你聊啥就推啥，手机App真能“偷听”？

App违法违规收集信息屡禁不止，用户授权须谨慎

魏银科 济南报道

刚和同事聊到新出的包包，购物App立马精准推送；朋友聚餐才提到出行计划，手机瞬间被旅游攻略、机票信息“攻占”……这类现象对于智能手机用户来说并不陌生，而且似乎有愈演愈烈的倾向。

2025年上海两会，市政协常委游闽键提交的《关于加强App偷听、窥探用户隐私治理的建议》，再次将人们的目光聚焦于“手机App‘偷听’”的治理问题。

手机App真的能“监听”我们吗？如果是，该找谁维权？如果不是，普通用户如何保护自己的隐私安全？

成本奇高、效率低下 正规App一般不会偷听

游闽键表示，相关调查显示，超过80%的智能手机用户担心自己的隐私被手机应用偷听或窥探，近三分之一的人表示反感App精准推送广告行为，但苦于缺乏有效的防范手段和维权途径，只能在担忧中使用手机。

“正是因为安装了很多应用App，让智能手机存有偷听我们日常对话的可能。”绿盟数据安全咨询专家曾令平说，合法合规的App获取语音权限是为了正常使用，并不会偷听我们。但一些恶意App可就不一样了，它们会偷偷开启麦克风权限，在后台悄悄“监听”我们的一举一动。

此外，黑客也可能瞅准手机系统漏洞，远程植入窃听程序，收集我们的语音信息。一旦被偷听，手机耗能会异常增加，可能会出现掉电过快、发热发烫、CPU和内存占用高等现象。

对于所谓手机App偷听，中国电子技术标准化研究院网安中心测评实验室副主任何延哲也遭遇过。他说，有一天他运动结束后膝盖疼，跟家里人聊天谈了膝盖问题，一会儿打开某短视频App时，弹出一位主播医生说膝盖疼该怎么办。

何延哲说，他仔细分析了这个短视频App，看到这位医生是科普主播，并没打广告，这不排除碰巧刷到的可能，或者此前因为查看运动类视频，被推荐算法认为可能会关注运动损伤防护。

何延哲表示，手机偷偷录音虽说技术上可行，但成本奇高、效率低下，还得冒着触犯法律的风险，并不划算。智能语音行业某头部公司的语音转文本服务，市场售价10元/万秒，成本价2元/万秒。大数据与人工智能专家刘鹏算了一笔账：日活一亿的App日偷听用户1小时，一年下来成本高达263亿元，商业上根本行不通。

随着智能手机操作系统安全性的不断迭代，App通过麦克风偷听用户超过1分钟，都会被操作系统切断，根本无法维持长期偷听状态。

此外，现在手机对于使用麦克风、摄像头等敏感权限都有“红点”提示，当麦克风权限被App调用，屏幕上方的角落里就有了提示……因此App监听可能性几乎不存在。

几乎所有App都会 和合作伙伴共享信息

如果手机没有被监听，如此精准的推送又是如何实现的？

很多时候我们感到被“偷听”，其实是AI算法推荐机制在起作用。多名互联网信息安全专家表示，消费者在购物网站、搜索和在网络平台购买某种商品后，App或SDK通过移动端应用后台收集用户的消费习惯信息，如用户常浏览的商品类型、价格区间、购物历史等，并进一步收集用户的身份特征。

另外，朋友圈关联的其他应用信息，通过银行账户资金往来短信等途径估算用户的收入水平，从而进行行为建模，给用户贴“标签”，为用户推送感兴趣的商品，甚至玩起大数据“杀熟”的把戏。“这种基于大数据构建的用户画像越丰富细致，广告推送就越精准，从而让我们产生被手机偷听的错觉。”曾令平说。

何延哲则表示，这背后的逻辑比较复杂，究其根本逻辑，主要是两个方面：一是需要收集用户在设备上的行为数据进行画像，其中应用程序列表就是常见现象，使用哪些应用程序就代表了用户的生活习惯；二是需要收集用户设备的唯一标识信息，比如安卓ID，首先把用户画像匹配的精准广告推送到对应设备上，并对广告是否被用户点击、购买等进行关联和统计。

因此，要完成互联网精准的个性化广告投放，这两方面缺一不可，要完成这个过程，往往需要App、SDK（通过第三方服务商实现产品功能的软件工具包）和广告联盟等多方角色参与。

北京师范大学法学院博士生导师、中国互联网协会研究中心副主任吴沈括表示，正常情况下，手机不存在窃听的状态。但不同的App之间有一个数据的交互，也就是SDK广告商联盟，通过App或SDK给用户画像形成标签后，通过数据交换被另一个App所使用。

央视记者查询10款主流App的个人隐私协议后发现，几乎所有的App，都会将自有用户个人信息共享给第三方或合作伙伴。

某购物网站隐私权政策中就提到，“为便于我们基于平台账户向您提供产品和服务，推荐您可能感兴趣的信息，识别会员账号异常，保护关联公司或其他用户或公众的人身财产安全免遭侵害，您的个人信息可能会与我们的关联公司和/或其指定的服务提供商共享。”

整治App侵犯个人隐私 各监管部门应通力合作

对于因算法推荐而产生的被“偷听”错觉，保护个人隐私是关键。

自2019年1月以来，网信办、工信部等四部门联合开展App违法违规收集使用个人信息专项治理行动，对个人金融数据安全的监管日益趋严。

已有一大批违法违规收集用户数据的金融类App被网信办、警方点名，重点针对违规收集个人信息、违规使用个人信息、不合理索取用户权限、为用户注销账号设置障碍四个方面、八类问题进行规范整改。

