行应用。但是，隐私计算当前尚处于起步阶段，当前主要受限于场景经验较少，计算复杂度高、多方交互效率低、模型性能等问题。但欣喜的是，头部的高科技、金融、能源企业已经在试点使用，尝试采用隐私计算作为基础，打造行业联盟或集团内的数据共享平台，以实现跨机构的数据合作模式。海外Google、Apple等科技巨头已经率先在手机上采用联邦学习或差分隐私做出有益尝试。国内头部智能手机制造商，比如OPPO也已经在手机应用上实现了差分隐私技术落地，正在向着更新的隐私技术应用发起攻关，争取为开发者提供更多有效案例。

2 我国个人信息保护监管环境

2.1 我国个人信息保护法律制度框架逐步形成

2.1.1 国家个人信息保护法律法规加速建设进程

为规范个人信息的收集使用，打击涉及个人信息违法犯罪行为，我国相继出台个人信息保护相关法律法规。从2012 年实施的《全国人民代表大会常务委员会关于加强网络信息保护的决定》、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）》、《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。自2021年1月1日施行的《民法典》强调，自然人的个人信息受法律保护。自2021年9月1日施行的《数据安全法》，明确了国家数据安全治理的顶层设计。另外，2021年8月，《个人信息保护法》正式颁布，成为我国个人信息保护立法进程上的又一里程碑，11月1日，《个人信息保护法》将正式生效。

2.1.2 相关监管部委"边治理、边完善"：开展APP专项违规个人信息治理的同时完善相关规定及标准

2019年四部委联合发布《关于开展APP违法违规收集使用个人信息专项治理的公告》，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。同时，制定发布的《APP违法违规收集使用个人信息行为认定方法》概括六类APP违法违规收集使用个人信息行为，并作为统一监管执法尺度。以此为依据，App专项治理工作组在2019年共开展6个批次的通报。此外，为配合APP专项治理工作，全国信安标委修订了《个人信息安全规范》，并编制了《移动互联网应用程序（APP）收集个人信息基本规范》，为企业提供合规指引。为进一步规范治理工作的评估指引，四部委联合发布了《常见类型移动互联网应用程序必要个人信息范围规定》，并于2021年5月1日正式施行。

工信部继2019年电信和互联网行业提升网络数据安全保护能力专项行动后，于2020年联合各省通信管理局按照《网络安全法》、《电信条例》、《电信和互联网用户个人信息保护规定》和《移动智能终端应用软件预置和分发管理暂行规定》的要求，依据《关于开展纵深推进APP侵害用户权益专项整治行动的通知》开展APP侵害用户权益专项整治工作，自2020年1月至2021年7月中旬共计开展15批次通报。

此外，公安部连续三年开展"净网"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。国家市场监督管理总局也开展"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。

移动应用相关国家合规要求及标准一览

序号	法规名称	分类	发布日期	施行日期
1	《中华人民共和国个人信息保护法》	法律法规	2021年8月20日	2021年11月1日
2	《中华人民共和国数据安全法》	法律法规	2021年6月10日	2021年9月1日
3	《中华人民共和国民法典》	法律法规	2020年5月28日	2021年1月1日
4	《中华人民共和国网络安全法》	法律法规	2016年11月	2017年6月1日
5	《消费者权益保护法》（第二次修订）	法律法规	2013年10月25日	2014年3月15日
6	《常见类型移动互联网应用程序必要个人信息范围规定》	部委规章	2021年3月12日	2021年5月1日
7	《儿童个人信息网络保护规定》	部委规章	2019年8月22日	2019年10月1日
8	《APP违法违规收集使用个人信息行为认定方法》	部委规章	2019年5月	2019年5月
9	《互联网个人信息安全保护指南》	部委规章	2019年4月	-
10	《APP违法违规收集使用个人信息自评估指南》	部委规章	2019年3月	2019年3月
11	《移动互联网应用程序个人信息保护管理暂行规定（征求意见稿）》截止2021年4月公开征求意见	部委规章	-	-
12	《移动智能终端应用软件预置和分发管理暂行规定》	部委规章	2016年12月16日	2017年7月1日
13	GB/T 39335-2020 个人信息安全影响评估指南	国家标准	2020年11月19日	2021年6月1日
14	GB/T 35273-2020 个人信息安全规范	国家标准	2020年3月17日	2020年10月1日
15	GB/T 37964-2019 个人信息去标识化指南	国家标准	2019年8月30日	2020年3月1日
16	TAF 移动智能终端及应用软件用户个人信息保护实施指南 截止2021年8月已发布第九部分	团体标准	2021年5月12日	-

2.2 个人信息保护的专项监督活动和侵犯个人信息的判罚趋势分析

2.2.1 针对APP的专项整改活动仍在大力进行中：据不完全统计，四部委及其省级单位在2019年至2021年8月份期间共通报整改2111款APP，通报下架470款APP

序号	行动	年份	机构	通报整改	通报下架	约谈	罚款
1	APP侵害用户权益行为专项整治行动	2019年	工信部	56	3	-	-
2	净网"2019"	2019年	公安部	100	-		
3	"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	2019年	国家市场监督管理总局	-	-	3536次	1946万
4	APP专项治理	2021年1月-2021年7月	国家互联网信息办公室	351	26	-	-
5	APP侵害用户权益行为专项整治行动	2020年1月-2021年8月	工信部	1604	441	-	-
	合计			**2111**	**470**		

2.2.2 强化平台自身责任，监管要求细化、深入：出现了针对平台责任的判罚案例，监管判罚依据从显性违规扩大至非显性违规

2020年7月，胡女士以上海某商务平台APP收集其个人非必要信息，进行"大数据杀熟"等为由诉至法院，要求退一赔三并要求该APP为其增加不同意"服务协议"和"隐私政策"时仍可继续使用的选项，以避免被告收集其个人信息，掌握原告数据。法院审理后认为，该APP作为中介平台对标的实际价值有如实报告及价格管控的义务，而该APP向原告展现了一个溢价100%的失实价格，未践行承诺。而且，该APP在处理原告投诉时告知原告无法退全部差价的理由，经调查也与事实不符，存在欺骗。故认定被告存在虚假宣传、价格欺诈和欺骗行为，支持原告退一赔三。除了消费者欺诈，法院明确了该APP作为电子商务平台方针对个人信息滥用应承担的责任。其判罚依据不仅限于个人信息收集未授权、信息出售、滥用等行为，还包括更细微的法律文本措辞、界面交互等不合理事项，例如：1）强制同意，用户必须点击同意该APP"服务协议""隐私政策"方能使用，如不同意，将直接退出该APP，是以拒绝提供服务造成对用户的压迫；2）用户画像绑定授权，该APP的"隐私政策"还要求用户授权该APP自动收集用户的个人信息，包括日志信息、设备信息、软件信息、位置信息，要求用户许可其使用用户信息进行营销活动、订单数据进行分析，从而形成用户画像。

从上述案件可以看出，平台方将逐渐成为执法重点，同时，判罚依据由显性的违规转向非显性违规，呈现多样化趋势。企业应更加关注合规工作中的更多细节，例如非必要信息的收集和使用，绑定授权、一揽子授权、第三方信息滥用等问题。

2.2.3 高额罚款频发，目前集中于金融行业，可能向其他行业扩展：进入2021年，针对侵犯个人信息的事件，央行开出3起超过400万的大罚单

自2020年以来，央行、银保监会连续开出多张百万元级罚单，涉及不当使用用户个人信息、系统数据质量及数据报送存在违法违规、网络安全工作严重不足等问题。2021年开年便对某国有大型银行开出了共计400万的大罚单，其后对某国有股份制商业银行和某城商行因其个人信息滥用和管理不当的问题也开出了超过400万的巨额罚单。
银行业成为大额罚单的首要重灾区，一方面在于银行具有庞大的用户群体，掌握了大量的用户数据；另一方面，金融数据是消费者普遍关心的最具敏感性的数据类型之一，其泄露及滥用往往会造成极大的经济损失；特别是，针对银行业的强监管环境，从银行业开始下重拳整顿，能达到降低主要风险，实现高执法效率的目的。可以预见，其他行业如医疗、互联网等，都存在用户数据触达点多、掌握数据量大的特点，那么参考银行业的监管思路，大额判罚的案例有可能出现在其它行业。

2.3《个人信息保护法》生效后的监管与司法诉讼的趋势分析

2021年8月20日，第十三届全国人民代表大会常务委员会第三十次会议通过《中华人民共和国个人信息保护法》（以下简称"个保法"），该法案于2021年11月1日起实施。个保法是我国第一部专门规范个人信息保护的法律。尽管我国的宪法、民法、刑法等法律中都有针对个人信息保护的规定，但条文大多零散分散，并未对个人信息保护进行完整、系统性规范描述，但这些零散的规定，为日后专门的个人信息保护立法的出台奠定了基础。个保法在这些法律的基础上形成了具备系统性、针对性、可操作性的完备的专门规范体系。从个人信息处理的基本原则，到个人信息跨境提供规则，再到数据主体个人权利，最后落脚至监管机构职责及法律责任。当中，对于个保法生效后，未来个人信息治理的趋势值得企业关注：

