你的银行信息值多少钱？60元！

10分钟手机定位找人，60元获得一个人的银行信息……自今年9月最高人民法院指定辽宁管辖的跨25省份侵犯公民个人信息系列案开槌以来，一些身份为协勤员、银行职员等“内鬼”依靠职务便利并利用监管漏洞，盗卖公民个人信息大肆敛财的事实浮出水面。目前，有10余起案件开庭审理，个别被告已被定罪量刑。

记者追踪调查发现，当前侵犯公民个人信息犯罪多由“内鬼”盗取信息后多层级贩卖，形成隐蔽性很强的黑色交易平台，亟须多管齐下，搭建有效的防范及治理体系。

协勤员盗卖公民个人信息 不到1年挣了7万元

9月13日，跨25省份侵犯公民个人信息系列案在沈阳开审。沈阳市大东区法院当庭审理后认定该系列案第一起案件的被告人王旭光构成侵犯公民个人信息罪，一审判处有期徒刑3年2个月，并处罚金7万元。随后，这一系列案又有多起案件分别在该市大东区法院、皇姑区法院审理或宣判。

据了解，王旭光于1999年到河北省某交警大队任职协勤人员，负责内勤和外勤工作。让人想不到的是，一直“勤勤恳恳”的他，竟变成了“内鬼”。

2015年8月至2016年5月，王旭光伙同在同一中队任职的协勤人员魏某、马某（均另案处理）在办公地点内，使用数字证书或其他正式民警的账号、密码登录公安综合管理平台，通过该平台网上查询车辆档案信息、驾驶员信息等公民个人信息，并通过微信联系、出售给他人。获得的赃款由王旭光通过微信提现，再转给另两人。3人违法所得共计约7万元。

“案件审理过程中发现，一些利用职务和履职便利的协勤员、银行职员、电信人员、快递公司从业者等成为信息泄露主要源头。”沈阳市大东区法院刑一庭副庭长朱丽娜说，堡垒通常都是从内部攻破的，此类人员犯罪数量大，侵犯公民信息的数量多，涉及信息类型广泛。

记者通过调查，绘制了“内鬼”盗卖公民个人信息敛财的路径图：有意无意间知道了有人想获取公民个人信息，存在快速获利机会，利用职务上的便利，抓住可能的空隙，躲过有关人员的眼睛以及监控镜头，大肆拷贝、提取公民个人信息。然后，卖给层级较高的下线。

关押在沈阳市于洪区看守所的被告人徐某某原是农行江西省赣州市分行的一名VIP柜员，2015年在帮助律师朋友查询一名客户的银行信息后，受引诱开始大肆查询客户信息，主要是卡号、余额，以每条60元至90元不等的价格贩卖。

多层级贩卖形成隐蔽的黑色交易平台

2015年11月，辽宁公安机关在侦办一起侵犯公民个人信息案件时，发现大量涉及全国各地贩卖公民个人信息犯罪的线索，后公安部将涉及25省份、涉案人员达100余人的侵犯公民个人信息案件指定辽宁警方侦查。去年5月，多地警方开展集中抓捕行动，铲除多个侵犯公民个人信息犯罪团伙。该系列案中的18起案件、63名被告人确定在沈阳辖区内的法院管辖。

“这个系列犯罪团伙划分为‘猎人’‘为人民服务’等9条专线，专线以专线主犯的微信或QQ名命名，由查询员、一级代理商、二级代理商、下游代理商和客户多个层级组成。”沈阳市中级人民法院刑二庭副庭长贾敏飞说，各团伙通过微信群或QQ群非法提供、获取公民个人信息。

每一条专线都是独立的链条，自上而下，上面为查询员，这是公民个人信息泄露的源头。接下来是“庄家”一样的一级代理商，是链条的主要嫌犯；再往下是不同层级的代理商及用户。“一般每个链条的上下线之间没有直接接触，从联系到交易，均在网上进行。”办案法官说。

记者注意到，上述9条专线几乎涵盖了公民个人信息的全部，比如车辆及航班信息、银行开户信息等。9条专线既独立又相互交叉，形成联系密切、架构清晰的作案集团。查询员之间相对独立，为代理商提供交叉服务。代理商之间信息交换特征明显，联系更为频繁，形成了相互勾结的黑色交易平台。

防范“内鬼”须完善监督制度堵死角

侵犯公民个人信息犯罪社会危害日益突出。办案人员认为，为遏制这类犯罪，要对拥有公民大数据的相关单位和企业加强管理，提升监督力度。并强化对存在问题的网络服务商的检查整治，及时整改各种隐患，实现源头防范。

