2021.7.13 星期二
编辑 唐 舸 王念平
新闻晨报

当个人信息在暗中“裸奔” 你的手机App可能比你本人更“懂你”

“滴滴企业版”等25款App日前被下架　大数据时代如何有效提升个人信息安全？

专家建言：国家监管、企业重视和个人防范需同时发力

晨报记者 何雅君

刚和朋友说想买件衬衣，购物App就推荐了多个品牌的衬衣，仔细一看，款式和颜色还都是你常穿的。想在手机上刷个剧，打开视频App，推送的剧目都是你喜欢的类型……大数据时代，看似没有感情的手机App，却可能比你本人更了解你，原因就是各种App暗中进行的个人信息搜集。商家在未经用户允许的情况下搜集个人信息，不仅侵犯个人隐私，甚至会威胁人身安全。

7月9日，国家网信办依据《网络安全法》相关规定，通知应用商店下架“滴滴企业版”等25款App，要求相关运营者整改违法违规收集使用个人信息问题。此前，网络安全审查办公室发布公告，对“运满满”“货车帮”“BOSS直聘”启动网络安全审查。为了确保关键信息基础设施供应链安全，维护国家安全，国家互联网信息办公室会同有关部门修订了《网络安全审查办法》，正在面向社会公开征求意见。

中国信息安全技能竞赛专家委员会专家杨蔚认为，数据集中化和权限集中化的背后，对数据安全的管理与保护提出了更高的要求，也是行业新的挑战。“App在合理合法的原则下来收集个人信息是有必要的，数据流动起来才有价值。限制数据采集无法保护数据安全，正确使用和妥善保护其实更加重要。这就需要国家的监管审查、企业的重视执行和个人的防范同时发力。”

App的悄然采集，让个人信息在暗中“裸奔”

打开招聘软件，填写简历上传，包括出生年月、身份证号、地址、学历、工作经历等个人关键信息就会留存在软件的后台系统中。使用打车软件下单叫车，App会定位你所在的位置，记录你每一次的出行轨迹和起点终点。各种App的出现，为大数据时代的生活带来了诸多便捷。然而，隐藏在背后的采集个人信息行为却让网民信息存在“裸奔”风险。

杨蔚，中国信息安全技能竞赛专家委员会专家，他的另外一个身份是北京众安天下科技有限公司CEO。他曾对个人信息安全做过专门的研究。他告诉记者，目前，市面上的多数App都有不同程度地采集个人信息的行为。比如，App在实名认证过程中采集了用户的身份信息、银行卡信息，如果App运营商对相关信息未做处理就进行存储，就会导致大量个人信息泄露。“多数APP为了确认用户存活数，都会采用短信验证的方式来确定是否为唯一注册。如果App服务商对用户的手机号处理不当，就会导致用户手机号码泄露。此外，App运营厂商为了存活量，几乎每一款App都会收集用户IMEI、设备ID等信息，这也属于个人信息采集的一种。”杨蔚说。

还有一些App会打着安全的旗号，通过购物支付、手机解锁、刷脸开门等渠道，采集用户的人脸识别信息。杨蔚介绍，人脸信息是用户的弱隐私特征，存在唯一性。然而，人脸识别应用五花八门，也没有统一的行业标准，大量的人脸数据都被存储在各应用运营方或是技术提供方的中心化数据库中。数据是否脱敏、安全是否到位、哪些用于算法训练、哪些会被合作方分享，外界一概不知。

不久前，“人脸识别时一定要穿衣服，摄像头拍到的可能不止是脸……”话题以1.7亿的阅读量跃上热搜，将网友带进了大型“社死现场”。从事后台审核的工作人员在进行人脸识别审核时，经常会看到很多人在洗澡、和另一半拥抱、没穿衣服等各种“奇奇怪怪”的场景。

部分网友质疑平台方未能提醒用户“人脸识别系统后台人工审核时，可以看到摄像头全景”。专家分析，从技术角度来说，人脸识别的图像被其他人看到的可能性是客观存在的。而一旦服务器被入侵，高度敏感的人脸数据就会面临泄露风险。

