

多次弹窗暗示存在风险 烦琐操作才能下载安装

“下个App还得手机厂商同意才行？”

□ 本报记者 韩丹东

“我自己的手机,想下个App还得手机厂商同意才行?”天津市某高校学生李女士从手机第三方渠道下载安装多款App时,都遇到不同程度的手机系统拦截的情况,手机上不仅弹出安全风险提示和安全性确认,甚至需要李女士输入系统密码才能安装。

《法治日报》记者近日调查了解到,不少人遇到过和李女士一样下载App时被自己手机拦截的情况。用户如果不通过手机的预装应用商城,而是通过其他渠道下载安装软件,手机总是会多次提醒存在风险或者要求变更权限,而且还强制要求输入系统密码,十分麻烦,甚至有些App在按照系统提示一番操作后也安装不了,还有些App因为系统各种阻拦也无法升级。

反复弹出的风险提示是否合理?非系统自带的应用商店,手机就能随意拦截吗?带着问题,记者进行了调查采访。

风险提示反复弹出 下载安装多次受阻

河南省安阳市的刘女士曾用某安卓手机下载某款交友软件,起初,她使用手机自带的应用商城搜索,发现并没有该App,只有很多同类型以及名字类似的App。

随后刘女士通过第三方渠道搜索该App,下载完成后进入安装阶段,系统弹出了红色感叹号提醒“该应用来源非应用商店,需要输入锁屏密码”。刘女士输入密码并选择继续安装后又出现了多次安全性提示,多次点击“已读风险提示”后才成功安装此App。

同样,北京市朝阳区的郭先生告诉记者,他使用手机在浏览器搜索并下载一款手游App,在下载完成准备安装时,手机上出现了红色的感叹号提醒“该应用来源非应用商店,需要输入锁屏密码”。郭先生输入密码并选择继续安装后又出现了多次安全提示,在多次选择“已知风险”“继续安装”并输入密码一系列操作下,才终于成功在该浏览器下载了这款App。

记者在郭先生的提示下,使用某安卓手机尝试操作下载该款手游App。记者在手机自带的浏览器搜索下载,点击“立即下载”后,页面会弹出安全提醒——“为提供更安全的应用服务以保护您的权益,建议优先安装经过手机自带的应用市场安全检测的应用”,并且还提示了该App涉及的权限,如位置信息、媒体文件和电话等。

在点击“继续安装”之前,还需要点击确认“已了解此应用未经检测,可能存在风险,您可以设置是否移入‘应用管控中心’”。记者点击该提示按钮,立刻跳转进入“设置”页面,同时跳出了一个弹窗,有“安装并移入‘应用管控中心’”和“直接安装”两个选项。记者点击“直接安装”,会直接跳转到手机预装应用商店下载安装类似的App。

而如果选择“安装并移入‘应用管控中心’”,又弹出一个选项“下次自动移入‘应用管控中心’”,点击安装后,还需要输入锁屏密码,页面显示安装成功后,还有“增强防护”的提示,并标注了“开启后,仅支持安装经过手机自带的应用市场检测的应用”。

不少手机用户在安装App的过程中,会遇到烦琐的提示和操作。这种情况通常发生在通过非手机预装应用商店下载App时,具体表现为弹窗风险提示、要求用户输入系统密码等,甚至下载安装后也会出现擅自关闭App进程、限制App联网等情况。然而,同款软件,在手机自带的应用商店中的App中能够一键完成下载安装,非常便捷。

