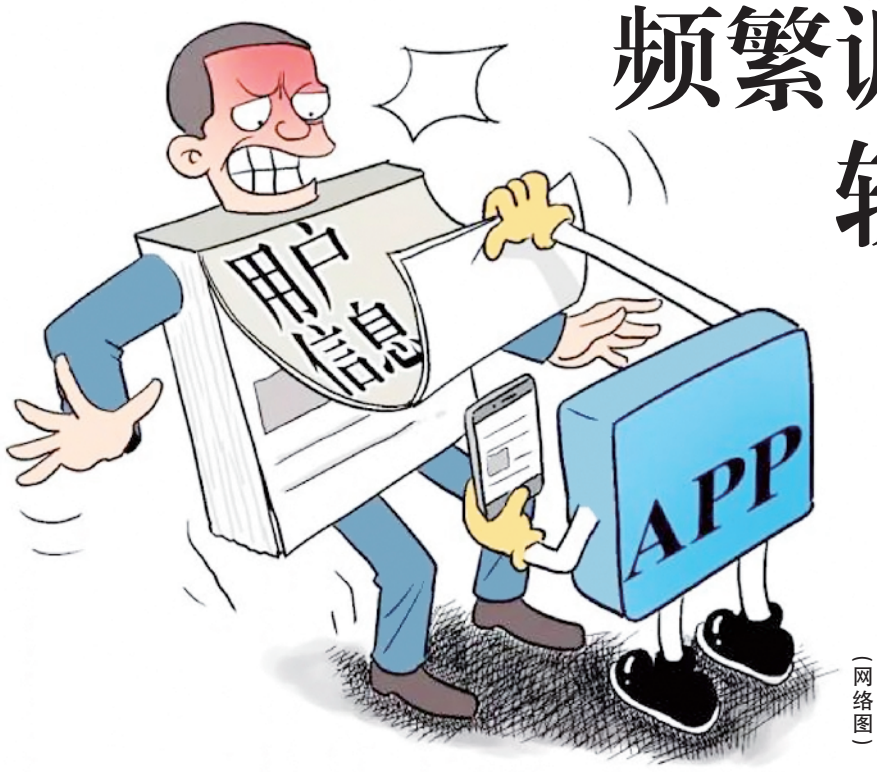
晚报广告咨询热线：6263965

投稿邮箱：xywbnews@126.com

频繁调取个人数据，软件后台在干啥？



（网络图）

11 月 1 日，个人信息保护法正式实施，个人隐私安全问题又重回大众视线。此前，就有博主晒出 iPhone 手机更新系统后，发现很多主流软件都在后台频繁获取用户信息，对用户隐私安全造成威胁。记者实测发现，确实有不少软件频繁调用个人位置和图片信息，甚至有社交软件一小时获取定位达到 75 次，如此频繁调用隐私信息，他们到底想干啥？

现　象

个人 App 授权后被频繁调取信息

市民刘女士向记者爆料，10 月 30 日，她在某 App 购物后，因频繁被推送“附近商品推荐”，于是便关闭了应用的位置权限。但没想到系统提示 “需要同意该隐私权政策才能继续使用”。刘女士选择了“仍不同意”按钮，没想到软件闪退且无法再继续使用。当她再次尝试，并在页面点击“查看协议”，才发现上面写着：“基于您的明示授权，我们可能会获取您的位置，为您提供附近的商品、店铺……您有权拒绝或取消授权”。当她点下不同意该协议按钮时，软件依旧无法使用。

不过，针对 App 过度索取手机权限的问题，网上就一直诟病不断，10 月 8 日，就有用户贴出截图称“iOS 版微信在后台反复读取用户相册”。根据用户描述，新版 iOS15 的“隐私”功能有“记录 App 活动”，可以存储 7 天内 App 访问位置或麦克风等数据。上述用户发现，某社交平台 App 在用户未主动激活应用的情况下，在后台数次读取相册，每次读取时间长达 40 秒至 1 分钟不等。

该用户同时表示，发现多款国产软件也存在后台频繁读取用户相册的行为。如此频繁地调取隐私数据，让很多网友开始担心自己的隐私安全问题。

体　验

一小时测试：微信要定位 75 次 美团读改照片 121 次

针对刘女士“不授权不能使用 App”的情况，11 月 2 日，记者进行体验，不过，在系统权限管理一栏中，“允许访问位置信息权限”页面发生了改变，与此前刘女士的情况不同，记者在选择“禁止”后，软件依旧能正常使用。

但调用隐私信息的情况却依然明显，记者利用能够监测 App 行为记录的手机，在开放权限的情况下，记录了微信、微博、抖音、美团、钉钉、淘宝、高德地图共七款常用软件的用户信息调用情况。

