大数据时代，信息泄露防不胜防 个人隐私如何不『裸奔』？

特别关注

大数据时代，每个人都无可避免地被卷入信息的洪流。无论是用户注册留下的个人信息，或是智能设备采集来的信息，用户的隐私正不断地被泄露，成为各类商家买卖获利的“筹码”。

公开数据显示，2011年至今，已有11.27亿用户隐私信息被泄露。对此，网络用户、利益链条的受益者、不尽完善的管理部门都需要对此负责。

本报记者 邓漪蒙 整理报道

图/TP

1 “语音助手”还是“窃听能手”？

或许大多数人还没有意识到，在互联网时代，自己已经变成了“透明人”。小孟最近发现，自己和朋友电话或者当面聊天提到的一些话题，时常会巧合地出现在某些短视频、新闻和购物App中。她由此怀疑是手机或者App在窃听自己的生活。

这样的怀疑并非空穴来风。一贯强调用户隐私的苹果公司，其语音助手Siri被曝涉嫌泄露用户隐私。据《卫报》报道，爆料人表示，苹果承包商经常会听取Siri语音助手收集的机密医疗信息、毒品交易和夫妇性生活的录音，用来评测Siri的各种回答是否准确、恰当。对此，苹果公司称这些数据“用于帮助Siri听写，从而更好地了解你，并识别你所说的话”。当你需要使用Siri时，就必须要接受Siri将你的对话上传到云端的可能，也就面临着自己的隐私被泄露的可能。

有办法避免么？恐怕很难。不仅仅是苹果手机，任何手机在“智能”的背后都潜藏着安全风险，除非你选择将手机中的语音助手彻底禁用，或是在涉及私密谈话时打开手机的飞行模式。但这样便可以高枕无忧了吗？如今家中的各类物联设备，从音箱到冰箱，都号称“更懂你”，而这个代价就是，用户的一举一动可能被这些智能设备监听、监控着。

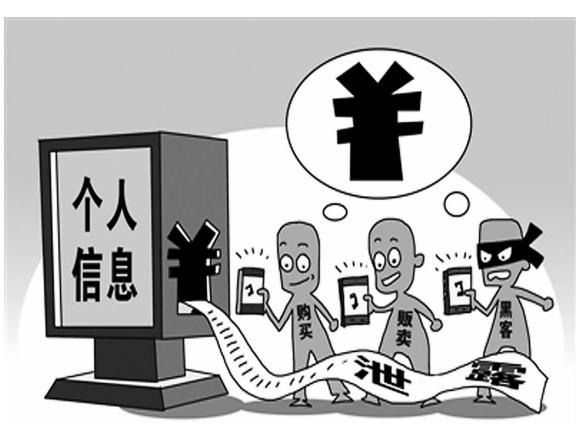
2 手机App变成个人隐私的“漏斗”？

除了语音助手，手机上安装的各种App也是侵犯用户隐私的“重灾区”。据统计，我国境内应用商店数量超过200家，上架应用近500万款。这些App在提供方便的同时，却成为个人信息泄露的“漏斗”，强制授权、过度索权、超范围收集个人信息的现象大量存在，包括手机号、通讯录、通话记录、短信等在内的关键个人隐私信息存在外泄隐患。

今年年初，中央网信办、工信部、公安部、市场监管总局四部门成立了App违法违规收集使用个人信息专项治理工作组。工作组专家表示，他们对包括餐饮外卖、地图导航、网上购物、金融借贷、即时通讯、社区社交等近20大类共计100个App进行用户信息收集情况统计后发现，很多App都存在强制超范围索要权限的情况，平均每个App申请收集个人信息相关权限数有10项，而用户不同意开启则无法安装或运行的权限数平均为3项。

的确，当我们下载App时，总会被要求匹配诸如开启定位功能和语音功能等权限。但现在普遍存在的现象是App过度索要授权，比如图片修改类软件，索要麦克风或者定位权限；新闻或购物软件，索要通讯录授权。这些都是个人隐私泄露的“导火索”。

专家提醒，为尽可能避免以上情况，建议尽量从正规的应用市场下载App。此外，需要关闭某些软件的访问权限。用户可以通过在“权限管理”模块内定期评审各App的权限，来控制和降低自己隐私泄露的风险。以微信为例，打开微信的授权，可以看到它的应用权限包括存储、您的位置、电话、相机、短信、身体传感器、通讯录和麦克风。其中，“您的位置”权限，假如用户不经常用微信群聊中的“定位”功能，是可以关掉的；而“身体传感器”权限，假如用户不经常使用“摇一摇”等功能，也能关闭掉；至于“通讯录”权限，其实在首次安装微信时导入通讯录中好友后，大部分人就不会涉及其在微信的使用，可以关闭掉；最后“麦克风”权限，假如你是个聊天打字党，不喜欢发送语音消息的，其实也可以将其关闭。这样将所有的App类似的权限关闭掉一些，就可以最小化的防止App采集自己的个人信息了。尤其是通讯录、短信、电话、麦克风、位置信息、上网记录等权限，要重点检查，尽量不要开放给App。



