

特别关注

聊什么就给推什么！

手机App在“偷窥”我们吗？

“滴滴出行”App存在严重违法违规收集使用个人信息问题，下架整改；哪吒汽车等57款App存在违法违规收集个人信息，被要求限期整改……一些App不同程度违规收集、使用用户信息，引发社会关注。那么，“偷窥”是如何发生的？我们要怎样守卫个人信息安全？

部分App“偷窥”用户信息

在社交媒体平台上，有关“手机是否在偷听聊天”的话题被网友不时更新。有网友称，“现在手机的偷听功能真是强大，刚才跟朋友聊天，朋友的手

机还是锁屏状态，我提到某品牌挖掘机，朋友打开手机后，到处都是该品牌的广告。”

那么，手机是否真的在偷听我们的聊天呢？“大家认为的‘偷听’，其实是App调用手机麦克风权限，搜集环境音的行为。”上海安识网络科技有限公司总经理、网络安全专家郭耀告诉笔者，在业内，App调用手机麦克风、摄像的权限，以及调用手机剪切板、通讯录、位置信息或存储的行为，一般称为“监听”，这里的“监听”其实不仅仅是“听”，还包含了“看”“读”“传”等活动。

笔者联系业内权威测评实验室证实，App即使不调用手机麦克风权限，也可以通过分析与用户、用户设备、用户所处环境相关数据的方式来“探测”用户需求，这些数据包括下载安装过的App名称、IP地址所处大致地理位置、用户的上网浏览历史、搜索痕迹等。

笔者曾在某社交App上进行感知测试：先后发布4条包含信用卡办理、婚纱摄影、婴儿纸尿裤和房产交易的公开信息（测试前，笔者没有在该手机的任何App发布或检索过类似信息），不到30分钟，某地产企业广告在3个不同的新闻资讯类App中做了首页推荐，某婚纱摄影广告也在另一款社交App上发布“头条推荐”。



遭遇“木马” 翟桂溪

今年5月，国家网信办组织对公众大量使用的部分App的个人信息收集使用情况进行了检测，105款App发现的问题包括：未经用户同意收集使用个人信息；违反必要原则，收集与其提供的服务无关的个人信息；未公开收集使用规定等。

想方设法逃避监管

笔者梳理发现，近几年，国家对App相关技术产业主体收集使用个人信息行为出台了规范文件，提出了具体要求。但部分主体并未完全承担起应有的责任，依然违规收集、使用用户信息，甚至利用部分应用商店安全检测不严，以及网盘、论坛贴吧、短信链接等渠道缺乏安全检测的漏洞扩散。

有些App首次启动时，在用户授权

情的情况下，利用手机内置加速度传感器来搜集手机扬声器发出声音的振动信号，从而实现对用户语音的“偷听”。

据研究人员介绍，由于手机中的扬声器和加速度传感器安装在同一块主板上，且距离十分接近，当扬声器在播放声音时所产生的振动可以明显影响手机内置加速度传感器的读数。因此，通过劫持手机内置加速度传感器，并收集其振动信号，即可识别甚至还原手机所播放的声音信号。

针对这些情况，各级监管部门不断强化日常巡查执法，适时开展专项整治，整改了一批不合要求的App。有的手机厂商也在优化相关设计，弹窗、亮灯等形式提醒用户有App在调用手机相应权限。然而，一些App受

利益驱使不断升级技术手段，逃避监管，使得用户信息的保护成为一项长期、复杂的工作。

多措并举，堵住“偷窥”漏洞

“对企业而言，它们有通过做广告营销进行营利需要；对用户而言，也应该有权利选择‘更多隐私’还是‘更多便利’。”网络安全专家何延哲认为，是否能够搜集用户的个人信息并进行相应的个性化广告营销，不能全是企业说了算，用户更应享有选择权。

