核心提示

近期，北京最大的一起非法出售、提供、获取个人信息案宣判，“侦探公司”人员、通信技术公司职员、通信业务运营商（包括移动、联通、电信）员工等23人走上被告席，也让这个隐藏在灰色地带的市场露出冰山一角。承办此案的检察官透露，本案的被调查者涉及全国多个省、市，大多数受害人并不知情。

记者暗访调查北京多家“侦探公司”和电子产品市场，电影中窃听、跟踪等场景，在现实生活中通过手机卡、百余元的窃听器就能实现。

这个灰色的隐秘市场亟须法律完善和加强监管。

“复制手机卡窃听”多为骗钱

“侦探公司”勾结通信运营商“内鬼”获取个人信息；记者调查“窃听乱象”，北京非法窃听器材市场泛滥

■“侦探”要价
3个月话单4000元
3个月短信8000元

“想知道你的老公去哪儿了吗，想抓住小三、二奶吗？”“经济调查公司帮忙讨债，定位你想找的老赖。”

类似这样的小广告，所谓的“侦探公司”、“调查公司”等以手机短信骚扰着众多手机用户。

他们宣称能拿到任何被调查者的“通话记录、短信清单、手机定位等信息”。

10月19日，记者假借调查婚外情为由，联系北京一家调查公司。

10月20日，这家调查公司的一名马姓人员约记者见面。

“只要你报出被调查者的电话号码，我们肯定能拿到通话详单。”马先生说，调查一个号码3个月的通话详单，需付费4000元。

“你们怎么拿到通话清单？”记者问。

马先生神秘一笑，他说用户查询自己的通话详单时，必须按通信运营商的系统提示发送和接收查询验证信息。“我们能在机主不知情的情况下向系统发送打印通话清单申请，然后我们的人直接拦截系统发回的验证信息，神不知鬼不觉，被调查者根本不会发现。”

记者询问，“我们的人”是不是通信运营商内部员工。

马先生一愣，“这个你就不要打听了。”

“能不能查短信内容？”记者问。

马先生表示，在此之前，短信内容的确可查，“查询3个月的，8000元，但最近追查得厉害，出多少钱也查不了。”

■“内鬼”帮忙
调查公司“盯上”运营商底层员工

8月5日，北京市第二中级人民法院宣判一起非法出售、提供、获取个人信息案。23名被告中，有5人是来自移动、联通、电信的“内鬼”，涉及包括座机、手机通话记录、短信清单、手机定位信息、座机手机登记信息等。

其中两名曾是10086客服人员的被告人供述，他们有权接触通话记录、短信清单以及登记信息中的身份证号、家庭住址等，虽然与通信运营商签有保密协议，但仍以此获利。

其中一名移动营业厅员工，从2009年3月至12月，共出售200多条机主信息，每条50元，获利1万余元。

■定位跟踪 输入手机号你就变“移动红点”

“只要对方开着手机，不管去了哪儿，在电脑地图上都有详细的跟踪点，误差不到10米。”这是“私人侦探”马先生向记者提供另一项业务——对被调查者进行手机实时定位。

根据“市价”，每定位一次要收800元，最迟需在每晚11时前进行，“否则查定位的人就下班了。”但马先生拒绝透露任何“查定位”的信息，只说“交钱肯定能办到”。

“最大非法出售个人信息案”中也有“查定位”的神秘人——北京京驰无限通信技术有限公司运维部经理谢新冲。

该公司是北京唯一拥有移动公司定位功能授权的单位，从事手机定位业务。中国移动对该公司有明确要求，如果对某个手机定位，机主必须知情。但谢新冲让这样的要求成为一纸空文。

法院认定，2009年3月至12月，谢新冲先后多次向“调查公司”提供90余个手机号码定位，非法获利9万元。

同时，谢新冲还出售手机定位软件。北京一家调查公司曾以1200元的价格，从谢新冲处购得定位软件，一个月可对一个手机号码做50次定位。

激活软件，输入手机号，被调查人的行踪就变成电子地图上移动的小红点，精度为5米~50米。

■远程窃听 “小盒子”装手机卡“谁都能窃听”

“大街上买张手机卡，插到这个小盒子里，想定位定位，想窃听窃听。”10月18日，北京百荣国际小商品城电子市场，一家店铺老板介绍着窃听器，柜台上公开售卖多种窃听器材。老板报价，单纯窃听的器材160元，复合窃听、定位功能的器材180元。

一个长宽约3厘米、高约1.5厘米的黑色塑料匣子，滑开匣盖，里面有一个跟手机一样的卡槽。

“装上普通手机卡，就能窃听定位。”老板拿出一张手机卡，装进卡槽，摁开匣子上的电源键。5秒钟后，电源键位置一个针孔大小的蓝色指示灯连续闪烁数秒，之后熄灭。

窃听器放在柜台上，老板让记者站到远处，拨通黑匣子里的手机卡号。

50米外，记者拨通该号码。两秒钟后，手机听筒内传出一名购买偷拍机的顾客和该老板砍价的声音。100米外，声音依旧清晰。

老板让记者向窃听器的手机号发送“DW”字母短信。数秒钟后，一条短信发回记者手机里，短信内容是窃听器所在的位置。查询地图，短信中显示的位置，与窃听器所在位置相差不足50米，哪条路，哪个方向，都显示得一清二楚。