有买有卖，泄露的数据一步步汇入黑色产业链

个人信息的直接泄露，会造成什么样的后果？对于泄露的数据如何一步步汇入黑色产业链，杨蔚进行了解释：“这些信息非常有价值，有人买就有人卖。既然下游有人愿意花钱，那自然就会有黑客去攻击这些目标。黑客非法获取这些信息，拿到数据以后，就会有人接手。这里面还有大量二道贩子的存在，在中间赚差价。”

杨蔚说，这个链条上的人分工特别明确，而且都是“专业”级别的团队操作。“有些人会专门去联系相关的培训机构或诈骗团伙，从而把手上的数据卖到下游。而下游这些团队，有专人负责诈骗的话术编写培训、线上通过第三方支付平台洗钱、线下ATM机提款等，分工非常明确。大量诈骗案件由此产生。”

而被App收集到的用户IMEI、设备ID等信息一经泄露，设备造假会变得更加容易。大多数App都会索要存储权限，一旦存储权限给予App后，App就可以任意读写甚至删除存储卡中的内容。

这意味着App服务商能够对用户手机端上的数据采集、应用管理等拥有了更高的权限，一旦相关服务商存在重大漏洞，有可能被恶意攻击者获取海量信息，后果不堪设想。同时，也对App服务商的数据管理提出了更高的要求。很多数据泄露事件的根源不仅仅来自黑客攻击，内鬼窃取数据的事件甚至高于黑客攻击。

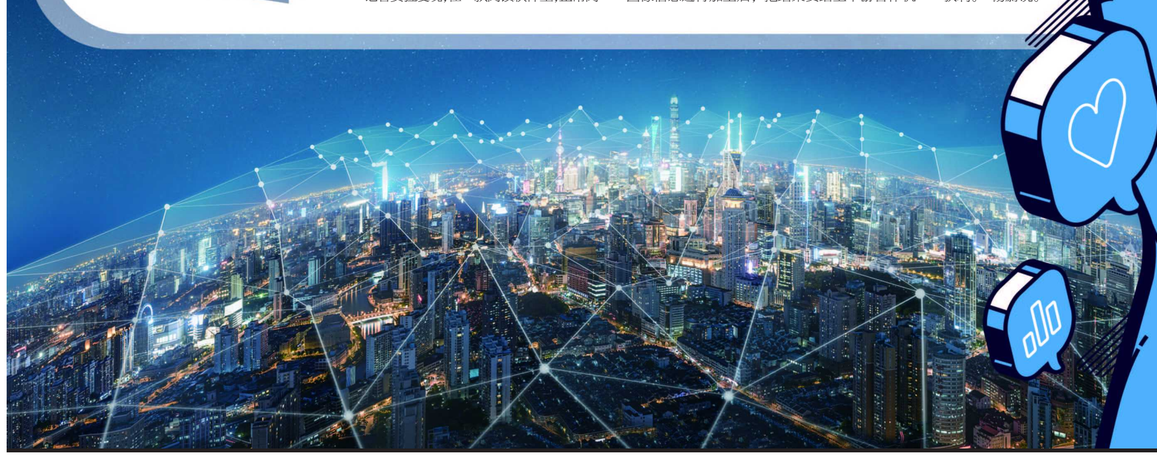
给用户画像，打上标签后推送低劣广告

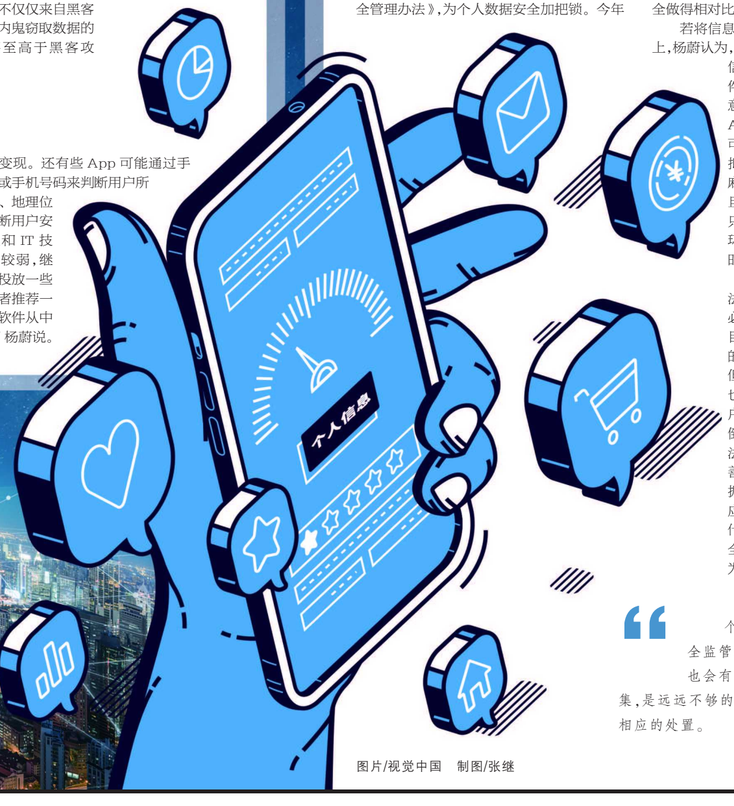
老人通过智能手机看新闻、小说时，手机屏幕总会自动蹦出一些“安全提示”：“病毒”“垃圾”“内存严重不足”。信以为真的老人往往会按照提示清理手机，但“安全提示”越清理越多，手机越用越慢。

