上海警方2017年以来破获侵犯公民信息案件1300余起

雷霆出击 让“行业内鬼”现原形

焦点

首席记者 潘高峰

“行业内鬼”已成为侵犯公民个人信息犯罪团伙的重要主体。并且，此类犯罪已经形成完整的利益链。今天上午，上海警方披露了近期侦破的多起侵犯公民个人信息犯罪团伙案件。这些案件均与特定行业从业人员有关。其中一起案件中，某公司两位前员工和两位现员工在不到半年时间里就非法盗取、交易公民个人信息1000余万条，涉案金额2000余万人民币。

警方透露，近年来，侵犯公民个人信息违法犯罪活动严重侵害了广大人民群众的合法权益，同时滋生了电信网络诈骗、盗刷银行卡、非法讨债等违法犯罪。去年5月，公安部组织开展打击侵犯公民个人信息犯罪专项行动，上海警方对非法获取、提供、买卖公民信息等侵犯公民个人信息违法犯罪持续严打，并逐渐建立完善打击侵犯公民个人信息违法犯罪的长效机制。

据统计，2017年以来，上海公安机关共破获各类侵犯公民信息案件1300余起，有效遏制了侵犯公民个人信息违法犯罪，震慑了违法犯罪分子。

祸起萧墙 业务员手握百万条个人信息

2017年11月，杨浦警方接到辖区一家公司报案：公司通过内部监测发现，部分业务员工作电脑出现大量浏览公司客户资料的异常情况，很可能涉及侵犯公民个人信息违法犯罪。对此，杨浦警方高度重视，立即成立专案组展开侦查。

通过公司内部排查分析，专案组发现公司员工陈某、刘某曾使用个人工作电脑大量浏览、下载公司客户资料。在进一步调查过程中，侦查员又在陈某、刘某的工作电脑中发现了大量EXCEL表格，含有该公司客户的身份证号、手机号、住址等公民个人信息，共计一百余万条。

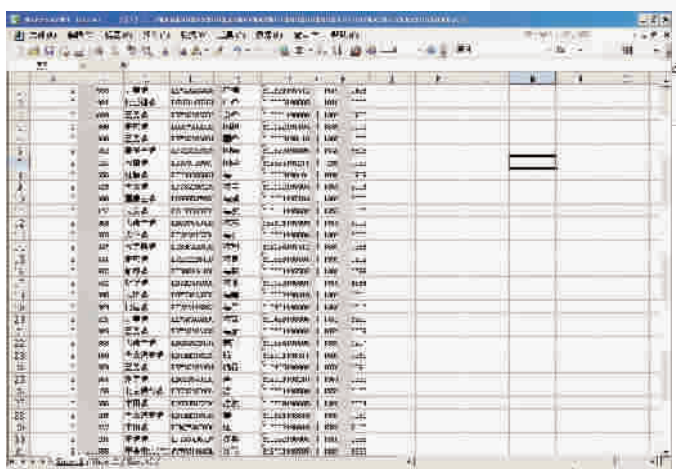
陈某和刘某只是公司的业务员，工作中既没有大量使用客户资料的需要，也没有浏览下载的权限。这些信息从何而来？通过连续数月的走访调查，专案组基本确认了陈某和刘某两人侵犯公民信息的违法犯罪事实。

但问题也随之而来。由于公司的电脑装有独立的内部工作系统，员工网上工作都在系统内网操作，一般无法直接与外部网络发送信息，下载的客户信息无法轻易对外复制或者传输。两位员工如此大量地盗取公民个人信息，肯定是为了谋利。那么，这些被窃取的信息是如何传输出去的呢？

顺藤摸瓜 两任员工勾结盗卖信息牟利

警方经过深入调查发现，公司电脑系统虽然看似与外部网络进行了“隔离”，但由于公司在网络购物平台上开设有网店，因此公司系统并未屏蔽这家网购平台。这会不会是被盗信息流出的通道？

果然，侦查员很快发现，陈某、刘某经常与网购平台中一家箱包店联系，通过这家店的客服聊天系统，将包含大量个人信息的“EXCEL”表格传送给对方。这家店由余某、把某经营，巧的是，两人之前也曾在这家公司任职。两人从公司离职后，开办了一家所谓的网络信息公司，并以提供“优质客户信息”为名牟利。至此，一个集非法获取、传输、贩卖于一体的侵犯公民个人信息犯罪团伙浮出水面。



■ 陈某、刘某利用职务之便非法获取大量公民个人信息 警方供图

经过4个多月的侦查，专案组充分掌握了余某、把某、陈某、刘某等人的犯罪证据。今年3月13日上午，专案组实施集中抓捕，警方先后在浦东新区中科路、安徽淮南等地，抓获余某、把某、陈某等12名犯罪嫌疑人。

据犯罪嫌疑人交代，去年5月，余某、把某找到在老东家任职的陈某和刘某，以金钱为诱饵指使两人利用职务之便非法下载、对外传输公司客户信息。双方约定，费用月结，每月“工资”1万元。余某、把某除了自己使用外，还将其出售给其他人，先后经过四五次转手，价格从8到10元每条不等，最高可卖到16元。至去年11月，犯罪团伙共非法获取公民信息1000余万条，涉案金额2000余万元。

