骚扰电话像“长了眼”一样,对你的需求“了如指掌”——

“牛皮癣”咋就这么难以根治?

你是否有过这样的经历?前脚刚下载某款炒股App,后脚就能接到各种荐股推销电话……现如今,骚扰电话越来越智能,像“长了眼”一样,对你的需求“了如指掌”。

骚扰电话“命中率”越来越高,背后有些什么猫腻?骚扰电话为何像“牛皮癣”一样难以根治?记者对此进行了调查。

CFP供图

骚扰电话对需求“了如指掌”

“我们这里有精选的几只股票,推荐您了解下呢!”接到这通电话后,厦门市民老杨很生气,直接挂断电话,把来电号码拉入“黑名单”。

让老杨想不通的是,现在的骚扰电话都像“长了眼”一样,对自己的需求“了如指掌”。不久前,老杨下载了一款炒股软件,刚开始使用,当天就接到了荐股电话。“对方是机器人,说是有几只股票经过人工智能分析未来会有‘行情’。”老杨说,此后类似骚扰电话层出不穷,一天至少四五通,多的时候十来通。

无独有偶。这类骚扰电话也让北京市民李先生不堪其扰。“不接怕错过工作电话或快递电话,接了后也屏蔽、举报过,但没啥效果。”李先生说,这些由机器人拨打的骚扰电话会不停更换“马甲”来电,即使“拉黑”也没用。

在黑猫投诉平台上,有400余条有关“使用机器人向用户拨打骚扰电话”的投诉。有的用户反映“几乎每天都能接到一个由机器人拨打的骚扰电话”,有用户表示注册某款App后,“就开始接到机器人拨打的骚扰电话”。

12321网络不良与垃圾信息举报受理中心公布的《2023年第三季度垃圾信息投诉情况盘点》显示,在2023年三季度骚扰电话投诉中,94.5%与商业营销相关,排名前三位的分别为贷款理财、欠款催收与房产中介。

记者了解到,利用人工智能开展电话营销正大行其道。在网络上搜索“外呼电销”,显示的搜索结果中大部分都是“人工智能外呼服务”。

电话“精准”骚扰背后的猫腻

现在的骚扰电话缘何越发精准?

在某二手交易平台上,记者使用指定关键词检索时发现,一些商家在商品简介中声称可以提供“精准客户手机号”。

一名商家向记者展示了其客户信息的采集渠道,包括两家短视频平台和一家“达人种草”类平台,每个客户的信息还包括其具体需求描述。当记者询问其数据来源是否合规时,该商家表示“您放心吧,我们不会干违法的事”。

“通过此类渠道获得的用户信息有可能是用户‘授权’提供的。”中国电子技术标准化研究院网安中心测评实验室副主任何延哲举例说,在一个二手车交易App里,客户想要了解某部车的底价,需填写手机号。如此一来,平台、二手车商、第三方销售人员可能都会获取该联系方式,“仔细查看软件的用户协议,会发现平台会要求用户‘授权’提供大量个人信息,甚至是以‘捆绑’方式向多方提供。”

记者发现,某“种草”类社交App的隐私政策提示,该App会将用户个人信息与“商业合作伙伴”进行“必要的共享”,这些“合作伙伴”包括但不限于平台第三方商家、第三方物流服务商、广告和统计分析类合作伙伴等。隐私政策还提示,当用户选择参加相关营销活动时,在“经过用户同意”后,会将用户姓名、性别、通信地址、联系方式、银行账号信息等与“关联方”或“第三方”共享。

“随着人工智能的使用,个人信息攫取和电话拨打效率大大提升了。”网络安全专家荣文佳说。

“你在购物App上的交易行为,在短视频App上的浏览习惯,在社交App上的发帖回复,背后都有人工智能在打‘电子标签’,也就是人们常说的‘用户画像’。”荣文佳解释说,这些“电子标签”会被脱敏并深度加工,而后分享给各大App的合作机构,而合作机构又能通过一些手段就这些“电子标签”与相应用户重新关联,这就是推送广告和推销电话都越来越精准的原因。

北京航空航天大学法学院副教授赵精武说,当前骚扰电话屡禁不止,主要治理难点在于个人信息泄露的来源难以确定,针对第三方营销公司业务人员故意或过失泄露客户信息的情况仍存监管难题。同时,部分App、网络平台等将个人信息买卖做成黑灰产业链,销售对象并不以特定行业为限,“用户无法确定自己的信息是从哪个平台泄露的,难以找到证据。”

如何治理骚扰电话“牛皮癣”

近年来,国家有关部门通过多种手段治理骚扰电话取得一定成效。2023年上半年,共拦截垃圾信息超90亿次,拦截涉诈电话14.2亿次和涉诈短信15.1亿条。工信部还推广“骚扰电话拒接”服务,强化电信网络诈骗一体化技防手段;印发《关于进一步提升移动互联网应用服务能力的通知》,加强App全流程、全链条治理。

