“我手机里的短信大多是垃圾短信”

专家：完善技术手段提升识别拦截能力

调查动机

近日，女演员周娇发布视频称，其孕期及生产后，丈夫多次收到涉黄短信，怀疑个人信息被泄露。

一石激起千层浪。不少网友跟评称，自己在妻子孕期注册母婴App后，也曾多次收到此类短信或被月子中心、月嫂公司、摄影公司的短信骚扰。还有网友反映称，在购房、购车之后，个人信息被装修公司、家具卖场、保险公司等获取，然后频繁遭遇垃圾短信。

实际上，针对垃圾短信现象，工信部早在2015年就发布了《通信短信息服务管理规定》，明确要求短信息服务提供者、短信息内容提供者未经用户同意或者请求，不得向其发送商业性短信息，违者可处一万元以上三万元以下罚款。

禁令之下，为何垃圾短信仍然频现，其治理难点在哪儿？记者对此进行了调查采访。

□ 本报记者 文丽娟

“我手机里的短信大多是垃圾短信。”北京市民张女士拿起手机给《法治日报》记者看，“你瞧瞧，这一周收到近300条短信，260多条是垃圾短信。”

被垃圾短信轰炸，起源于一周前她用手机号码注册了一款看房App。之后，她每天都会收到数十条短信，内容五花八门，有新楼盘上市的，有二手房降价的，有房屋出租的，有家具卖场的……

张女士不堪其扰，想把所有陌生号码的短信设置成“拒收”，又担心遗漏重要信息。

受到如此困扰的何止张女士一人。有人去医院做孕检，很快就收到推销奶粉、月嫂服务等诸多与婴幼儿有关的短信；有人去证券公司开户，很快就收到炒股、融资的短信；有人去4S店买车，很快就收到各种各样的修车、保险短信。无处不在的垃圾短信，让人直言防不胜防。

多位业内人士近日接受记者采访时说，用户没有订阅或者不想接收的短信即为“垃圾短信”。这些短信往往是由一些商家通过非法手段获取用户的手机号码后发送的，甚至有商家为了获取更多利益，采用各种手段制造诱饵，引诱用户点击链接或者发送回复短信，从而达到欺骗或者诈骗的目的。垃圾短信问题亟待加强治理。

垃圾短信无孔不入 相关产业链已形成

与张女士一样，来自湖南长沙的周女士也收到过不少垃圾短信，诸如“划算节预售开抢，积分抢兑专属券”“30万方低密度别墅大盘，恭迎雅鉴”“今日订好房，享超值优惠”等。她向记者展示了今年以来收到的垃圾短信，从电商广告到中介推销，包罗万象。

“也不知道他们是从哪儿得到我手机号码的。”周女士无奈地说。

有些垃圾短信还隐藏着诈骗和涉黄风险。

重庆市民王先生近日收到一条来自所谓“农业银行”的短信，称其农行信用卡已达到提升额度标准，可致电咨询办理。王先生拨通电话，对方一番说辞后便向其索要银行卡号和验证码。他这才反应过来，这可能是一个骗局。

在北京市民孙先生的手机里，有大量培训机构发来的垃圾短信——两年前，孙先生带孩子在外面玩时，广场上有推广跆拳道的培训机构人员免费送小玩具，条件是留下手机号码。孙先生免费领取了一个小玩具，从此各种幼教类的短信接连不断。

更让孙先生气愤的是，他还收到了不少涉黄短信，有的宣传语不堪入目，有的号称可以上门服务，有的带一个链接让点击看私照。

360手机卫士发布的《2022年上半年度中国手机安全状况报告》（以下简称《报告》）显示，2022年上半年度，垃圾短信的类型分布中，广告推销短信最多，占比为94.9%。这一比例，在2020年第一季度为92.2%。

根据《报告》，2022年上半年度，诈骗短信占比5%，包括赌博诈骗、疑似伪装诈骗、兼职诈骗、股票诈骗等；其他违法短信占比0.1%，包括违法金融信贷、疑似伪基站发送、色情短信等。

“该时间段，短信平台‘106’开头号段是传播垃圾短信的主要号源，占比高达96.8%。利用短信平台、虚拟运营商传播各类型短信依然是主要途径，从获取用户联系方式到群发短信已形成完整产业链条。”《报告》称。

