手机APP过度采集，窃取贩卖屡禁不止……

个人信息要多加几道保护锁

不久前发生的一系列事件让个人信息安全再成舆论热点：华住旗下多家酒店品牌疑似发生大规模信息泄露事件，数据涉及约1.23亿条官网注册资料、1.3亿条入住登记身份信息；有“暗网”用户声称手握3亿条顺丰快递客户数据，包括寄收件人姓名、地址、电话等个人信息，并积极叫卖……

网络时代，我们的个人信息安全状况如何？谁是个人信息泄露的幕后“黑手”？护航个人信息安全，政府和企业需要再做些什么？

手机应用软件过度采集个人信息

个人身份信息最容易被侵犯

全国消协组织受理的消费者投诉数据显示，今年上半年，电商平台、社交平台软件等非法采集消费者个人信息现象成消费投诉新热点，位居十大投诉榜榜首。不久前，中消协发布的《APP个人信息泄露情况调查报告》（以下简称《报告》）也反映，遇到过个人信息泄露情况的人数占比为85.2%。

“网络具有即时性与虚拟性，加上个人信息被广泛采集却未受到良好保护，公民个人信息一旦泄露，普遍存在举证难、损失认定难的情况，因此，个人信息泄露问题没得到有效治理。”中国法学会消费者权益保护法研究会副秘书长陈音江说。

“个人信息主要有三种形式：第一种叫个人隐私信息，这是隐私权保护的范围；第二种叫个人身份信息，如身份证号码、电话号码、个人账户信息等，用个人信息权予以保护；第三种是衍生数据，是对网络上留存的海量的个人数据进行加工处理形成的新数据，已经与个人的身份信息脱敏。”中国人民大学法学院教授杨立新认为，个人隐私信息和个人身份信息都要依照法律的规定进行支配，只有衍生数据才可以在大数据时代中进行商业处理。

杨立新认为，最容易被侵犯的个人信息是身份信息，各类商业推销、电信诈骗等大多是基于个人身份信息泄露而出现的。《报告》显示，约86.5%的受访者曾收到推销电话或短信的骚扰，约75.0%的受访者接到诈骗电话，约63.4%的受访者收到垃圾邮件，这是最常见的三大问题。此外，消费者还面临着收到非法链接、个人账户密码被盗等风险。

据介绍，去年3月，公安部开展了打击整治黑客攻击破坏和网络侵犯公民个人信息犯罪专项行动，仅4个月就侦破相关案件1800余起，查获各类被非法倒卖公民个人信息500余亿条。

《报告》发现，个人信息泄露的两条最主要途径，一是经营者未经本人同意暗自收集个人信息，二是经营者或不法分子故意泄露、出售或者非法向他人提供个人信息，这两者均超过调查总样本的60%。

据了解，部分APP会“私自窃密”。例如，部分记账理财APP会通过留存消费者的个人网银登录账号、密码等信息，并模仿消费者网银登录的方式，获取账户交易明细等信息。有的APP在提供服务时，采取特殊方式来获得用户授权，这本质上仍属“未经同意”。例如，在用户协议中，将“同意”之选项设置为较小字体，且已经预先勾选，导致部分消费者在未知情况下进行授权。

另外，手机APP过度采集个人信息呈现普遍趋势。“最突出的是在非必要的情况下获取位置信息和访问联系人权限。”中消协秘书长朱剑雄说，“比如，像天气预报、手电筒这类功能单一的手机APP，在安装协议中也提出要读取通讯录，这与《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定》明确规定的手机软件在获取用户信息时要坚持‘必要’原则相悖。”

《报告》还发现，在安装和使用手机APP时，很少有用户仔细阅读应用权限和用户协议或隐私政策。“不授权就没法用，只能被迫接受。”不少消费者在接受采访时表示。

“双方当事人无法进行面对面协商，这决定了消费者只能先接受平台提出的交易规则，否则就无法进行交易。”杨立新说，问题的关键在于，网络交易平台提供的交易规则是否合法，“对此，商务、市场监管等有关部门在实体和程序上都做了规定。若交易规则内容违法，消费者可以主张废除该规则，也可以行使撤销权撤销该交易，造成损害的还可以请求损害赔偿。”

与此同时，个人信息买卖已形成一条规模大、链条长、利益大的产业链。“这条产业链结构完整、分工细化，个人信息被明码标价，流通变现环节主要包含三个方面。”据中国人民大学法学院博士后刘笑岑介绍，上游环节负责“源头供货”，非法获取或向他人提供个人信息，主要来自于黑客攻击和“内鬼”外泄；中游环节负责对从上游处获取的个人信息进行处理与再加工，通过买卖、交换等形式形成规模化市场；下游环节负责“应用变现”，将所获个人信息应用于电信诈骗、恶意营销等不法渠道以牟取高额利润。

在公安部今年的“净网2018”专项行动中，公安机关对侵犯公民个人信息犯罪、黑客攻击破坏犯罪和非法销售“黑卡”犯罪进行严厉打击，半年内抓获犯罪嫌疑人8000余名，其中涉电信服务商、互联网企业、银行等行业内部人员300余名，黑客1200余名，缴获“黑卡”270余万张。

引导行业建立个人信息分级分类保护体系

据统计，目前有近40部法律、30余部法规涉及个人信息保护，包括民法总则、刑法、消费者权益保护法、网络安全法以及新近通过的电子商务法。

杨立新认为，现有的法律法规已经足以保护个人信息，问题在于，侵害个人信息构成犯罪的，能够追究其刑事责任，但对于侵权行为，仍然制裁不力。“重点是加强司法上的民法保护，在惩戒手段、赔偿问题上落实落细，加强对侵害个人信息权行为的打击力度，承担赔偿责任。”“个人信息保护的主管机关还未确定，目前公安、工信、网信、司法等多家部门都在管，需拧成监管合力。”刘笑岑认为，还处于立法计划当中的个人信息保护法，将来应致力于解决这些问题。

个人信息泄露的源头是什么？“问题出在过度采集上。”陈音江说，“合法、正当、必要”六字是目前相关法律对个人信息采集和使用的规定，必须贯彻落实，同时要尽快明确，哪些事项必须通过实名制注册或办理，哪些事项无需实名，避免信息采集主体过多、实名登记事项过度。

“如何引导行业对于个人信息进行分类，构建分级分类保护体系，这是当前个人信息防泄露问题要着重考虑的一项。”腾讯守护者计划安全专家马瑞凯说。

受访专家表示，个人信息获取、存储和利用的环节众多，许多信息的传播又具有隐蔽性和复杂性，做到切实保障公民个人信息安全，需要公民、信息采集机构、技术人员和有关部门协同共治。就企业管理层面而言，要推动数据防窃密、防篡改、防泄露等安全技术的研发和部署，有效降低不法分子窃密风险；就监管部门而言，要进一步加大对电信诈骗、网络诈骗等违法犯罪活动的打击力度，持续形成高压态势，保护消费者的合法权益。**（据《人民日报》）**