【清朗数字生活 守护信息安全】警惕应用程序过度索权陷阱，筑牢个人信息保护防线

个人信息的安全守护，既有着法律法规的刚性约束，也需要普通用户提升防范意识，远离应用程序过度索取、违规收集个人信息的陷阱。在移动互联网深度融入生活的背景下，部分App、小程序运营主体及第三方服务商，利用用户对权限授权的认知盲区，超范围收集、违规传输甚至因技术漏洞泄露个人信息，导致用户遭遇广告骚扰、精准诈骗，甚至敏感隐私信息被非法获取。以下结合民生消费领域专项整治中的典型案例，拆解应用程序过度索权及信息泄露的套路与风险，明确个人信息保护与维权的正确方式。

典型案例：应用程序违规处理个人信息的多重陷阱

案例1：未获授权后台偷采信息，基础权限成“信息窃取通道”

用户在使用某民生服务类App时，仅完成下载登录操作，未收到任何权限授权弹窗，也未对相机、存储、应用列表

等权限进行确认，而 App 后台已默认收集用户安卓 ID、应用包信息、手机外部存储文件等个人信息。该行为直接违反个人信息保护相关规定，用户的设备基础信息被悄无声息窃取，为后续信息滥用、倒卖埋下隐患，用户可能因此收到定向推送的广告，甚至面临设备信息被用于网络诈骗的风险。

案例 2：酒店小程序违规传输位置信息，用户隐私“被共享”不知情

用户打开某酒店住宿类小程序进行预订时，小程序在未告知、未取得用户单独同意的情况下，自动调用小程序位置权限获取用户实时经纬度信息，并直接将该信息同步给第三方地图工具，由地图工具转化为具体地理位置后反馈给小程序。整个过程用户完全不知情，个人位置信息被违规传输，不仅侵犯了用户的信息决定权，还可能导致用户的出行轨迹、住宿偏好等隐私被第三方获取，存在被精准跟踪、诈骗分子利用位置信息实施骗局的潜在风险。

风险拆解：应用程序违规处理个人信息的核心套路

索权阶段：权限与功能脱节+诱导/强制授权，抓住用户认

知盲区

1.超范围索取权限，将非必要权限作为使用前提，如天气类App要求读取短信、点餐类App要求访问通讯录，以“不授权则无法使用”的捆绑策略逼迫用户妥协；

2.反复弹窗诱导授权，对与基础业务功能无关的权限（如休闲类App索要位置信息）多次弹窗提醒，利用用户嫌麻烦的心理促成授权；

3.隐藏权限授权提示，将权限请求嵌入晦涩的用户协议中，未以显著方式告知用户收集、使用个人信息的范围、目的，用户在不知情的情况下“被动授权”。

处理阶段：违规收集+非法传输+保护缺失，无视用户信息安全

1.未征得用户同意，在后台默认收集、读取个人信息，绕过用户授权环节实施“偷采”，涉及设备信息、存储文件、应用列表等多类信息；

2.未经单独同意，将用户个人信息同步、传输给第三方服务商，且不向用户告知信息接收方、传输内容及使用目的，违反信息传输的合规要求；

3.重收集轻保护，部分运营主体及第三方服务商虽合法收

集个人信息，但未采取必要的安全保护措施，存在身份验证不完善、系统漏洞未修复等问题，导致信息易被非法获取；

4.第三方平台漏洞牵连下游主体，提供技术支持的第三方平台自身存在安全缺陷，却未及时整改，导致其服务的所有子系统、合作方均面临信息泄露风险，隐患覆盖范围广、影响人数多。