经过一小时的观察，在七款软件皆处于后台状况下，记者发现，高德获取位置信息 32 次，修改系统设置 8 次；钉钉获取位置 18 次，读取剪贴板 10 次；美团获取位置 16 次，读取及修改照片和文件 121 次；抖音获取位置 11 次，读取及修改照片 24 次；淘宝获取位置 24 次；微博获取位置 32 次，读取及修改照片和文件 16 次；微信获取位置 75 次，修改系统设置 9 次，读取及修改照片和文件 22 次，读取剪贴板 5 次。

而此前的 5 月 26 日，记者也曾做过类似测试，在拒绝定位权限的情况下，微信曾有过 6 分钟索取定位信息 800 余次的情况。

此前微信回应称，iOS 系统为 App 开发者提供相册更新通知标准能力，相册发生内容更新时会通知到 App，提醒 App 可以提前做准备，App 的该准备行为会被记录成读取系统相册。

当用户授权微信可以读取“系统相册权限”后，为便于用户在微信聊天中按“+”时可以快速发图，微信使用了该系统能力，使用户发送图片体验更快速流畅。

微信表示，上述行为均仅在手机本地完成，最新版本中将取消对该系统能力的使用，优化快速发图功能。

揭　秘

软件在后台调用权限是正常需求吗？

奇安盘古隐私安全业务负责人赵帅表示，在个人信息保护方面，操作系统的权限设计是为了让 App 收集使用个人信息的行为受到限制，让用户能够主动去控制 App 能否采集特定类型的个人信息，如通讯录、地理位置等。后台调用权限的行为在特定场景下是合理的，比如我们用手机导航的场景，虽然切换到后台，但我们仍在使用这个 App；也有一些场景是非必要的，比如我们将 App 切换到后台，暂时不用这个 App 提供服务，那么这种情况下的后台调用权限可能就已经超出正常需求的范围。

民间互联网安全组织网络尖刀创始人曲子龙认为，从技术角度来讲，调用次数其实并不能直接说明问题，还是以它的应用场景实际做了什么才能确认是否合规。

软件收集用户隐私权限的边界在哪

关于 App 手机用户数据，赵帅表示，从技术角度上看应分为几种不同的情况：包括系统权限保护的个人信息，如通讯录、录音、定位等；未受用户权限保护的个人信息，如用户主动录入的身份证号码、病历、婚姻状况等；用户在使用 App 过程中产生的一些使用偏好信息，这些可能由 App 主动记录产生，如喜欢听的歌曲、经常去的餐馆等。

对于系统权限保护的个人信息，软件应充分明示并征得用户同意后，才能调用这些权限获取个人信息，并应确保获取的范围、频率、方式符合最小必要的原则。对于用户主动录入的信息，应当充分说明录入的合理性及可能造成的影响，给予用户选择是否录入的权利。对于软件使用过程中收集的数据，应该做到明确告知用户，并说明后续的用处。

用户信息被收集有哪些风险

曲子龙说，隐私泄露之后被精准推送广告并不是最大的风险，不良企业会通过大数据杀熟，甚至不法软件装入手机后获取通讯录及相册权限，经过分析提取用于实现“个人身份信息盗用”“定向网络诈骗”等用途。建议用户不要轻易让第三方软件获取通讯录及相册权限，相册中也尽量不要存放身份证、银行卡等包含敏感信息的照片内容。

曲子龙认为，必要权限按照行业区分，法律上国家已经规定得很明确了，大部分产生争议的是一些个性化的内容，比如支付宝是一个支付软件，但是里面加了小程序后就变成了“公众应用平台”，属性发生变化获取的权限也自然跟着发生变化，最好的方式是应用内的第三方服务如果仅是偶尔使用的应用，都采用二次授权，并且即用即授权原则，如果长期使用的应用则制定权限开关，用户随时可以手动关闭停止授权，可能会是一个较好的解决方案。

说　法

调权限属正常行为 但平台要掌握好度

中国电子技术标准化研究院网络安全研究中心测评实验室副主任何延哲表示，此前权限强制、滥用的问题突出，用户不想用这个功能，平台却强制使用，个人信息保护法出台以后，这个问题基本解决了，用户可以自由选择。他表示，如果权限被开通后，获取的信息是否在合理范围内使用，是需要考虑的问题。

App 索要相机权限一般是为了拍照、扫二维码，要地理位置就是定位导航，这些在相关隐私协议里都写得很清楚。但目前仍有些细节确实存在问题，比如读取的次数，本来可能只需要 10 次，最后获取了 20 次。

此前的情况更严重，读取次数能达到几百次上千次，如今次数只是个位数和十位数之间，这在检测过程中一般不会被判定成违规，“需要调权限有很多是因为安全风控的问题，比如账户异地登录，平台会拿这个去判断，原因非常复杂，只要控制在十几次内，基本上都不是什么问题。”何延哲表示，后台读取也是同样的道理，也是需要看频率，如果账户存在异常会通过后台读取进行探测，不一定会将数据读走。“这要看是单纯验证位置，还是上传数据，后台的事情不合理因素更多，需要具体问题具体分析。”　（据《北京青年报》）