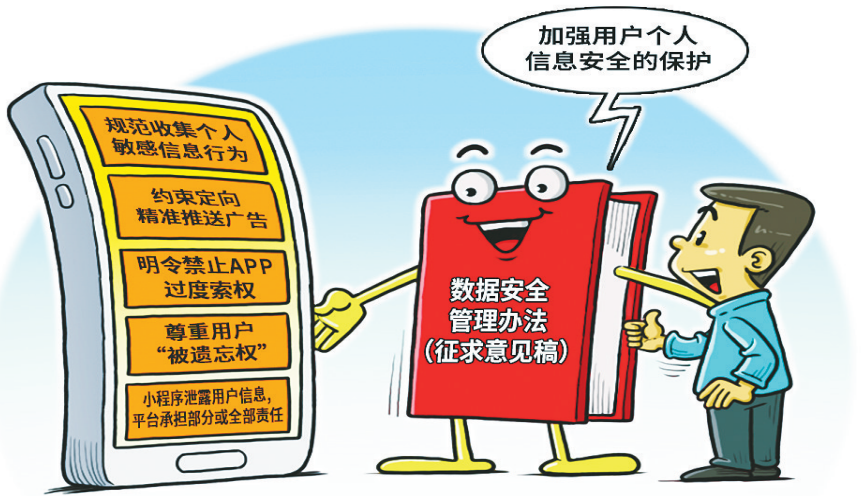
《数据安全管理办法(征求意见稿)》发布

向过度索权的手机APP开刀

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）》，对公众关注的个人敏感信息收集方式、广告精准推送、APP过度索权、账户注销难等问题进行了直接回应。



1 如何规范收集个人敏感信息行为？　网络运营者需向网信部门备案

在社交平台上做个心理测试需要提交手机号，线上办个会员卡要提供姓名和身份证号……个人敏感信息越来越多地被不同渠道广泛收集。如何规范这种收集行为，防止信息被泄露、滥用？

办法第十五条规定：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。备案内容包括收集使用规则，收集使用的目的、规模、方式、范围、类型、期限等，不包括数据内容本身。

根据国家标准化管理委员会等部门去年实施的《信息安全技术个人信息安全规范》，不仅身份证信息和电话号码属于个人敏感信息，个人指纹、声纹等生物识别信息，邮箱地址、网页浏览记录、精准定位信息都属于个人敏感信息范畴。

业内人士认为，从“不知道谁掌握敏感信息”到“收集前需要备案”，备案制无论从数据安全还是用户隐私保护来看，都是一种进步。中国信息安全研究院副院长左晓栋表示，这样可以对收集者追根溯源，从源头保护个人信息安全。

2 如何约束定向精准推送广告？　标识需清晰且用户可拒绝

刚用APP叫外卖，就在浏览资讯APP时收到相关广告，这样的精准广告让不少人觉得惊心。这种利用用户浏览痕迹进行精准画像，通过定向推送获得广告收入的方式，在办法中规定了约束性条款。

办法第二十三条规定：网络运营者利用用户数据和算法推送新闻信息、商业广告等，应当以明显方式标明“定推”字样，为用户提供停止接收定向推送信息的功能；用户选择停止接收定向推送信息时，应当停止推送，并删除已经收集的设备识别码等用户数据和个人信息。

中华全国律师协会网络与高新技术专业委员会副主任兼秘书长陈际红表示，定向推送技术在带来便利之外，产生了大数据歧视等问题。办法明确要求互联网平台充分尊重用户的选择权，可以让用户免受太多广告骚扰；要求平台需将此前收集的用户设备识别码和个人信息等内容删除，表明了对保护用户信息的重视。

3 如何应对APP强迫授权或默认勾选？　明令禁止

不给“一揽子授权”就不让用APP，或者在某个不起眼的选项前设置“默认勾选”……这些行为都将被明令禁止。

办法第十一条规定：网络运营者不得以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，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。

个人信息主体同意收集保证网络产品核心业务功能运行的个人信息后，网络运营者应当向个人信息主体提供核心业务功能服务，不得因个人信息主体拒绝或者撤销同意收集上述信息以外的其他信息，而拒绝提供核心业务功能服务。

中国社会科学院信息化研究中心秘书长姜奇平认为，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。

4 注销账号和删除个人信息难怎么办？　尊重用户“被遗忘权”

