

搜集个人隐私方式日益隐蔽 使用手机 App 留心躲避隐私陷阱



今年8月的最后一天,一款名叫ZAO的AI换脸手机App火了,用户只要把照片上传到这款App上,就可以和一众明星换脸。“逆天”的功能并非ZAO火的全部理由,涉嫌违法的指责让这款App开始刷屏。

使用ZAO的用户协议上提出“同意授予ZAO及其关联公司以及ZAO用户全球范围内完全免费、不可撤销、永久、可转授权和可再许可的权利”,这意味着包括肖像在内的个人信息被霸道地收集,并且可能被其他企业使用。

9月3日,针对曝光的“ZAO”App用户隐私协议不规范,存在数据泄露风险等网络安全问题,工业和信息化部网络安全管理局对北京陌陌科技有限公司相关负责人进行了问询约谈。

听来虽然令人震惊,但ZAO绝非首个收集个人信息的App。记者梳理发现,近年来,手机App对个人隐私的搜集日益严重,虽然几经曝光,但相关企业的态度却暧昧不清。ZAO的意外走红,从一个侧面再次暴露出我国公民个人信息保护的短板和难题,在相关立法出台之前,公众使用手机App前一定要留心躲避其中的个人隐私陷阱。

□据《法制日报》

过度采集个人信息趋势普遍

消费记录被购物App分析,出行住宿被旅行App掌握,行车线路也被导航App知道得一清二楚……在互联网大数据面前,普通用户几乎是“裸体”的,而一旦这些数据被泄露,后果不堪设想。更为严重的是,一些手机App从一开始的信息采集就是过度的。

2018年8月29日,中国消费者协会发布《App个人信息泄露情况调查报告》称,手机App需要获取的权限种类繁多,过度采集个人信息呈现普遍趋势。

2018年11月28日,《100款App个人信息收集与隐私政策测评报告》由中消协对10类共100款App进行综合评测后发布。报告显示,100款App中,超过九成App列出的权限存在涉嫌越界,即存在过度收集用户个人信息的问题。

被测评的10类App为通讯社交、影音播放、网上购物、交易支付、出行导航、金融理财、旅游住宿、新闻阅读、邮箱网盘和拍摄美化,基本囊括了公众日常使用App的全部类型。“位置信息”“通讯录信息”“手机号码”是过度收集或使用个人信息最常见的内

容,除此之外,用户的个人照片、个人财产信息、生物识别信息、工作信息、交易账号信息、交易记录、上网浏览记录等,均存在被过度使用或收集的现象。

今年初,中央网信办、工业和信息化部、公安部、市场监管总局对外发布《关于开展App违法违规收集使用个人信息专项治理的公告》,中消协、中国互联网协会等部门联合成立App专项治理工作组,对用户数量大、与民众生活密切相关的App的隐私政策和个人信息收集使用情况进行评估。

然而,在专项治理的凌厉攻势下,App过度采集个人信息的问题并未得到遏制。

今年央视3·15晚会介绍了个人隐私信息通过手机App泄露的案例。主持人现场使用一款名为“社保掌上通”的App查询个人社保信息,一旁的网络安全专家通过抓取分析数据包发现,用户的信息在查询时已被发送至一家大数据公司的服务器。

7月16日,上述App专项治理工作组发布通知,称有40款App在个人信息收集方面存在问题,且未公开有效联系方式。工作组敦促这40款App的运营者30日内完成整改,并向工作组提交整改报告。这份通知显示,WiFi万能钥匙、同花顺、墨迹天气、安居客、糗事百科、起点读书等常见的App,都在需要整改的名单之中。

搜集个人隐私方式日益隐蔽

2018年,某品牌新上市手机配备了升降式前置摄像头,在需要调用的时候,这个摄像头会自动从手机内升起。不过,一些用户发现在使用某些浏览器等不需要调用前置摄像头的App时,摄像头还是会自动升起,而这意味着用户的隐私可能遭到泄露。

由此,不少网友表示,暴露个人隐私的不会只有一个前置摄像头,事实上,手机麦克风、GPS定位、指纹收集器、联网数据、语音通话等都可能记录着用户的数据,一些App则将这些数据予以收集。