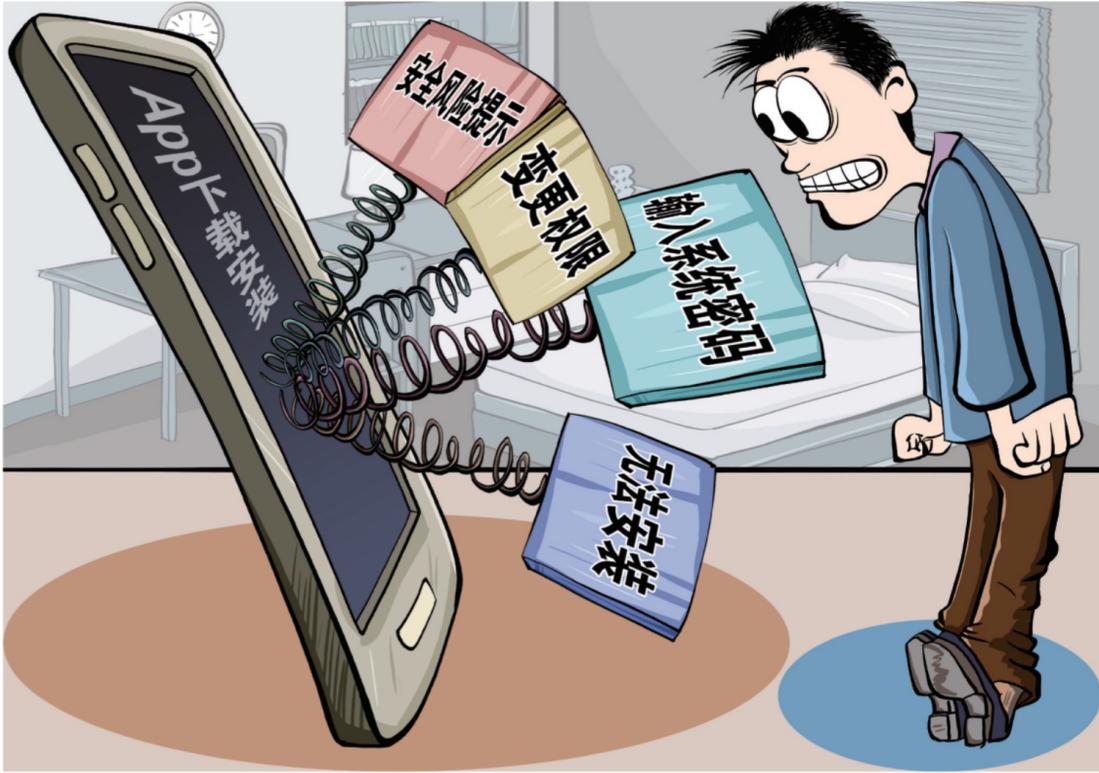
天津市河西区某高校学生陈先生告诉记者,他使用某安卓手机从第三方渠道下载一款游戏App,在下载安装包时,手机上出现了显著的红色字体提示“该应用未经许可可收集个人信息”以及“安全守护提示您注意应用风险,如仍需安装可继续下载安装包”等风险提示内容。

选择“继续下载”后又跳转到了另一个提示“检测到风险”的页面,页面上又一次显示了红色感叹号“无法识别应用安全风险”,在页面下方有三个选项,分别是:查找类似应用、无视风险安装、取消安装。

“如果选择查找类似应用,页面就会跳转到应用商城,并出现类似的App。”陈先生说。

厂商拦截外部链接 涉嫌构成垄断行为

记者调查发现,一些手机厂商推出的纯净模式也增加了用户通过外部链接下载App的阻碍。一些手机自带纯净模式,可开启增强防护,仅支持安装经手机自带的应用市场安全检测的应用。如要安装外部应用,需要关闭增强防护开关,关闭时又要经过多次点



击确认。此外,手机厂商还对第三方应用商店的下载和通过第三方应用商店下载别的App进行设限和拦截。

在普通模式下,记者使用某安卓手机在一外部链接下载一款App,安装过程中会弹出安全提醒,称这是未经安全检测的链接,是否“允许下载”。允许之后,需要输入锁屏密码才能继续安装,然而记者在应用商店里也搜索到了该App,对比发现,下载的两个App并没有任何差别。唯一的差别就在于,在应用商店里下载App更顺利,轻松实现一键安装,没有其他步骤。

但当记者开启手机的纯净模式,继续使用通过外部链接下载的该App时发现,进入安装界面首先会提示是否允许安装软件,“这会让设备和软件容易受到外来的攻击”;用户点击同意后再次提示,应该从手机自带的应用市场选择类似的软件安装;如果用户继续点击安装,则会要求用户输入锁屏密码才能解锁安装过程。

对此,业内人士告诉记者,手机提示下载了不可信软件,可能会有捆绑安装或者有木马,从普通用户角度来讲心里可能会比较慌,一般不会选择继续安装。App的运转需要手机操作系统的支持,但是手机不仅对第三方渠道的App下载安装进行拦截,还不允许有下载软件功能的App上架到手机自带的应用商店,对第三方应用商店进行全面的拦截,需要用户多次验证账号、输入密码增加安装难度,对消费者的个人信息权益和知情权都有损伤。

那么,手机会拦截通过非手机预装应用商店下载的App,设置风险提示、输入密码等障碍,这种拦截行为是否合理?