- **明确规定互联网平台服务方的责任。**
  重要互联网平台服务提供者拥有巨大的用户数量，触点丰富，且业务场景类型复杂，涉及多方主体，往往面临极高的数据隐私合规风险，同时也肩负着对网络服务提供者的规范及引导作用。个保法中第五十八条对重要互联网平台方的义务予以规定，比如：要求平台方建立合规制度体系、独立机构监督、明确平台内服务规范及服务提供者义务、停止对严重违规方提供服务、发布社会责任报告等。这些专规对于平台管理及产品服务提供者的教育大有裨益。

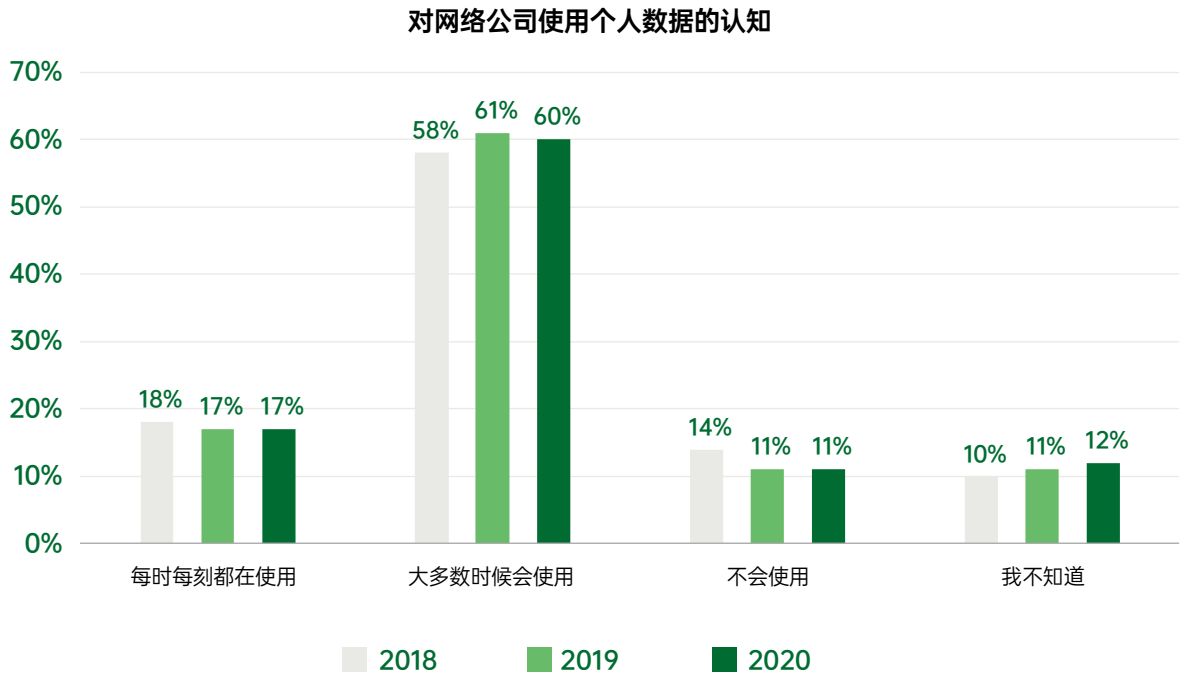
- **多元化的个人信息保护履职体系。**
  与大部分国家的集权式监管不同，中国采用统筹协同制的个人信息保护监管体系。国家网信部门作为总统筹方，国务院有关部门在各自职责范围内负责个人信息保护和监管管理工作，兼顾了行业差异性。在地方层面，县级以上地方人民政府有关部门作为具体实施监督方，履行个人信息保护和监督管理职责，兼顾了地区差异性，形成了行业监管为横轴、地方监管为纵轴的网状监督体系，这将有利于个保法的落地，但是对于个人信息处理者的企业，需要投入更多资源和成本以符合不同维度的要求。

- **分级化的法律责任和公益诉讼的影响。**
  在法律责任部分，个保法总体借鉴了欧盟《一般数据保护条例》GDPR的监管思路，规定了高额处罚，大幅提高了个人信息处理者的违法成本，并依据违法程度轻重不同，规定了多元化的处罚措施甚至追责到个人。同时，也明确将个人信息纳入可提起公益诉讼的范畴。就在个保法颁布的一周内，最高人民检察院下发《关于贯彻执行个人信息保护法推进个人信息保护公益诉讼检察工作的通知》，明确各级检察机关在履行公益诉讼检察职责时，应当从严把握几个方面：1）敏感个人信息应当严格保护，比如生物识别、宗教信仰、特殊身份、医疗健康、金融账号、行踪轨迹等；2）特殊群体的个人信息需要特别保护，比如儿童、妇女、残疾人、老年人、军人等；3）重点领域（教育、医疗、就业、养老、消费等）处理的个人信息，以及处理100万人以上的大规模个人信息应当重点保护；4）大数据"杀熟"情况，对因时间、空间等联结形成的特定对象的个人信息加强精准保护。同时，最高检开展为期一年的公益诉讼质量提升年专项行动。基于《通知》要求和专项行动开展，未来将出现更多个人信息保护领域的典型公益诉讼案例，民事诉讼、公益诉讼成为个人信息处理者在个人信息保护方面的新考验、新挑战。

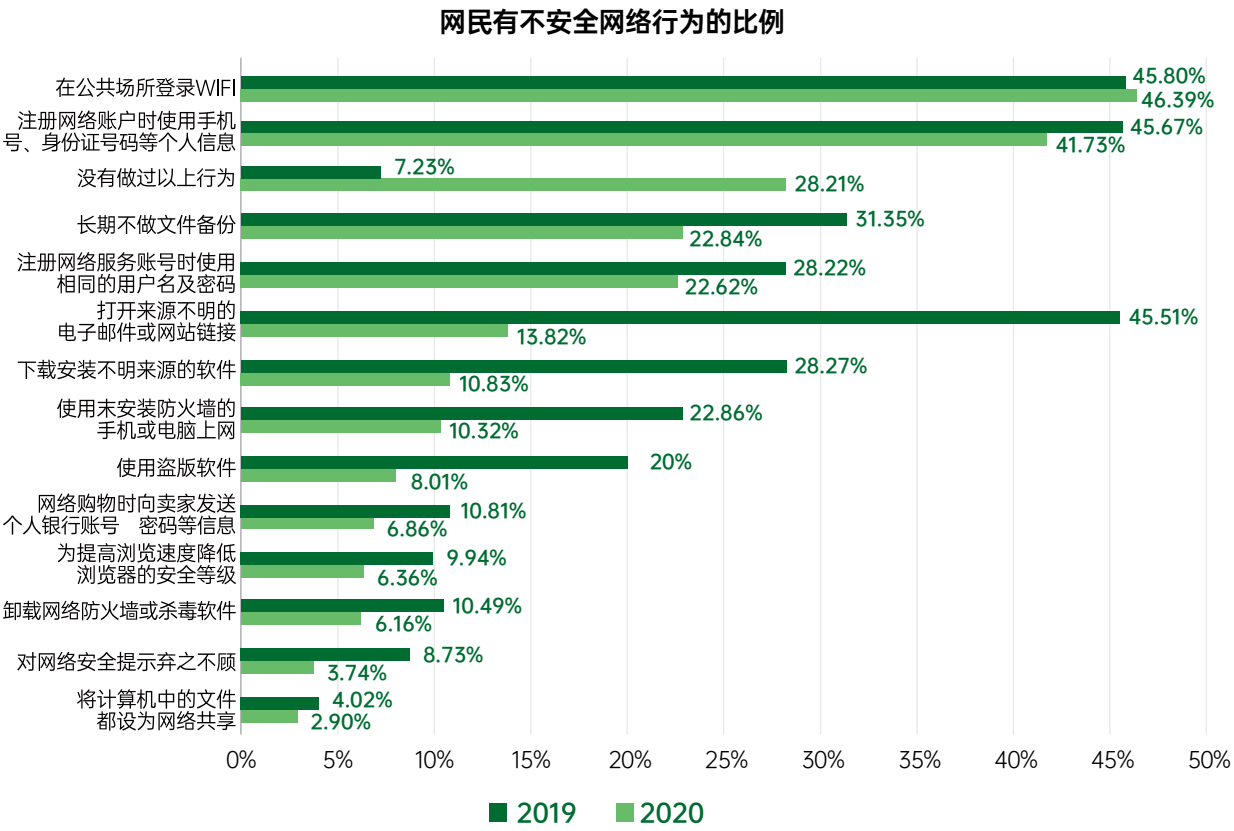
3 我国网民对移动应用（APP）个人信息保护的关注点

3.1 用户的认知程度以较快速度逐年提升

从下图一可以看出，大部分的消费者在使用在线服务时，都能意识到企业在使用他们的个人信息，并且这一现象比较稳定，消费者保持着比较强的个人信息保护意识；在下图二中可以看出，2020年消费者表示没有做过所列不安全行为的比例较2019年有明显上升，相应地，各类不安全行为的比例绝大多数呈下降趋势。同时用户的认知程度与监管动态、行业发展步调基本一致，用户认知的提升，必然给行业及监管提出更高的要求。