信息泄露现象严重 打上标签定向投放

据业内人士介绍，“106短信”指的是三大通信运营商提供的网关短信平台，设立初衷是给银行、证券等部门与用户联系使用的，便于用户辨识、避开短信陷阱，但后来渐渐被一些代理商用来群发垃圾短信，反而成为骚扰用户的工具。

“卖家发送广告短信使用的手机号码等个人信息，有些是自己收集积累的，有些是其他机构倒卖的。如今商家在接触消费者时，都会特意留下消费者的手机号码。并且现在个人手机信息泄露源较多，在售卖个人手机信息的黑市里，有针对特定市场和行业推出的数据包。”奇安信行业安全研究中心主任裴智勇说。

中国司法大数据研究院社会治理发展研究部部长李俊慧告诉记者，垃圾短信的发送主体分为两类，一类是以营销推广为目的商家或个人，将购买或者自己收集的用户手机号码进行分组并打上标签，然后根据不同的标签，定向投放垃圾短信；另一类是以实施违法犯罪为目标的不法分子，包括类似招嫖、实施电信网络诈骗等，发送渠道既有类似“伪基站”模式，也有类似“网络群发工具”等。

垃圾短信带来的风险不容小觑。《报告》提出，垃圾短信发送成本低、传播范围广的特点被黑灰产业利用，成为传播违法诈骗类短信的重要渠道，并在短信内容中利用关键词、变体字等实现“攻防”。并且越来越多的短信文本内容“短小精悍”，无法仅从内容上辨别其实质。

上海市消保委前不久发布的《2022年消费者权益保护领域需要关注的问题》指出，很多消费者反映“106短信”鱼龙混杂，很容易掉入陷阱：点击短信进入链接，可能被不法商家套取个人信息、落入高利贷陷阱，甚至链接到钓鱼网站，盗取账户资金等；如果消费者回复“T”退订，可能被标记为活跃用户而受到变本加厉的持续短信轰炸；更有甚者，不法商家把电话号码再低价卖给其他同业公司，之后消费者就会收到各类骚扰信息和电话。

需求旺盛成本低廉 垃圾短信屡禁不止

为治理垃圾短信，工信部于2015年发布实施《通信短信息服务管理规定》。2020年8月，工信部就《通信短信息和语音呼叫服务管理规定（征求意见稿）》公开征求意见，再次强调用户未明确同意的，视为拒绝。用户同意后又明确表示拒绝接收的，应当停止。基础电信业务经营者应当建立预警监测、大数据研判等机制，通过合同约定和技术手段等措施，防范未经用户同意或者请求发送的商业性短信息或拨打的商业性电话。

此后，工信部又陆续召开相关会议，要求电商平台全面自查自纠零售、金融等相关产品的短信营销行为，不得未经消费者同意或请求擅自发送营销短信。

在此背景下，垃圾短信为何屡禁不止？受访的业内人士分析，市场需求旺盛、信息泄露频繁、发送垃圾短信成本低廉、执法力度不够等是主要原因。

在裴智勇看来，不同于网上导流和App广告的广撒网式获客模式，短信可以说是精准度、触达率和性价比最高的获客渠道。因此，一些电商卖家为了推广，成为发送垃圾短信最多的群体之一。

在某电商平台上，记者以“通知短信”为关键词进行搜索，跳转出来多个店铺，宣传语多为“各种短信，会员通知，物业通知，物流通知，商超促销，店铺活动”等。

记者以“美容院经营者给客户发信息”为由联系了几家店铺。一位卖家发来价目表：“100元1800条短信，500元10000条，1000元21000条，5000元120000条。”这也意味着，如果购买量大，平均一条短信仅4分钱左右。卖家告诉记者，发送短信与本人手机无关，用的是“106”开头的企业网关号码，在群发平台里将手机号码一键导入，编辑好短信内容，就可以群发短信，还可以过滤错号、重号。

甚至有商家为节省广告成本，非法购买无线电设备，建立“伪基站”发送推销短信。据李俊慧介绍，通过“伪基站”，卖家可以强制连接周边一定范围内用户的手机信号，获取用户信息，并可冒用任意号码随意发送短信，短短几分钟便可群发上万条，一些不法分子还利用“伪基站”发送虚假广告和诈骗信息。

