

■本报记者 唐玮婕

试想一下，你只是在和朋友闲聊的时候无意间提起，想去试试某家西餐厅。5 分钟后拿出手机一瞄：今日头条已经为你推送了三条与西餐相关的广告和资讯。问题是，此前你从未在其它手机应用软件（App）或者浏览器上，做过相关的搜索。怪了，今日头条怎么知道我想吃西餐？

是惊喜？还是惊吓？年初，“我可能被‘今日头条’偷听了”成了网络上的热门“槽点”，许多人怀疑这款 App 会调用手机上的麦克风，把“偷听”来的个人隐私数据卖给了广告商。

惹上麻烦的，还不只是今日头条，近期，一连串的“侵犯用户隐私”事件接连曝出，360、百度、支付宝等企业也身陷其中……当我们把自己的日常生活完全交给 App “打理”时，我们很少想过这样一个问题：这款 App 可靠吗？

“偷开麦克风”，图啥？

对于“偷开麦克风”的强烈质疑，今日头条很快给出官方回应：从技术上看，目前声音信息的处理，远达不到通过麦克风去获取个人隐私的水平，今日头条也绝对不会在用户不知情的情况下收集用户隐私数据。

记者采访了几位业内专家后得知，以目前的技术水平，手机应用软件调用麦克风录制用户日常语音，根本就是小事一桩，用户担心手机麦克风搜集自己的信息，并非杯弓蛇影。在美国，多款安卓游戏最近就被媒体曝出会偷偷调用手机上的麦克风，来监听用户周围的声音。原来，这些游戏安装了一款来自阿方索（Alphonso）公司的软件，可以通过识别电视广告和节目中的音频信号来收集人们正在观看的数据。这些信息将出售给广告商展开分析，从而提高广告准确性。

不过专家也同时表示，从成本和效率上来说，不仅这些语音数据的记录、传输和保存工作成本巨大，而且以目前自动语音的识别水平，全部用机器完成面向广告推送的关键词捕捉，“性价比”超低。

麦克风会不会是“卧底”，各有各的说法。以苹果手机为例，苹果官方表示，所有应用商店中的软件在上架时都要经历审核，在后台获取麦克风权限的软件也会出现在“设置-隐私”列表中，如果在没有获得用户同意的情况下擅自获取麦克风权限，将遭到下架的处理。

应用商店对调用麦克风设立了严格规定的管理权限，这从一个侧面反映出 App 拥有者对麦克风的“垂涎”程度。如果不是有偷窥的“引诱”，这些五花八门的软件究竟为啥要集体盯上“麦克风”，进而采集用户的语音信号呢？如果打开手机中的“隐私”设置一看，很可能你会吓一跳：绝大多数 App 都在向用户索取随时访问手机麦克风的权限，类别包括电商、出行、社交，甚至音乐、理财等等。动不动要打开用户手机上的麦克风，有这个必要吗？

让我们来看看发生在百度身上的故事。就在 2018 年伊始，百度遭到了江苏省消费者保护委员会的投诉，指控其旗下 App 涉嫌“监听电话、定位”的不当行为。

此前，江苏消保委表示，用户在安装手机百度、百度浏览器两款 App 前，未被告知百度公司获取各种权限的目的。作为搜索及浏览器类应用，上述权限并非提供正常服务所必须，已超出合理的范围。而百度的回应和今日头条几乎是一个套路：“百度 App 不会、也没有能力‘监听电话’，而百度 App 敏感权限均需授权，且用户可自由关闭”。

链接

360：公共场所全程直播？

去年年底，一篇题为《一位 92 年女生致周鸿祎：别再盯着我们看了》的文章引发关注。文章称，360 旗下水滴直播平台侵犯公众隐私，多个 360 智能摄像机用户将自己在餐厅、网吧、健身馆等公共场所监控到的视频，在 360 旗下直播平台——水滴直播进行直播，导致其他用户个人隐私受到侵犯。网友可以通过直播观看、点评摄像头下公众的“一举一动”。

对此，360 董事长周鸿祎还一度指责该文章对 360 水滴直播蓄意抹黑，有多处不实，并表示这篇文章有“黑公”之嫌。但在仅仅几天之后，舆论重压之下的 360 公司就宣布主动、永久关闭水滴直播平台。公告称，由于内部业务调整，水滴直播自即日起停止运营，360 智能摄像机将专注提供可靠的安防监控功能，为用户提供服务。