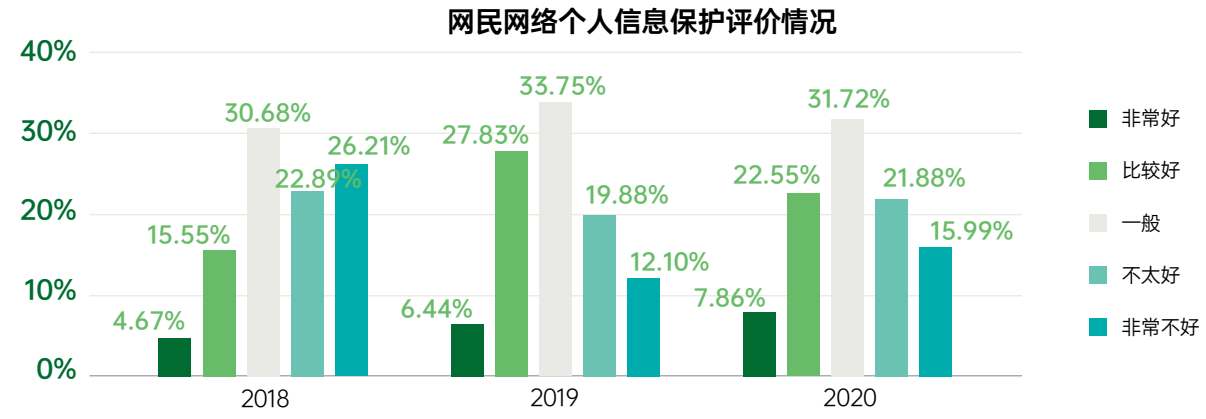
数据来源: 德勤《2020德勤中国移动消费者调研》2018~2020



数据来源：《全国网民网络安全感满意度调查统计报告》2019~2020

3.2 近五年，用户对我国网络安全满意度较低，但逐年提升

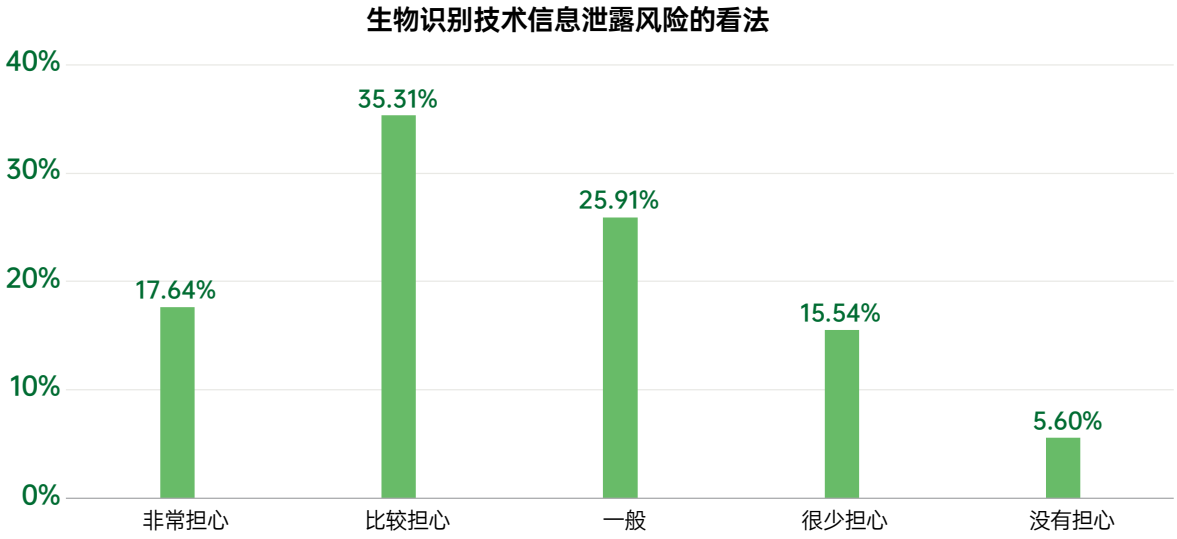
根据下图数据，近五成受访者认为当前我国网络个人信息的保护状况欠佳，有超过四分之一的受访者认为网络个人信息的保护状况非常不好，只有两成的受访者认为我国网络个人信息的保护状况比较好或非常好。我国网民对个人信息保护状况认为不太好及非常不好的比例从2018年的49.1%下降到2020年37.87%，在三年中满意度最高是2019年，认为“比较好”及以上有34.27%，到2020年满意度有所回落至30.41%，但情况仍然比2018年有所提升。这得益于国家相继出台的网络安全及个人信息保护的相关法律法规，以及监管部门的治理行动和企业各界的共同努力。



数据来源：《全国网民网络安全感满意度调查统计报告》2018~2020

3.3 用户对生物识别技术的使用还是存在疑虑

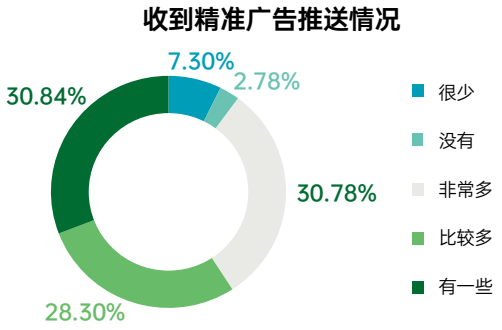
用户比较担心生物识别信息泄露风险，根据下图数据，有近52.95%受访者对生物识别技术，如人脸识别、指纹识别等，表示比较担心或非常担心，其中认为非常担心的比例为17.64%，而认为完全不担心的占比仅5.60%。企业仍应重点关注用户密切关注的敏感个人信息使用的情况，提高个人信息处理透明度，加强个人信息保护，最大限度地建立用户信任。

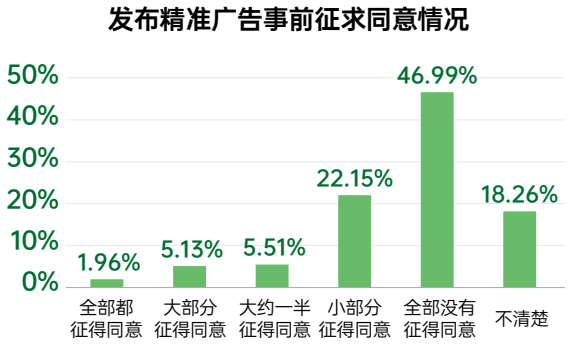


数据来源:《全国网民网络安全感满意度调查统计报告》2020

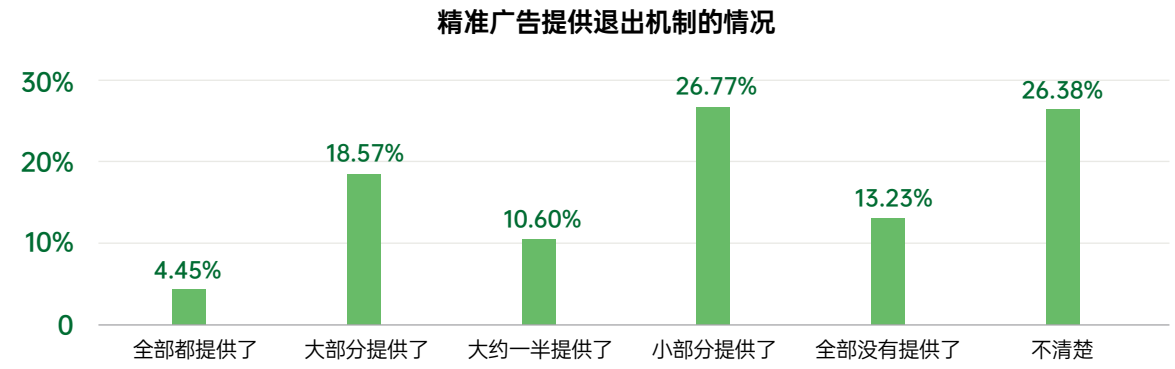
3.4 广告推送仍是用户关注的重点，对现有精准广告推送机制普遍表示不满

根据全国网民网络安全满意度调查活动的公开统计报告，有约九成受访者在日常上网过程中会收到精准广告推送，近半数受访者认为此种做法未获取其同意，且有一成左右的受访者认为没有提供退出机制。如下图，有接近60%的受访者表示会收到比较多或非常多的精准广告推送，而很少及没有此种情况占约10%；46.99%的受访者认为经营者发布精准广告之前没有征得用户的同意，而仅有约7%的受访者认为，大部分或全部征得了同意；同时，也只有约23%的用户认为全部或大部分的精准广告提供了退出机制，从精准广告退出机制占比数量看，该机制的设置仍有提升空间。