何延哲建议，有关部门要加紧制定出台相关行业标准，对个性化广告的数据搜集范围、数据处理流程、用户的控制机制等做出相应规定，充分保障用户的各项权利。

与此同时，监督力度要跟紧。专家表示，现有技术监管手段由于自动化检测能力低、覆盖范围受限，很难实现全面均衡监管，需要紧跟App技术发展前沿，及时更新监管技术手段。用户可定期检查敏感App的手机权限获取详情，积极向网信部门举报恶意程序线索，与监管部门等共同维护个人信息安全。

App相关技术产业主体更要积极承担主体责任，按照相关规定的要求划定底线和红线，厘清App运行所需要的合理个人信息需求，提升履责水平。浙江大学网络空间安全学院教授周亚金提出，手机厂商应该为用户建立起防止被App随意偷听的“第一道防火墙”，例如在未来的系统更新中新增“一键关闭前置摄像头”或“一键撤回App麦克风使用权限”等操作。 □颜之宏

近期，从国家到地方都出台了针对性举措，剑指“大数据杀熟”。比如，国家市场监督管理总局发布了《关于对<价格违法行为行政处罚规定（修订征求意见稿）>公开征求意见的公告》（以下称意见稿），《深圳经济特区数据条例》近日公布，将于明年1月1日起施行。不过，据笔者调查发现，在一些领域，平台“杀熟”情况仍然存在。

“杀熟”仍然存在

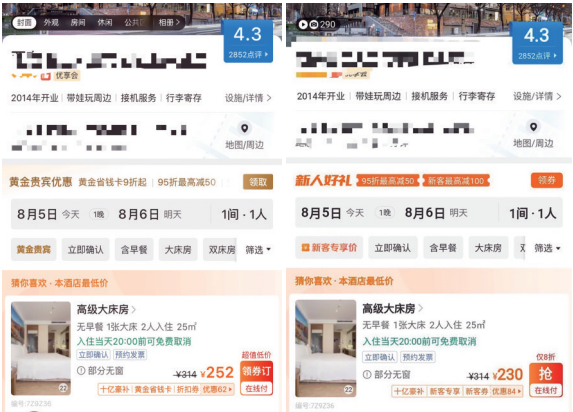
7月初，意见稿中新增了“新业态中的价格违法行为”内容。意见稿提到，电子商务平台经营者利用大数据分析、算法等技术手段，根据消费者或者其他经营者的偏好、交易习惯等特征，基于成本或正当营销策略之外的因素，对同一商品或服务在同等交易条件下设置不同价格的情形之一的，给予警告，可以并处上一年度销售总额1‰以上5‰以下的罚款，有违法所得的，没收违法所得；情节严重的，责令停业整顿，或者吊销营业执照；今年7月，深圳市公布《深圳经济特区数据条例》，明确提出对“大数据杀熟”给予重罚——情节严重的，可处5000万元以下或者上一年度营业额5%以下罚款。虽然依法治理“大数据杀熟”的脚步没有停歇，但笔者近日调查发现，“杀熟”行为在一些常用平台仍不同程度存在。

在某在线旅游平台上，西安同一家酒店同等房型的客房，享有9折优惠的黄金会员手机页面上显示的优惠后价格为252元，普通会员手机页面折后价格是230元。

根治“大数据杀熟”困难重重

北京市消协调查显示，超八成被调查者认为，“大数据杀熟”现象如今相当普遍，且有超五成被调查者表示有过被“大数据杀熟”的经历。今年年初，中消协表示，有些经营者利用算法进行价格歧视。一是对新老用户制定不同价格，会员用户反而比普通用户价格更贵。二是对不同地区的消费者制定不同价格。三是多次浏览页面的用户可能面临价格上涨。四是利用反复促销规则和算法，实行价格混淆设置，吸引计算真实价格困难的消费者。受访专家表示，“大数据杀熟”具有智能化、系统化、批量化、隐蔽性等特点，想要根治仍然困难重重。