腾讯：“天天看我们的微信”？

2018 年一开头，腾讯成了又一个掉在隐私“坑”里的“倒霉蛋”。吉利集团董事长李书福在某论坛上突然“放炮”：“我心里就想，马化腾肯定天天看我们的微信，因他都可以看。”

不难发现，江苏消保委和百度之间一个重要的分歧点就是，手机百度、百度浏览器，是否存在过分调用用户数据的問題。

越界获取，“过度”惹来祸患

其实手机 App 看上的权限，还有很多。麦克风只是冰山一角。

来自互联网第三方研究机构 DCCI 互联网数据中心的《2017 年中国安卓手机隐私安全报告》显示，相比 2016 年，非游戏类 App 在 2017 年越界获取“通话记录”权限的由 3.2% 增长到 6%，越界获取“彩信记录”权限的比例由 0.2% 增长到 14.3%；教育类 App 中，获取“使用话筒录音”权限的比例由 65% 增加到 68%，获取“打开摄像头”权限的 App 比例由 53% 增加到 74%；而投资理财类 App 越界获取“读取通话记录”“读取位置信息”“打开蓝牙开关”和“访问联系人”权限较多，分别有 7.7%、5.7%、4.2%。

有意思的是，不少 App 常常钟情于和自身功能几乎“浑身不搭界”的权限，比如手电筒 App 会要求读取位置信息，理财 App 会提出读取通讯录等等。而如用户拒绝某些权限的申请调用，这款软件还会在使用过程中反复弹出调用权限的申请，甚至就索性无法使用了。

如此“越界”，自然是为了尽可能获取更多用户数据。所谓“得数据者得天下”。一些 App 开发者“不管有用没用，拿到权限再说”的做法，其根本目的，是为了积累自己的大数据资源，这无论对商品和服务的精准推送、广告投放，还是软件改进来说，都是至关重要的。

更深层次看，对于很多贴着科技标签的互联网企业来说，收集用户的各种信息，在市场上抢占先机，不仅是做生意的核心竞争力，更是在资本市场上讲故事的先决条件。如果看到数据背后超越营销功能的价值，或许就不难理解一些 App 为何会去过度索取消费者的权限，尽一切可能收集用户信息了。

法律界人士表示，目前国内对于 App 过度调取用户权限的相关法律和监管比较滞后，一旦“越界”后具体的惩治措施并不明确。实践中，也尚未有 App“越界”调用权限后被追责或受到处罚的判例。此外，我国目前对个人信息的保护还仅限于刑法，在民法和行政法上还存在不少真空地带，这直接导致相关保护规范力度不足，措施不够。

由于存在各种监管盲区，受利益驱使，目前相当多的企业都无视用户个人信息的保护。对于用户而言，手机 App 搜集到的信息越多，用户所面临的危险也会越大；一旦恶意盗取用户数据的行为发生，隐私信息被不法分子所窃取，后果可大可小。

需要指出的是，很多用户往往习惯在安装手机应用时，一路允许授予大量的权限。因此，专家也建议大家要关注手机上 App 的权限设置情况，禁止 App 调取不必要的权限。

选择，隐私换取生活便利

曾几何时，我们还不怎么关注自

你有没有遇到过，自己说过或者无意间关注到的东西，居然在使用另外一款 App 时获得了“精准推送”，这时候你只能感叹“大数据”真是无孔不入。

纽约时报日前在一篇报道中称，在谷歌的 Play 商店上，有超过 250 款手机

游戏 App 被发现存在偷偷使用手机麦克风监听的行为。这些手游自带的麦克风权限会在你观看电视广告、或者节目表演时收集音频信号，用于今后的精准广告推送服务。

消息曝光之后，相关应用的开发者发布声明，表示旗下产品不会在未获得

然地凸显了出来。如今，社会各界普遍认识到这一问题的严重程度，隐私也就成了今年的一大舆论焦点。

事实上，在移动互联网、智能手机普及的今天，我们已经无法限制自己的隐私信息被互联网公司所掌握。用部分的个人隐私换取生活便利，大概是现代人不得不做出的选择。以地

用户授权的情况下，擅自调用启动用户的麦克风。不过，这样一则语焉不详的简单声明，对消除用户的疑虑毫无帮助。在事件不断发酵过程中，更多人对

自己的手机开始“杯弓蛇影”起来。在个人生活几乎被 App 完全控制的今天，我们还能保存多少个人隐私？

图 App 来说，当你在愉快地使用免费导航功能的时候，所有的位置信息其实都已经留下了痕迹。这是不是就意味着，对于个体来说，隐私保护就是空谈呢？

对于近期集中爆发的 App 搜集个

App 瞄上“麦克风”