构建分类保护体系 运用技术做好拦截

业内人士指出，垃圾短信问题依然严峻，需要强而有效的监管。

“治理垃圾短信，是一个系统工程。不仅要从制度上规范，还需要产业链上的各个环节群防群治，需要有关部门齐抓共管，加大执法力度。”李俊慧说，在这条产业链上，不容忽视的是信息泄露问题。

“信息泄露时有发生，归根到底还是因为收集个人信息的主体，没有采取有刚性约束的管理措施或手段，没有有效的监测预警机制，使得类似‘内部人’或‘相关人员’外泄的可能性变大。”李俊慧认为，企业亟须建立健全内部管理制度，推动数据防窃密、防篡改、防泄露等安全技术的研发和部署，对数据库、服务器、服务器网络、客户端网络、客户端等关键节点做好防护工作，有效降低“内鬼”和不法分子窃密风险。

他建议，加强对涉信息泄露、贩卖案件的大数据分析，找准致使信息泄露、贩卖的关键行业、关键主体、关键岗位和关键人员，有针对性地建立内部的相关个人信息接触、处理、存储等相关管理要求。

北京声驰律师事务所律师何淑光提醒，要警惕App越界索权现象，“App运营商抓取到的信息越多，越有精准营销的优势，而信息收集过度，又会增加泄露或贩卖的风险”。

在何淑光看来，可引导App运营商构建分级分类保护体系，区分可使用、可交易的商业数据信息和不可使用、不可交易的数据信息，划分个人一般信息和个人隐私或敏感信息的边界。根据相关数据信息的属性、所属领域和类别，对数据信息权利人可能造成的影响等多方面进行分类，再根据具体的类别给予相应级别的保护。

“消费者也要注意提升个人信息保护意识，尤其是在网络注册账号、留下联系方式等信息时，注意个人信息用途，养成非必要不提供的良好习惯。此外，还要注意隐私条款或者协议内容，看清楚勾选协议内有关个人信息使用权限等内容。”何淑光说。

除了把好信息安全关外，信息发送渠道关口也要守住。

受访专家一致认为，整治垃圾短信，运营商应该承担起基本责任，可以从技术、管理等各个层面去探索，比如采用云计算、大数据等技术手段，提升垃圾短信识别和拦截能力、做好垃圾短信溯源核查工作。收到用户投诉后，要及时按照电信管理机构的规定，采取措施。对因垃圾短信问题受到行政处罚的企业，要及时将其纳入电信业务经营不良名单，并向社会公布。

上海市消保委的建议是：运营商在发送“106短信”时主动标注发送者实名，消费者在收到短信时大致就能判断真假，避开消费陷阱；主管部门制定出台部门规章，要求在“106短信”内容中强制标注发送者实名，以保护消费者合法权益。

漫画/高岳

新买的手机号怎么已染上一身“老毛病”？

上海奉贤检察院办理“接码”案推动诉源治理

□ 本报记者 余东明 张海燕
□ 本报通讯员 孙晓光

明明是新买的手机号，注册各类手机应用时却显示不是新用户，甚至接二连三收到各种广告推销电话和垃圾短信，这究竟是怎么回事？

近期，上海市奉贤区人民检察院接连办理了多起通信业务经营者或从业人员窃取公民个人信息案。一些不法从业人员在为客户实名开通手机卡的过程中，擅自用实名认证后的新手机号注册多种软件，并将手机号码及相关验证码提供给上家获利，这类“接码”行为已经严重侵害公民个人信息。

短信验证码被偷走

“您的手机号已绑定其他账号”“您好，我们公司有最新的理财产品”……

接连收到上述短信后，上海市民孟女士十分纳闷：这个手机号码才刚开始用，就已充满使用痕迹——广告推销电话、垃圾短信，一些平台账号竟已被激活，甚至还更新了绑定手机。这个新手机号码平日里一直是自用，近期她也不曾修过手机，不知道这些骚扰电话与信息从何而来。

直到民警找到孟女士，问及她是否曾在某通信店购买并实名认证新的手机卡，她才回忆起办手机卡要求实名制认证时，店主不仅要了身份证，还用她的手机操作认证校验流程。经警方告知，与她一样在这家店购买手机卡、新手机，甚至进店修手机的顾客，其手机号都被店主汤某用来“接码”赚外快了。

