

苹果手机“后门”洞开极易被窃密

业内专家建议限制使用以防数据安全隐患



能随时提取用户短信息、通讯录或者照片,随时知晓用户的位置信息,即使手机关机也无济于事,甚至还可能被暗中变成窃听器或跟踪仪……

近日,国内外媒体均有报道美国苹果手机通过一种未公开的方法,可提取私人信息。iPhone 的泄密“后门”掀起一场轩然大波。

用户数据“一览无余”破解成本较低

苹果手机对内置的 GPS、麦克风、摄像头、短信等产生私人信息的设备管理,都是通过操作系统。与笔记本电脑和传统手机相比,这种数据模式更容易被“一览无余”,且破解成本较低。

打个比方,就像是智能手机把海量数据先分门别类,再打包装箱,只要看一下箱子外面贴的标签,就基本能看穿箱子里的一切。

此外,苹果手机开创了“手机商店”的应用生态,愤怒小鸟、乐动力等五花八门的手机软件,都要先对接操作系统,才能调用所需的手机设备完成服务。例如,很多年轻人都喜欢装着手机去跑步,因为手机里的运动软件能记录下跑动路线、跑步速度、消耗热量,甚至还能自拍分享,或缴费升级软件。

实际上,用户享受这些新奇服务的同时,软件在后台已经接通了操作系统开放出来的位置、摄像头、通讯录等端口,个人信息也就不知不觉从手机里流向了各种软件开发商。

“即使是关机了,有些后台的数据通信依然在运行。”华东师范大学计算机应用研究所所长顾君忠教授告诉记者,关机只是手机呈现给用户的状态是关掉了,内部部分模块依然在转。比如手机时钟,SIM 卡与基站间握手通信等一直在运行。

“除非拔掉手机电池,彻底断电,手机才真正无用。各款智能手机中,只有苹果电池是内置,无法拔除。”顾君忠坦言,到底是有意而为,还是设计独到,苹果自己不公开说明,用户很难搞得清。

苹果应自证与美国联邦调查局有无关系

“我们设计了 iOS,使其诊断功能不会侵犯用户隐私和安全,同时为企业 IT 部门、开发者及 Apple 提供解决技术问题所需的信息。用户必须先解锁其设备,并在其他电脑访问此有限的诊断数据之前同意信任该电脑。用户必须同意分享此信息,而且数据绝不会在未经用户同意的情况下被传输”——对于本轮“后门”事件,苹果在发给本报的声明中这样表述。

对此,国内多位业内人士并不完全信任。复旦大学计算机科学技术学院副教授杨珉指出,苹果手机

提供的云服务,定期备份用户通讯录和照片,万一手机丢失,云端数据就会自动下载到新手机。这一功能的实现某种程度上说明,苹果手机将用户信息抓取到了其服务器上。苹果服务器又都是在美国,它如何处置和使用这些数据,我国是无法监管到的。

飞象网总裁项立刚认为,苹果具有非常强大的收集数据的能力,如果它一直坚持自身清白,那就必须拿出证据,自证未与美国联邦调查局合作过。特别是去年针对“棱镜门”事件,斯诺登就曾披露过美国情报机构可以直接进入苹果、微软、亚马逊、facebook 等多家美国互联网公司的服务器获取用户数据,对特定目标加以监视。

“苹果手机是硬件、软件和云服务完全一体化的封闭系统,外部企业 and 安全厂商无法插手;而国产手机常用的安卓系统相对开放,可以通过实施二次开发、安全‘加固’一定程度上提高安全性。”互联网实验室创始人方兴东强调。

对此,杨珉教授指出,苹果手机 IOS 操作系统相对比较封闭,对其系统测试投入巨大,目前国内针对该系统的科学研究还比较少。

解决“泄密手机”隐患亟待第三方监管

智能手机的类似安全隐患一直都在,亟需有关部门制定监管规则,加强有效管理。

“整合你智能手机里的软件信息,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。”据一份报告统计显示: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%的应用要求发短信息权限。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。

青橙手机 CEO 王讯表示,随着越来越多手机“后门”的揭开,手机安全将是用户在选择智能手机时考量的主要原因之一,目前国内市场上还没有一款以信息安全为卖点或主打方向的手机。“根据特定消费者的特定需求,设计加入指纹传感器、人脸记录等生物识别技术的 C2B 信息安全功能。”

在方兴东看来,现在只有由政府出面制定战略,推进中国自主可控的国产手机操作系统,才是应对全球智能手机“大佬”们“猫腻”的好办法。未来,类似“隐私手机”或有望率先在国产手机中诞生。