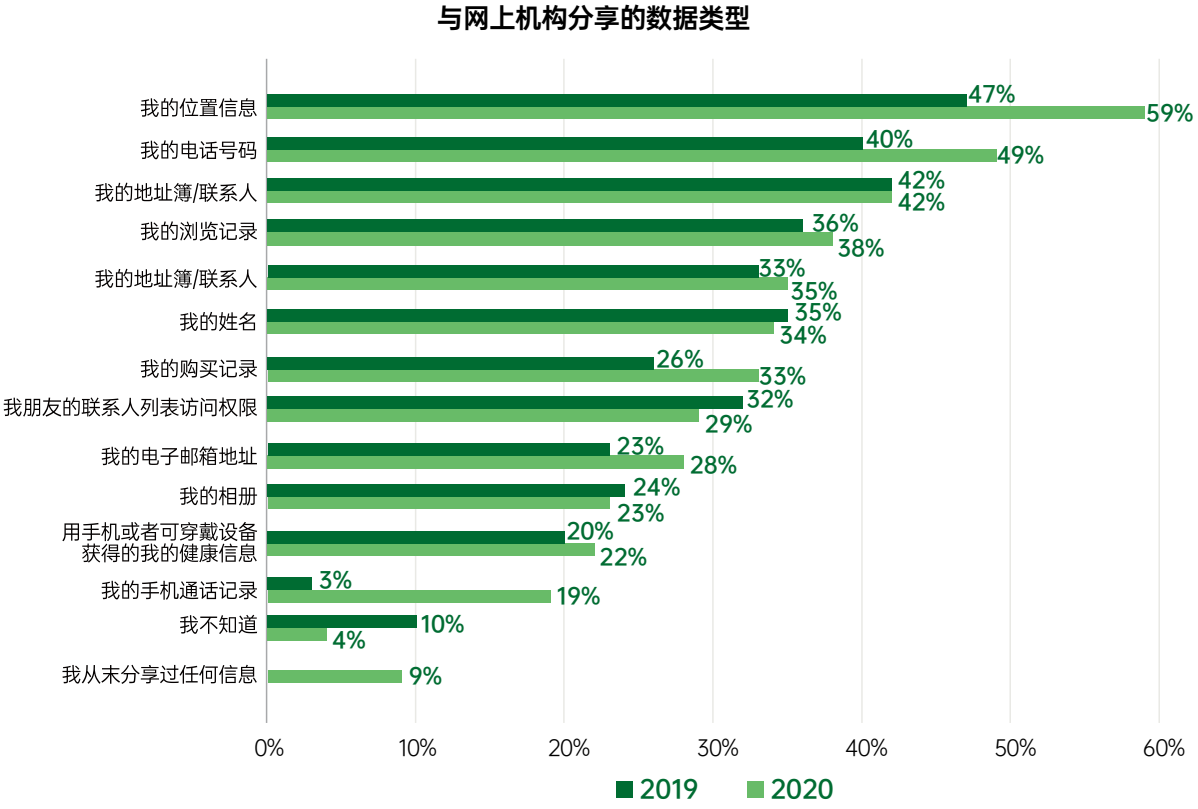
数据来源:《全国网民网络安全感满意度调查统计报告》2020



数据来源:《全国网民网络安全感满意度调查统计报告》2020

3.5 用户对分享给移动应用企业的数据细节有较高的关注，企业应审慎收集和使用个人信息，同时避免过度索权

在消费者与网上机构分享的数据类型的调查中，六成的受访者知道自己的位置信息被共享给了移动应用企业，还有将近一半的受访者共享了自己的手机号码。企业应在收集和使用的个人信息前，对收集和处理个人信息的范围按照法律法规要求进行评估，以实现产品功能所必要，收集个人信息，申请权限，对用户关注较高的个人信息类型如位置信息、手机号码、联系人等，在收集时采取审慎态度，并且避免索取非必要的权限。

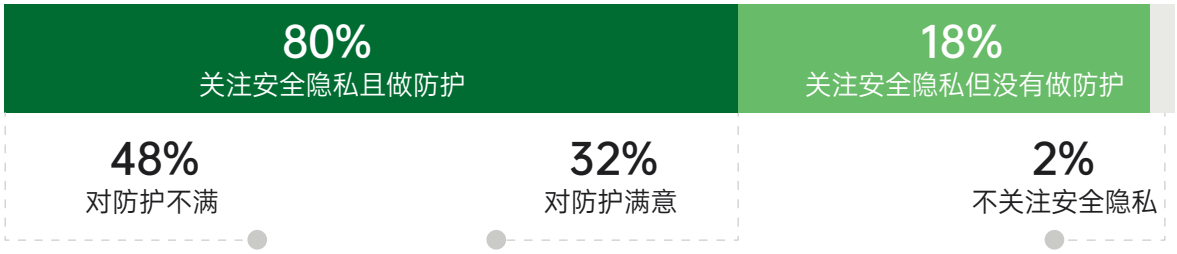


数据来源: 德勤《德勤中国移动消费者调研》2019~2020

3.6 手机用户对安全隐私敏感度较高，但对现有防护措施并不满意，比起便捷性更在意安全性，也更信任自我防护

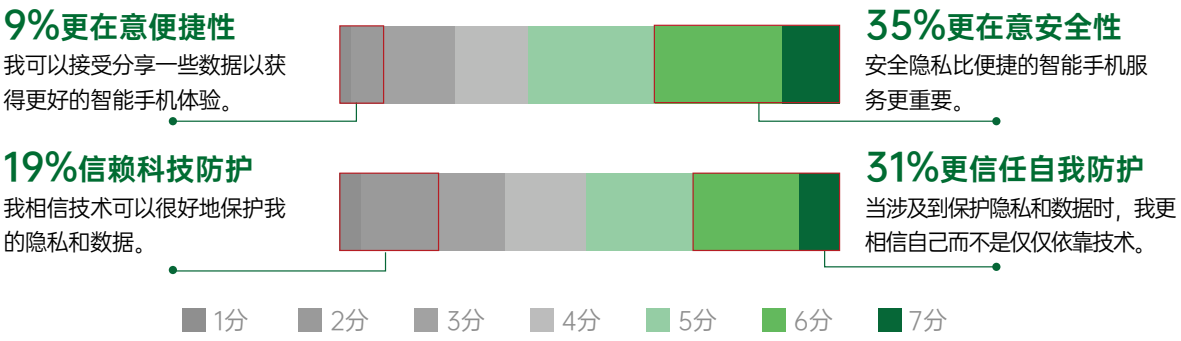
手机用户普遍关乎安全隐私问题，其中80%的受访者在日常生活中设置或采用了安全防护措施，但仅32%表示满意，安全隐私的防护体验提升仍有较大空间。在"分享数据得到更好体验"和"安全隐私更重要"之间，更多用户选择倾向更在意安全性，用户维护个人信息权益意识越来越强烈清晰。而在"信任自我防护"和"信赖科技防护"之间，更多用户倾向更信任自我防护，这意味着对于企业而言，合理确定技术与用户安全隐私防护的界限尤为重要。

以下哪种描述最符合日常生活中您对安全隐私的关注状态?



