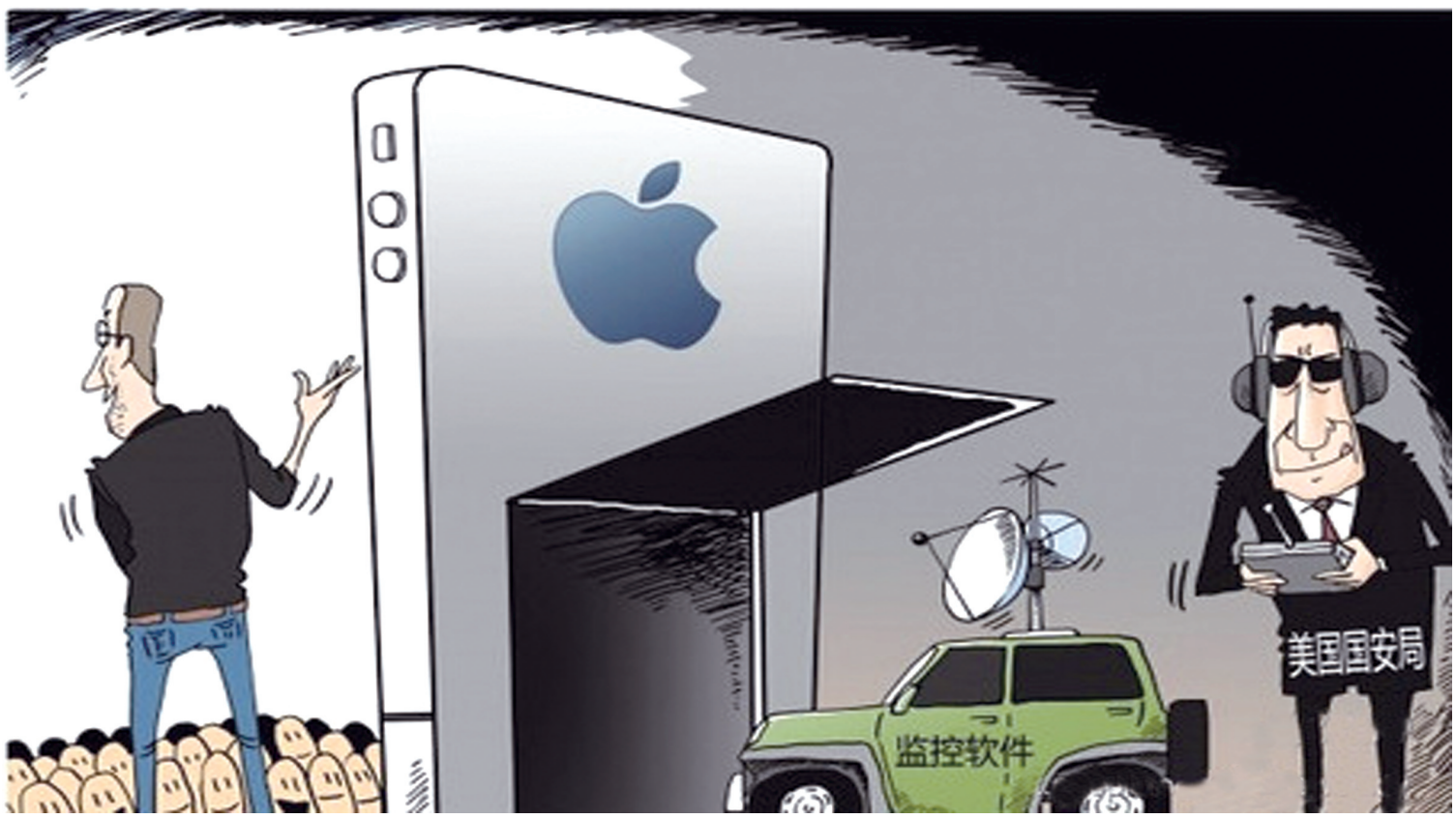

苹果陷“窃密门” 手机用户难觅安全岛

苹果承认可“偷偷”获取用户信息，遭集体诉讼；专家称手机窃密为普遍问题

年前，在互联网萌芽的年代，人们常说，“你甚至无法确定坐在对方电脑面前是不是一条狗”。那时候，人们在互联网上是隐形的。

十年后，技术更迭迎来大数据时代。人们发现，手机厂商、软件厂商、电商平台们知道你的生日、爱好、生活习惯、联系方式、聊天记录，甚至连你的家庭成员信息都可以了如指掌。最明显的例子是，曾被公认比较安全的苹果手机也被曝存在后门，用户在不知情的情况下，其手机通讯录、短信、地理位置等信息被以“后台诊断”的名义泄露出去。