目前，陈某、刘某等2名犯罪嫌疑人已被依法逮捕，余某、把某等10名犯罪嫌疑人也被依法采取刑事强制措施。

贪心不足 离职员工带走大量客户资料

无独有偶，上海黄浦警方今年1月破获的一起侵犯公民个人信息案件，背后同样有“内鬼”的影子。

今年1月初，市民张先生接到一家理财公司打来的推销电话。张先生当场委婉谢绝了销售人员的盛情邀约。挂上电话，细心的张先生思前想后：自己平时生活一向很谨慎，从不向陌生人透露自己的个人情况，但方才电话那头的销售人员却把张先生的家庭住址，车辆号牌，车辆保险状况说的一清二楚。自己的个人信息究竟从哪里泄露的？张先生忧心忡忡，决定报警求助。

巧合的是，黄浦分局南京东路派出所当时正在侦办一起经济类刑事案件，结果发现涉案的一家理财公司为提升工作业绩，非法获取并使用了保险公司的客户信息进行电话推销。这家公司正是张先生向警方报案所提及的理财公司。

1月18日，黄浦警方组织警力对这家理财公司开展突击检查，当场在公司员工杨某、王某、汪某、项某等人的电脑中查获了大量保险公司保单原件照片和文档，涉及非法获取公民个人信息50余万条。

犯罪嫌疑人杨某到案后交代，他在担任理财公司销售团长期间，将自己保存的一些公民个人信息分发给手下的员工，要求员工利用这些个人信息上记载的电话号码逐个联系客户，推销理财产品。这些公民个人信息是杨某在一家保险公司工作时，利用职务便利私自收集的客户资料，其中包括保单原件照片，电子文档等，详细记录了客户姓名、电话、地址、购买保险时间、投保人姓名、被保险人姓名等信息资料。

目前，由于杨某等四人的行为构成了对公民个人信息的严重侵犯，因涉嫌侵犯公民个人信息罪被黄浦警方采取刑事强制措施。

铁腕重典 杜绝内鬼需要更多制度约束

有人将数据信息称为“数字时代的石油”，蕴含天价利益。这些“石油”谁采集，谁监管，尤其是对其中最敏感的公民个人信息如何保护，已成为大数据时代全球都面临的挑战。前不久，美国社交软件巨头Facebook爆出泄密丑闻，更让人警醒。

据上海警方透露，在去年破获1300多起侵犯公民个人信息案件的基础上，今年警方采用高科技手段加大打击力度。多警种合成作战，已成为打击此类犯罪的“标配”。上海市公安局组建了专项行动领导小组，全警动员，保持持续高压严打，坚持“既打上游、又打下游”的原则，对侵犯公民信息犯罪及其关联犯罪进行全方位、全链条打击。尤其是对利用公民个人信息实施诈骗、盗刷银行卡、敲诈勒索、暴力讨债等关联犯罪行为，一查到底。

打击犯罪只是末端。要更加有效保护公民个人信息，还需前端发力。业内人士指出，这绝不仅靠公民个人增强防范意识。当前，无论是警方还是媒体都在反复提醒：妥善处置快递单、车票、购物小票等包含个人信息的单据，在微博、QQ空间、论坛等社交网络尽量不要填写个人详细信息，慎用公共场所免费WIFI。但很多时候，公民不得不给出个人信息，否则就办不成事。因此，源头管理更重要的是通过制度化、科技化的手段，使可以接触到公民敏感信息的人，无法也不敢盗用牟利。

从警方侦破的案件来看，不少掌握公民个人信息的企事业单位，对有权限接触信息的内部人员缺乏相应管理约束措施，使犯罪分子有可乘之机。各种中介平台容易成为套取公民个人信息的“信息中转站”。一些犯罪嫌疑人往往通过房产中介或商务咨询公司等，以注册会员提供服务的形式查询、交换、手机、发布、买卖公民个人信息，包括姓名、联系方式、住址等具体信息。目前，上海市公安局网安部门已经在投资理财、房产中介、汽车销售保养、医疗、物流、网站等相关行业推进开展普法教育，同时针对重要信息系统和存储大量公民信息的行业系统、网站服务器等强化安全监管。

仅有教育肯定是不够的。业内人士建议，应当尽快建立基于大数据的各级审核制度，过程录像监控制度等，对公民个人信息的储存、加工、流转、应用进行规范，明确公民个人信息分级，实施等级保护措施。同时设置更高的技术门槛，比如，必须有两个人以上同时使用密码方可提取个人信息，同时设计次数记录功能，录屏功能，让一切操作有章可循，有迹可查。

通过法律严惩犯罪也必不可少。去年5月9日，最高人民法院和最高人民检察院联合发布了《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》。《解释》明确了侵犯公民个人信息罪的定罪量刑标准，将公民个人信息分为敏感信息、重要信息和普通信息，相对应的如果侵犯公民个人信息数量分别达到50条、500条、5000条的标准，就可能构成犯罪。对于“内部人”犯罪，则规定“减半计算”予以从重打击。