“随着移动互联网技术的不断发展,用户在享用各种智能终端创新应用的同时,不可避免地也将许多个人数据交了出去。不过,手机或网络企业在使用公民数据信息的同时,也有义务妥善保管。如果因为泄露或者未经用户授权转交第三方而给用户造成损失,理应追究相应的责任。”杨珉建议,尽快开发针对手机操作系统的数据检测工具,由专业的第三方检测机构提供客观权威的检测报告,才能真正实现手机数据安全的有效监管。



■ 用户享受 iPhone 新奇服务的同时,也面临隐私外泄的危险

本报记者 陈梦泽 摄

苹果“店大欺客”官司缠身

新一代 iPhone 手机即将闪亮登场,第三季度财报光鲜亮丽,最近苹果公司可谓风光无限。不过,树大招风,苹果的负面新闻也不少。

手机屡次陷入“隐私门”

这并不是苹果手机第一次陷入窃取用户隐私的质疑。

2011 年,韩国 2.76 万用户对苹果公司发起诉讼,称其通过手机周边的无线网络收集用户位置信息,要求苹果公司赔偿约 1.6 亿元人民币。数月后,一名用户胜诉,苹果公司向其支付约合 6100 元人民币的赔偿款。

同年,就手机定位事件,苹果公司收到来自韩国广播通信委员会开出的全球第一张罚单,被指控违反位置信息保护法相关规定,被处以 300 万韩元的行政罚金。

2013 年,“棱镜门”揭秘者斯诺登披露,苹果手机设计电池拔不出,因此即使关机也照样被监听。美国国家安全局可利用技术,使苹果手机看似已关机,但实际进入低电源运作状态,从而调阅手机里面的信息,定位情报监控用户。

2014 年 7 月初,央视报道苹

果手机具有搜集记录用户位置的功能,详细记录了用户的移动轨迹,不仅包括用户常去的地点名称,还包括在这个地点停留的时刻及次数。

据称,即使关闭手机定位功能,苹果公司仍可获取用户位置。这些信息被记录在未加密数据库中,苹果还曾将用户数据供给美国情报部门。

版权和劳工纠纷层出不穷

近年,苹果公司的官司可谓此起彼伏,从未间断。根据美国媒体统计,自其成立以来,光是大规模的诉讼就有 30 多起,而去年一年,苹果在全球遭遇的版权官司有 59 起。

7 月,苹果公司同意为最新一笔官司付出高达 4.5 亿美元的和解费,原因是其涉嫌操纵电子书的定价,其中 4 亿赔给消费者,而 5000 万美元则是律师费。

上月底,加州最高法院宣布,4 名前苹果员工对苹果公司违反加州劳动法的诉讼改为集体诉讼,此举意味着两万名苹果现任和前任员工都可能将苹果告上法庭。

这起诉讼原本由布兰登·费

尔策等 4 名前苹果雇员在 2011 年 12 月向法院提起,费尔策等 4 人指控苹果公司未按照加州劳动法合理安排用餐时间和休息时间,另外在薪水支付上也违反有关法律。经过两年多时间的指证和法庭辩论后,法官上月决定将该诉讼升级为集体诉讼,两名律师将可代表两万名苹果雇员。

按照法庭披露的文件显示,一名苹果员工声称自己曾经连续工作 5 个小时得不到休息。而另外一人则投诉,苹果要求自己 3 天之内必须入职,但薪水却晚付了两天。苹果在上诉初期向法院提交的材料显示,该诉讼可能涉及 18000 名员工。如今,这个数字已经增加到了两万人。

遭遇集体诉讼对苹果来说并不奇怪,之前苹果刚刚和谷歌、英特尔和 Adobe 等 IT 巨头一起支付 3.24 亿美元,与起诉这几家公司联合压低工资以及防止互相挖角的高技术员工和解。而最新的一个诉讼是,音响界巨头 Bose 三天前正式起诉老对手 Beats Electronics 侵犯耳机降噪专利,而后者刚刚以 30 亿美元的价格被苹果收入囊中。

驻美记者 徐东海

专家:公职人员应弃用 iPhone

iOS 开“后门”,“果粉”成“裸粉”,数以亿计的苹果用户听到消息震惊了。

“中国博客教父”方兴东建议“公职人员弃用苹果免遭泄密”,不少专家都认为国家工作人员、大型国企高层以及军方、警方等公职人员,应明确规定不用苹果手机,因为这关系到国家安全和

经济安全。

对此,多数人表达了赞同。新浪一项调查显示,近七成网友支持国家工作人员、大型企业高管及军队禁用苹果手机。公务员蒋青华表示:“手机不能变成窃听器,变成别人的提款机,厂家自律的同时,政府必须对管理体制狠心动手术。”

网友小舟大航调侃,“一个设备可以比你妈还了解你,未来的人们是否还有‘隐私’这个东西?”他认为,若要坚守隐私的最后一道防线,法律的规范必须提上日程了,虽然法律并不能解决所有问题。但是对于一个不会游泳的人来说,有个救生圈已经最好不过了。 本报记者 王文佳