对于很多贴着科技标签的互联网企业来说，收集用户的各种信息，在市场上抢占先机，不仅是做生意的核心竞争力，更是在资本市场上讲故事的先决条件。如果看到数据背后超越营销功能的价值，或许就不难理解一些 App 为何会去过度索取消费者的权限，尽一切可能收集用户信息了。

目前国内对于 App 过度调取用户权限的相关法律和监管比较滞后，一旦“越界”后具体的惩治措施并不明确。实践中，也尚未有 App“越界”调用权限后被追责或受到处罚的判例。此外，我国目前对个人信息的保护还仅限于刑法，在民法和行政法上还存在不少真空地带，这直接导致相关保护规范力度不足，措施不够。

在专家看来，公民隐私保护意识的提高有利于形成保护个人隐私的良好氛围，但这其实还只是第一步，更关键的是要对数据的拥有者提出要求，强化对巨头企业行为合法性的行政监管。尤其是针对消费者被侵权，但尚未察觉损失的情况，要有针对性地对企业展开检查，建立适当的个人信息侵权行为行政处罚机制，一旦发生数据和信息泄漏，必须倒查追责，让隐私保护更加规范。

人隐私事件，有业内专家从另一个角度入手，没给出不同的解释。科技自由撰稿人宁宇在自己的公号上发表文章，认为从商业的角度来看，用户对 App 搜集个人信息的行为，其实也不必过于杞人忧天。宁宇认为，大公司关注的是群体行为，因此对于客户行为的分析，往往是针对某个维度进行

然后在此基础上给个体贴上兴趣、行为特点等各种维度的标签，再按照标签来划分群体，进而完成相关的分析。简单来说，单个用户在这些企业面前，很可能就只是一个又一个的标签。智能推送信息，最多能做到增加交易的成功率，尽管可能产生一定程度的骚扰，但不会带来太大的负面和麻烦。

因此，对于 App 搜集个人信息，既不要麻木不仁，也不必杯弓蛇影、草木皆兵。用户真正需要关心的是，如果这些数据信息被恶意盗用，甚至根据个体情况，来编造谎言、制造骗局，从而给用户带来财物和精神伤害，这个责任，应该由谁来承担？

在专家看来，提高公民隐私保护意识，有利于形成保护个人隐私的良好氛围，但这其实还是第一步，更关键的是要对数据的拥有者提要求，强化对巨头企业行为合法性的行政监管。尤其是针对消费者被侵权，但尚未察觉损失的情况，要有针对性地对企业展开检查，建立适当的个人信息侵权行为行政处罚机制，一旦发生数据和信息泄漏的情况，必须倒查追责，让隐私保护的问题更加规范。

尽管李书福这番推论并没有拿出“实锤”，但他颇为感性的叙述却击中了不少人内心的担忧。他说：“现在个人信息安全是一个非常大的问题，人几乎是全都透明的，没有任何的隐私和信息的安全。”

腾讯对这种说法很快就做出了回应，微信不留存任何用户的聊天记录，聊天内容只存储在用户的手机、电脑等终端设备上；微信不会将用户的任何聊天内容用于大数据分析；因微信不存储、不分析用户聊天内容的技术模式，传言中所说“我们天天在看你的微信”纯属误解。

支付宝：“晒账单”成了强行授权？

还没等微信这波“保护隐私”的热议散去，支付宝就用实际的行动给自己抢了戏。

本来在微信朋友圈晒一晒支付宝的年度账单正让大家乐此不疲，结果这场颇为“成功”的社交媒体营销却遭到质疑：在看账单之前，客户可能“被同意了”《芝麻服务协议》。

这个协议里都有哪些条款呢？包括“直接向第三方提供相关信息”，可以“将信息进行分析后并推送给合作机构，而且无须另行获得授权”，甚至“有权不支持您撤销第三方的信息查询授权”。不仅如此，即便是“服务终止后，仍可

继续保留信息和数据”。另外协议里还有这样的条款：对于第三方因为芝麻信用提供的信息而做出不利于您的行为，您是理解的，不会因此让芝麻信用担责。

此事立马引来网友的强烈吐槽，国家网信办网络安全协调局还约谈了支付宝（中国）网络技术有限公司、芝麻信用管理有限公司有关负责人，要求切实采取有效措施，防止类似事件再次发生。