后果阶段：信息泄露+滥用倒卖，引发多重连锁风险

违规收集、传输、泄露的个人信息，大多会流入网络黑灰产，经倒卖、传播后被不法分子利用，给用户带来不可逆的多重危害：

1.遭遇广告骚扰，用户手机号、位置信息、消费偏好等被用于定向推送广告，干扰正常生活；

2.面临精准诈骗，不法分子利用掌握的用户姓名、年龄、生活习惯、财产信息等，编造虚假场景实施电信诈骗，诈骗成功率大幅提升；

3.敏感隐私曝光，如患者疾病信息、未成年人身份信息等被泄露，侵犯用户人格权益，还可能引发名誉损害、生活困扰；

4.身份被盗用，用户身份证号、银行卡关联信息等被非法获取后，可能被用于冒名贷款、注册非法账号等，给用户造成财产损失和法律风险。

核心风险：应用程序违规处理个人信息，用户面临的四大不可逆危害

1.信息控制权丧失：用户对自身个人信息的收集、使用、传输失去主导权，未被告知、未同意的情况下，信息被随意采集、流转，隐私权益被直接侵犯；

2.信息泄露无边界：电子信息的传播特性导致泄露的个人信息可快速遍布网络，一旦泄露难以追回、删除，用户长期处于信息被滥用的风险中；

3.财产与人身安全受威胁：信息被黑灰产倒卖、不法分子利用后，用户极易遭遇电信诈骗、身份盗用，引发直接财产损失，部分敏感信息（如位置信息）泄露还可能带来人身安全隐患；

4.维权举证难度大：用户难以察觉后台的违规收集、传输行为，发现信息泄露时，往往无法精准定位责任主体，也难以留存有效证据，维权过程耗时费力。

风险防范：移动互联网时代，个人信息保护自保指南

面对应用程序五花八门的权限请求和潜在的信息安全风险，守护自身个人信息安全，核心是“严授权、勤检查、善规避、勇举报”，牢记5点自保原则，远离“隐私刺客”：

1.拒绝非必要授权，对频繁索权说“不”：安装、使用App/小程序时，仔细甄别权限与业务功能的关联性，天气类App拒读短信、点餐类App拒访通讯录，对与基础功能无关的权限坚决拒绝；对反复弹窗、诱导授权的应用，直接卸载并远离。

2.及时注销闲置账号，删除留存个人信息：对不再使用的App/小程序，切勿仅卸载了事，需通过官方渠道完成账户注销，并删除平台内留存的姓名、手机号、身份证号等个人资料；若平台未提供注销、删除信息功能，可认定为违规并进行举报。

3.定期检查权限设置，关闭闲置授权：利用手机操作系统的权限管理功能，定期检查已安装App的权限开启状态，及时关闭长期闲置应用的相机、位置、麦克风、存储等非必要权限，从源头切断信息收集通道。

4.关注官方违规名单，提前规避风险：关注网信、公安等执法部门定期发布的违规App/小程序公告，对被通报的问

题应用，不下载、不使用，已安装的及时卸载，从源头规避信息安全风险。

5.留存证据及时举报，遭遇违规主动维权：发现应用程序存在未授权收集信息、违规传输隐私、技术漏洞泄露信息等行为时，留存好截图、操作记录、通信记录等证据，通过 12345 市民服务热线等官方渠道投诉举报，由执法部门依法依规处置。

结语：坚守合规底线，筑牢个人信息保护“双重防线”

个人信息是数字时代的重要“个人资产”，其保护既需要监管部门的严格执法，也需要用户的主动防范，更离不开运营主体的合规自律。监管部门持续开展专项整治，查堵漏洞、查处违规，为个人信息保护筑牢“监管防线”；而应用程序运营主体及第三方服务商，更应坚守合法、正当、必要的个人信息处理原则，摒弃“重收集轻保护”的思维，采取必要的安全保护措施，履行信息保护的主体责任。

作为普通用户，更要提升个人信息保护意识，摒弃“嫌麻烦、随便授权”的不良习惯，守住“不随意授权、勤检查

权限、及时注销账号”的底线，主动学习个人信息保护相关知识，让每一次对非必要权限的“拒绝”，都成为守护自身隐私的重要一步。唯有监管、运营主体、用户三方协同发力，才能真正筑牢个人信息保护的“双重防线”，让移动互联网的便利与安全兼具，让数字生活更清朗、更安心。