去年11月24日，政府多部门联合发布关于开展“清朗·网络平台算法典型问题治理”专项行动的通知，明确将大数据“杀熟”现象列为重点整治对象，要求App不得超范围收集用户个人信息用于内容推送等。

随着《中华人民共和国个人信息保护法》《App违法违规收集使用个人信息行为认定方法》《常见类型移动互联网应用程序必要个人信息范围规定》《互联网信息服务算法推荐管理规定》等法律法规的施行，个人信息保护虽有所改善，但一些侵害用户隐私的现象仍屡见不鲜。

通过调研，游闽键发现，许多App技术设置不规范。比如，没有遵循最小权限原则，部分App调用的摄像头、麦克风拍照、录像、语音输入等功能，与App服务本身不相关。甚至一些恶意App可能会在用户使用手机时偷偷开启摄像头或麦克风，窃取用户的隐私信息。

目前相关部门对App违法违规收集用户信息，主要以随机抽查、算法备案的方式开展，一方面检查覆盖面有限，另一方面，对存在侵害用户权益行为的App，多数仅通报要求限期整改，监管力度不够。

游闽键提出，各监管部门应通力合作，加大事前、事中、事后全链条监管，即备案、抽查、委托第三方审计评估，加大对侵犯用户隐私App的曝光、处罚力度。

他还建议，联合开展专项治理活动，加大对涉网络社交、网络游戏、生活服务类等领域移动应用程序巡查力度。网信办、公安、市场监管、通信管理等部门协同推进建设信息监测基础平台；建立App安全评估认证体系，重点围绕移动应用程序违法违规收集使用个人信息等突出问题，进行常态化巡查、治理。

个人应提高隐私保护意识 谨慎给App授权

用户的个人隐私保护意识也很重要。在下载应用软件时，应优先选择官方应用商店的合规App。安装过程中，务必仔细查看麦克风、摄像头等敏感权限申请，非必要坚决不授权。同时，别忘了及时更新手机系统和软件，以坚固的“防护铠甲”抵御黑客入侵。

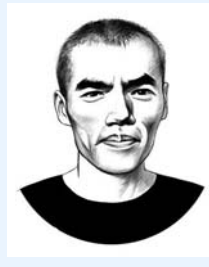
北京市京都律师事务所高级合伙人、中国计算机协会数据安全产业专家委员会专家委员王菲提醒，用户下载App，在勾选相关隐私政策协议时，需要仔细阅读。比如，App或SDK获取哪些权限，权限中哪些是开启状态，不相关的、涉及隐私的要手动关闭，把所有不影响正常使用的授权全部关闭，避免在不知情的情况下被收集个人信息。

曾令平建议，除了谨慎授权App权限，防止个人信息泄露外，在公开网站上也要“守口如瓶”，不轻易填写个人真实信息。不明网站千万别点，来历不明的App坚决不碰，公共场所的免费Wi-Fi更要慎用。

专家表示，随着专项行动的稳步推进与落实，以及用户越来越重视隐私保护，我们日常感觉被手机“偷听”的困惑或将逐渐减少。

评论

“隔屏有耳”就欠重拳出击



评论员 沙元森

很像是“隔屏有耳”，你聊啥，手机App就推啥。这种事情很多人都遇到过，但也无可奈何。上海市政协常委游闽键决定较一次真。

他在上海两会期间参加委员现场咨询活动，来到市通信管理局的“摊位”，直截了当地提问：“App的备案是通信管理局在负责的，有没有什么监管机制？有没有一些能够做在前面的动作？”

这些问题确实直击要害。针对个人信息保护，我国已经出台《个人信息保护法》以及《App违法违规收集使用个人信息行为认定方法》等法律法规。除了通信管理局，网信办、公安等多个部门都有相应的监管权力。

但是，问题的症结在于事前监管乏力，事后追责低效。很多用户能感觉到屏幕后肆无忌惮的“偷听”，但是又无处“申冤”。用户要举报，就得固化证据，固化证据之后还要公证，一般人耗不起时间和精力。

有备而来的游闽键提出，各监管部门应通力合作，加大事前、事中、事后全链条监管，即备案、抽查、委托第三方审计评估，加大对侵犯用户隐私App的曝光、处罚力度。这些建议都“扎到了穴位”，但是能取得多大“疗效”，还要看监管部门能否真正认识到“隔屏有耳”的严重性。

在很多人看来，App偷听固然让人不舒服，但也不是多大的问题，它不就是为了更精准地推送信息吗。“君子之心事，天青日白，不可使人不知”，在这种文化的熏陶下，很多人对个人隐私缺乏保护意识。很多App运营者习惯了用户的隐忍和默认，“偷听”也就成了其常规设置，否则在市场竞争中就会趋于被动。

无论相关企业怎么解释，从技术层面解决“隔屏有耳”并不难，无非是几行代码的问题。这个问题长期存在，却得不到根治，用户懒得较真只是一个方面，根本还在于处罚没力度。用户被偷听，不是偶发现象，很多监管部门工作人员自身可能也是受害者。其实不需要用户举报，监管部门也应该主动破解这种“群体无意识”，对无差别的侵犯予以重拳出击。

近来，围绕网络平台的算法治理，监管部门办理了一些典型案例，形成了很好的警示效应。治理“隔屏有耳”，也应推出几个典型案例，让屏幕背后的“偷听者”，真切感受到后果严重。