专家表示，在大数据时代，不仅苹果存在“泄密门”，包括谷歌 Android 在内的所有接入移动互联网的智能手机都逃不出信息泄露的危险，相关法律缺失以及监管部门对隐私保护不力是手机泄露用户隐私的主要原因。

苹果承认存在“后门”

在上周五的“黑客大会”上，知名iOS黑客、早期iOS越狱开发团队成员乔纳森·扎德尔斯基展示了如何从苹果设备上攫取数据。这些“服务”的运行不会告知用户，也无法被禁止。

被人揪住小辫子后，美国苹果公司不得不承认，该公司员工确实可以通过一项未曾公开的技术获取iPhone用户的短信、通讯录和照片等个人数据。即可利用该技术通过“授权”电脑绕开备份加密，进入已联网的iPhone中。

苹果为自己辩解称，这个技术是为诊断功能服务的，只是为了向企业信息部门、开发者和苹果公司提供故障信息，不会对用户隐私和安全带来影响。

这个回答带来更多质疑。一位安防行业分析师认为，既然开发者可以使用，那么执法机构也能够利用这些工具。更有人猜测，情报机关是否也可以利用这些工具。毕竟去年美国“棱镜门”揭秘者斯诺登就曾表示，美国国家安全局可以在iPhone关机的情况下通过麦克风监听用户。这种说法随后也得到了专家的证实。

本月初，央视曝光苹果手机搜集记录用户位置，认为苹果手机详细记录了用户位置和移动轨迹，该功能不仅记录用户常去的地点名称，还详细记录用户在这个地点停留的时刻及次数。而且这些记录被存放在未加密数据库中。

苹果对此称，苹果从不获取或了解某个用户的“常去地点”信息，也不允许任何应用对其进行访问。用户如果不想记录，可以把这项功能关掉。但专家马上反驳称，即使关闭了“常去地点”功能，后台数据库文件依旧会记录这些信息。专家质疑如果公司不获取这些信息，为何记录得那么详细？

在这些窃取隐私事件背后，隐藏着一个核心事实，就是苹果用户是在自己完全不知情的情况下发生数据泄露的。到底透露了哪些数据，这些数据被谁获得，谁能使用这些数据，用户无法知情。除了已知的泄密路径外，还有多少隐秘的窃取隐私手段没有被发现，用户也无从知晓。

可以知晓的事实是，一些国家的政要已不再使用iPhone。

原告称苹果向美政府提供用户信息

“泄密门”事件使苹果再次面临集体诉讼。据媒体报道，一位名为马晨的华人女性已在美国加州圣何塞法院向苹果公司提起集体诉讼，代表个人及其他iPhone用户起诉苹果手机利用定位信息获取用户资料，侵犯用户隐私。马晨已于7月24日递交诉讼书。该案件将于2015年1月12日开庭审理。报道称，原告根据苹果公司手机销售数据，代表1亿手机用户向苹果公司提出集体诉讼。

原告在诉讼书中提到，她在使用任何苹果手机包括目前的iPhone5S时，都没有收到苹果公司追踪、记录以及传送用户信息的通知。在没有得到苹果公司询问、未经本人同意的情况下，她对苹果公司每天详细记录其行踪并上传至苹果公司数据库的行为毫不知情。并且，iOS系统没有向用户提供“有效”的方法来关闭定位服务。