数据来源：OPPO&益普索《2021年-中国智能手机用户安全需求洞察报告》

下列安全隐私相关说法，您更认同（7分制）？



数据来源：OPPO&益普索《2021年-中国智能手机用户安全需求洞察报告》

4 移动应用（APP）企业如何切实保护用户个人信息、改善用户的“信任危机”

面对当前比较复杂的移动应用个人信息保护生态，作为企业方应该如何实施APP的个人信息保护，以期企业在满足法律法规要求的同时构建用户对企业个人信息保护的信任？

下面我们以OPPO在移动应用个人信息保护的实践作为蓝本进行介绍，抛砖引玉，希望将OPPO对个人信息保护的思考和实践经验分享给公众，同时呼吁企业和消费者参与到个人信息保护实践中，共建APP个人信息保护生态。

OPPO作为手机厂商及移动应用平台方，长期积极推动移动应用的安全合规工作开展。在持续的业务实践中，OPPO时刻关注个人信息保护领域的最新变化，洞察分析移动应用产业现状、我国立法动态及监管趋势、消费者个人信息保护关注点和产业面临的挑战，结合OPPO自身业务特点，逐步建立了一套**移动应用安全治理的实践。**

OPPO移动应用安全治理实践框架图

4.1 建立完善的安全与个人信息保护组织

4.1.1 明确组织职责，分工协作

OPPO成立了安全与合规委员会来制定安全与合规总体战略规划，统筹推进个人信息保护整体工作。

安全与合规委员会下设安全与隐私管理的三道防线，协同推进安全隐私工作的落地。

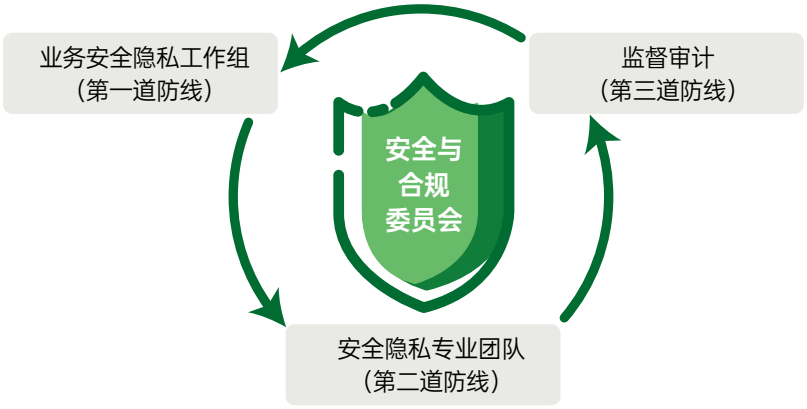
- 第一道防线，由业务部门安全与隐私合规代表/安全SE（System Engineer，系统工程师）构成，主要向业务负责人及安全与合规委员会汇报，负责产品安全隐私策略的具体落地应用、自查自纠等。

- 第二道防线，由专职的安全隐私部门构成，主要向安全与合规委员会汇报，负责安全隐私能力的建设与支持、推动产品安全隐私策略的落地。

- 第三道防线，由审计部门担任，主要向安全与合规委会员汇报，负责产品安全隐私策略落地的审计，发现风险，推动业务整改。

三道防线紧密结合，各司其职。公司同时建立清晰的问责机制，督促各级部门履行自己的职责，在发生违规情形时，将由公司进行对应的问责处置。

OPPO安全与隐私管理"三道防线"



4.1.2 通过有效的运营机制促进安全隐私目标的达成

安全与合规委员会根据公司战略制定安全与隐私的目标，同时，建立了运营机制，通过持续的运营机制和活动来推动目标的达成。包括但不限于建立业务安全隐私指标，通过安全专项来落实安全隐私目标，并定期考核业务安全隐私目标的达成情况，对结果进行公示，并对目标达成优秀的部门及个人进行激励。

4.2 打造贯穿产品全生命周期的数据与个人信息保护标准和流程

4.2.1 个人信息保护嵌入产品全生命周期

OPPO在个人信息保护实践中，除了遵照国内外法律法规要求，还积极对标行业和标准的最佳实践，并在产品开发各个环节融入这些要求和经验（Privacy by Design，Privacy by Default）。

在产品需求设计阶段，所有新增或变更个人信息处理活动（如个人信息的收集、使用、分享、跨境传输等），都需要完成安全与隐私合规评审（包含隐私影响评估、数据保护影响评估等）。评审应综合评估个人信息收集是否满足数据隐私保护原则、交互设计是否尽到充分告知义务、是否存在强制索权、数据传输存储等环节的安全保护是否充分、是否给予用户足够选择和向用户提供行使权利的便利渠道等具体事项。为了充分沟通业务逻辑和合规要求，以及在必要情况下提出相应的解决方案，业务的产品负责人、开发负责人、部门安全与隐私合规代表/安全SE、法务、安全隐私评审人员等角色均需要参加评审过程，并就产品合规事项逐一达成一致结论。只有通过安全与隐私合规评审的需求设计方案才能进入开发流程。

在产品开发过程中，开发人员应遵循企业内部的开发编码规范和安全算法使用规范。针对APP产品接入三方组件和SDK引入安全合规漏洞的问题，OPPO专门建立了三方组件、SDK准入规范和检测扫描工具，只允许在产品中使用满足要求的三方组件（含SDK）。在产品上线之前，除了常规功能和性能测试、安全测试等，涉及个人信息处理的产品还需额外通过专项合规测试。测试人员专门负责对待上线产品的个人信息保护合规情况进行复核，确保产品实现满足最新的个人信息保护合规要求。

产品在发布前需要确保满足一系列安全与隐私合规要求，包括通过产品安全与隐私合规测试等。产品运营时也要求运营、客服、安全与隐私和法务团队在规定时间内响应用户个人信息权利请求。

在整个过程中，安全隐私专业团队负责把控关键节点，并持续推动合规标准更新和落实。OPPO安全隐私专业团队负责及时同步最新监管要求，研讨行业最佳实践，将要求融入到企业内部制度规范和流程中，并通过安全开发流程管控，及时发现和控制产品中的合规风险，推动产品团队进行整改。OPPO子午互联网安全实验室和OPPO安珀实验室严控安全与隐私合规检测关卡，推动数据安全与隐私合规要求的切实执行，为用户建立稳固的事前安全防线。为了确保公司从管理层到普通员工均熟知OPPO对用户数据保护的承诺及具体要求，OPPO定期组织全公司范围的课程学习、测验，由安全隐私专业团队进行专业培训，并将测试通过情况纳入考核指标。

OPPO安全隐私融入产品研发全生命周期

4.2.2 全流程的数据安全管控体系

尊重和保护用户的个人信息和合法权益是OPPO对用户的一贯承诺。为此，OPPO建立了一套完善的覆盖数据全生命周期的数据安全管控体系，通过安全团队与业务团队紧密合作在业务各场景落实。例如上文介绍的个人信息保护嵌入产品设计实践也是数据安全管控体系落地的具体实例。此外，以数据分类分级为基础，OPPO细化了数据生命周期各个阶段对应的安全保护要求，并通过安全测试、内外部审计等方式对各合规情况进行检查评估。

首先，根据OPPO业务特点和行业最佳实践经验，OPPO制定了适应自身发展和符合合规要求的数据分类分级规范和详细的示例表。为促进去标识化技术的应用，还规范了部分场景中数据敏感程度降级策略。

以数据级别为依据，OPPO进一步通过数据安全规范规定不同级别的数据，在收集、传输、存储、使用、分享、销毁等环节应遵循的不同保护措施，包括技术措施和管理措施。例如，收集阶段应对确保符合数据最小化原则、验证数据质量和完整性；敏感级别较高的数据在传输和存储时应对数据内容单独进行加密；整个数据处理过程需进行日志记录，并对日志信息采取严格的保护措施，确保所有的数据操作可以被追溯和审查；敏感数据操作需进行实时自动化审计；运维、运营场景中，对可能涉及到用户个人信息的场景也需要做必要的隔离和特殊保护；对超出留存期限或用户要求删除的数据应采用规定的技术及时删除或匿名化。对于不同的数据保护措施，也制定了相应的技术和管理规范，详细列出了要求的技术参数、管理流程。例如，加密算法禁止使用的模式、最低密码强度要求、业务数据访问权限申请开通流程、权限管理操作规范等等。

根据审计团队工作计划或特殊专项工作要求等，OPPO联合内部及外部专业审计团队，定期或不定期组织实施安全与合规审计工作，并向安全与合规委员会汇报。根据审计结果，安全与合规委员会对业务合规情况进行公开奖惩，并推动整改和内部制度升级完善。

4.3 构建个人信息保护的数据安全技术防御体系

OPPO在数据安全技术方面，以六层防御系统为基础，打造数据安全防御体系，运用AI、大数据等新技术，实现智能化数据安全防护能力，将安全活动贯穿产品全生命周期，为产品安全提供强有力的保障手段，为用户提供安全可靠的互联网产品和服务，共同保障用户个人信息安全。

4.3.1 六层防御系统，打造数据安全防御体系

- **第一层防御系统，移动端安全**
  OPPO通过为移动应用提供专业、高效、便捷的一站式应用安全解决方案，涵盖应用加固（含SDK加固）、移动端安全密钥管理、安全组件等安全与隐私保护能力，有效对抗多种反编译逆向攻击，提升移动应用安全指数。