图/TP

3 生物识别信息暗藏大风险？

随着网络技术的发展，除了传统的用户隐私信息，生物识别信息泄露成为新风险点。哪些属于生物识别信息？我们的指纹、虹膜、人声和动态、静态的脸像都是典型的生物识别信息。因这些个人生理特征信息很难被更改，所以被广泛用于身份认证、交易和支付环节。

不久前，一款名叫“ZAO”的换脸手机App走红，用户协议上提出“同意授予ZAO及其关联公司、ZAO用户全球范围内完全免费、不可撤销、永久、可转授权和可再许可的权利”。这意味着，如果用户在安装后使用该软件，包括肖像在内的个人信息将被收集，还可能被其他企业使用。

另一则新闻也值得关注。在国家网络安全宣传周上海地区的活动上，上海信息安全行业协会副主任张威提醒公众，在拍照时自己比的剪刀手很容易泄露身份信息，基本上1.5米内拍摄的剪刀手照片就能100%还原出被摄者的指纹，在1.5米–3米的距离内拍摄的照片能还原出50%的指纹，只有超过3米拍摄的照片才难以提取其中的指纹。

专家表示，指纹、虹膜、人脸、声音等生物识别信息是比身份证号码、手机号更重要的个人隐私。也因为如此，这两则新闻才在网络上引起了轩然大波，提醒我们要不断提高自我保护意识。就拿“剪刀手”来说，拍照摆动作可以用剪刀手，但尽量距离得远一些，或者发到网上前先用图像处理软件进行模糊处理。

当然，除了提高保护个人隐私的警惕性，公民的网络安全也亟待国家相关部门尽快推进专门的个人信息保护法规的制定和出台，为个人信息提供系统性、体系化的保护。此外，在隐私保护和数据安全的问题上企业责无旁贷，在用科技为用户提供便利性的同时，也要加大网络安全的投入，为用户的信息筑起一道“防火墙”。

4 如何保护自己的个人信息？

事实上，除了手机和App，商家想要获取用户的个人信息还有很多渠道。有些用户已经察觉，各类商家总能准确地洞察他们的购买需求。比如，购买完房子后接到装修公司和甲醛清除公司的电话；怀孕后接到月子中心和早教中心的推销电话；车险到期后接到各类保险公司的电话……这一切都是巧合吗？

买房、买车、买保险、怀孕、外卖……我们身处商业社会中，信息也在不断地被贩卖，甚至还形成了完整的信息售卖产业链条，保险公司、银行、高利贷者、商家和骗子都能以极低的价格购得个人数据。

记者在百度上输入“个人数据”或“手机数据”等中文关键词，就能看到多个专为出售和购买个人数据而设的QQ和百度贴吧群组的信息。因信息贩卖获利简单且利润高，吸引了不少企业化运作的犯罪团伙为之铤而走险。

近日，上海警方就成功破获了一个贩卖公民个人信息的犯罪团伙，在犯罪团伙搭建的网站注册会员后，只要在账户充值且满足交易金额，就可以买到他们想要的大量公民个人信息，包括房产、金融、母婴等十余种，涉及公民个人信息达上亿条。面对个人信息随时可能被贩卖的现实，我们应该如何保护自己的个人信息不被他人非法获取呢？

专家提醒，为尽量保证自己的个人隐私不“裸奔”，以下几点应注意：一、所有证件概不外借。如出生证、身份证、学生证、社保卡等各种证件。二、不要随便留个人电话及真实姓名。如商家为了搞促销，往往会以赠送小礼品的方式，让客户领礼品时留下电话等个人信息，万不可贪图小便宜而留下真实的个人信息。三、不要扫来源不明的二维码，这可能是盗取个人信息的软件，也有可能是盗取微信或支付宝的账号密码的软件。四、及时处理收取快递的签名。快递公司买卖用户信息的案例屡禁不止。我们在收取快递时可以留下自己的化名，快递单尽量撕碎后扔到垃圾桶内。五、不要随意连接来源不明的免费WiFi信号。不法分子在公共场所设置与附近店名相似的免费钓鱼WiFi信号，当用户的手机或笔记本连接上这些免费网络后，通过流量数据的传输，黑客就能轻松盗取用户手机、笔记本里的照片、电话号码、各种账号密码等个人隐私信息。