不少网民反映，想注销APP账号不容易，并且之前登记的个人信息难以消除。

办法第八条规定：收集使用规则应突出个人信息主体撤销同意，以及查询、更正、删除个人信息的途径和方法。

第二十一条规定：网络运营者收到有关个人信息查询、更正、删除以及用户注销账号请求时，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。

“突出‘被遗忘权’保护也是办法的一个亮点。”中国信息安全研究院副院长左晓栋说，以网购为例，消费者在购物网站完成交易后删除相关信息，这样的合理诉求理应得到满足。

5 小程序泄露用户信息怎么办？　平台承担部分或全部责任

目前，一些社交类和支付类APP大量接入第三方小程序服务，这些小程序经常向用户收集个人信息。如果用户个人信息被泄露，平台是否可以免责？

对此，办法明确规定，不可以！

根据办法第三十条规定：网络运营者对接入其平台的第三方应用，应明确数据安全要求和责任，督促监督第三方应用运营者加强数据安全管理。第三方应用发生数据安全事件对用户造成损失的，网络运营者应当承担部分或全部责任，除非网络运营者能够证明无过错。

左晓栋表示，办法规定了平台与第三方应用需要共同承担相关责任，这样可以倒逼网络经营者，加强对用户个人信息安全的保护。

据新华社

相关链接

8亿用户的APP被曝超范围收集用户信息

号称可“一键连接WiFi”的APP WiFi万能钥匙已成为不少人的手机必备。公开数据显示，其月活跃用户已经达到8亿。然而，这款“蹭网利器”，近期却被曝光超范围收集用户信息。

广东省公安厅近日公布，2019年一季度，广东警方共监测发现1670余款APP存在超范围收集用户信息行为。其中WiFi万能钥匙、钱聚易等10款APP问题突出，特别是WiFi万能钥匙问题最多，共超范围收集了7类信息。据通报，WiFi万能钥匙(4.3.56版本)存在读取用户短信或彩信、联系人，收集用户设备上已知账号，使用用户设备摄像头或麦克风等问题。

APP超范围收集用户信息现象并不少见。根据爱加密大数据中心提供的数据，截至2019年3月底，该中心已收录安卓应用270多万个，iOS应用190多万个，30%以上的APP存在不同程度的越权、超范围收集等行为。

暨南大学网络空间安全学院院长翁健表示，“获取用户设备上已知账号列表”易泄露用户隐私。攻击者有可能利用掌握的账号，实行撞库等网络攻击，即从安全性较弱的账号中获取的用户名密码，来推测强安全措施的账号和密码。

此外，调用权限发送短信也是手机木马的主要传播方式之一。翁健介绍，应用程序可通过该种方式将带有病毒的链接放入短信中，并依次发送给用户相关联系人，一旦有人点击该链接，则会感染病毒。

延伸阅读

APP可获取权限多达40条

手机APP到底可以索取哪些权限？记者通过查阅某Android论坛发现，Android各类权限接近40个，被列入“危险权限”达24个，包含日历、相机、通讯录、定位、麦克风、传感器、短信、内存等。

值得注意的是：上榜的每个危险权限都属于一个权限组，用户一旦同意授权，那么该权限组中其他权限也将同时被授权。这也就意味着，如果用户通过了“通讯录”授权，那么“通讯录”权限组的其他权限——读取通讯录、写入通讯录、得到账号——都将同时被授权。

DCCI互联网数据研究中心联合腾讯社会研究院发布的《网络隐私安全及网络欺诈行为研究分析报告(2018年)》显示：2018年上半年Android端获取隐私权限的手机APP占比相较于2017年下半年提高1.4%，达到99.9%，几乎所有的Android端手机APP都会获取隐私权限。iOS端获取手机隐私权限的APP比例呈上升趋势，2018年上半年iOS端获取手机隐私权限的APP比例已达到93.8%。在现实中，一部分移动开发者在申请获取手机权限时采用的是“多多益善”原则，甚至个别移动开发者为追求短期利益，存在售卖用户隐私信息的行为，造成大量用户隐私信息泄露。

记者调查发现，通过APP授权获取利益的情况确实存在。一部分通过大数据买卖；还有一部分是直接变现的收入。

“安卓开发者账号”的一位群友向记者透露，“目前市面上最值钱的是贷款数据，可以通过贷超APP获取，一条信息至少五毛以上”。

“安卓开发者账号”的另一位群友则向记者吐槽了自己因为“授权”中招的经历。“下载了某软件以后，短信一直发，各种扣费”。他向记者展示，目前该软件在某用户量最多的Android APP商店上依旧可以下载，下载量已逾千。