聊什么来什么 手机APP到底有没有在偷听？

在APP经历了多轮监管的今天，APP到底有没有监听依然是很多用户挥之不去的迷思。

网友小A刚提到想换手机的色彩和配置，在电商平台点击购买，系统就自动选到了她想要的暗紫色和256gb内存。网友小B在老公面前接了一个雅诗兰黛客服的电话，当晚老公的APP里就出现了化妆品广告。网友小C和朋友狠狠吐槽了“丑萌”的香肠嘴拖鞋后，一模一样的鞋就出现在她的APP推荐主页上……

类似的经历在社交平台上随处可见，随之而来的便是对于为什么“APP比你更懂你”的质疑和吐槽。值得注意的是，尽管个人信息保护领域的法律法规不断完善、监管部门对APP的治理力度不断加强，在APP的个人信息保护水平得到显著提升的当下，公众对于APP监听的质疑却并未随之消退。

APP真的在偷听用户说话吗？在技术层面上可实现吗？如果不能实现，精准推送又是如何做到的？记者采访了多位技术专家，试图从原理和运作机制层面揭开迷思。

质疑长期存在，权威测试未发现偷听行为

事实上，对于APP监听的质疑不是这两年才产生的。每当有用户在社交平台陈述自己“聊到什么就被推荐什么”的经历，总会引发大量网友的共鸣和讨论。不少机构和媒体也曾尝试模拟类似场景，希望得出APP是否真的监听的结论，但往往很难完全排除外界干扰得出确定的结论。

记者梳理发现，近年来，国内多个互联网大厂都曾公开回应过这类质疑。

2018年1月，有用户质疑今日头条利用麦克风权限“偷听”。今日头条对此回应：“从技术角度看，目前声音信息技术的处理，也远达不到通过麦克风获取个人隐私的水平。今日头条也绝不会在用户不知情的情况下收集用户隐私。”

2019年3月，有媒体称经测试，饿了么和美团外卖APP在用户谈话提及某种食物后出现相关推荐的概率较高。对此，美团、饿了么均予以否认：饿了么称“既没有做类似的产品设置，也不具备相关技术条件”，美团则强调“根据麦克风收录的语音关键词为点外卖的用户做推荐”的行为并不存在。微信团队也曾表示，微信上的广告投放是基于用户的合法授权和数据技术支持实现，微信绝不会监听、监视用户聊天并推送广告。

2021年1月，央视新闻《共同关注》栏目曾专门针对质疑，邀请权威专家进行实验。专家通过检测发现，目前还没发现哪款APP在真正意义上有把语音信息上传之后的偷听行为。

监听成本高、效率低、法律风险巨大

记者注意到，上述互联网大厂在回应APP监听质疑时，通常会强调不具备相关技术条件，以及相关推荐是基于用户行为数据生成的。那么APP监听在技术上是否可行呢？

2019年，中央网信办、工业和信息化部、公安部、市场监管总局四部门成立的APP违法违规收集使用个人信息专项治理工作组（下称“APP治理工作组”）。时任APP治理工作组专家的何延哲认为，APP监听可能主要有两种方式：静默录音和“侧信道”还原。

静默录音是指APP在获得用户对于录音权限的授权后，在不通知用户的情况下，实现后台静默录音。不过专家实测发现，使用ios系统和Android 9及以上系统版本的手机，已经采取了限制机制，APP无法实现后台静默录音，否则前台会出现明显的正在录音的提示。即使采用“监听并提取关键字”的方式，静默录音最长只有1分钟左右，而手机未锁屏且将APP置于前台时，才能实现长时间的无感录音。

另一种“侧信道”还原的方式是通过手机中的加速度计、陀螺仪或其他传感器获取数据，再利用深度学习等技术恢复语音数据。但这种技术门槛高，实现过程包括深度学习模型的建立、训练、环境干扰因素影响等，在非实验环境下是否能被有效使用还是未知数。

因此，何延哲曾在央视节目里指出，偷拍偷录虽然在技术上可以实现，但是这种方式成本高、效率低，而如果采用利用系统漏洞、安装恶意程序等突破系统限制的违法方式，则存在高昂的法律风险。

“开启麦克风，手机容易发热……一旦屏幕锁定，它（APP）就听不了了。”他表示，即便APP可以监听，它还得向服务器传输语音数据，会让手机明显卡顿，而且企业需要大量服务器去存储这些数据。另一方面，由于APP无法辨认录到的音是否为机主本人，也就很难据此进行推送。

