企业太“任性” 用户变“透明” 国家立规矩

APP“偷窃”隐私信息何时休

如今，人们几乎都使用智能手机并下载各类APP。这些APP在提供方便的同时，也可能“偷窃”手机号、通讯录、通话记录、短信记录等隐私信息。5月24日，APP专项治理工作组发布的《百款常用APP申请收集使用个人信息权限列表》显示，在10大类26项个人信息相关权限中，平均每个APP申请收集数目达10项。这些信息很容易落到不法分子手里，成为敲诈勒索等违法犯罪活动的工具。

为遏制APP强制授权、过度索权、超范围收集个人信息现象，5月28日，国家互联网信息办公室发布《数据安全管理办法(征求意见稿)》(下称《办法》)，对公众关注的个人信息安全问题直接回应。专家表示，《办法》着眼于公众反映强烈的个人信息泄露问题，对“任性”的APP立规矩，将对该行业产生重大影响，倒逼网络经营者加强对用户个人信息安全保护。

APP的套路让用户“很受伤”

这些天，来自北京的谭先生在一款理财APP上还完自己所欠借款后，立即将APP删除了。原来，去年下半年，他在该APP上办理了一笔1万多元的现金贷，分6期归还。在还完前5期后，他因回乡未能在规定时间内还款，结果对方每天打电话骚扰其通讯录好友，还通过辱骂、威胁、恐吓等方式催促还款。回想起这段经历，谭先生仍然心有余悸：“现金贷很可怕，这个APP能轻松获得我通讯录好友信息更可怕。”

你有没有过这样的经历——刚在购物APP上浏览完一些商品，随后另一个新闻资讯客户端就向你推送类似商品广告；刚在社交APP上说想出去聚餐，稍后就收到一堆餐馆广告推荐；刚在购房APP上浏览完毕，信用贷款电话就打了进来……如果有类似遭遇，那你的隐私信息很可能已经泄露。

谁动了我们的个人信息？就是这些你刚刚浏览过的APP。这些APP收集用户隐私信息，给用户带来很大影响。总结起来，可按程度轻重分以下几类：

一是给用户“画像”，帮助商家精准推送广告。所谓精准推送，就是APP通过收集、分析用户上网浏览记录，结合用户定位和性别等身份信息，绘制成用户肖像，从而实现广告精准推送。信息收集方式多为强迫用户授权或默认勾选，否则无法使用该APP。

为测试是否被“画像”，记者下载并注册了一款社交APP，先后发布论文写作、信用贷款、儿童摄影等3条信息，记者此前并未在其他终端发布或检索过类似信息。隔1个小时，记者登录自己手机上其他几款新闻类APP，赫然出现了和这3条信息相关的广告。

专家表示，这种广告被称为“程序化广告”。平台根据用户行为给其打上对应“标签”后，在后台以竞价或自动个性化方式为广告主做精准投放。按照规定，投放此类广告可事先不经用户明确授权，但应确保用户有拒绝权利。不过，大部分APP目前并未设置相应关闭按钮，或者将按钮藏在多个操作步骤之后。

二是把用户信息视为“资产”，许进不许出，注销账号和删除个人信息难。很多用户发现，注册一个APP账号只需一个手机号及其注册码，而想要注销一个账号往往很难。即便注销了账号，想清空个人信息更难。

网经社电子商务研究中心法律权益部向记者提供了一个用户投诉案例：李先生计划停用某共享单车，注销手机号。因为当初注册该APP时使用了个人身份证号，担心信息泄露的李先生申请注销用户账号并解绑身份证。该APP客服人员要求他提供个人身份证照片及手持身份证照片。李先生认为这种行为具有强制获取个人敏感信息嫌疑，让人无法接受。

专家表示，APP运营者不能过度收集用户信息。在收到用户请求时，APP运营者应当在合理时间和代价范围内予以查询、更正、删除或注销账号。

三是泄露用户隐私信息，导致用户利益受损。用户信息泄露存在很多情况，比如APP用户隐私信息数据库被黑客入侵、平台出现漏洞等导致信息泄露；比如APP将用户信息“打包”出售或用户信息经公司“内鬼”窃取售卖，被不法分子利用等。

网经社电子商务研究中心法律权益部分析师姚建芳对记者表示，目前接到的用户投诉案例集中在信息泄露方面，主要为购物类、金融服务类APP，用户因此遭到恐吓、电信诈骗、资产被盗刷等损害。

北京盈科(杭州)律师事务所方超强律师对记者表示，根据《网络交易管理办法》，电商平台在获取个人信息的同时有义务保护信息安全。但在现实中，对“平台存在漏洞导致信息泄露”缺乏相应判断标准，用户因此很难对平台进行追责。

哪些收集用户信息行为“越界”了

在中央网信办、工信部、公安部、市场监管总局指导下，APP专项治理工作组近日发布的《百款常用APP申请收集使用个人信息权限列表》显示，餐饮外卖、地图导航、网上购物、短视频、金融借贷等近20类共100个APP，基本都会收集用户26项个人信息中的某几项；超过九成APP获取用户精准定位；金融借贷类、工具软件类APP获取用户信息项目相对较多。其中，360手机卫士收集使用个人信息相关权限数最高，达到23项，用户不同意开启则APP无法安装或运行的权限数达11项。

