# 危险的苹果：设计电池拔不出被指为跟踪留后门


## 苹果牌“跟踪器”

如果人们早点了解 iPhone 的定位功能，也许以调查婚姻忠诚度为生的私家侦探就会失业了。

就像豪车的车主不会去使用 80%的附加功能，普通人甚至不了解一部智能手机 80%的功能。央视最近做了一些科普教育。7 月 11 日，央视曝光苹果 手机有一项大众知之甚少的定位服务，打开设置中的“常去地点”，机主每天去过哪里，停留多长时间，去过几次都被记录在案，数据之详尽，完全可能达到引发家 庭矛盾的级别。难怪路人看着央视记者操作自己手机，脱口而出：这可不能被男朋友看到！

苹果的“定位服务”始于 2010 年，搭载 iOS 操作系统的 iPhone4 手机可以追踪用户每分钟的行踪，记录用户在任何一个地方停留的时间，并 且将用户资料上传至苹果公司服务器上。此后，苹果手机的换代产品 iPhone 4S、iPhone 5、iPhone 5C 以及 iPhone 5S 都有定位功能。

在央视采访中，专业人士在计算机上调出深藏在 6 层目录下的定位数据包，机主停留地点的经度、维度、高度、速度等值，精确到了小数点后 8 位。而用 户在留下这些轨迹时，根本无需开启手机的定位功能。也就是说，你可能只是在有 WiFi 的咖啡馆旁边走过，甚至没有蹭一下网，或者只是打开了一款和定位无关的新闻或游戏 App，你的行踪就暴露了。

这款随身携带的“手机形状追踪器”让人感觉芒刺在背。如果关闭定位服务会怎么样？首先，关闭后可能让 iPhone 的地图、导航等一些功能失效。更让人抓狂的是，即使用户将定位功能关掉，在你使用看似无关紧要的 App 时，后台系统还是能默默地将你所在地点、时间等信息 完整记录下来。

针对央视的曝光，苹果公司很快发出声明，这项功能是为了更好地为用户提供服务，强调不会将手机用户的详细资料透露给任何第三方，但是并未对传送用户数据至数据库进行否认。

很快有人拿起法律武器对准苹果。7 月 24 日，一位名为马晨(Chen Ma 音译)的华人女性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。原 告诉求最重要的一条是，在苹果公司不对消费者进行有效通知、在传输数据前未经用户明确同意前提下，永久性禁止苹果继续搜集由定位服务产生的高度敏感隐私的 用户数据。

事实上，苹果的定位服务惹上官司，这已不是第一次。2011 年，韩国 2.76 万用户就曾对苹果总部、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(约合人民币 18200 元)罚款。

当时美国、法国、德国也对苹果公司进行了类似的疑惑调查，韩国最先做出违法裁决以及处罚决定，一时间备受关注，只是过轻的处罚力度让这个官司更像是对苹果的一种保护。

2013 年，美国一名法官也审理了类似的侵权诉讼，原告表示在使用任何苹果手机时，没有收到苹果公司追踪、记录以及传送用户信息的通知。但法官最终裁定原告在购买 iPhone 前没有阅读苹果的隐私条款。

## 后门钥匙在谁手中？

就在 iPhone“定位服务”闹得沸沸扬扬之际，美国安全专家乔纳森·扎德尔斯基又为苹果补上一刀——你以为手机泄露的只是你的行踪，那就年轻又天真了。

7 月 18 日，在每年一度的 HOPE/X 黑客和开发会议上，老牌 iOS 黑客扎德尔斯基演讲时抖出猛料，iOS 存在多个后门，用来攫取 iPhone 和 iPad 中用户短信、通讯录和照片等个人数据。

扎德尔斯基曾出版《iOS 应用安全攻防》(Hacking and Securing iOS Applications)一书，在黑客界算得上大神级人物，他的这一曝光让人们意识到，一台 iPhone 在手，不止是自己的行踪尽在苹果掌握，其他个人 信息也不是秘密，苹果公司唾手可得。

比如一款名为 com.apple.pcapd 的服务，通过 libpcap 网络数据包捕获流入和流出 iOS 设备的 HTTP 数据。据扎德尔斯基称，这一服务在所有 iOS 设备上都是默认激活的，在用户不知情的情况下，能通过 WiFi 网络监测用户的信息。