据报道，起诉书声称苹果公司已经向包括美国政府在内的第三方机构提供了用户的相关信息。美国政府已经向苹果公司发送超过1000次获取信息的请求。

此前苹果就曾因泄露用户信息等原因被告上法庭。2011年，韩国2.76万用户曾对苹果总部、苹果韩国分公司发起诉讼，称其通过手机周边的无线网络收集用户位置信息。最后，因违反韩国《位置信息保护法》，苹果公司被处以300万韩元罚款。

2011年，美国国会能源与商业委员会向苹果发函，要求苹果公司解释追踪用户信息的详情。苹果公司表示，定位数据并非用户所在位置，而是苹果一个关于用所在地周围无线网络“热点”和手机信号塔位置的数据库。2013年，美国一名法官审理了类似的侵权诉讼，原告被裁定在购买 iPhone 前没有阅读苹果的隐私条款。

手机应用普遍“越权”

想要逃离iPhone的用户会发现，高速互联的智能时代，没有真正的安全岛。

记者查阅360公司此前公开的一份手机安全报告显示，资费消耗、隐私窃取以及恶意扣费是手机恶意软件的主要危害，其中，谷歌Android平台感染量高达1137万余人次。2013年上半年，新增手机恶意软件97%来自Android平台。

瑞星安全专家唐威表示，从技术角度而言，这种悄悄收集用户隐私信息的能力并不“专属”于苹果。

唐威称，大量的手机应用均可以实现类似的功能。“一个音乐软件，非要获取定位功能；一个手电筒软件，也要定位功能；一个电子小说软件，非要获取用户短信阅读权限，还要定位功能；一个播放器软件，不仅要定位，还要拥有打电话权限。更有一些软件，要求获取电话录音功能。”一位安全工程师表示，这些“越权”要求，已经成为当下智能手机市场的普遍状态。

该工程师表示，不少软件公司获取这些功能时，并没有明确的目的，只是希望获得最多的信息。因为在大数据时代，信息是高价值的。“但如果这些个人信息外露，被不法分子或企业内部人士用来作恶，比如上传录音等，消费者的隐私将毫无保障。”

360的报告统计显示，九成以上的应用要求读取已安装应用列表和设备号相关权限，五成以上应用要求读取位置信息权限，24.2%的应用要求发短信权限。打开摄像头、读取联系人、读通话记录权限的应用也均占到两成以上。此外，还有15%以上的应用要求拥有录音权限、窃听功能、读短信记录和打电话权限。

一位安全工程师表示，截至目前，智能手机软件泄露用户隐私的行为越演越烈，因为没有监管部门来推动用户隐私保护，相关法律仍然缺失。

唐威表示，当前的局面，不是某一个厂商、或某个人能推动的，需要社会各层面人士的共同努力。首先国人隐私保护意识需要提高；立法部门要对一些行为作出法律界定，制定法律；国家监管部门需要加大监管，对违法行为及时追责、查处。

■专家观点

“大数据时代都是透明人”

北京大学商务智能研究中心主任王汉生此前在接受新京报采访时表示，根据公开的文献，在美国只要提供邮编、性别和出生年月，87%的人就可以被独立识别出来。目前国内电商可以通过一个人的购买行为，识别到一个人的部分特征，但这个人是做什么的，什么年龄、什么爱好，一般情况下，企业还是不知道的。但如果有人把电商获取的数据和其他数据对接，就能识别到具体的人了。

一位安全行业业内人士则表示，最近两年发生了很多互联网泄密事件，不少网站在用户隐私保护方面并不完善。“所以，即使手机软件获取的信息不完整，但整合网站被盗数据库泄露的信息，再进一步分析，那就非常可怕了。”

该人士表示，只要愿意，这些幕后人士可以对网民进行相当精准的定位。“比如，从你网购的信息，他可以知道你的名字、手机号，家庭住址、家庭信息，甚至你的网银账号。在整合你的智能手机软件信息，他能知道你的朋友圈、常去的位置，由此可以知道你的职业、爱好、生活轨迹。”

“虽然素未谋面，但这些人可能比你的朋友还要了解你。”这位安全行业人士表示，在大数据时代，网民没有隐私可言，尤其是经常上网的人，基本上属于裸奔。

（据新京报）