实名制手机号码关联了姓名、身份证号码等多种重要个人信息，除通信功能之外，还被广泛用于社交软件、银行理财软件、社会公共服务软件等以验明公民身份，属于重要的公民个人信息，与之相应的“接码”业务随之而生。

“每个人的手机号可以在不同的平台上分别注册获取验证码。我在店里帮客户实名登记手机号，通过实名认证后就可以注册使用软件了。在客户不知情的情况下，我下载短视频、购物等App并获取验证码，然后把这些验证码发给群里的上家，如果对方能够成功登录，就会给我转账或发红包。”在讯问时，汤某向办案检察官交代了赚外快的操作流程。

同步追责网络黑灰产

为牟取非法利益，不少像汤某这样的“行业内鬼”，利用工作便利，将实名认证的手机号码在各购物网站、视频平台等注册新账户，各平台发送验证码后，一并将手机号和验证码提供给上家。

据了解，如果是有效手机号，能够成功验证注册平台，“内鬼”们可获利1元到14元不等。带有即时验证码的手机号码若被提供给他人，手机卡主极有可能被冒用身份，其个人信息还可能经过层层转手被用于电信网络诈骗等黑灰产业链。

在办理“接码”类案件时，奉贤区检察院加强办案研究，明晰法律适用，破解办理难点；强化公检协作，与公安机关会签工作办法，实行类案指引，确定实名制认定信息等证据收集要点，明确证据规格。检察机关经审查认定，汤某违反国家有关规定，将提供服务过程中获得的公民个人信息向他人出售并获利，情节严重，其行为已触犯刑法，涉嫌侵犯公民个人信息罪，依法应当从重处罚。

同时，因汤某经营通信器材店，其经营范围及服务人群为不特定群体，其违反国家规定出售公民个人信息的行为，不仅触犯了刑法，还违反了民法典、网络安全法等相关法律规定，造成众多不特定公民的个人信息被泄露，侵害社会信息安全，对社会公共利益造成损害，依法应当承担相应的民事侵权责任。

为此，奉贤检察院组建“刑事+公益诉讼”专业化办案团队协同履职，公益检察室同步介入刑事案件侦查，引导公安机关同步收集、固定民事侵权事实、公益受损程度等方面的证据，追究罚金刑、民事公益损害赔偿责任。

2022年9月，奉贤区检察院对汤某提起刑事附带民事公益诉讼，经过审理，法院判决汤某犯侵犯公民个人信息罪，判处有期徒刑6个月，缓刑1年，并处罚金1.2万元。法院同时支持了公益诉讼起诉人全部诉讼请求，汤某对其出售公民个人信息所造成的损害承担赔偿损失6000元，并在媒体上公开赔礼道歉。

诉源治理加强防范

汤某一案后，奉贤区检察院又陆续办理4起类案，被告人均为第三方授权企业店员或个体经营者，他们也受到了相应的法律制裁。

案件虽已办结，综合治理工作并未止步。检察官调研了解到，手机号码开卡服务分为直营或授权，5起案件均反映出，被授权开卡业务的第三方经营者一定程度上存在流程管理不规范、从业人员法律意识薄弱等问题。

检察官走访涉事企业连锁门店，调研业务流程及员工管理培训情况，剖析企业经营管理漏洞，就发现问题向该企业宣告送达检察建议，督促企业依法规范经营。

针对手机通信个体经营者管理薄弱问题，奉贤区检察院与区通信公司座谈，分析手机卡开户实名制认证等环节的法律防范问题，就加强对授权经销代理商的管理、开展行业治理等提出建议，及时关注、及早预防，筑牢公民个人信息保护的行业防线。

此外，检察机关依法向相关监管部门制发行政公益诉讼诉前检察建议，建议其就侵害消费者个人信息的违法行为开展行政执法活动，加强行业监管，保护消费者个人信息安全，维护社会公共利益。

在近日的检察建议“回头看”活动中，行政监管部门对侵犯消费者权利的违法行为立案调查，督促经营者落实主体责任。相关企业完善并落实《客户信息安全管理办法》，明确业务办卡流程，定期开展员工法律培训等。经营门店落实公司现行管理制度，设立“开卡专员”并实行业务流程监督，店内屏幕滚动播放警示教育片，提醒店员遵守法律法规，严守行业规定。