  构建了端云协同、多产品联动的智能实时APP安全隐私治理体系——OPPO智能护盾， 贯穿APP的测试、上架、下载、安装、运行、升级、卸载、下架全生命周期， 提供安全漏洞扫描、个人信息保护合规检查、恶意行为检测等服务，打造绿色安全的开发者生态，为手机用户提供全方位的安全隐私保护。

- **第二层防御系统，网络安全**
  OPPO通过动态防火墙系统实现安全区域划分与隔离，根据不同区域以及业务需求，确定安全策略，并可以跟随业务扩容实现自动扩展。

  在互联网出口部署流量分析和流量清洗，实现网络恶意流量的检测及清洗，支持缓冲区溢出、SQL注入、暴力猜测、DDoS攻击、扫描探测、蠕虫病毒、木马后门、间谍软件等各类入侵攻击的检测和防御，为用户使用安全可靠互联网业务提供保障。

- **第三层防御系统，接入层安全**
  接入层采用统一接入网关，并结合Web应用防火墙，通过防御SQL注入、XSS跨站脚本、常见Web服务器插件漏洞、木马上传、非授权核心资源访问等OWASP常见攻击，过滤海量恶意访问，避免Web应用服务和系统数据泄露，保障Web应用和服务的安全与可用性。

- **第四层防御系统，业务层安全**
  OPPO提供业务安全风控服务，支持帐号安全保护、虚拟财产保护、虚假流量识别等，提供多种业务风险场景下的安全保障，确保各类异常行为特征都能被及时发现和响应。

- **第五层防御系统，主机层安全**
  态势感知系统提供了基于环境动态、整体的洞悉信息资产安全风险的能力，能够主动的对信息资产环境进行风险探测，通过及时同步最新风险信息库，确保实时、准确识别安全风险。并通过可视化技术，提供清晰的安全状态与趋势视图，为安全运营人员制定有效风险应对措施提供依据。

  主机入侵检测系统支持定期检测主机及核心软件的配置安全情况，实时监控主机异常登录、恶意程序、恶意链接、Webshell等攻击风险，提升业务后台运行环境安全等级，降低业务数据泄露风险。

- **第六层防御系统，数据层安全**

  通过密钥管理服务，帮助业务/用户创建和管理密钥，保护密钥的保密性、完整性和可用性，满足多应用多业务的密钥管理需求，保障数据传输以及存储的机密性。

  基于OPPO数据分类分级标准，采用自定义的脱敏技术对敏感数据脱敏，保障用户数据安全。

4.3.2 运用AI、大数据等新技术，实现智能化数据安全防护能力

OPPO采用大数据技术，将安全数据整合并不断进行沉淀，形成安全大数据；通过AI分析引擎，对海量安全数据进行深度挖掘分析，有效发现并感知威胁；整合安全能力，实现策略联动，对威胁做出更加智能的预警及处置，为互联网业务提供更加智能的安全防护能力。

OPPO数据安全技术防御体系图

4.4 尊重用户权益，完善数据主体权利保障机制

OPPO尊重用户权益，致力于实现用户隐私与数据主体权利，并为用户提供便捷的权利行使途径。

4.4.1 权利类别与保障方式

- **知情权**

  用户对其个人信息的处理享有知情权、决定权。OPPO尊重用户的知情权，在用户访问我们的网站或者使用我们的产品或服务时，我们提供详细的个人信息保护政策以帮助用户了解OPPO处理个人信息的实践。

- **访问权**
  用户有权查阅、复制其个人信息。对于部分产品或服务，用户可以在OPPO产品/服务的页面直接查阅、复制其个人信息，例如，用户可以随时通过登录OPPO官方商城以查阅其历史订单信息。对于其他未提供直接查阅或复制个人信息的OPPO产品或服务，用户可以通过与OPPO数据保护官取得联系以行使其享有的查阅或复制权利。

- **更正权**
  用户享有对其个人信息更正、补充的权利。当用户在使用OPPO产品/服务的过程中发现其个人信息不准确或者不完整的，可以在产品/服务页面更新或通过与OPPO数据保护官取得联系以确保用户的个人信息准确无误且最新。

- **删除权**
  用户在法律法规规定的情形下，有权请求OPPO删除其提供的个人信息。通常而言，当用户的个人信息对于OPPO的产品/服务的实现不再必要时，或者该个人信息的保存期限已届满等情形下，OPPO会主动删除用户的个人信息。用户也可以通过产品/服务页面或通过与OPPO数据保护官取得联系，以主动请求删除其个人信息。

- **撤回同意权**
  OPPO基于用户的同意处理用户个人信息，用户有权撤回其同意。用户可以通过删除信息、关闭设备权限设置、更改相关产品或功能设置页面等方式改变其授权OPPO收集个人信息的范围或撤回其授权。

4.4.2 全球用户数据权利保障平台

数据主体权利平台（Data Subject Rights Platform，DSR）是为用户提供投诉和问询的平台。用户可以根据自己想要问询的商品/服务类型，对OPPO个人信息处理活动的任何问题或者疑虑进行问询或投诉。目前平台提供数据权利行使、隐私投诉、数据泄露报告等多种咨询类型，用户可以在问题中上传文字、图片等附件详细描述投诉或问询内容。
（DSR：https://www.oppo.com/cn/privacy-feedback/）

OPPO数据主体权利平台

OPPO安全隐私官网DSR入口

4.4.3 数据保护官邮箱

OPPO正式任命内部数据保护官，依其授权履行数据保护官的职责。包括提供数据保护方面的信息和建议，对企业数据与隐私合规以及数据保护方面所做的工作进行监管，并与用户进行沟通，协助实现数据主体的数据权利。

如果用户对OPPO的个人信息保护的做法有任何问题或疑虑，都可以通过数据保护官邮箱（privacy@oppo.com）直接与OPPO的数据保护官取得联系。

4.5 优化用户体验，主动打造产品安全隐私特性，提升用户信任

OPPO通过对用户和行业洞察，挖掘用户痛点，通过深入分析和调研，确认产品需求开发落地，提供给用户使用。在安全隐私特性设计和优化过程中，OPPO将用户的参与感、掌控感，以及功能使用的便捷性、可靠性也纳入考量，给予用户更强的安全感。OPPO将持续打造产品安全隐私能力，致力于给用户提供更好的安全隐私体验。

4.5.1 帐号：打造全场景、高等级、安全可信的帐号防护体系

- **多重防护**

  为了保障用户帐号安全，OPPO帐号采取主动验证结合被动扫描的方式，包括环境安全检测、多因素认证、防暴力破解、帐号申诉等多重维度确保帐号安全性。

  首先，用户在高风险场景中或敏感操作前会额外增加一种或多种验证，如：当检测到环境不安全时，在修改密码前需增加紧急联系人验证码或其他校验方式，通过后才可进行修改。

  其次，OPPO帐号会进行一系列业务风控检测（帐号防撞库破解、环境安全检测、防暴力破解）来确保当前的安全程度，以匹配不同等级的校验方式。

  当帐号丢失或被盗、忘记密码、被他人更换了手机号等情况下，可以进行帐号申诉，以保障用户可以继续使用原帐号，帐号申诉时需要提供帐号使用记录、帐号历史信息、密保问题答案、实名认证信息等。

- **设备管理**

  用户可以轻松管理自己帐号下登录的所有设备，查看已登录设备信息，如果用户发现自己帐号在未知的设备上登录，还可以将帐号从该设备上踢出，保护用户的数据资产及隐私安全。

- **敏感操作提醒**

  当某帐号的敏感信息，如密码、手机号、邮箱、紧急联系人、实名认证等发生变更时，该账号的用户都会收到短信提醒。同时，用户也可以在登录记录中查看历史记录，获知登录时间、登录设备等信息，以及时发现潜在风险。

4.5.2 云服务：为用户提供端到云、云到端、端到端的全链路数据安全保障

- **数据传输加密**
  云服务在业界主流的HTTPS安全协议基础上，综合利用云端的硬件加密机集群、高等级加密和身份认证算法等构建第二层应用层数据加密隧道，确保用户数据传输安全。

- **数据存储加密**
  云服务使用基于硬件加密机（HSM）的安全密钥管理服务（KMS）为每个用户生成独一无二、定期更换的数据加密密钥（DEK），并结合高等级加密算法加密用户数据，确保用户存储在云端的数据都得到高等级的安全防护。

- **数据防丢失**
  为了减少硬件故障、自然灾害或其他灾难带来的数据丢失风险，OPPO在多地建立数据中心，采用数据及服务的高可用性方案，为用户提供安全可靠的服务。

- **云服务数据管理**
  云服务为用户提供了数据同步、备份和云盘的功能，使用户可以安心使用云服务功能，自由管理保存在云盘的数据。

4.5.3 浏览器：通过技术特性驱动，给用户提供“放心搜、安心看”的浏览器

OPPO通过技术特性驱动，给你提供“放心搜、安心看”的浏览器。

- **恶意网址警告**
  当用户使用浏览器访问网址前，浏览器会对网址内容进行多维度的安全分析和检测，精确识别钓鱼、木马病毒、博彩等恶意网址。当检测到恶意网址时用户会收到警告提示，降低因访问恶意网址面临的数据泄露以及财产损失的风险。

