新闻热线：010—58884062
E-mail：adaxuqian@126.com
■责编 许 茜
科技日报 2018年1月24日 星期三

数据时代，别忘捂紧“信息钱袋”

行业观察

崔 爽

从日常购物到休闲娱乐，如今使用智能手机的我们会留下许多“数据脚印”。一方面，这给我们带来了便利，算法根据大数据推荐的新闻、歌单越来越对胃口。另一方面，暴露在外的“脚印”也增加了隐私泄露的风险。

近日，腾讯社会研究中心与DCCI互联网数据中心联合发布了《2017年度网络隐私安全及网络欺诈行为分析报告》，该报告对1129款手机应用获取用户隐私权限的情况进行了统计。上述报告显示，在852款安卓应用中，有98.5%都获取了用户隐私权限，iOS用户中的这一比例高达81.9%。而获取权限的途径既有用户主动授权同意的，也不乏如前段时间支付宝年度账单一般使用“套路”得到的。

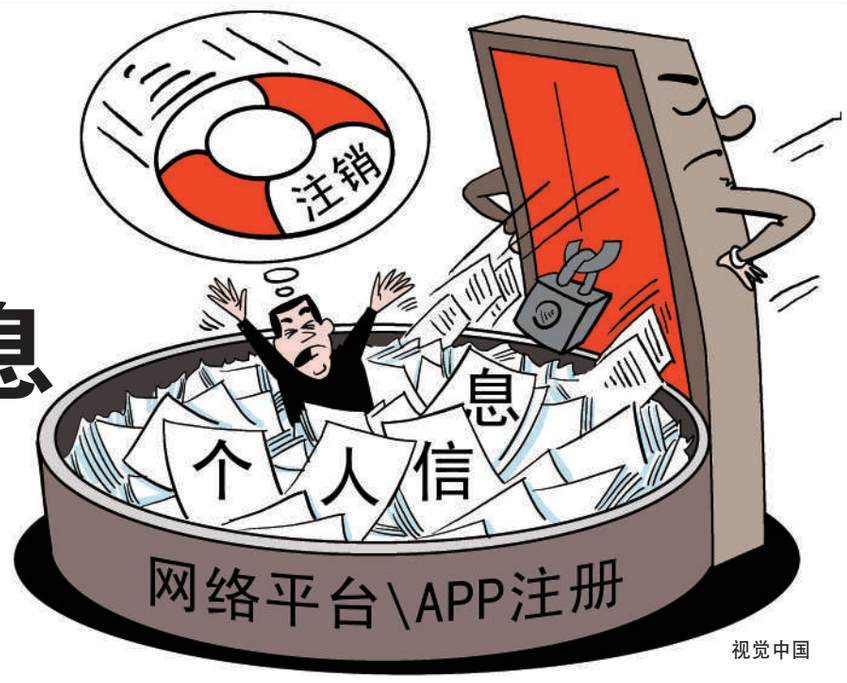
如今，数据已成为“无形财产”，越来越多的人意识到它的商业价值。按照相关要求，网络运营者收集使用个人信息必须遵守合法、正当、必要三项原则，但现实是他们的手纷纷伸入用户的“信息钱袋”，却没有清楚交代这么干的理由。

比如，前几天被工信部信息通信管理局约谈的百度、支付宝、今日头条三家，都是因为对用户个人信息的使用规则、使用目的告知不充分，名不正言不顺地就把超出服务所需、甚至与服务无关的数据打包拿走了。

在公民个人信息法律保护方面，现阶段并非无法可依。依据《网络安全法》第40至43条的规定，用户知情同意是基本要求，网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。此外，对于违反法律法规或双方约定的网络运营者，用户有权要求其删除或更正。

好消息是，监管也在发力。刚刚公布的国家推荐标准《个人信息安全规范》将于2018年5月1日正式施行。该规范指出个人信息只能归用户本人所有，企业使用时可以考虑引入利益分配机制，这将进一步为企业收集、使用数据提供行为参照。

删得掉的APP 删不掉的注册信息



视觉中国

本报记者 付丽丽

小王这几天有点烦。他想注销掉一款APP，却发现怎么也注销不掉。“账户信息被永久保存在这个APP里，很担心个人隐私会被泄露出去。”小王说。

像小王这样的人不在少数。生活中，各种各样的APP在给人们带来便利的同时，也平添了不少烦恼。这些删不掉的信息是否会造成安全隐患？

注销账户不等于用户信息被清除

“用户因生活、工作等日常需要，会注册很多手机APP账户。但在注销账户时，时常会碰到难题，‘进门容易出门难’的问题一直没有解决。”1月21日，北京理工大学软件安全研究所副所长闫怀志在接受科技日报记者采访时说。

