轻点“同意”隐私交出去

手机应用滥用授权致信息泄露 专家建议安装前细读协议

网上约车、购物、叫外卖、导航……从早上睁眼到晚上睡觉，我们每时每刻都在享受着手机App带来的便利。但与此同时，你的微信昵称、头像、位置、通讯录、电子邮箱信息、QQ账号密码，甚至身份证号码、银行账户都“裸奔”在互联网海量“大数据”当中。而这些隐私信息，基本上都是自己在下载安装App时“同意授权”的。记者下载了30多个App，其中三分之二以上的App要求获取定位权限。猎豹移动安全专家称，App滥用隐私权限的现象非常普遍，建议用户在安装前仔细看授权协议，安装后也可选择关闭部分授权。

案例 朋友欠钱 自己收到催款短信

日前，市民李女士莫名收到以借贷宝App为名发来的催收短信，称其朋友贷款，而短信中不但公布了其朋友的手机号、身份证号等个人信息，还带有大量恐吓咒骂字眼。记者从短信中看到，内有李女士朋友，也就是借款人的姓名、手机号、身份证号等个人信息，发短信的人自称是“借款公司的”，称借款人在借贷宝借钱时由李女士担保，并咒骂称如果借款人不还款，李女士及家人将遭遇厄运。

随后记者联系到借款人，对方承认确实从借贷宝平台上的机构借了钱。但他并没有将李女士填为担保人，而是“手机软件会调取通讯录，向有过通话记录的联系人催收短信。”

记者随后也在借贷宝使用过程中发现，软件会向用户申请读取手机通讯录的权限，在其《隐私条款》和《用户注册协议》中，也有内容称如逾期未偿还本息，借贷宝可能与第三方共享用户信息等。

无独有偶，市民郭先生近日也收到不少催收公司发来的信息，因自己的一个初中同学在借款平台上借了钱未按时偿还，催收方就通过同学手机通讯录找到了他这里。不仅收到催款短信，郭先生还接到了许多讨债电话，甚至传说中的“呼死你”也用上了，“响了十几个小时，未接电话得有好几千，但由于号码不同，地域不同，想拦截都拦不住。”

现象 很多人下载应用并不看条款

记者调查了解到，几乎所有的手机App应用在下载安装时，都需要同意应用的《隐私条款》。比如，记者下载高德地图App后，要点击“进入”地图，就跳出来了高德地图的隐私条款。仔细阅读发现，这款App上可能会收集的个人信息实在是太多了：包括位置信息、上传的图片以及IP地址、设备信息、浏览器类型等，在注册高德账号时，会收集账号名称、昵称、密码、密码保护问题、手机号码等，还有电子邮件地址、淘宝账号、支付宝账号、微信、QQ、车辆品牌、车牌号码、车辆识别代码、发动机号、机动车驾驶证、住宿信息、行程信息、支付信息等。更关键的是，高德地图还会将这些信息提供给第三方，并授权高德地图间接向第三方获取相关信息。

但很多“手机控”在下载安装App时不会注意看授权权限条款，便直接同意安装。北京晨报记者随机采访了20余位市民，竟然没有一个人表示在下载App时会详细看“授权条款”。“字太小了，而且都是一长篇，所以基本不看。”市民李女士说。

但就是点击“同意”这么一个简单的动作，用户的隐私就这么交出去了。

中国互联网协会理事长邬贺铨说，“只要你的手机里安装了导航软件，无论你在哪里，我们都能很快通过手机里App提供的数据找到你。”在他看来，“有的App应用本来跟位置并没有太多关系，可是App会强行搜索你的位置信息，而你的位置信息根本屏蔽不了。”

案例 四成应用会申请获取位置信息

今年9月份，江苏省消协工作人员通过现场检测发现，在手机下载的100多个App中，79个App可获取定位权限，23个App可直接向联系人发送短信。点开“电话与联系人”一项，有14个App甚至可以监听电话和挂断电话，结果非常惊人。在所获取的个人信息中，“位置信息”和“读取通讯录和短信”是最容易被读取。

据相关人员介绍，大多数App都有获取精确位置的权限，由GPS定位可精确到10米。各个开发企业给出的理由是需要进行一系列社交模块建设。但在实际操作中，实现社交功能，只需获取大致位置权限即可，根本无需GPS精确定位。

对于“读取通讯录和软件”信息，大部分开发企业表示，App需要通过验证码避免用户重复注册，同时起到推荐作用。这使得用户的通讯信息完全暴露在软件公司面前。另据央视财经频道此前报道，除了偷录声音、获取定位外，误下载到一些“山寨”App时，机主的银行账号和密码则可能受到威胁。

专家支招 下载后应用前 关闭部分权限

对此，猎豹移动安全专家李铁军告诉北京晨报记者，手机App滥用权限的现象已经存在多年了，而且这种现象在安卓系统更严重一些。

李铁军介绍，造成手机App滥用权限的情况分几种，一种是大量正常App在开发过程中，给未来留有发展空间，“这个行业的一个特点就是用户群越来越大的时候，功能也会无限拓展，就需要更多的权限。比如说，原来没有要求定位的，当它现在有一个社交功能后需要用到定位，或者发展O2O之类的都需要定位。”所以很多开发者就未来规划的目标会需要事先“占个坑”，先把权限申请下来。而还有一种情况是，消费者可以看到的手机权限设置，并不是全部授权。相当一部分程序在消费者没有操作任何权限设置，软件就已经自动安装完毕了。

不过，李铁军也表示，避免用户隐私泄露还是有一些办法来解决，比如安卓系统在6.0的时候，系统的安全管理功能会提供机主对一个具体App来管理它的使用权限，用户如果发现有些程序申请的某些权限觉得“越权”，就可以在权限管理当中，把相应的权限关掉。

律师说法 非法获取个人信息并盈利将获刑

北京市诺恒律师事务所主任律师林悟江认为，一些手机APP要求取得与自身业务没有任何关联性的用户信息的授权，属于恶意取得授权，解决这一问题的核心关键在于个人信息保护法律法规的进一步完善，比如立法禁止经营主体取得与自身业务没有关联性的信息授权、一事一授权、授权用途必须明确具体等。

就目前而言，如果手机APP的经营主体恶意取得授权、滥用授权，并非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的；非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的即构成侵犯公民个人信息罪，将处三年以下有期徒刑或者拘役，并处或者单处罚金。**（据《北京晨报》）**