- **无痕模式**
  在无痕浏览模式下，浏览器不会留存用户的浏览记录、搜索记录、以及“自动填充”的信息。

- **隐私空间**
  当用户使用特定网址进行下载时，浏览器会将用户下载的内容放入浏览器内置的自有权限目录中，避免被系统其它应用扫描到该文件的存在，从而实现私密空间，用户下载的特定内容不希望在相册或其它文档系统中被发现，可通过该功能将文件隐藏起来，从而保护隐私。

- **下载防护**
  当用户下载APP时，浏览器会自动识别非安全应用，并做风险提示和协助拦截，避免用户下载到恶意的APP，同时主动提供经过官方认证的安全下载路径，帮助用户安全高效完成APP下载需求。

4.5.4 软件商店：APP全流程应用管控

OPPO软件商店对每款APP均进行了全方位、深度的自动检测与人工检测，严控APP的"审核-上架-下载-安装-更新-管理-反馈"的全流程。

- **APP安全隐私检测**
  为了确保软件商店上架资源的安全性，OPPO采用了自研的应用检测系统，配合人工检测，再结合第三方安全检测能力的辅助，每一个APP上架前都必须经过5大方向15项自动化检测与147项的人工检测，全方位、全天候，贯穿上架、下载、安装、使用、卸载、下架的全流程跟踪，只为给用户更安全的保障。

- **未知来源安全管控**
  当用户正在下载的应用来源于未知渠道时，软件商店会对该应用进行安全检测，若发现有病毒、广告插件、无图标应用等，则会进行风险提醒。

- **APP透明度**
  对于软件商店已上架的APP，在APP详情页用户可以查看APP的隐私政策、敏感权限和对应权限用途描述。

- **APP投诉**
  用户可以通过APP详情页进行投诉，随时举报移动应用是否有恶意广告、恶意扣费、病毒木马、侵犯隐私等问题，软件商店将根据投诉内容进行验证，核实确认后，软件商店将及时进行处置。

4.6 建立应急响应处理机制

为及时响应及处理OPPO产品与服务的安全隐私事件，OPPO建立以下应急处理机制和流程。

- **OPPO安全应急响应中心（OSRC）**
  OPPO通过建立安全应急响应中心，收集外界安全专家提交的安全与隐私漏洞，补充来自外部视角的产品安全隐私监督，及时发现及处理漏洞，可以很大程度上降低产品的安全风险。

  同时，OPPO也建立了个人信息的泄露事件应急处理流程，应对可能发生的个人信息泄露风险处置，确保应急处理的及时性与合法性。

- **外部事务的应急响应**
  OPPO建立了专门的应急响应小组，主要负责处理以下事务：

  - 洞察监管治理态势，研究标准及处理原则，融入内部合规制度，指导产品安全合规运行。
  - 及时跟进监管通报事件，积极组织产品/服务整改，响应及处置合规问题。
  - 响应来自用户针对产品的安全隐私问题的反馈或咨询等。

4.7 建立全球合规体系

在安全隐私实践上，OPPO始终以高标准要求自我。OPPO主动推动与第三方权威认证机构在欧盟GDPR数据监管、自证合规、专业能力提升等方面进行深度合作，不断优化和提升OPPO隐私保护水平，为数据资产合规运营保驾护航。目前已通过多项国内外和行业安全合规资质认证，如TRUSTe、ePrivacy、ISO 27001、ISO 27018、ISO 29151、ISO 27701、CSA STAR等。

此外，OPPO多项金融类业务今年通过了PCI-DSS（Payment Card Industry Data Security Standard）第三方支付行业数据安全标准权威认证。

CSA STAR
云安全认证

TRUSTe
企业隐私与数据
治理合规认证

ePrivacyseal
隐私保护认证

IOS/IEC 27001
信息安全管理
体系标准认证

IOS/IEC 27701
隐私信息管理
体系标准认证

IOS/IEC 27018
公有云个人身份
信息管理体系认证

公安部信息系统
安全等级保护认证

PCI DSS
支付卡行业
数据安全标准认证

4.8 共建行业安全与隐私生态

OPPO始终相信，健康健全的行业安全与隐私生态能够帮助APP产业得到更长久的发展。作为行业一员，OPPO通过多种渠道积极与众多互联网企业、安全公司、民间社团和个人密切合作，推进安全交流和资源共享，探讨和输出行业最佳实践，持续推动行业生态建设。

OPPO安全应急响应中心（OSRC）不但是OPPO面向全社会收集并响应安全漏洞与情报的平台，也承担着OPPO与安全业界同仁合作、交流平台的重任，持续致力于保障OPPO亿级用户及多元化业务和产品的安全与隐私，是OPPO安全生态体系建设中的关键一环。自2018年成立以来，OSRC已参加了30多场海内外知名安全峰会/论坛，通过公众号、论坛、媒体等渠道发布众多技术类文章，定向触达专业人员人次10万以上，同时，OSRC吸引来自全球59个国家的、超过2500位安全研究者加入，与OSRC共同建设着OPPO的全球安全防护体系。此外，OSRC通过举办OPPO安全网络安全挑战赛的形式积极吸引高校和研究院同学的关注，激发更多人群投身安全事业，参与安全前沿问题研究和讨论的热情。

OPPO子午互联网安全实验室以“保护用户的安全与隐私，为品牌注入安全基因”为使命，持续关注并深耕于业务安全、Android安全、IOT安全、红蓝对抗、隐私保护等领域。成立以来，子午除了将安全隐私能力应用于自有业务外，还积极回馈业界，多次在国内外安全会议发表演讲、论文，在业界首次公开发布“快应用安全与隐私检测项”，发现多个行业通用安全隐私问题并获得公开致谢。

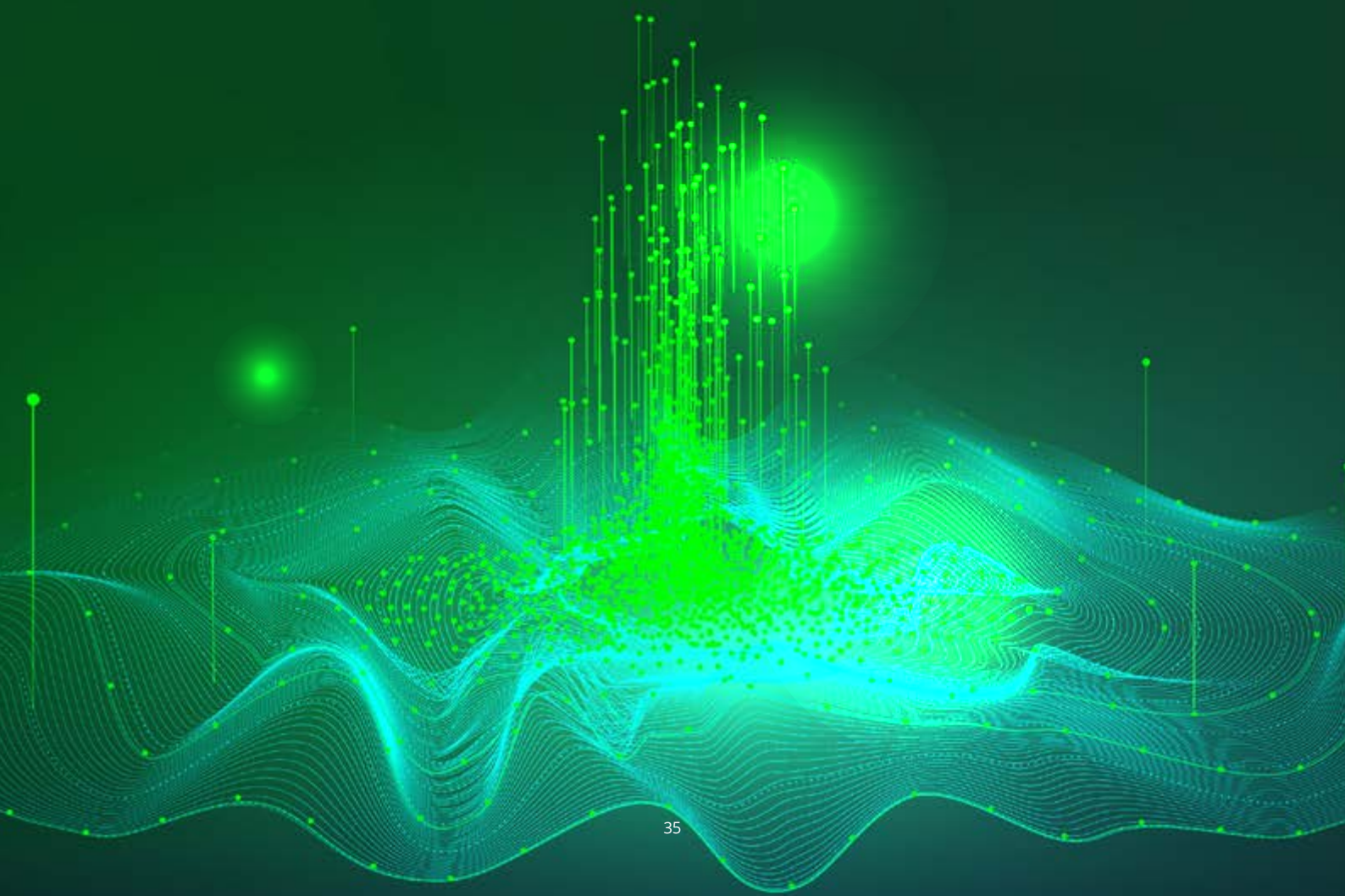
OPPO安珀实验室以用户数据安全和隐私保护为核心，专注于智能终端安全、物联网安全、可穿戴设备安全、漏洞挖掘、威胁监测及数据情报等领域，着力聚焦前沿技术研究，构筑安全攻防与隐私保护能力，为合作伙伴及用户打造信息安全堡垒，向消费者提供安全可信赖的产品和解决方案。安珀实验室自成立以来，在主流操作系统、移动浏览器、物联网设备等方向多次向业界知名厂商提交漏洞研究报告，参与各类学术和产业会议并分享技术研究成果，不断促进行业内技术交流与合作，共同建设合作共赢的安全生态。