此外,三家电信运营商已于2019年10月面向全国用户推出“骚扰电话拒接”服务,用户可免费开通此项防骚扰服务。例如,中国移动用户可以发送短信“KTFSR”到10086,或拨打10086转人工服务开通。截至2023年6月,“骚扰电话拒接”服务用户规模超5.4亿,累计依据用户意愿提供骚扰电话防护超460.3亿次。

北京邮电大学教授曾剑秋表示,骚扰电话根治存在难度,其根本原因在于商业推销需求长期存在。“骚扰电话成本低、可变现,这种经济利益驱使骚扰电话形成产业链,骚扰新方式层出不穷,给治理带来困难。”

根据个人信息保护法,收集个人信息,应当限于实现处理目的的最小范围,不得过度收集个人信息。处理个人信息应当遵循公开、透明原则,公开个人信息处理规则,明示处理的目的、方式和范围。不得以个人不同意为由拒绝提供产品或者服务。违反该法规定,构成违反治安管理行为的,依法给予治安管理处罚;构成犯罪的,依法追究刑事责任。然而,因为个人信息泄露方式多样化,监管机构难以实现全面、及时、有效的监管。

赵精武建议,应加大对个人信息泄露投诉渠道的宣传推广力度,鼓励全社会增强个人信息保护意识,同时督促应用商店采取安全保障措施,对上架App是否存在非法收集个人信息行为进行事前核验、事中复查及事后屏蔽,做好问题上报工作。

对外呼平台频频被用于拨打骚扰电话的问题,曾剑秋建议,应加强网络技术投入和研发,实现信息贩卖、泄露可追踪、可取证,设置消费者“一键举报”等功能。

何延哲等专家还建议,相关电信服务提供商应强化运用人工智能等科技手段的监管能力,用“魔法”打败“魔法”,“人工智能提升了骚扰电话的拨打效率,有关平台同样应运用人工智能对此类行为深度学习,及早发现并阻断利用人工智能呼出骚扰电话的违法违规行为。”

专家提示,就普通用户而言,防范骚扰电话的方式主要有三种:一是开启手机自带的“防骚扰”功能或使用电信运营商提供的“骚扰电话拒接”服务;二是关注微信公众号“12321受理中心”,点击“我要投诉”填写相关信息;三是遭遇骚扰电话“轰炸”时,保留相关证据,拨打110向警方报案。 新华社记者**颜之宏**

新闻评论

整治骚扰电话 不能仅靠“被动防御”

生活中,形形色色的骚扰电话、垃圾短信让人不胜其烦。要彻底解决骚扰电话的难题,只靠当事人的“被动防御”是远远不够的。

要知道,在如今这样的互联网时代,个人隐私近乎透明,一个人经常无法知晓谁会拨打自己的电话,根本轮不到你说同意不同意。进一步地说,即使用户明确表示拒绝了,但拨打方可以换一个电话,或者换一个人继续对用户进行“骚扰”。此外,让发送垃圾短信方“提供拒绝接收的方式”也存在漏洞。以我们熟知的代码“TD”为例,在很多垃圾短信中,“TD”都被标注为“退订”骚扰短信的代码,但在实际上,它很可能就是发送者设置的“陷阱”。用户一旦回复“TD”,随后会有更多的垃圾短信向用户推送。

由此看来,应对电话骚扰,用户的“被动防御”固然不无效果,更重要的还是相关部门更积极主动地作为,从源头入手,对骚扰电话“下猛药”。

一方面,行政手段是必需的,骚扰电话之所以屡禁不绝,根源在于个人信息被肆无忌惮地收集和滥用。对各种泄露公民个人信息的行为,要做到“露头就打”。对电信运营商,严格按照“谁接入谁负责”的原则,敦促其采取多重手段识别和拦截骚扰电话,让不作为、慢作为的运营商付出应有代价。

另一方面,相关部门还应走出路径依赖,借助经济手段应对骚扰电话难题。美国人也曾饱受骚扰电话的困扰。1991年,美国的电话用户保护法做出规定,禁止使用自动拨号系统拨打受话端付费的电话;禁止使用预录语音讯息拨打住户电话。根据该法的相关规定,如果一个人在12个月之内接到两个以上该法禁止拨打的电话,就有权请求禁止令的救济,并可在实际损失额与500美元两者中选择一个较高的赔偿金。他山之石,可以攻玉。我国骚扰电话久治不绝,很重要的一个原因就是骚扰和反骚扰的成本与收益严重不对等。对此,相关部门不妨转变思路,引入惩罚性赔偿制度,调动社会各界的积极性,动员各方面力量参与治理。

骚扰电话,拨打一百次是骚扰,拨打一次也是骚扰。相关部门只有多管齐下,坚决做到对骚扰电话“零容忍”,才能真正有效地解决这一问题。 **齐鲁**