今年的央视“3·15”晚会调查揭露，老人手机上的清理类软件，藏着这样的安全陷阱。杨蔚分析，这是另一种相对隐蔽的、通过信息泄露来获取利益的方式——广告诱导。

记者实验发现，在一款阅读软件里，正常阅读过程中出现了“安全清理”提示，点击后，一款名叫“智能清理大师”的App自动下载成功，但清理过程中仍会跳出“清理手机缓存”提醒，点击后，手机又下载安装了另一款清理软件。在不断地“提醒、下载、清理”过程中，更多App被自动安装。

杨蔚分析，这些App表面上是在清理手机垃圾，背地里则在大量获取手机数据信息，对使用者进行用户画像，打上标签，再将各种低劣广告源源不断地推送给用户。“也有一些App在对用户画像信息进行加工后，把结果卖给上下游合作机构进行变现。还有些App可能通过手机定位或手机号码来判断用户所在区域、地理位置，推断用户安全意识和IT技能相对较弱，继而精准投放一些广告或者推荐一些流氓软件从中获利。”杨蔚说。





图片/视觉中国　制图/张继

国家层面监管外，企业也须提高保护用户信息意识

App信息安全问题层出不穷，影响到的不仅仅是个人。碎片化的信息一旦聚合起来，通过大量算法进一步加工，能得出很多影响决策的结论，甚至会影响到国家安全。

针对个人信息泄露问题，工信部开展了纵深推进App侵害用户权益专项整治行动，先后多次向社会通报和下架了多款侵害用户权益行为App。而在今年315国际消费者权益日主题活动上，工信部表示，将继续开展App问题治理，进一步强化消费者个人信息保护。

“这两年，国家网信办、公安部、工信部都在针对App开展专项检查、抽查，力度很大。”杨蔚说。

在法律层面，有关数据安全的要求也越来越多。此前，国家网信办已经发布了《数据安全管理办法》，为个人数据安全加把锁。今年6月，第十三届全国人民代表大会常务委员会第二十九次会议通过了《中华人民共和国数据安全法》，将于今年9月1日正式实施。

除了国家层面的监管，企业也必须要提高保护用户信息的意识。在数字经济时代，做好个人信息保护是企业应当坚守的基本底线，也是企业长久健康发展的基础支撑。

但在信息安全的道路上，企业自身也面临着一些难题。杨蔚分析，当App所属企业的规模还未壮大时，企业对于信息安全、产品规范、数据收集和保护的投入能力都很有限，于是导致了更多的安全隐患和问题。有些企业并非主动向外泄露用户信息，而是产品本身不完善，给犯罪团伙提供了可乘之机。“这种情况在中小企业中尤为明显，头部企业的信息安全做得相对比较好。”杨蔚说。

若将信息安全的把关责任都归在用户身上，杨蔚认为，这也不合理。“企业将上传个人信息设置为使用产品的前置条件，用户若要使用App，必须同意上传这些信息。虽然国家要求App在注册阶段告知采集信息可能带来的风险，但App官方拟定的条款非常专业，且密密麻麻，绝大多数用户没有耐心看完，且也未必有能力看懂这些条款，只能直接点选‘同意’。这样的大环境，使得用户在保护个人信息时十分被动。”

