谁让我们的个人信息在“裸奔”？

——部分 APP“过分”收集用户信息调查

看小说的 APP 要读取用户短信、贷款类 APP 要访问摄像头并拍照、上网类 APP 要读取用户通讯录……伴随着移动互联网的飞速发展，大量 APP 在不知不觉中收集了一些与自身业务无关的信息，个人信息在网络空间中“裸奔”的现象屡禁不绝。

8 亿用户的 APP 被曝超范围收集用户信息

一款号称可“一键连接 WiFi”的 APP WiFi 万能钥匙已成为不少人的手机必备。公开数据显示，其月活跃用户已经达到 8 亿。然而，这款被视为“蹭网利器”的 APP，近期却被曝光存在超范围收集用户信息的行为。

广东省公安厅近日公布，2019 年一季度，广东警方共监测发现 1670 余款 APP 存在超范围收集用户信息行为。其中 WiFi 万能钥匙、钱聚易等 10 款 APP 问题突出，特别是 WiFi 万能钥匙问题最多，共超范围收集了 7 类信息。据通报，WiFi 万能钥匙(4.3.56 版本)存在读取用户短信或彩信、联系人，收集用户设备上已知账号，使用用户设备摄像头或麦克风等问题。

APP 超范围收集用户信息现象并不少见。根据爱加密大数据中心提供的数据，截至 2019 年 3 月底，该中心已收录安卓应用 270 多万个，iOS 应用 190 多万个，30%以上的 APP 存在不同程度的越权、超范围收集等行为。

“这么做多是为了收集用户的经济状况、消费偏好、活动区域等信息，对用户进行精细的人物画像，以支持产品研发更新，或精准推送广告。”广东省公安厅网警总队案件科副科长黄建邦说。

暨南大学网络空间安全学院院长翁健表示，“获取用户设备上已知账号列表”易泄露用户隐私。攻击者有可能利用掌握的账号，实行撞库等网络攻击，即从安全性较弱的账号中获取的用户名密码，来推测强安全措施的账号和密码。

此外，调用权限发送短信也是手机木马的主要传播方式之一。翁健介绍，应用程序可通过该种方式将带有病毒的链接放入短信中，并依次发送给用户相关联系人，一旦有人点击该链接，则会感染病毒。

过度索权套路多 “迷魂阵”里走不出

一款主打便捷连网的 APP 为啥要索取这些“八竿子打不着”的信息权限？

记者在安卓手机应用市场上下载该 APP 后发现，页面弹出的窗口询问“WiFi 万能钥匙需要以下权限，是否允许？”包括用户位置、电话、信息、通讯录、相机等权限，但只有点击“允许”才可下载。

该产品有关负责人表示，目前，WiFi 万能钥匙除了提供 WiFi 连接以外，产品中也提供资讯、社交等其他服务，广东警方提到的额外获取的权限，是所有社交软件都会需要获取的正常权限。

记者发现，安卓版本的 WiFi 万能钥匙产品内，确有所谓的社交功能“附近的人”，然而记者点击后发现，使用“附近的人”功能需要另外下载“连信”APP。不仅如此，该 APP 的下载安装并未经过应用市场。截至记者发稿时，“连信”APP 在安卓应用市场内仍无法通过关键字搜索出来。

业内人士表示，此举意味着 WiFi 万能钥匙的相关产品“连信”APP 未经过安卓应用市场的审核，即使用户可以自主选择提供或不提供相应权限，但用户下载使用仍存在一定的风险。

此外，WiFi 万能钥匙调用的权限实际上是为另一款 APP 使用，这是为其他 APP 规避监管“打掩护”，既侵犯了用户的知情权，同时也把用户拉进了“迷魂阵”——难以辨别哪一类信息权限是与产品服务直接相关的。

那么是否关掉所有的权限即可保护用户个人信息呢？事实上并不容易。

翁健表示，有的权限看似与 APP 运行无关，其实后台的服务需要这些权限。然而，有的开发者故意将 APP 的超范围权限与正常权限的模块“打包”，导致在阻隔了 APP 的超范围权限后，正常程序无法运行。

专家建议从源头端加强公民个人信息保护

黄建邦表示，正因为企业收集这些信息的成本远低于可能的收益，导致很多 APP 索权无度，也就有了“不管有用没用，先收集来再说”的心态和做法。

对于如何从源头端保护用户个人信息，专家建议，首先应用商店要做好把关，对上架下载量大的 APP 要求经过人工检测，并确立一个原则——每个 APP 只给最低的信息收集权限，且每次信息收集都要获得用户许可。

近日，由中央网信办、工信部、公安部、市场监管总局指导成立的 APP 专项治理工作组起草了《APP 违法违规收集使用个人信息行为认定方法(征求意见稿)》，该征求意见稿将 APP 违法违规收集使用个人信息分为 7 种情形。翁健认为，该文件明确了违规 APP 行为的具体认定标准，有助于网络安全法的相关要求真正落地见效。

黄建邦呼吁，从立法的角度对用户个人信息进行分类分级管理，明确 APP 收集哪一类信息需要哪些授权程序，可探索信息收集备案制，信息收集只有经过法律授权而非简单用户授权才可行。

(据新华网)