信息时代,信息海量,一些不法商家与个人为了获取利益,大肆买卖个人隐私,侵犯个人权利 IC供图

倒卖个人隐私利益链

银行、医院、学校、物业等单位的个别工作人员——内鬼,掌握大量公民个人信息,他们利用职务之便将信息出卖给无正当职业的普通网民或者不法商务调查公司,后者将信息转手出售牟利;保险、房产中介、招生培训等行业的从业人员从前者获取信息后,开展电话销售或其他不法行为……在利益的驱动下,个人信息"产业链"渐成规模。

制图 李荣荣

看不见的内鬼,看得见的利益

个人隐私 就这样被 金钱追逐

赵先生车险10月底到期。就在之前的一个多月里,他每天都能接到七八个推销电话车险的电话。让赵先生不解的是,这些来自不同保险公司的推销员竟然都能清楚地报出他的车牌号、上牌日期和车价。

相比之下,刘女士的经历更为不堪。前些天,已经工作两年的她无意间在一家求职网站上发现了自己两年前投出的简历。她的生日、身高体重、家庭地址、教育经历、特长爱好等诸多的个人信息一目了然。"感觉自己像是被扒光了衣服,暴露在大庭广众之下。"

在这个愈加网络化的信息社会中,越来越多的陌生人能准确知道你的联系方式、你的婚姻状况、房产、汽车等各种个人信息,你就像是赤身裸体站在陌生人面前。你惊讶、愤怒、恐惧,但无可奈何。个人信息的商品化,几乎使得每个人都像是拴在一根利益链条上的蚂蚱,无处可逃。

是谁让我们变成了没有隐私的"透明人"?谁又有权将你的个人信息演变成炙手可热的商品?如何杜绝个人隐私被买卖,个人最基本的权利被侵犯,正日益成为信息社会亟待破解的难题。

□快报记者 陈曦

代发短信 一本万利的生意

"湖居玉道,冠领南京,××××一线湖居9900元起!"

"美移民进入无风险时代!芝加哥会议中心官方发布会,周六14点南京中山东路××××楼。"

"世界首款微型摄像笔,集摄像、录音、拍照、U盘、手写笔功能,科技与文具完美结合。普清版390,高清版490,货到付款!"

"我行将于10月25日从您账户划出1200元,详情咨询025-××××。"

"小灵通或固话拨打××倾听清纯校园女生情感实录,体验都市寂寞女人狂野激情。"

从楼盘推销、移民咨询到提供性服务,从办假证到倒卖假发票、作弊工具,从虚假中奖信息到各种诈骗广告,快报记者打开手机,基本每天都能收到三五条这类短信。是谁让这些短信肆意横行?一位业内人士向记者披露了其中的操作内情。

林小姐曾就职于苏北一家广告公司,附带经营代发短信的业务。客户以房地产公司和家电、卖场居多。通常5万条起发,房地产则是20万、50万起步,上百万条发的也有。发一条赚1分钱,10万条就是1000元。用户号码则从运营商那里购买,几万个号码起步打包出售,一个号码五六分钱,低则三四分钱。出售用户号码的"内鬼"通常是管数据库的或级别更高的人员。"一般的临时工不敢也没那个权限。"

相关公司或个人可根据客户要求针对不同群体发送信息。高端客户"手机话费多,看上去比较有身份",教师、公务员等群体"单位可能会统一办理号码",也可以针对城市、郊区、农村等不同区域的用户群发送。短信公司得到一份名单后,只要有人想买,就可以重复利用,可谓一本万利。

短信发送的方式有三种。"通过运营商的短信平台发,运营商开始是自己经营,因为投诉较多,内部人士就把这个业务外包出去;自己购买群发器,插上手机卡不停往外发送;还可以通过网上的短信平台发,但只能从中赚很少的差价。"业内人士介绍。

据了解,这样的交易网络,在通讯运营商中均存在。"不过钱一般都给个人拿去了。"

记者根据一垃圾短信上面留的电话拨打过去,对方称,这些短信都是通过短信群发器发送的,用户的号码也是他们输入号段自动检索的。据了解,这种地下短信群发公司全国各地都有,还有一些人购买群发工具,在家中从事非法的群发短信业务。

业内人士透露,他们之所以能够大量群发短信,是因为他们可以从运营商那里批发短信,批发价都比普通短信1角钱的价格低。

由于门槛低,近年来,短信公司竞争越来越激烈,经营方式也由专营转变为附带经营。南京涉及此类业务的广告公司也不少,某公司业务员曾多次联系本报相关记者打听开发商老总号码以便联系业务。

