

从填表到刷脸,谁在过度收集个人信息?

“我在教育机构平台领了份考前复习资料,只注册了账号,推销电话就跟着来了。”江苏苏州的小李至今没想通,自己的个人信息怎么就被“广而告之”了。

每一次“授权”背后,都可能藏着一次信息的“越界”。从填表到刷脸,到底谁拿走了人们的个人信息?新华网记者就此展开调查。



国家计算机病毒应急处理中心检测发现71款违法违规收集使用个人信息的移动应用

根据中央网信办、工业和信息化部、公安部联合发布的《关于开展2026年个人信息保护系列专项行动的公告》，依据《网络安全法》《个人信息保护法》《网络数据安全管理条例》《App违法违规收集使用个人信息行为认定方法》等法律法规和有关规定，经国家计算机病毒应急处理中心检测，71款移动应用存在一项或者多项违法违规收集使用个人信息情况，现通报如下。

1、在App首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；以默认选择同意隐私政策等非明示方式征求用户同意；隐私政策难以访问；个人信息处理者在处理个人信息前，未以显著方式、清晰易懂的语言真实、准确、完整地告知个人处理者的名称或者姓名、联系方式、个人信息的保存期限等。涉及26款移动应用如下：

国家计算机病毒应急处理中心官网截图。

1 谁在收集个人信息

根据《中华人民共和国个人信息保护法》，个人信息是指以电子或其他方式记录的与已识别或可识别的自然人有关的各种信息(匿名化处理后的除外)。简单地说，凡是能“辨认出你”的信息，如姓名、身份证件号码、联系方式、住址、账号密码、财产状况、行踪轨迹等都属于典型的个人信息。然而，这些信息的收集边界正在被不断突破。

近日，国家网络安全通报中心通报，经国家计算机病毒应急处理中心检测，71款移动应用存在违法违规收集使用个人信息的行为。

“因为好奇，点击了某网贷App‘查看额度’，结果就接到了各种借贷的电话。”正在北京读研究生的小李告诉记者，仅一次不经意的操作给他引来了无数推销电话。

对外经济贸易大学数字经济与法律创新研究中心主任许可对此表示，App所谓的强制授权表现为三种形态：不提供信息就不能使用App；一次性要求开启多个无关权限；超范围索取与业务场景无关的个人信息。“这本质上是一种诱导，或是利用技术架构和信息不对称进行的一种设定，是一种‘技术上的强制’。”他认为，即便不构成法律意义上的强制，这类做法至少违背了当事人的自愿原则，“存在一定的违法性”。

线上如此，个人信息在线下同样难以“藏身”。

“该到续保的时候，不同保险公司的电话没完没了。”陕西西安的郑先生面对保险公司的推销电话颇为无奈，“有时一天接到几十个电话，开什么车、现在的险种，他们比我还清楚。”

许可说，不少线下场景的信息收集更是重灾区，保险、中介、培训班、各类会员登记，都是个人信息泄露的高发地带。

记者走访发现，不少小区

为了“便于管理”，在大门和单元入口安装了面部识别系统，省去了刷卡环节。然而，这却让不少业主忧心忡忡。

“不光要上传照片，连家庭关系都得填。”北京市朝阳区的江先生说，出于安全考虑可以理解，但一想到个人信息可能泄露，“心里就发慌”。石景山区的罗女士担忧更深，“孩子在小区里玩，都让人不踏实了”。

杭州互联网法院副院长王杨沁如明确表示，个人信息保护法第六条确立了“最小必要”原则，收集个人信息，应当限于实现处理目的的最小范围，不得过度收集。超出“必需”范围的，有可能会涉及过度收集。

“如果小区门禁只有面部识别一种方式，就构成了技术上的强制，这是不被法律允许的。”许可强调，2021年最高人民法院《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》已经明确：小区门禁不能将面部识别作为唯一验证方式，必须提供刷卡等其他替代途径。

当然，生活中有些需要提供个人信息的情形是法律所允许的。

许可指出，个人信息采集以同意为原则，但法律同样明确了例外：为履行合同所必需、为履行法定义务、应对公共安全事件，以及新闻报道和舆论监督等。他举例说明，打车提供位置和联系方式，就属于“为履行合同所必需”，法律允许，无需单独同意。

然而，“为履行合同所必需”提供个人信息的情况，并不等于个人信息可以脱离场景随意使用。

“不需要同意，绝不意味着个人对这些信息不享有任何权利。”许可指出，知情权、查阅权、复制权、更正权、删除权、转移权——这些权利在任何情形下都应当完整享有。

2 谁在泄露个人信息

山东青岛的何女士为了接听孩子升学的重要电话，特意办了一个新的手机号，从未告诉任何人，也未向外拨打。然而，就在完成志愿填报后的关键期，从这个号码拨打进来的房产中介、培训机构电话接踵而至。类似的情况还有，湖南郴州的小刘仅一次看牙后，便频繁接到多家私立口腔医院的推销电话。