OPPO关注新技术发展，更关注新技术应用带来的风险和益处。在运用新技术（如人脸识别、语音识别、大数据、人工智能等）开展业务前进行安全与隐私合规评审，持续关注外部监管动态，更新内部合规制度，并积极探索在新技术应用场景下个人信息保护最佳实践。为构建领先的安全与隐私保护技术，OPPO与高校、实验室共同合作科研项目，对安全与隐私保护先进技术进行专项研究和突破，并推动在企业内部的试用。OPPO还聘请多位业内知名安全隐私技术专家、法学教授为外部顾问，为安全隐私工作提供方案指导和能力支持。同时，OPPO还引入业内头部咨询公司，实施数据与隐私保护专项，结合行业最佳实践打造OPPO个人信息保护技术体系。

OPPO安全隐私专业团队还积极通过国内各类标准组织输出实践经验。截止2020年底，安全隐私专业团队牵头和参与的隐私安全标准达到20多个，为移动互联网行业和大安全领域的标准化建设贡献力量。通过标准协作，OPPO与业内其他厂商、广大互联网公司、监管机关等充分交流，将厂商能力和解决方案输出讨论，厘清互相存在的误解，弥合认知差距，增强标准可执行性，并为监管治理提供参考。

作为APP分发平台，OPPO软件商店也积极响应监管要求，在配合监管行动、向开发者同步宣导要求、提升自身检测能力方面等都认真履行自身责任。2021年截至8月底，商店已协助监管方下架322款出现问题的APP，并为开发者提供整改建议，切实履行分发平台合规义务。配合APP治理活动，OPPO不但推动内部专项整改排查，也通过邮件通知、客服通知、更新上架规范等方式及时向开发者同步监管最新要求，扩大开发者触达范围，促进整改治理。在应用检测能力强化方面，在过去的2021上半年中，OPPO智能护盾共处理应用和游戏上架申请50万余次，其中14万次未通过审核。通过持续技术对抗，共发现并下架色情、博彩、欺诈、恶意广告、隐私窃取等类型的恶意应用1400余款，精度达99.99%。OPPO也在积极推动内部应用的检测标准输出，为广大开发者提供合规指引，推动行业合规共建。

5 行业生态倡议及消费者个人信息保护建议



5.1 行业生态个人信息保护倡议

作为个人信息保护责任主要的主体，分发平台方、APP开发运营方、SDK提供者及相关供应商企业等诸多主体，共同承担着优化行业生态，促进有序行业规范建立的责任。各类主体提高主体责任意识，强化个人信息保护重视程度，厘清自身与其他类型第三方的合作关系，基于法律法规对各类主体的不同要求履行各自特定的义务，并建立必要的风险评估及个人信息泄露事件应对等合规机制，是建立良好行业生态的重要保障。基于此，我们提出以下倡议。

5.1.1 提升个人信息保护水平，主动打造安全隐私功能

APP开发运营者完善个人信息保护制度和工作机制，提升安全保障技术能力，积极开展个人信息保护评估，加强对第三方SDK安全审核和管理，并将个人信息保护融入产品全生命周期，保持主动心态，吸取行业最佳实践，主动检测，主动合规，做好用户个人信息保护的事前防护措施。同时，持续洞察用户个人信息保护关注点，提供更好的安全隐私功能及体验，以化解用户隐私保护的“信任危机”。

SDK提供者完善个人信息保护合规体系，吸取历史经验，在提供服务的过程中采取必要安全措施以保证用户个人信息安全，并向APP开发运营者及最终用户公开收集使用个人信息规则。

APP分发平台加强APP上架审核和在架监测管理，对APP上架基本信息进行公示，将APP个人信息合规要求作为审核重点，拒绝存在恶意行为和明显违规的APP上架申请，及时处置在架监测过程中发现的和监管部门要求下架的违法违规APP。

5.1.2 加强行业协同与合作，分享隐私保护能力，提升行业隐私保护水平

行业间各主体协同合规和加强合作，更加促进行业良性发展。我们倡议，APP分发平台对在架APP开发运营者提供监管政策宣贯，并为其合规整改提供建议；APP开发运营者在上架前，主动进行合规检测，并配合APP分发平台提供必要的信息；SDK提供者主动向APP开发运营者提供其收集使用个人信息规则，并在出现合规事件时积极配合APP开发运营者完成整改。除此之外，优势企业可以通过推进标准和指南的制定，向行业宣传推广其实践经验，主动探索隐私保护技术创新应用等方式，带动行业个人信息保护水平提升。

5.1.3 加强行业用户教育力度，提升用户防护意识，同时降低因认知差异带来的隐私焦虑

少数媒体和公众对于企业在合规开展业务过程中的一些措施存在误解，加之用户安全防护意识尚不完全成熟，导致认知差异给当前良好的行业生态带来一定的挑战。企业可以积极探索多渠道，多触点与媒体和用户沟通，在宣传用户如何增强自身安全防护措施的同时，通过知识科普向媒体和公众解读个人信息保护政策、以及个人信息保护背后的安全保障能力构建等内容，降低因认知差异带来的隐私焦虑。

5.2 消费者个人信息保护建议

如上所述，良好行业生态的建立，需要监管、行业、消费者多方共同努力。同时，治理水平、行业自律、消费者认知三方是相辅相成，共同稳步提升的。因此，消费者主动提升风险防范意识，养成安全使用习惯，不仅有助于避免风险事件，保障消费者个人信息安全，更重要的是，能够反哺监管要求的落实及更新，促进行业各主体的自律及主动合规。

我们建议，在日常互联网产品的使用中，消费者可以保持以下良好习惯：

- 在正规应用商店或者APP产品提供者官网下载APP，不点击来源不明的链接进行下载安装；
- 使用APP及相关服务前，仔细阅读个人信息保护政策，充分了解APP收集和使用个人信息的类型、目的和方式，以及如何行使用户权利方式等内容；
- 谨慎授予APP使用敏感权限（如位置、相机、麦克风、通讯录等），可以在使用APP特定功能或服务时打开相关敏感权限，不使用时关闭；
- 多使用APP提供的隐私功能或隐私设置，主动、合理行使自己的对于个人信息的权利；
- 发现安全隐患时，及时联系APP产品提供方，可以有效减少安全事件带来的不利影响；
- 遇到侵犯用户个人信息情况时，及时联系产品提供者或向有关机构进行投诉。

致谢

《移动应用（APP）个人信息保护白皮书》由OPPO和德勤创作团队共同完成。

感谢参与到白皮书内容创作过程各位努力和付出:
韩方、薛梓源、肖腾飞、刘桃松、何智聪、杨晓丹、申燕茹、付艳艳、赵鹏阳、刘文园、沈海涛、彭星、刘湛卢、罗元海、曾德康、陈海龙、陈勇、肖楠。

同时，也特别感谢个人信息保护领域专家在白皮书修订过程中的帮助和宝贵建议:
陈纲、胡珀、洪延青、聂君、王红阳、吴沈括、魏巍、杨正军。

（以上排名不分先后）