“个人认为，App在合理合法的原则下来收集个人信息是有必要的，数据流动起来才有价值。目前，我们国家的数据安全监管的重心放在数据合法采集上面。但实际上，数据即使被合法采集，也不代表它是安全的。即便是用户同意采集，数据也会有可能被倒卖、被滥用。限制数据采集无法保护数据安全，正确使用和妥善保护其实更加重要。只考虑数据的合法采集，是远远不够的。应该考虑的是，采集后的数据用什么样的方法和机制来保护其安全，并且及时发现危害安全的行为，进行相应的处置。”杨蔚说。

个人信息保护·监管建议

对违法行为加大处罚力度，强化威慑作用

为了有效提升公民个人信息保护水平，杨蔚建议，国家应加速推进个人信息保护法律的制定，强化政府相关部门对个人信息安全的监管，加大公安机关对涉公民个人信息违法犯罪的打击力度，强化互联网企业的行业监督、行业自律，不断增强公民个人信息保护意识。

首先，监管部门应持续性加强对个人信息采集的监管力度。数据安全监管机构定期对各行业领域涉及的企业机构开展监督执法，督促企业落实法律数据安全合规性评估要求。在个人数据保护方面，监管机构对标数据保护法，对企业违反合规性评估要求的行为进行执法处罚。企业应该基于法律法规和相关标准要求，积极开展数据安全自评。

目前，新出台的《数据安全法》已经确立了数据分类分级管理、数据安全审查、数据安全风险评估、监测预警和应急处置等基本制度，为国家数据安全保护提供了有力的法律保障，并指明数据安全保护的方向。不过，数据安全保护和个人信息保护的法定义务以及具体制度执行还需要监管机构来保障落实。因此，对于数据安全保护不仅要建立事前预防、事中监督和事后处理的监管制度，还需要综合运用抽查审计、事件通报、行政处罚和刑事制裁等监管手段，加大对违法行为的处罚力度，强化处罚的威慑作用。

个人信息保护·防范建议

拒绝App“霸王条款” 举报不符要求的数据采集

国家能做的，是监管、审查和对个人信息保护的推动，但最终还是要落实到企业自身的重视和执行当中。

杨蔚认为，企业端应承担保护用户信息的责任，减少对用户信息的采集，加强自身的网络安全建设，借助专业的安全机构、民间安全力量对企业系统网络环境进行评估，建议采取安全众测、渗透测试的方式来对系统进行全面的安全检查等。

一方面，企业自身要对自身产品及业务进行评估；另外一方面是要寻求专业机构和安全力量的帮助，协助完善产品安全能力，保障用户数据隐私安全。他建议：“针对当前的数据安全的形势，应该以数据为中心、以组织为单位、以能力成熟度为抓手，来开展数据安全治理。其目的不只是为了合规，更是为控制风险、提升能力。只有这样，才能更好地适应变化，真正保护好数据安全。”

对于用户，杨蔚也给出了防范个人信息被过度采集的建议。比如：尽量从正规渠道下载手机App。关闭手机App的隐私使用权限，为不同类型的手机App设置不同的账号密码。在外不要随意连接免费无线网络，晚上睡觉关闭网络通讯。临时使用的权限用完尽量关闭。

如遇App设置“不开启权限不能用”的霸王条款，可以先去“违法和不良信息举报中心”举报，然后适当更换同类App。长时间不用的App尽量卸载，防止被其他App调用，从而导致敏感信息泄露。“总之，个人用户要学会说‘不’，遇到不符合要求或者严重采集数据的情况应及时举报。”

> “个人认为，App在合理合法的原则下来收集个人信息是有必要的，数据流动起来才有价值。目前，我们国家的数据安全监管的重心放在数据合法采集上面。但实际上，数据即使被合法采集，也不代表它是安全的。即便是用户同意采集，数据也会有可能被倒卖、被滥用。限制数据采集无法保护数据安全，正确使用和妥善保护其实更加重要。只考虑数据的合法采集，是远远不够的。应该考虑的是，采集后的数据用什么样的方法和机制来保护其安全，并且及时发现危害安全的行为，进行相应的处置。”
>
> ——中国信息安全技能竞赛专家委员会专家 杨蔚