而一款名为 com.apple.mobile.file_relay 的服务让用户为个人信息上的安全锁形同虚设。这一服务完全绕开了 iOS 的备 份加密功能，泄露的情报包括用户的地址簿、CoreLocation 日志、剪贴板、日程表、语音邮件等。这一服务最早出现在 iOS 2 中，在后来的版本中不断得到扩充。

扎德尔斯基指出，黑客甚至能利用这一服务从推特内容中窃取用户最近的照片、最近的时光轴内容、用户的 DM 数据库、认证令牌等，认证令牌能用于“远程窃取未来所有的推特信息”。

专业人士的指控让苹果难以淡定，7 月 23 日，苹果公司在回应中首次提到“后门程序”基本信息，称这是为 iOS 诊断功能服务，向企业的 IT 部门、开发者和苹果维修人员提供所需信息。

“不管用户有没有开启‘向苹果公司发送诊断数据’选项，这些服务都在传送数据。如果这些服务是为了诊断功能服务的，那应该在用户启用诊断模式时 才工作。不幸的是，用户根本没办法关闭这些服务。事实就是，每台手机上这些服务都是默认激活的，而且无法关闭。用户也没有收到任何关于是否将个人信息从手 机上发出去的询问。很难相信苹果公司说的是实话。”扎德尔斯基认为。

苹果的辩解没有让内行的扎德尔斯基满意，7 月 25 日，扎德尔斯基在其个人网站上回应，称这些“后门程序”可以突破加密的备份文件，获取用户数据，并非是开发者或运营商用来测试网络或调试应用。

“我从不认为这些服务仅仅是为了诊断功能设计的。这些泄露的信息完全是个人性质的。而且苹果获取这些信息时完全没有知会过用户。一款真正的诊断 工具在设计时会尊重用户，在它需要获取某些数据时告知用户，并且遵守备份加密协议。告诉我，为什么苹果向用户保证手机上所有备份的文件信息是加密的，却又 设计一个后门去绕过加密？”

既然远超诊断维修的必须性，苹果收集这么多个人信息数据流到了哪里？扎德尔斯基的研究一经公开，各国媒体的箭头都指向了美国国家安全局(NSA)。

“我没有指控苹果和 NSA 合作，不过就现有的资料来看，我怀疑苹果的某些服务可能被 NSA 用来收集潜在目标的信息。我并没有推测苹果和 NSA 之 间存在某种巨大的阴谋，但是 iOS 上运行的某些服务确实不应该存在，这些服务是被苹果公司有意强加的，用来突破备份加密，获取用户那些本不应该被获取的个 人信息。”

## 拿什么拯救隐私？

普通人没办法让黑莓专门为自己定制一部手机，拿什么保护自己的隐私？一些人从电影里学到一招，最好的方式是把电池取下来，但是，苹果公司的手机设计成电池不可拆卸。名义上是为了让苹果手机更薄、更好看。

斯诺登曾表示，苹果手机故意设计电池拔不出，因此即使关机也照样定位发情报，别人可以调阅手机里的信息。斯诺登早前在香港与何俊仁等律师庆祝生日时，要求这些人先将手机放进冰箱屏蔽信号，否则美国一下子就可以追踪定位到机主。

不过，真正热衷捍卫自己的隐私权的只是少数人，大部分人对苹果手机泄密的反应是“So what？”虽然人们对苹果公司每天详细记录自己行踪并上传至数据库的行为感到惊讶，但也不会因此把自己的苹果牌“追踪器”扔进河里。

在信息时代，人们已经习惯了让渡一部分隐私，作为从传统封闭生态迈入现代便利生活的代价。接受手机泄密，就像习惯各种封闭空间和开放空间无死角无盲点的监控探头，只要有需要，随时随地能拼凑出一个人的行动轨迹。

大多数人对泄密渐渐无感，是因为不认为自己的个人数据重要到会被单独提炼，这些只是大数据中的一粒尘埃。苹果公司 2010 年时曾向美国国会解释手机定位功能，称用户数据只会被匿名储存，不会暴露用户身份。

而对于商业机构而言，在大数据时代，成千上万的记录经过建模分析就是无价之宝。饭店会根据客户的行动线路推送餐饮广告，互联网金融公司会根据用 户的消费记录确定其经济能力，决定授信额度。凭借收集的用户个人资料、所在位置信息，苹果、安卓能轻而易举地向广告主销售个人化广告。

随着人们的生活越来越依赖智能手机，对隐私泄露的容忍度也越来越高，至少在这把剑真正落下来之前是这样。