需要说明的是，APP不是不能收集用户个人信息，但不能“越界”、过度，不能强制、超范围索要权限。

那么，APP目前收集的个人信息里，哪些属于不宜收集的隐私信息？中国消费者协会此前发布的《100款APP个人信息收集与隐私政策测评报告》显示，多达91款APP列出的权限涉嫌“越界”过度收集用户个人信息。其中，用户位置信息、通讯录信息、手机号码等个人信息是被过度收集或使用的主要内容。此外，用户照片、财产信息、生物识别信息、工作信息、交易账号信息、交易记录、上网浏览记录、教育信息、车辆信息以及短信信息等均存在被过度使用或收集的现象。

不过，对于企业收集这些隐私信息是否属于“越界”行为，也有不同声音。腾讯社会研究中心和DCCI互联网数据中心今年1月发布的《2018年度网络隐私及网络欺诈行为研究分析报告》显示，安卓端“越界”获取用户隐私权限的APP正在逐渐减少，到2018年下半年，仅有2%的APP存在“越界”行为。该报告认为，判断APP是否“越界”获取隐私权限的标准是APP向用户提供的功能是否必须用到相应权限。也就是说，如果确属APP功能需要，且经用户授权同意，那么，APP相关收集行为就不算“越界”。

中国社科院信息化研究中心秘书长姜奇平对记者表示，APP索权是否“越界”，应以用户是否需要而非企业是否需要为界。他说：“很多收集的数据并不是APP自己需要的；有些甚至打着倒卖的坏主意，这对消费者个人隐私、信息安全来说是很大隐患和伤害。”

用户黏性不是企业违规的“底气”

为切实解决APP过度索权造成的用户信息安全问题，5月28日，国家互联网信息办公室发布《数据安全管理办法(征求意见稿)》，对公众关注的诸多问题进行了直接回应。

比如，对于规范个人敏感信息收集方式，《办法》规定，网络运营者以经营为目的收集重要数据或个人敏感信息的，应向所在地网信部门备案；为约束定向精准推送广告，《办法》规定，网络运营者应当以明显方式标明“定推”字样；针对APP强迫授权或默认勾选等，《办法》规定，网络运营者不得以默认授权、功能捆绑等形式强迫、误导个人信息主体同意其收集个人信息；针对用户注销账号和删除个人信息难、小程序泄露用户信息后平台责任问题等，《办法》也进行了明确规定。违规者根据情节轻重将面临关闭网站、吊销相关业务许可证或吊销营业执照等处罚；构成犯罪的，依法追究刑事责任。

由APP专项治理工作组起草的《APP违法违规收集使用个人信息行为认定方法(征求意见稿)》也在5月26日结束意见反馈。这份《认定方法》对APP运营商7种违规收集使用个人信息情形进行了规定，被认为是判定APP是否“越界”的重要标准。

“把信息采集主导权、选择权交给消费者，是信息服务的原则性问题。为了收集信息采取胁迫或者误导行为，都是坚决不能被允许的。”姜奇平认为，APP治理此前长期收效不大，根本上说是因为一些经营者处理不好社会责任和商业利益的关系。“这不是简单的技术问题，甚至不完全是产业问题，是企业态度问题，现在提升到一定高度来解决很有必要。”

随着相关规定落地，更严格的监管措施势必会对众多APP运营商产生影响。相对来说，很多大型互联网企业因为在用户隐私保护方面投入较早、公众监督更多，受到冲击较小。一些中小型APP运营商则在个人信息保护方面问题较为突出。这意味着，相关以算法推荐为主要机制的APP，对接入的第三方应用监管不力不到位的平台，存在强制授权、过度索权、超范围收集个人信息的APP运营商将面临整改命运，严重违规的将被清理出市场。

北京亿达(上海)律师事务所律师董毅智对记者表示，多年来，用户基于对APP服务的信任而建立起的黏性，如今却成为某些APP进行差别定价、数据反复买卖的“底气”，这亟须警惕。同时，这些发布的规定也对同行业、跨行业之间企业联手利用用户个人信息划出了“红线”。

对此，相关政府部门将建立APP个人信息安全认证制度，由具备资质的认证机构依据国家标准对APP收集、存储、处理、使用个人信息等行为进行评价，对符合要求的产品颁发证书和标识；同时鼓励搜索引擎和应用商店优先推荐认证APP。

相关监管是否会束缚技术创新呢？姜奇平认为，这个问题需要具体分析。他说，对APP的治理涉及市场治理、社会治理、政府监管等多个层次，是一个综合问题。在市场配置资源失灵、行业自律不佳等情形下，完善相关法律法规、开展专项整治就极为必要。

“当然，如何平衡好保护与开发利用的关系，这是衡量互联网相关立法和监管质量的重要标准。比较好的做法是既不影响企业技术创新，又能够制止相关歪门邪道行为。这需要各方汇集足够智慧、形成治理合力。”姜奇平说。 (彭训文)