不难看出，APP监听或许并不是企业进行广告营销、定向推送等日常运营中的合理选择。

精准推荐倚赖用户画像、大数据分析

公开资料显示，专家和媒体其实都对精准推送背后的技术原理做出过多次详细解释，但效果并不好，这或许是因为推送实在是太精准了，有时如同“读心术”一般。如果APP没有监听，如此精准的推送又是如何实现的？

“APP可以把一个用户做360度画像。”何延哲解释，这既是多年积累的结果，也是多个渠道汇聚的结果。而画像的准确性主要是通过根据用户的购买记录、浏览记录、搜索记录甚至是下载过的APP清单等信息进行大数据分析。“无数次的推送中，总有几次押准的，人总是会对押准的这几次印象特别深，就会形成误解。”

除了“巧合”外，从底层技术来看，基于用户信息的个性化广告推送在行业内有个统一的名称——程序化广告，其核心是通过合法的程序化广告系统，依据用户在授权信息中所表现的偏好，提供相匹配的广告内容。

通常平台是通过收集和标记用户的浏览偏好和广告行为，形成多维度的用户画像，比如你的年龄在25-30岁之间，相比服饰类，你可能更爱浏览美妆类产品等等。这些标签或出自广告投放者，或来自第三方的数据管理平台。

例如钢琴商想投放广告，他可能会找任意一家互联网平台投放钢琴广告，这些平台会根据在授权信息中出现“钢琴”“音乐”等相关标签的用户来推送广告。整个投放过程均通过程序化广告系统自动完成，参与各方通过技术手段将用户信息去标识化、群体标签化。

在整个过程中，用户标签并不会被交换或共享，广告买卖双方也无法在广告投放过程中获取对方用户的行为或个人信息。多位从业者也向南都记者表示，一个由标签组成的用户画像，并不能对应到可识别的真实个人。

记者查阅相关资料发现，2021年12月，某短视频博主散布“vx被监听，1分钟教你关闭”等未经核实的内容，被法院判定侵犯原告名誉权。审理法院指出，个性化广告已经成为了互联网广告的一种比较常见的模式，发生广告个性化推荐结果并不意味着APP实施了监听。各个平台一般会根据用户的浏览偏好、使用记录等进行收集和标记，形成用户画像，并据此进行广告投放。

提供灵活管理方案，平衡用户体验与个人信息保护

APP监听误解之所以长时间以来被反复提及，是因为用户难以对其证实，企业又无法对其证伪。不过记者梳理发现，相关法律法规和手机厂商已经分别从监管和实操的层面对APP的行为做出了规制。

比如个人信息保护法规定，收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。

目前，很多手机操作系统已经提供了“摄录指示器”的功能——APP一旦调用“麦克风”“摄像头”权限，状态栏就会出现常驻的图标提示。有些手机系统还提供了“单次授权”方式，用户仅在此次使用APP期间授权相关权限，退出APP后权限恢复关闭状态。

“其实，用户接受个性化服务，并不会以牺牲隐私为代价。”中国政法大学数据法治研究院教授张凌寒曾对媒体表示，平台往往是为了方便了解用户类型而设定用户画像，如果仅仅是针对用户的行为特征和消费习惯，而不具有可识别性，则不构成个人信息保护法所定义的个人信息。

个人信息保护法还进一步要求，个人信息处理者通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。该条款针对的场景就包括个性化推送。

2020年12月，南都发布的《个人信息安全年度报告》中对50款头部APP进行个性化推荐相关测评发现，其中6款APP没有提供关闭选项。时隔两年，经记者实测，目前，测评中的头部APP都已经增加了关闭个性化推荐的按钮。

张凌寒认为，目前大部分企业都设置了算法退出机制，有利于实现用户“个人自治”。但实践中只有少数用户会直接关闭个性化推送，且很多人会选择再次打开，因为关闭该功能后，用户所接收到的信息与其兴趣相关度降低，会影响用户体验。

因此，她提出企业应在目前的退出机制基础上，提供更灵活的个性化推荐管理方案，以平衡用户体验与个人信息保护。此外，还应建立有效的数据保护机制，通过展示平台保护数据的能力来化解用户顾虑，实现数据利用的目标。

何延哲则建议，手机厂商也应进一步完善透明化机制、完善手机软硬件安全机制设计，防止被恶意利用，还应及时发布安全补丁，并提醒用户更新。用户也可以主动采取一些措施，比如更新手机操作系统到最新版本；仅在使用相关功能时开启“麦克风、摄像头”等权限，用完后关闭。如果APP强制要求开启，应不再使用该APP，并向相关部门举报。

据《南方都市报》