三类"抢手货" 点对点营销

"上个星期刚拿到新房钥匙,今天就接到2通电话、4条短信,问要不要装修的,推销地暖、空调、卷帘门、防盗栅栏和家电的。"尹先生忧心忡忡。"预产期下个月,小宝宝还没出生,奶粉商、做胎毛笔的就来电预约了。"准妈妈潘女士心怀不满。

跟那些铺天盖地的垃圾短信不同,点对点营销显然有效得多。据观察,三类人群正成为个人信息泄露的重灾区。

一是新楼盘业主。信息来源是开发商或物业。中介公司和装修公司最青睐这类信息,尤其是刚刚交房的新楼盘业主名单。一来业主有需求,其次他们还没产生抗拒心理,生意比较容易成功。当这些名单上的人被"扫荡"过一遍后,名单的含金量就大大降低。而同样数量的别墅业主名单,价格肯定高于普通住宅业主名单。

二是新生儿。产妇们的经历大致相同:宝宝没出生,就有人来推销奶粉;出生后,婴儿摄影机构的电话总能掐准时间,提醒你何时拍满月照、周岁照;接着,保险公司、早教机构也会瞅准时机找上门来。婴儿名单不会"贬值",随着小宝宝的长大,这类名单可以被商家、保险、教育机构一直使用下去。信息来源主要是医院。

三是私家车车主。这属于比较"保值"的名单,来源主要是汽车经销商和车辆管理部门。买得起车的人被认为具有一定的消费能力,所以除汽车维修店外,高档住宅、高尔夫球俱乐部、高档会所、人寿保险、车友俱乐部、保健品、高端礼品等各种业务都会找上门。此外,各银行VIP卡用户、老板或经理人、高档俱乐部会员名单等也因为同样理由受青睐。

这些准确度高得令人惊讶的信息究竟怎样到了对方之手?

其实,获取个人信息的方法十分原始——利诱关键人员。按照规定,开发商、物业、医院、车辆管理部门等都是严格禁止内部人员泄密的。一家物业公司负责人坦言:"没有必要为这么点蝇头小利,冒风险买卖业主信息,到时候业主遭到骚扰,肯定先想到物业,不是自己惹麻烦吗?"同时,也没有哪家高档俱乐部愿意把会员名单透露给竞争对手。

然而,地下交易防不胜防。某物业公司的负责人曾多次接到业主投诉,为此他们特地在员工条例中写明,如果泄露业主信息,会受到相应惩处。但是,在经济利益的驱动下,顶风作案的人依然存在。当然,也不排除管理文档的员工疏忽大意,没有锁上抽屉,资料被人窃取复印的可能。

南京神秘客购走百万元限量版包的新闻轰动一时,媒体也曾试图通过种种渠道挖掘出购买者的信息,但遭到商场和专柜的委婉拒绝。大公司、大机构基于行业规范和维护形象的需要不可能出卖客户隐私,但利益面前,个别从业人员的职业操守却无法保证。

资深保险经纪人谢平向记者透露,她曾以每条8角的价格向奶粉商购买过新生儿信息,在社区医院负责疫苗工作的朋友也会向她无偿提供信息,她也曾从相熟的居委会工作人员那里获得社区内的家庭信息。总之,搜集信息的渠道很多,而付出的代价,取决于关系的远近或有无共同利益。

热衷理财的刘先生经常会接到电话,向他推销某个委托理财产品,或是推荐股权投资基金,甚至一些地下炒金公司也会找上门,门槛大都较高,数百万元起步。对这类电话,刘先生并不反感。让他不解的是,他的号码是怎么泄露的?

跟银行接触密切的私募经理屈海峰跟记者分析,一些基金经理会从银行内部人士那里获得高端客户信息,且不需要花钱,因为募得的资金还是会选择在该银行开户。"公司募得资金,个人有了资金出口,银行存款也不流失,三方都有利的事情。有时候,银行人员也会从中分红。"

灰色利益链的 冰山一角

通讯、银行等行业的工作人员大量掌握公民个人信息,个别人利用职务之便将信息出卖获利;无正当职业的普通网民或者商务调查公司获取信息,转手出售牟利;保险、房产中介、招生培训等行业的从业人员获取信息开展电话销售或其他不法行为……在利益的驱动下,个人信息"产业链"渐成规模。