用户注销APP难，究其原因，闫怀志分析，出于留住用户目的，平台可能不愿提供注销选项。有的APP平台虽然提供注销选项，但注销流程繁复。比如，注销有些APP，需要在特定时间段内没有修改绑定、更换密码以及敏感操作等。

其次，有的APP平台出于安全考虑（如淘宝APP），设置了较为苛刻的注销条件，注销门槛很高。只有在确认注销操作为用户的真实意愿且不会产生安全问题和商业纠纷时，平台才允许用户注销。

闫怀志表示，用户注销APP后，平台有可能会留存两类信息：一是用户注册信息，如用户名、密码、身份证号、手机号、邮箱等基本信息；二是用户的历史操作信息。比如，用户的访问信息、消费信息及支付信息等。

“需要指出的是，即便用户成功注销了APP账户，也只是从用户侧实现了信息的‘伪消除’。如果想彻底消除这些信息，还要依靠APP平台自身。”闫怀志强调。

用户信息多存于后台数据库

既然很难彻底清除，那这些信息又会被保存在哪儿？

对此，闫怀志介绍，用户的注册信息和历史操作信息大多会被保存在APP后台数据库。具体而言，信息既可能被保存在平台运营商自己的数据中心或私有云中，也可能被保存在公有云中。此外，平台还可能将这些信息进行备份。

“与传统数据中心的存储方式不同，APP平台使用的云存储涉及到网络设备、存储设备、计算设备、接口设备等诸多软硬件系统，其核心是存储设备。”闫怀志说，通常用户资料被保存在云存储设备，管理这一设备的是云服务提供商。负责云存储安全的不仅有云服务提供商，还有租用云存储服务的APP平台运营商。

当前，云计算服务一般有三种模式，即SaaS、PaaS和IaaS。SaaS（Software as a service）意为软件即服务，PaaS（Platform as a Service）意为平台即服务，IaaS（Infrastructure as a Service）意为基础设施即服务。

“在上述三种服务模式中，云服务提供商和APP平台运营商对云计算资源的控制范围是不同的。”闫怀志说，这就决定了双方承担的责任是不同的，云服务商因完全控制云计算的设施层（物理环境）、硬件层（物理设备）和控制层，因而应对此承担完全的安全责任。应用软件层、软件平台层、虚拟化计算资源层的安全责任则由云服务提供商和APP平台运营商共同承担。

信息清除不复杂 关键看APP运营商

“客观来讲，由于云平台的重要性，云服务提供商一般会在虚拟化安全、数据安全、应用安全以及管理安全等方面采取措施，以此保障云存储的系统安全性。”闫怀志说。

闫怀志认为，云平台数据存储的安全保护工作是一项系统工程，它涉及云计算系统物理和环境安全、网络和通信安全、设备和计算安全及应用和数据安全。我国即将出台《网络安全等级保护2.0标准》，该标准对云计算安全提出了扩展要求。APP平台运营商如果租用云存储设备存储数据，也要按照相关要求承担相应的安全责任。

其实，在账户被注销后，想要删除存储在APP平台的注册信息和历史操作信息，这一操作在技术上实现起来并不复杂。

“但问题在于，APP平台运营商有无动力和意愿去删除这些信息。对于普通用户来说，几乎没有渠道和能力来控制。因此，必须依靠法律法规和制度，从政府监管层面来解决账户注销和信息清除问题。”闫怀志说。

的确，工信部赛迪网络安全研究所所长刘权曾表示，国内90%的安卓手机安装的APP都存在漏洞。

数据保护应有规可依、有规必依

在我国，公民个人信息泄露已成顽疾。业界普遍认为，我国尚未施行针对数据保护的综合性立法，而且现有涉及数据保护的法律法规和标准的操作性不强。与国际先进水平相比，尚存在一定的差距，尤其是在体系化、覆盖面、深度与有效性方面差距更为明显。

在闫怀志看来，想要切实保障数据安全，就必须构建起完善的安全保障体系。而安全保障体系的建立，离不开信息安全法规和标准的支持。因此，在数据保护领域，法律法规和标准至关重要。有关数据保护的法律法规问题涉及面很广，它涉及到信息安全犯罪和信息隐私等问题，需要从立法、司法等层面，逐步建立并完善针对上述问题的防控措施，以保障网络空间的数据安全。

