

禁令之下,为何垃圾短信频现

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,然后频繁接收到垃圾短信。

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。



(网络图)

“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。

多名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”“30万平方米低密度别墅大盘,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培训机构的免费送小玩具,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的商家或个人,将购买或者自己收集的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”。

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。

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。”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。

(据《法治日报》)