“学校、医院这类单位掌握着海量个人信息，但限于人员、技术等要素，信息采集和管理常常委托给第三方。”许可教授分析，这种外包模式可能给信息保护带来隐患。

山西省公安厅网安总队负责人介绍，太原公安机关侦破一起涉及学校、培训机构、眼科医院等领域“内鬼”侵犯公民个人信息案件，涉案金额超22万元。

个人信息究竟通过何种路径泄露，历经多少环节，最终流向何方？

安徽省合肥市公安局网安支队网络案件侦查大队教导员陆宇介绍，经持续深挖侵犯公民个人信息黑灰产业链，发现泄露信息存在多种途径，爬虫盗爬后台、木马植入、钓鱼链接诱导，以及从电商、招聘、公示等公开渠道抓取零散信息、清洗整合建库倒卖的“技术流”手段也层出不穷。

这些涵盖教育、医疗、快递等各类信息的数据，其非法交易已形成闭环的灰色产业链。

陆宇介绍，在从源头获取信息后，一些仍

装成运维人员的小型技术工作室便介入分拆标注，抬升数据价值；流通端存在多级中间商，他们往往注册空壳公司，打着市场调研、数据咨询的幌子进行分销；最终，这些信息流向终端的违规小微企业甚至是诈骗团伙。

疯狂的倒卖行为背后，必然有庞大的需求。究竟谁是买家？

根据近些年破获的多起案件，安徽省合肥市公安局网安支队网络案件侦查大队勾勒出一幅清晰的买家“画像”。陆宇介绍，占比最高的是电信网络诈骗团伙，他们依托精准信息实施定向诈骗，大幅提升作案成功率。其次，部分中介、培训机构批量采购信息，用于电话、短信骚扰式推销。还有假借私家侦探名义，获取住址、资产、婚姻信息，实施跟踪、勒索等非法活动，更隐蔽的是通过网络进行黑灰产运营，收购实名账号、手机号刷控评、薅平台福利、搭建非法工具。

不仅如此，个人信息在交易过程中还被明码标价。从单一的通讯录信息，到包含户籍、征信、医疗等高敏感内容的“精准客户群”，价格从每条几分钱到数十元不等。山西省公安厅网安总队负责人告诉记者，长治公安机关侦破的一起为境外电诈集团提供免验证微信号的侵犯公民个人信息案件，涉案资产达2000余万元。

暴利驱使下，原本属于隐私的个人信息成了可以议价的“商品”，个人信息该如何保护？

3 如何守护个人信息安全

记者在国家计算机病毒应急处理中心官网查阅发现，自2018年3月官网中首次公布检测发现违法移动应用以来，共发布监测涉及超过千余款违法App。

北京大成律师事务所资深律师鲁宁表示，对于超范围采集、非法泄露个人信息行为，过往监管以事后被动处置为主，多在群众投诉、信息泄露事件爆发后开展调查、督促整改。2026年网信部门、工信部、公安部联合专项行动显著强化常态化事前风险排查，构建“源头预防、过程管控、事后严惩”全链条监管体系，从业务设计前端降低信息泄露隐患。

“公众对个人信息的担忧实际涉及收集、滥用和泄露等三个层面。”许可分析，采集是风险的开端，真正的危害发生在滥用和泄露环节，而且极难预防。因此个人信息保护法采取了“全链路保护”策略，在采集环节就予以严格规制。

“所有收集、处理个人信息的企业与机构均负有法定合规义务。”鲁宁提醒，必须完整梳理数据收集、存储、使用、传输、销毁全流程，常态化开展安全漏洞自查，完善加密、访问管控等安全防护体系，严格规范内部数据操作权限，将个人信息合规内嵌为日常运营的硬性要求。

个人在日常该如何保护隐私信息不被泄露呢？

许可建议，公众可以把握三个原则：首先，对来路不明的App、网站和链接保持警惕，不要轻易点击同意或提交信息；其次，充分利用选择权，对于“单独同意”的内容不要轻易同意，所有单独同意原则上都不会限制用户对App基本功能的使用；第三，一旦发现问题，积极投诉举报，“现在投诉举报反馈很快，要用行动来保护权益，不能只停留在意识上”。

陆宇提醒，在使用App时，仅开放基础功能必需权限，关闭位置、通讯录等非必要授权；线下活动不填写身份证、住址等敏感信息；定期清理闲置账号、解绑授权、更换平台密码。此外，谨慎使用各类AI生成工具，严禁上传身份证、人脸视频、私密文件，防止个人信息被用于AI训练留存或扩散泄露。

“日常上网时，许多无意识的行为可能造成信息泄露。”杭州互联网法院法官沈莹特别提醒，在社交平台不要晒身份证、户口本、车票机票、病历、房产资料等敏感证件。同时也要注意，不随意公开居住小区、学校单位、作息轨迹、出行计划等生活隐私信息。在公共场所不连接无密码陌生公共Wi-Fi。

一旦遭遇个人信息泄露，可以通过12377、12315、平台官方渠道举报侵权行为，遭遇批量泄露、敲诈或精准诈骗立即报警。(据新华网)