去年5月,南京市建邺区破获过一起个人信息非法交易案。案件的主角是一名刚毕业的大学生,作案工具是一台电脑。电脑中存储了包括私家车主、航空VIP会员、高尔夫会员、医院患者、企业老总、楼盘业主、银行客户等海量个人信息,信息被分门别类存进20多万个文件夹,每个文件夹中都有几百条甚至几万条个人信息。这些信息的来源是网络,通过安装一种软件能够在"阿里巴巴""慧聪"等网站上自动采集,主要采集的是企业名录,采集结果以EXCEL文件的形式,保存在电脑里。为了倒卖这些信息,此人还专门租用一个美国虚拟空间,开办了"风中网",留下两个QQ号,以及3个虚拟电话,并绑定了3部手机。通过出售个人信息,一年内获利三四万元。

尽管有关部门加大了打击力度,但记者依然能够搜索出大量此类网站。比如一家专门出售老板信息的商务网站首页显示,新到2011年9月新注册企业名录,包含安徽、福建、广东、河北、江苏等地共计6.2万条老板信息,明码标价300元。

今人担忧的是,因出售、非法提供、非法获取个人信息衍生出来的其他犯罪也在不断触动着公众的神经。今年8月,上海司法机关查获了一起买卖银行客户信息案件,涉案人员共达19人。其中,出售资料的源头来自几家银行的员工。

出售的客户信息资料,主要包括客户征信记录以及银行卡卡号。其中,征信记录主要包括个人基本信息、姓名、证件类型及号码、通讯地址、联系方式、婚姻状况、居住信息、职业信息等;同时,还包括信用交易信息,比如信用卡信息、贷款信息。但这并不涉及到银行卡卡号。但银行内部员工可通过内网查询获得客户银行卡卡号、开户时间、开户银行、余额等,并能查询到账户流水。

据涉案员工介绍,一条征信报告10元,"打包"查全家50元。而一个件,作案人在网上从银行内鬼那里购买客户个人信息,包括姓名、身份证号、手机号、卡主住址等。

今年11月,一起北京最大的非法出售、提供、获取个人信息案,则揭开一个隐秘市场的冰山一角。面对不设防的个人信息体系,高官与庶民同忧。

23名被告中,部分是江湖上的"私家侦探",还有的是相关运营商的工作人员。法院认定,他们利用工作之便,将手机用户的定位信息、电话清单、姓名和家庭地址等个人信息非法出卖给私家侦探,以作调查婚外情和讨债用。

至于交易行情,250元购买三个月的固定电话水单,500元购买两个月的手机通话水单,1000元可以对一个手机号码一个月内做50次定位。无论你身处何方,只要你的手机处于开机状态,然后输入你的手机号码,几秒钟之后,你的行踪就变成电子地图上一个移动的小红点,精确度达到5米-50米。

这起案件由一名"嫉妒的官太太"无意中揭开。一名退休副部长的妻子,因怀疑丈夫有外遇,委托私家侦探调查追踪丈夫,最终导致前副部长的隐私被泄露。

快报记者以客户身份致电南京某宣称可以提供此类服务的调查公司,对方在经过声音处理后给记者回电。得知记者想"找人",对方推荐一款精确度可达到10米-100米的手机卫星定位软件,报价1280元。当记者表示怀疑软件的可靠性时,对方称可以提供仪器定位,"这个要靠运营商的网络支持,没有授权是根本做不出来的,但我们内部有关系。"经过一番讨价还价,对方给出2000元的打包价,包括一个月的通话、短信清单和一月50次的手机定位。

移动互联网时代 隐私被搜集无处可逃

如果说,房、车、存款、教育、医疗等任何个人生活所需的现实绑定的都可能成为个人信息泄露的渠道,那么随着移动互联时代的到来,互联网服务对我们生活的全方位覆盖也正在对我们的个人隐私形成巨大的威胁。

前不久,索尼PSN网络的黑客门事件颇为轰动,由于黑客攻击,索尼PSN网络近万名注册用户的姓名、家庭住址、电子邮件、生日、用户名和登录密码等个人信息泄露,甚至还包括了用户信用卡的详细信息。

事实上,自从互联网服务诞生以来,服务提供商搜集用户个人信息的行为就已诞生,例如最早期的电子邮箱服务、BBS社区交互等,都需要进行个人信息注册,不过那时信息注册所涉及到的细节较少,而且在真实性上也没有太多的要求。

到了移动互联网时代,用户个人信息的价值空前凸显,互联网企业搜集用户个人信息的行为也开始无所不用其极。这一切,从理论上都是为了能够为我们提供更加快捷、便利、安全的互联网服务,但当这些庞大的个人信息数据被存储到了互联网企业的数据中心之后,究竟将会怎么用,我们是无力去追究的。