难以察觉，隐蔽性强。中国政法大学传播法研究中心副主任朱巍认



图为两名不同会员用户（左：黄金会员，右：普通会员）预订同一时间同一房型价格对比。

『大数据杀熟』现象调查与对策

『看人下菜』精准投放

为，“大数据杀熟”问题频繁出现、屡禁不止，很大程度上在于其有一定的隐蔽性，一方面，消费者不经多部手机或者多人同时比对，很难察觉这一情况。另一方面，消费者即便发现价格歧视也难以固定证据，因为消费者并不知道价格A和B之间的差距是怎么形成的，在某些情况下“素人补贴”等情况都会造成单价的不同，消费者很难仅凭借价格的差异来判断平台是否在“杀熟”，同时也给平台留下了解释的空间，导致消费者举证不易、维权困难。

“看人下菜碟”，区分用户。部分平台对于苹果手机用户也会“格外关照”。复旦大学孙云金教授的团队在针对网约车平台的调查中发现，苹果手机用户在打车过程中更有可能被舒适型车辆，即优享、专车等价格相对较高的车型接单，且这一比例是非苹果手机用户的3倍。此外，苹果手机用户所能享受到的打车优惠也更少。

“精准投放”，诱导消费。专家表示，比如基于算法的推荐广告，似乎总能“猜中”消费者的喜好，从电线杆上的“牛皮癣”变成朋友圈里的“精准投放”，时刻诱导、干扰消费者。专家表示，一些平台会分析消费者的消费习惯和喜好，推荐消费者搜索价格区间的商品或服务，多次浏览页面的用户可能面临价格上涨。

业内专家认为，“大数据杀熟”更深层次的问题在于平台对用户数据的保护和利用不当，除提升监管强度提高相关行为的违法成本外，还要不断强化日常的制度约束。

北京市消协曾建议，采取技术手段和技术设备，建立相应的大数据网上监管平台，针对网络信息平台进行全天候的在线监管，提高对各种隐性大数据利用违法行为的查处能力。同时，可建立诚信激励和失信黑名单制度，一旦发现企业存在通过“大数据杀熟”损害消费者知情权、选择权和公平交易权的行为，不仅要对其给予行政处罚，还要将其纳入诚信黑名单。 □邱兆翔

周末评论

你前脚刚说了想吃火锅，后脚打开手机就看到App在给你推荐附近的火锅店——究竟是巧合，还是App在偷听我们谈话？据报道，笔者近日对手机App是否存在偷听用户的情况进行了一个实际测试。实验证实，App只要获取了手机麦克风权限，并连接网络持续在前台运行，在理论上完全能够做到偷听用户讲话，并且在用户毫无察觉的情况下偷偷录音。

很显然，抛开大数据画像等专业话术，App偷听用户信息，再给用户精准推送广告，基本上是成立的。这意味着，在即便不使用App的情况下，安装在手机里这些本来用于方便工作、生活的各种软件，也可能在无时无刻地“监控”我们。这种异化和倒置关系，明显背离作为工具App的初衷。

精准推荐落地是移动互联网技术发展到了必然阶段的必然表现。企业通过不断开发优化人工智能、大数据算法等底层技术，让App具备根据用户偏好推荐靶向产品或服务的能力。但有个

别企业对用户隐私过度窥探、对用户数据违规交易，并以此作为实现和强化精准推荐的信源基础，无疑增加了人们对隐私泄露的担忧。

有人说，在大数据时代，每个人的上网信息都处于“裸奔”状态，但手机App可以偷听用户谈话等私密信息居然是真的，这还是让人细思极恐。精准推荐等新兴技术对企业发展具有促进作用，但其应用需要得到市场的认可、用户的信任，不能让某些违法违规行为污名化了新兴技术。

不必讳言，“偷听”及背后黑色产业

链无异于社会公害，对此绝不能小觑。要保护个人信息，除了在手机操作系统的权限设置里，找到麦克风权限等，检查有哪些App被授权使用，然后根据需要关闭授权。出现了非法窃听导致严重后果的情况，更有必要对违法案件进行严厉打击。《刑法》第284条明确规定，非法使用窃听、窃照专用器材，造成严重后果的，处二年以下有期徒刑、拘役或者管制。由此看来，要有法律常态化亮剑，让不法行为受到应有的法律惩治，让不法分子尝到法律惩治苦果，才能有助于消弭窃听带来的不良社会影响。 □吴学安