承办检察官说，售卖手机卡号的通信店、经办业务的营业厅等地是接触公民个人信息的第一道关卡，从业者应遵守最基本的职业操守，行业也应加强对从业者法律教育，不要因为蝇头小利触犯法律，否则必将承担法律责任。

下载前公司超万份简历出售获刑

□ 本报记者 徐伟伦
□ 本报通讯员 王天娇

从事招聘工作的于某从北京某人力资源公司离职后，借用前同事账号下载了原公司资源库中的1.3万余份简历，并将部分简历出售给他人，非法获利1.6万余元。

近日，北京市顺义区人民法院对这起侵犯公民个人信息的案件进行公开审理，并当庭宣判，认定于某的行为构成侵犯公民个人信息罪，判处其拘役6个月，缓刑8个月，并处罚金1.7万元，没收违法所得，同时须在国家级新闻媒体上公开赔礼道歉，赔偿公民个人信息损失共计1.6万余元。

《法治日报》记者从庭审现场了解到，于某与孙某此前在北京某人力资源公司任职，该公司职员均使用某通信软件办公，软件内含有公司的个人简历资源库。2022年5月末，于某离职，公司将其通信软件账户注销。为寻找新工作，于某开始准备个人简历，他想参考相关简历信息，便向前同事孙某借用其通信软件账户。孙某未曾多想，便将账号密码告诉了于某。

登录孙某账号后，于某见资源库内个人简历可任意下载，便滋生了转卖个人信息获利的想法。随后，于某利用孙某通信软件账号，从公司招聘系统内下载了上万份包含个人信息的简历。

受害公司通过后台日志监测到有人在非工作时间、非工区IP大量下载个人简历信息，遂报案，后于某被公安机关查获。于某向公安机关供述，2022年6月29日至7月15日，他以查看、学习简历内容为由，借用前同事孙某办公软件账号，从公司人才库里下载了大量简历，这些简历中包含姓名、身份证号、工作履历、教育背景、家庭住址、电话等个人隐私信息，此后他通过将部分简历出售给他人的方式，非法获利16400元。

公诉机关认为，被告人于某非法获取并出售公民个人信息，构成侵犯公民个人信息罪，且于某的行为侵害了不特定多数人的个人信息权益，损害了社会公共利益，据此提起刑事附带民事公益诉讼。

4月11日，顺义法院公开审理了这起侵犯公民个人信息刑事附带民事公益诉讼案件。中华女子学院的百余名学生进行了现场旁听。

庭审中，控辩双方围绕“被告人侵犯公民个人信息数量、违法所得数额、赔偿金数额、被告人的量刑情节等”焦点问题，充分举证、质证，发表了陈述及辩论意见。合议庭休庭合议后，当庭对被告人于某作出上述判决。

“同学们要增强个人信息保护意识，同时要充分掌握个人信息安全防护技能，不点击陌生链接，不下载来路不明程序，不转发有害信息，保护好个人账号和密码，防止信息泄露，同时也要养成良好的生活习惯，妥善处理包含个人信息的缴费单据、快递单、身份证复印件等资料，避免被恶意利用。”庭审结束后，顺义法院刑事审判庭庭长宋素娟为学生们上了一节普法课，围绕“侵犯公民个人信息”定罪量刑的标准、法律后果等，对我国个人信息保护法进行了深入解读，并就刑事附带民事公益诉讼的审理程序进行了介绍。

学生们纷纷表示，通过此次旁听庭审，直观地感受到法律的威严和违法带来的惨痛教训，加深了对个人信息保护相关法律知识的理解和认识，日后会加强对个人信息的保护。

“本案被告人的此类行为不仅侵犯了公民的个人隐私，被泄露的隐私还容易被进一步用于其他违法犯罪行为，侵犯相关信息所有者的人身财产安全，这一行为在触犯刑法的同时，也侵犯了社会公共利益。”宋素娟说，判决彰显了司法机关打击侵犯公民个人信息行为、保障人民群众信息安全的决心和力度，也提醒公众在保护好个人隐私的同时，在工作和日常生活中，不要随意散播、发布他人的个人信息。