“从数据保护的实践上来说，一要加快推进相关法律、法规及标准的出台，做到有规可依、有规必依。”闫怀志说。

好在这种局面正在发生改变。1月12日，工信部就个人信息保护问题约谈百度、支付宝及今日头条三家企业，要求其本着充分保障用户知情权和选择权的原则立即进行整改，不得收集服务所必需以外的用户个人信息，不得将信息用于提供服务之外的目的，不得非法向他人出售或提供个人信息等。

闫怀志表示，在数据保护领域，可借鉴欧盟将于2018年生效的《通用数据保护条例》。同时，要加强合理运用安全技术的能力，化解数据“开放共享”与“隐私保护”这对突出矛盾。此外，要加强相关的监管工作，切实提高用户的安全意识和系统的安全防护水平，做到事前能预防、事发有反制、事后能补救。

隔屏有耳，你正被APP监听

第二看台

本报记者 翟冬冬

近日，据《纽约时报》报道，Google Play商店的250多款游戏APP存在监听用户的行为。这些游戏通过安装特殊的软件来监听用户家中的电视，以分析其观看电视节目的习惯。该软件由一家名为Alphonso的公司开发，目前Alphonso拒绝提供使用该软件的APP名单。

Alphonso声称，这种收集行为已得到用户允许。在安装带有这个软件的游戏时，部分游戏会提示用户，但大多数游戏只在隐私政策中提示相关条款。尽管Alphonso表示，他们只会监听电视等发出的声音，但这种做法还是令人担忧。此外，据称在关闭这些APP后，该软件还能继续收集用户信息。

匹配音频数据

“该软件的内容自动识别系统采用了一种较为成熟的技术。”北京邮电大学网络空间安全学院副教授辛阳向科技日报记者解释，该技术主要是将一段数字音频转化为数字指纹，并将数字指纹与电视节目音频数据库进行匹配。像国外的音乐识别软件Shazam，国内的QQ音乐、酷狗音乐等众多厂商都采用了这种技术。

“Alphonso就采用了Shazam的音频内容识别技术。”辛阳说，Alphonso利用安装在用户手机中的APP收集音频片段，并把这些片段提供给Shazam公司。Shazam利用自身技术进行识别，并将监听到的信息再卖给Alphonso。

辛阳介绍，将音频转化为数字指纹最常用的一种方法就是，对音频进行傅里叶变换之后得到这段录音的频谱，然后通过判断短时能量及短时过零率去噪，同时利用节拍修正、音调校准等方法进行修正，从而获得相对准确的音调序列。最后，利用模糊匹配算法、动态时间规整算法等多种方法匹配音频。

为精准营销提供便利

据Alphonso官网消息，Alphonso搜集用户信息的主要目的在于将信息提供给广告商，从而让广告商实现精准营销。

辛阳说，这些监听到的信息可以描述用户的生活习惯、思维习惯以及喜好，从而绘制用户画像、构建行为特征库，进而实现对用户行为的预测。

“这对大多数企业来说是宝贵的资源。”辛阳说，可以想象，如果能准确预测用户下一步的行为或者喜好，就可以提供针对性的服务。例如，广告商用其进行点对点的营销，产品制造商可以用其来指导下一步生产计划等。因此，该平台的获利方式就是把收集到的用户信息转卖给其他商业公司。

360手机卫士安全专家葛健也表示，部分恶意APP为了获取更大的商业利益，通过分析监听信息定向推送广告，侵犯用户的个人隐私。

葛健认为，如果一旦被监听，用户的隐私、商业机密等信息都有可能被泄露出去。一旦上述信息被获取，不法分子极有可能冒充他人身份对用户实施定向诈骗。

辛阳介绍，目前还没有证据表明Alphonso公司所监听的对象仅限于电视和电影等设备。一旦被监听的用户涉及政府要员、企业高管，那么就有可能造成极为严重的后果。

“这种行为泄露了大量的用户隐私，还造成手机电池损耗等问题。”辛阳说，同时这种行为也违反了我国《移动智能终端应用软件预置和分发管理暂行规定》和《中华人民共和国网络安全法》，对公民信息安全造成严重威胁。

如何防范监听？

“防监听的关键在于管控APP的权限。”辛阳说，目前iOS、安卓等主流移动端操作系统都集成了应用权限管理功能，苹果和谷歌的应用商店都要求APP在访问麦克风时，须征得用户同意。

然而，据记者观察，不少APP在安装时就强制用户同意使用麦克风。

辛阳建议，如果是安装了iOS系统的设备，请打开“设置”，进入“隐私”菜单，然后查看“麦克风”的设置。如果是安装了安卓系统的设备，请打开“应用&通知”，进入“应用权限”，然后点击“麦克风”查看设置情况，关闭APP中不需要的权限。

