

Z 综合工人日报 新京 中国消费者报

近日,某购物APP自行删除用户手机视频引发热议,再次将APP权限及用户隐私保护问题推上风口浪尖。

据《工人日报》报道,有用户下载一款医疗健康手机应用(APP),被要求填写姓名、手机号等隐私数据,即便在卸载这款APP后,依然接到四通骚扰电话,其中不乏医美机构询问植发等,甚至是推销借贷。

个人信息被智能手机应用过度违规采集问题屡次被曝光,此前,多款医疗健康类APP就因过度收集个人信息被监管通报。

在使用医疗健康类APP求医问药时需要注意哪些问题?相册、位置、身份证号、通讯录等私密信息,为何在各类应用后台一览无遗,有的数据甚至成了可以买卖的第三方产品?如何堵住个人信息泄露漏洞?



建隆漫画

健康隐私信息 如何不被恶意窃取?

专家建议,应明确不同类型APP需要提供的信息范围,开通便捷的举报渠道,保护个人隐私

线上咨询诊疗后 不同商家相继来电推销

去年底,95后王先生因脱发问题下载了一款医疗健康手机应用,按照流程,他填写了手机号、姓名,并且上传了面部信息以及脱发照片,让医生做初步线上诊断。

医生给出诊断结果后,提供了治疗方案,但王先生考虑价格较高并未接受,并停止咨询和卸载了该应用。但之后一周,他先后接到了四五个电话,均是不同医美机构询问其有无植发意愿,甚至还有贷款公司问其是否需要借贷,此时的他感觉个人信息被泄露了。

记者在手机应用商店随机下载了一款高评分微整形医美APP,安装后进入界面第一步是注册填写手机号码、所在地等信息,甚至需要选择“魔镜”功能进行面部识别,才能进入咨询界面。

某互联网软件开发公司技术工程师高雯雯在接受采访时表示,一些手机应用收集个人信息的目的,一是为了验证APP各方面合理性,例如,一个新页面放在首页,运营人员会根据收集的行为信息获得反馈,进而调整优化功能;二是为了用数据构建用户画像,进行个性化推荐,此外还可能将信息提供给所需服务的第三方。

“现在市场上相当一部分手机应用属于过度收集个人信息。”高雯雯说,制作一款简单APP的成本非常低,任何一家公司花几万元用固有模块拼装修改一下就能开发。但是,如果APP不正规,可能会有第三方接口和插件,数据会直接泄露给第三方。由于开发成本较低,数据还可能被破库和内部人员贩卖。

获取隐私信息范围广 关联服务公司共享用户信息

今年4月,好医生APP(版本6.1.3)因涉嫌隐私不合规问题,被国家计算机病毒应急处理中心通报。去年8月,禾连健康APP(版本9.2.4)因收集与提供服务无关的个人信息,且存在未经同意向他人提供个人信息等问题被通报。再早之前,工信部就曾通报批评过广东壹号大药房连锁有限公司旗下的1药网APP私自收集个人信息并共享给第三方等问题。

企查查数据显示,目前共有超4000个医疗相关APP。高雯雯说,有的APP获取的隐私信息范围大到惊人,远超出国家规定范围。

记者在所下载APP个人信息使用隐私协议中看到,基本信息、面部特征、个人财产信息、上网记录、常用设备记录均会被收集。在如何共享、转让、公开披露您的个人信息一节中,协议还要求除了在明确同意、法律规定、自行同意的情况下,还会与关联的服务公司共享,其中的服务提供方有小额贷款公司、保险业务公司。

北京中银律师事务所高级合伙人杨保全表示,消费者下载安装医疗APP的一个原因是出于便捷目的,即去医院之前的自我诊断、用药问询、导诊挂号等,因此,医疗健康类APP相较于其他类型,收集的信息更为隐私,诸如人的身体数据、健康状况以及生理情况等,这些数据也需要更加严格的管理。

医疗健康APP运营已有基本准则

与电子商务、消费金融、音视频平台等其他领域相比,医疗健康APP涉及的用户隐私风险尤其大。

一方面,在寻医问药和自我保健过程中,一些缺乏上网经验的用户,很容易将平台运营方视为“类医院”的主体,卸下心防,一问就答,向其提供核心隐私数据。

另一方面,手机通讯录、面部特征、财产状况等核心隐私数据一旦被不法分子掌握,可能被用于破解银行账户、手机系统、人脸识别门禁等,给用户造成信息安全威胁,甚至是生命财产损失。

事实上,国家高度重视医疗健康APP的数据安全工作,不同层面都明令遏制过度收集个人隐私数据。如国家网信办等多部门联合制定的《常见类型移动互联网应用程序必要个人信息范围规定》就明确,APP不得因为用户不同意提供“非必要”个人信息,而拒绝用户使用其基本功能服务。

其中,也不乏针对性规定。如对于女性健康类,基本功能服务为“女性经期管理、备孕育儿、美容美体等健康管理服务”,无须个人信息,即可使用基本功能服务;对于问诊挂号类,基本功能服务为“在线咨询问诊、预约挂号”,把必要个人信息限定为手机号码,患者姓名、证件类型和号码、预约挂号的医院和科室;问诊时需提供病情描述。

为顺应健康产业、公益事业的需求,前不久,国家卫健委等印发的《“十四五”全民健康信息化规划》提出,采取“原始数据不出域、数据可用不可见”等方式,有序推动健康医疗大数据共享应用。

在此背景下,有关部委、省份也在探索将个人的居民健康档案信息、基本医保参保信息授权给第三方的商业健康保险投保、理赔,申请慈善救助等业务情景使用。

而上述探索都有以下共同特征:隐私数据共享需要遵循国家安全、医疗安全、产业安全、个人健康安全等多重目标;数据类别和数据量需要满足完成业务需求的“最小可见”“最小可用”原则;数据共享要求全程留痕、接受第三方审计并实现终身追责。

这些,无疑都是包括医疗健康APP在内的各类平台运营的基本准则,需要各方认真对待、严格落实。同时,应用商店要强化相关APP合规评估,用户也要加强个人信息保护与维权意识。

□声音

要让用户协议 保护用户隐私

无论是医疗健康类还是其他类型的APP,隐私协议都不能成为“隐秘的角落”。用户协议、隐私协议暗藏陷阱,侵犯了广大用户的合法权益,要予以遏制。

对此,一方面需要广大用户增强维权意识、防范意识,在注册APP前,认真阅读用户协议、隐私协议,要小心“埋雷”“挖坑”,不能为了便利让渡个人权利。另一方面,有必要出台相关规定规范APP运营,如制定用户协议范本,防范部分企业侵犯用户权益,在用户协议上玩文字游戏。用户协议要尽可能地简洁明了,不能用复杂的条款“绕晕”用户。相关部门则要加大执法力度,重点整治APP侵犯用户隐私等痛点问题,畅通用户举报渠道等。

用户协议要能保护平台和用户的合法权益,实现“双向保护”,形成“双向约束”。用户隐私不能成了APP的“囊中之物”,要让用户协议发挥积极作用,对各种侵犯用户权益的违法违规行为,则要露头就打,让其失去生存空间。