比如，在徐某某案件中，根据他的供认，每一次获取信息尽管是在银行柜台的前台，但都选择了监控探头的死角。每一次都能轻易得手，从未被人发现。类似的监督监控死角需要引起重视，尽快查遗补漏。同时，相关单位的内部防控机制也要进一步完善。

“公民个人信息泄露不是一个技术问题，而是一个态度问题，一个管理问题。”辽宁省律师协会会员陈宝龙建议，应当加快立法的速度，不论是什么样的单位或部门，只要泄露个人信息就要担责，从长远看，行业信息安全管理亟待补上责任漏洞。 据新华社

相关新闻

仅用3.8元！

身份信息、通话记录、消费账单、人脉关系、门牌号全买到

你的通话记录里，最常用的30个联系人是谁，你家住何处，经常在哪儿活动，余额宝里还有多少钱，在什么时候买过几件内衣……这些你以为的私密信息，其实都可以被轻易查到。

你在互联网上产生的所有数据都可以被“人肉”出来

记者调查发现，一个隐藏在现金贷平台背后的数据产业链正在悄然活动。具体做法是，现金贷平台向数据公司购买所谓的“数据产品”，由后者通过爬虫技术，爬取用户在移动通信运营商、淘宝等知名电商网站、微信支付宝等社交网络上的行为轨迹，以及包括央行征信报告、水电煤使用等在内的生活信息，作为平台放贷前评估用户风险的“风控奇招”。此举在维护现金贷企业一己之利的同时，将用户的个人隐私置于极大的风险当中。

日前，记者通过随机检索，在一家名为探知数据的科技公司，仅花了3.8元就买到了自己的详细运营商报告。

报告达33页，内容涉及记者的基本身份信息，近半年的通话记录详情、账单消费、出行信息和人脉关系等，并有详细的量化评分。

数据显示，这半年时间里，记者共煲了3次超过一小时的“电话粥”，累计通话时长达214分钟。

在消费记录方面，记者每月的手机话费在200元左右，半年充了6次话费，最大单笔充值金额为500元。

此外，报告还记录了出行信息。比如今年国庆期间，记者曾往返惠州、广州和深圳三地。过去半年有过一次出境旅游，在日本待了10天。

更令人惊讶的是，这份运营商报告里还根据联系次数，将与记者进行过通话的1000个手机号码罗列出来，包括完整号码、归属地、通话时长、最早和最后通话时间等。

其中常用的30位联系人更是被单独拎出，统计了近24小时、1–7天、7–30天、30–90天、90–180天5个通话时段的联系次数。

此外，报告中还能看到借款人的身份信息，定位到经纬度、门牌号的居住地址等，还有所谓的风险信息扫描。比如入网时长，黑名单通信记录，民间借贷、银行、P2P平台与互联网小贷等通信记录，甚至还有公检法和澳门通信记录等。

记者从探知数据的一名产品经理处获悉，该公司可提供的服务产品还包括电商、社保、公积金、央行和学信网，查询结果五花八门。换句话说，在某个时刻，从个人的衣食住行到生活工作社交，你所产生的任何互联网数据都有可能被“人肉”出来，并进行多达5000个维度的解读。

大数据公司私自保存他人信息属违规行为

据记者了解，爬虫技术是一项被广泛应用于互联网行业的技术。在现金贷领域的应用，爬虫技术常见于抓取用户相关的运营商数据、电商数据等信息，作为人工智能风控技术的数据补充。

根据网安法规定，企业收集个人信息应当经过被收集者的同意。也就是说，只有经过用户同意，企业收集个人信息才算合法。

在华东政法大学教授高富平看来，用户同意的前提是知情。“平台要访问获取我哪些信息，用于什么目的首先应该明确告知，超出这个范围则不能再用。在明确主体、信息范围、使用目的三个条件后，只有用户发自内心自愿同意后，才算真正的知情同意。”

很显然，用户并不知道自己会被爬取出这么多具体的信息。

据网贷行业数据安全专家韩洪慧介绍，爬虫爬取数据做了一个取巧的行为，即引导用户去访问自己的账户系统，比如手机营业厅、淘宝等，用户自己输入账户密码后，爬虫就进入账户系统爬取信息。用户自己打开了门，但其实不知道爬虫爬取了多少信息，也控制不了爬取的信息以后还会被用在哪里。

韩洪慧对记者表示，大数据公司在帮助金融机构了解和分析客户的同时，也保存了数据。这样私自保存是违规的。数据积累越多，风险也越大。“毕竟数据不是自己业务产生的自然数据，再加上万一保存不好泄露了，就成了定时炸弹。”

据《南方都市报》