支付宝和芝麻信用则用“愚鑫至极”作为道歉词，承认：“用户在查阅自己的支付宝年度账单时默认勾选‘我同意《芝麻服务协议》’这件事，肯定是错了”，同时调整了默认勾选的页面，并告知用户取消授权方法。

百度：监听电话偷窥隐私？

当你使用“手机百度”和“百度浏览器”这两款手机应用的时候，有没有想过不知不觉中隐私就被偷窥了？针对百度公司涉嫌违法获取消费者个人信息等相关问题，江苏省消费者权益保护委员会提起了消费民事公益诉讼，而南京市中级人民法院已正式立案。

对于“监听电话”、“读取短彩信”、“读取联系人”这些指责，百度发表声明称，百度的手机应用没能力“监听电话”，当百度相关应用获取任何

数据

个人信息泄漏

霸王条款是“主凶”

■张斌

近日，德勤发布了《2017 中国移动消费者调研》，其中涉及移动消费信息安全的部分格外引人注目。调查显示，有过半受访者认为，使用移动设备正在导致个人信息泄漏。

超过半数受访者确认，企业正在搜集使用消费者的个人信息，并向第三方提供此类个人信息。企业在经济利益的推动下收集并向他人提供消费者信息，导致用户信息泄漏事件频发，垃圾短信、网络诈骗等行为层出不穷。

联系方式、通讯录泄漏最为普遍。消费者向企业提供的个人信息中，最为常见的是联系方式，近四成用户向企业提供其电话号码，位列第一，约三成用户与企业分享姓名、地址和邮编地址信息。

霸王条款是信息泄漏“主凶”、包括涉及 App 安装的霸王条款。总体来看，未阅读却接受隐私条款的用户高达八成，34% 的用户表示总会在没有阅读的情况下接受条款。从不同年龄段来看，年轻人更易在未阅读的情况下接受条款。调查中受访者普遍认为，大多数消费者接受条款却未阅读的原因，并非其个人隐私保护意识薄弱，而是企业的服务只能在接受其条款的情况下才能使用，消费者为使用服务不得不接受条款。

业内人士指出，为杜绝越来越多的信息泄漏事件、缓解用户对个人信息泄漏的焦虑情绪，监管部门应借鉴发达国家的经验，在立法层面上进一步强化个人信息保护。

为了适应信息大数据时代个人信息保护的新要求，2016 年 4 月，欧洲理事会和欧洲议会分别表决通过了《欧盟一般个人信息保护条例》（GDPR），条例于 2016 年 5 月生效并将于 2018 年 5 月正式实施。此次个人信息保护法规的改革，提出了很多针对数字化时代的新要求。

根据 GDPR 第七条的规定，“信息控制者”对个人信息的处理和利用必须以信息主体的“同意”许可为前提。在信息的数字化实践中，个人接受服务时往往被要求明确接受或者默认接受大量的声明，由此使得个人很难在短时间内找到或读懂与个人信息使用有关的条款。为此，GDPR 特别提出要求，有关个人信息使用许可的条款，需要区别于其他服务条款，应当以“容易识别”、通俗易懂的形式表现出来，条款不得与其他服务条款“捆绑同意”，也不能以沉默、不作为等默示方式认定为“同意”。与此同时，个人信息主体在作出许可同意后，有权随时撤销该授权许可，信息控制者应当事先告知个人该项权利，并保障撤销权行使的便利性。



用户权限时，都会在安卓系统规定的合理使用范围内，弹窗提示用户是否同意授权以获得相应服务。

同时，百度还辩称，部分网友使用百度后，几分钟后就接到营销电话，是因为网友访问的网页被不法分子植入了恶意代码，而不是百度把你的手机号卖给了别人。

今日头条：调用麦克风偷录用户对话？

一波未平一波又起。眼见越来越多人关注隐私泄漏，今日头条也来凑热闹。据网友爆料，老婆元旦去摘草莓，一没在头条搜索“草莓”，二没在头条看“草莓”类资讯，转头就收到了和草莓有关的推送文章。这名网友打开老婆的手机，发现今日头条使用了麦克风的权限，怀疑其在手机后台偷偷调用手机麦克风，监听用户说话，然后再将讲话内容与头条资讯、广告进行匹配。

无独有偶，在社交平台上更多类似让人“惊吓”的案列开始传播开来。对此，今日头条紧急发布“致广大用户关于授权今日头条使用手机麦克风的说明”，称“除非用户授权头条使用麦克风，否则无法收到语音信号”；“今日头条用户信息积累靠的是用户点击，而在技术上无法通过麦克风收集声音信息的方式获取个人隐私”。