登录社交网站,我们需要实名注册;开通认证微博,我们也要实名注册;至于进行网络购物,我们不仅要实名注册,甚至还需要提供真实有效的银行账户进行捆绑;就算是玩个网络游戏,我们同样也需要填上一大堆有关自己的真实信息……不仅如此,如果你最近逛上了街旁、冒泡之类的LBS(位置信息服务)应用的话,你除了要提供自己的实名信息外,还得随时随地打开手机的GPS,向网站汇报你的位置信息。

除了我们的姓名、性别、年龄、家庭住址等信息外,我们平时登录网站喜欢浏览哪类新闻、最常用的搜索关键词、最喜欢购买的书籍类型、最热衷的社交圈子,甚至最常去的地方等信息也都成为了"个人信息"的一部分。而围绕着这些"个人信息",一些行之有效的互联网商业模式已经应运而生。

刘娟是从业四年的淘宝卖家,去年,她购买了淘宝第三方应用平台的流量统计插件服务。让她颇感神奇的是,这款插件不仅能提供简单的产品销售记录统计,甚至还能做到对到访的用户IP地址访问记录的查询。"这样一来,用户到我们店之前看了什么货品我们就可以轻松掌握了,这对于我们调整货品的风格和售价什么的还是很有帮助的。"

这还只是比较文明的个人信息售卖案例,同样是针对淘宝平台货品的访问记录,部分非正规第三方服务商宣称可以提供基于IP地址的用户名查询服务,而卖家通过购买这种服务就可以轻松获得曾经访问过自己店铺或者产品页面的用户的淘宝用户名,进而对这些用户展开主动的产品促销信息推送,而这种做法对于买家来说则往往意味着骚扰。

不久前苹果和谷歌曝出的存储手机用户位置信息的事件则是证明个人信息价值链前途无限的又一个典型案例。虽然两家公司都极力否认自己存在存储用户位置信息的新闻,但是其搜集行为却从来没有中止过,谷歌首席执行官拉里·佩奇更是在一封内部电子邮件中直言:搜集用户位置信息对公司移动战略空前重要。

如果说在互联网1.0时代,正如那个著名的笑话所言——"你不知道你聊天的对象是不是一只猴子",那么,在移动互联网时代,电脑屏幕前的你正在成为一个无隐私可言的透明人。

"个人信息" 边界有多大?

人民网此前开展了一次有关个人信息泄露的调查,结果显示,90%的网友曾遭遇个人信息被泄露;有94%的网友认为,当前个人信息泄露问题非常严重。

信息社会,信息成为商品,个人信息更是商机无限的重要商品。但个人信息的边界在哪里?谁有权将你的个人信息商业化?个人信息流动存在巨大的市场需求,又该如何加以规范?近年来,立法保护公民个人信息显得越来越紧迫。

2009年2月28日,十一届全国人大常务委员会第七次会议通过了刑法修正案(七),明确规定了出售公民个人信息、非法提供公民个人信息以及非法获取公民个人信息三个罪名。刑法修正案(七)施行以来,司法机关逐步加大了对涉及公民个人信息犯罪的查处力度。

根据刑法修正案(七)第七条规定,公民个人信息是指国家机关或金融、电信、交通、教育、医疗等单位的工作人员,在履行职责或者提供服务过程中所获得的公民个人信息。

法律专家认为,该法条仅规定了公民个人信息的来源,却未对公民个人信息应当具有哪些要素作出规定。

据介绍,有些信息属于显而易见的公民个人信息,即此类信息只能通过特定机关获取,如户籍底卡,通话记录、新生儿信息等。但在更多情况下,公民个人信息的来源并不确定,或者来源并不能被法律列举的几类行业所涵括但明显包含个人隐私信息,如车主信息。车主信息明显属于应当保护的公民信息,但它的来源可能是汽车4S店,而对4S店能否被交通业所涵括的认识不尽一致,导致实践中对此类案件的处理意见分歧很大。

来源于法律规定的上述行业的信息是否都可划入公民个人信息也存在疑问。例如,企业信息包括企业名称、地址、邮编、法定代表人的姓名及联系方式,这类信息有可能是从工商部门获取,虽含有法定代表人的信息,但并非针对公民个人隐私,此类信息能否认定为"公民个人信息"也是存有争议的。

相关专家表示,刑法或司法解释并不能够确定"公民个人信息"的边界,这应该是上游法应该解决的问题,具体来讲,那就是个人信息保护法。

(文中人物均系化名)