今年3月,有媒体报道称,某些App涉嫌“偷听”用户信息。随后这些运营企业均作出解释性答复。但事实上,App搜集个人隐私的方式并不局限于“偷看”“偷听”。

据了解,一般来说,App的安装和使用只能对一些必要的权限征求使用人的同意。在使用安卓系统的手机中,有以下几个权限最常被调取,其一是“读取已

安装应用列表”,借此可以了解和析用户的使用习惯;其二是“读取本机识别码”,主要用来确定用户的身份;其三是“读取位置信息”,通过获取位置,搜集用户的活动范围,例如导航类软件就必须调取这一权限。

然而,在现实生活中,许多App普遍存在越界索权现象,比如视频软件要求读取运动数据、资讯类App要求开启相机和麦

克风录音权限等,“为了给您提供更好的服务,我们请求获取这些权限……”则成为要求获取相关权限的普遍话术。

手机App使用权限被滥用、隐私条款内容不达标有可能造成用户隐私泄露,进而引发个人信息非法买卖、电信网络诈骗等互联网安全事件。

强化权限管理防范隐私泄露

总的来说,解决手机App过度收集个人信息的问题,需要立法者和执法者共同寻求符合互联网发展规律的破解之道,同时也需要App开发管理者规范行为、明示隐私条款,各应用商店也要认真履行平台审核责任。

2012年《全国人民代表大会常务委员会关于加强网络信息保护的决议》提出,“国家保护能够识别公民个人身份和涉及公民个人隐私的电子数据”“网络服务提供者和其他企业事业单位及其工作人员对在业务活动中收集的公民个人电子信息必须严格保密,不得泄露、篡改、毁损,不得出售或者非法向他人提供”。

网络安全法规定,网络运营者不得违反法律、行政法规的规定和双方的约定收集、使用个人信息,并应当依照法律、行政法规的规定和与用户的约定,处理其保存的个人信息。

目前,刑法、民法总则、消费者权益保护法、网络安全法、电子商务法等,都涉及个人信息保护。但虽有相关法律规定,互联网企业对公民个人信息的收集并未得到规范。加强个人隐私保护、对个人信息保护专门立法成为近年来的普遍呼声。今年两会期间,官方通报,全国人大常委会已将制定个人信息保护法列入本届立法规划,相关部门正在抓紧研究和起草,争取早日出台。

不过,在目前阶段,普通手机用户能做的就是尽量提高警惕,防范隐私泄露。业内人士提醒,用户尽量选择知名App商店下载应用软件;在安装和使用手机App时,注意阅读应用权限和用户协议或隐私政策,查看其中是否有隐私“陷阱”;下载后对App做权限管理,一般情况下,关闭App“资费相关”和“隐私相关”的大部分权限并不影响App正常使用(某些App需“定位”功能的除外)。

一些手机具有权限推荐功能,根据App的功能属性,推荐用户开启或关闭权限。安卓系统用户可以通过手机设置中的“权限管理”,iOS系统用户可以通过“隐私”,看到自己下载的App软件都有哪些权限,权限中哪些是开启状态,不相关的、涉及隐私的手动关闭。推荐定期筛选一遍,把所有不影响正常使用的授权全部关闭,避免“流氓软件”在不知情的情况下收集个人信息。

值得注意的是,在平时使用手机App时不要随意登录未知WiFi,随意刷二维码。此外,即便是无意将App某个权限关闭,也不要担心,比如提示无法进行视频聊天等,使用时打开相关权限即可。

全国联网电脑体育彩票“排列3”开奖公告
第2019244期中奖号码:090
全国联网电脑体育彩票“排列5”开奖公告
第2019244期中奖号码:09014
中国福利彩票“双色球”开奖公告
第2019105期中奖号码:
红色球号码:02.13.15.17.26.33
蓝色球号码:01

中国福利彩票3D玩法
第2019244期 中奖号码:575
全国联网电脑体育彩票“七星彩”
第19105期开奖公告
本期开奖结果:2393340
中国福利彩票15选5玩法开奖公告
第2019244期
中奖号码:02.06.12.13.15

拍卖公告

受委托,我公司将公开拍卖一批书画艺术品,本场拍卖会作品丰富,欢迎社会各界人士咨询与竞买。
联系电话:0551-63518705
预展时间:2019年9月16日-9月17日 09:00-18:00
拍卖时间:2019年9月18日(星期三) 09:00-18:00
预展/拍卖地点:合肥伯爵假日酒店
合肥政务区金寨路与南二环路交口
合肥嘉胜拍卖有限公司
2019年9月9日