葛健说，现在高版本的安卓系统已能单独设置每个应用程序的录音权限。从使用便利性的角度考虑，相关研发人员可添加一个可以控制所有麦克风的开关。用户还可安装专业安全软件，定期为手机进行恶意程序查杀，确保手机处于安全环境之中。

在硬件方面，葛健建议，可以设计一些麦克风是否处在工作状态的提示灯，或设置一个硬件开关锁，决定是否让麦克风工作。

IT辣评

点评人：本报记者 王小龙

微信支付落地首个无人快闪店 这是线上到线下的有益尝试

1月20日，微信支付首个无人快闪店正式落地上海万象城（吴中路店）。只需一部手机，顾客就可完成从进店、选购商品到买单的全过程。与市面上很多无人商店的模式类似，顾客需通过微信小程序扫码进店，店内商品都贴有RFID标签，用于识别顾客选购的商品，顾客在选好商品后扫码支付，小程序会自动从顾客的微信支付余额或所绑定的银行卡内扣除货款，支付完成后顾客即可开门离店。

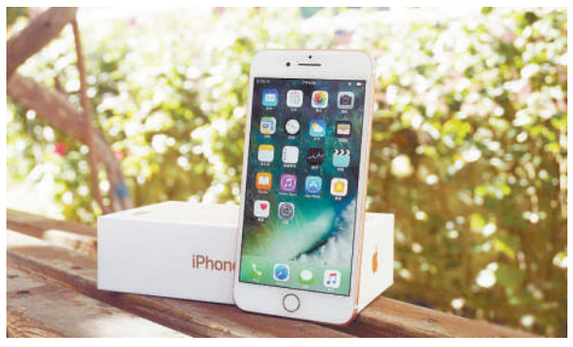
点评：腾讯终于亮出了自己的无人商店解决方案。比起售卖商品，它将多的注意力放在了商圈内多品牌的合作上。在前不久举办的2018微信公开课PRO现场，腾讯高级副总裁张小龙曾表示微信下一步的计划是探索线下生活，而这次的快闪店可能就是微信发展线下的一次尝试，同时也是其智慧零售解决方案的一个样本。在打通消费身份和微信身份之后，腾讯想让每个人都成为有效流量，进而产生商业价值。

深圳交委反对滴滴投放小蓝单车 是问题总得面对

一度停止运营的小蓝单车日前宣布，用户可以通过滴滴APP直接使用小蓝单车，但此举却遭到深圳市交委的明确反对。1月19日，深圳市交委发声明表示，收到滴滴出行违规投放的举报，正在调查；在小蓝单车运维不到位等问题相应处理结果明确前，滴滴不得以小蓝单车的名义在深圳运营和投放。

点评：1月9日，滴滴出行、小蓝单车曾各自发布公告，宣布由滴滴托管小蓝单车。17日，滴滴宣布了它的共享单车平台，将小蓝单车联入滴滴，并首先在北京和深圳上线。这次合作对双方来说真是双赢：滴滴通过合作拿到了小蓝单车的车子、品牌和投放资质，为其进军共享单车行业节约了大量的时间；小蓝单车除了对用户有一个交代外，还能从滴滴那里获得一笔资金。但用户和管理部门真正关心的是押金问题，滴滴给出的解决方案却是——不直接退款，兑换成等额滴滴乘车券。深圳交委的态度无疑让滴滴和小蓝单车的“如意算盘”落了空。

苹果承诺用户可选择关闭“降频” 早知今日何必当初



近一个月以来，苹果手机陷入“降频门”风波。苹果公司通过系统升级造成旧款iPhone性能降低的行为引起消费者的严重不满。日前，上海市消保委已就此事发函问询苹果公司。19日，苹果在回应中表示，将通过新的软件更新保障消费者在电池状况与手机性能调整方面的知情与自主选择权。将在系统更新中加入一个全新的功能，让用户清楚看到电池的健康程度；更新系统后，用户可以自行选择是否要“降频”。

点评：“用户体验”是苹果公司最常提到的一个词，也是苹果公司在设计和产品上为世人所尊重的一个重要原因。但这次偷偷让手机变慢的做法，辣评君无法赞同也没法理解。或许从商业角度上来看苹果的做法没有错，但我的手机我做主，要不要延长续航、要不要降频都应该由消费者自己来决定。与其面对各种质询、诉讼，还不如早早把知情权还给消费者。苹果你真该改改了！

（本版图片除标注外来源于网络）