销售人员在演示窃听器如何使用。

10月19日至21日，记者走访北京中关村等多家电子市场，各种窃听、定位器材虽然形态各异，包装上均未显示厂家地址和联系方式。

对此，北京邮电大学信息经济与竞争力研究中心主任曾剑秋分析，这种窃听器插入手机卡实际上就是异形手机，具备自动接听和定位功能，“不算什么高科技”。

■暗访 “相同号码窃听通话短信”

“想知道你老婆跟谁幽会吗？想知道你的生意对手有什么新创意吗？报出他的手机号，我们能复制出一张和他手机号码相同的手机窃听卡，他的电话、短信、位置让您尽收眼底。”

类似短信不少手机用户都接到过。究竟有没有这种窃听卡，记者展开调查。

10月18日下午，记者联系到一家自称能制售手机窃听卡的公司。对方称，只要告知需要窃听的手机号，就能复制出窃听卡，号码与被窃听的一致。

用户可将窃听卡装到一部手机里，无论是被窃听者主叫还是被叫，装窃听卡的手机都会发出嘟嘟声，能听到被窃听者的谈话，短信内容也能同时接收，此外还可定位被窃听者的位置。

当晚，该公司联系记者，称只要将1200元钱打进指定账户，报出需要窃听的号码，次日就能制造出来并安排送货。

记者坚持验货付款，对方答应次日见面交易。随后，记者报出此前购买的131号段手机号码，让对方复制窃听卡。

“窃听号”来电 拒绝验货

10月19日13时许，一名自称“阿强”的男子给记者打来电话。记者手机显示是此前提供的131号段号码的来电，对方不停询问“声音清晰不清晰”。

挂断电话后，“阿强”打来电话，称为缩短交易时间降低风险，要求记者直接往其提供的账号上打款，之后他迅速过来将卡交给记者。记者坚持要将窃听卡装到自己手机里，测试后才能打款。“阿强”反复强调，刚才通话已证明的确已经制造出了窃听卡，“再次通话，怕被机主发现。”

纠缠了20分钟，见记者始终拒绝先打钱再收卡，“阿强”恼羞成怒，“你要是不打钱，我们马上联系被窃听的那个人，把你窃听对方的事捅出去。今天你要也得要，不要也得要。”

联系“被窃听者” 威胁要钱

几分钟后，另一名手持上述131话段号码手机的记者果然接到来电。一名南方口音的女子自称是送快递的，“有你一份快件，但地址模糊了，告诉我你在哪儿，我给你送去。”记者随口说出一个地址，对方随即挂断电话。

很快，记者再次接到“阿强”的电话，称已知道被窃听者的具体地址，“给你一天时间考虑，你要不付款，我们就去找对方要钱。”

随后，记者联系了十多家自称能制造手机窃听卡的公司，并声明自己已多次受骗，不测试不放款。谈到此时，各公司都以各种理由结束洽谈。

对此，中国移动、中国联通客服均表示，只凭号码复制能窃听通话的手机卡“都是骗人的”。

专家称复制卡多为诈骗

10月21日，工信部电信研究院副总工程师陈金桥表示，从理论上说，只知道手机卡号，普通号卡是能够被复制的，“早在几年前，2G手机号卡的加密技术就曾被黑客破解过，复制出来的卡可以实现监听功能。”

陈金桥称，但掌握破解技术的人和厂家非常少，小的厂家和公司不大可能做到只知号码便能复制出有监听功能的卡，“很多不法之徒是在利用监听作为诱饵进行诈骗。”

对于“窃听号”来电，北京邮电大学信息经济与竞争力研究中心主任曾剑秋教授解释，这是使用改号软件，用电脑程序做出来的号码。

■律师说法
私自使用、买卖窃听设备都属违法行为

北京嘉安律师事务所苏怀东律师认为，监听器材属于国家专控产品，其生产、销售、持有和使用都受到严格限制。只有国家安全部门和公安部门在特定条件下进行调查时才能使用，私自使用、买卖窃听设备，都属违法行为。

■如何防范
看好你的手机和卡

中国工业和信息化部电信研究院副总工程师陈金桥称，目前，3G卡是完全未被破解的手机号码卡，“建议有条件的普通卡用户升级成3G卡。”

作为终端的用户，专家提出以下建议：

1.需做到保护好自己的卡和卡密码，不要轻易下载软件到自己的手机上。

2.有人送手机要重装系统，一切“窃听”软件都是跟手机绑定的。

3.陌生人发来的彩信不要轻易点击查看，尤其是带有链接的彩信，尽量不要点击进入该链接。

4.手机上网时浏览正规网站，尽量选择手动输入网址，避免被一些带有窥私软件木马的网站攻击。

5. 手机上的传输端口，如蓝牙、红外、USB等，不用时尽量关闭。 （据《新京报》）

真相 就足力