对此,清华大学法学院副院长、教授程啸表示,手机厂商提供硬件和软件服务,如果不能确保公平对待市场上的应用程序,为了自身利益在消费者安装软件时设置障碍,会导致数字服务市场的不正当竞争,形成垄断。厂商通过“重大风险提示”等手段,会让消费者对从其他渠道下载安装App产生恐惧,这侵害了其他应用程序提供者的合法权益。

泰和泰(重庆)律师事务所高级合伙人朱杰律师表示,手机厂商(应用商城经营者)利用这种拦截行为,实现不正当的商业目的,是“以合法行为掩盖非法目的”。反不正当竞争法明确不正当竞争行为是指经营者在生产经营活动中,违反本法规定,扰乱市场竞争秩序,损害其他经营者或者消费者合法权益的行为。如虚假宣传、混淆行为、经营者利用技术手段,通过影响用户选择或者其他方式,妨碍、破坏其他经营者合法提供的网络产品或服务正常运行。反垄断法规定,经营者达成垄断协议,经营者滥用市场支配地位

等属于垄断行为。“如果手机厂商在具有技术优势,具有市场支配地位的情况下,通过拦截行为限制了用户选择,影响了其他经营者的正当竞争,那么很大可能是构成不正当竞争或者垄断的。”朱杰说。

北京市东卫律师事务所律师徐婧媛说,部分手机厂商通过设置将下载、安装键变暗以及“该应用来源外部,未经过安全检测、恶意”等提示,让用户放弃在第三方平台下载并为自己应用商店引流,不仅构成对第三方下载平台的侵权,而且严重侵害了用户的合法权益,涉嫌违反多项政策法规。

徐婧媛进一步解释说,这些行为构成恶意干扰用户终端上其他互联网信息服务提供者的服务,或者恶意干扰与互联网信息服务相关的软件等产品的下载、安装、运行和升级,也可能构成欺骗、诱导用户不使用其他互联网信息服务提供者的服务或者产品,涉嫌违反了《规范互联网信息服务市场秩序若干规定》;手机厂商作为互联网信息服务提供者,已构成利用移动互联网应用程序侵犯他人合法权益,违反了国家互联网信息办公室发布的《移动互联网应用程序信息服务管理规定》;手机厂商的行为侵害了用户的知情权和选择权,破坏了市场竞争秩序,侵害了用户的合法权益,已经涉嫌违反工业和信息化部发布的《移动智能终端应用软件预置和分发管理暂行规定》。

消极影响不容忽视 行业生态需要治理

记者查询公开资料发现,手机厂商设置对外部链接的强行“净化”,拦截,曾产生过相关纠纷。

例如,2021年6月,第三方应用商店TapTap起诉某手机品牌不正当竞争。据媒体报道,TapTap是一个集手游分发和内容社区为一体的服务平台,这起案件事涉“TapTap及其平台上架游戏,遭遇某手机品牌拦截安装”。

2023年11月,TapTap发出质疑另一手机品牌,称该手机品牌的安全守护功能是为了拦截用户从第三方应用市场下载游戏,从而迫使游戏开发商接受该手机品牌的高额分成。此外,TapTap还指责该手机品牌在用户下载和安装非合作游戏时有意设置过多的阻碍,使用户体验受到影响。

中国社会科学院法学研究所研究员金善明表示,通过对智能手机市场研究发现,智能手机预装应用商店领域有以下问题值得关注和重视:一是禁止软件开发商通过网页或自身官网直接向用户提供和其预装应用商店具有竞争性的功能或其他替代方案,比如提供软件的下载功能,这种情形具有典型的

反向条款特征,不仅控制了交易渠道,也限制了用户的选择权,存在损害竞争的可能性。二是手机系统会对从其他渠道下载的软件进行“骚扰性提醒”,即名义上是向用户提醒非预装应用商店下载的软件具有潜在风险,实质上诱导甚至是诱导用户删除该软件。此外,部分手机仅对与自身没有利益相关的应用软件进行风险提示,而对与己有关联关系的软件则不进行任何提示,其结果造成交易待遇的不同和不同。

“诸如此类的交易方式或交易条款安排,对软件开发、技术创新、用户选择权、市场竞争、消费者福利等方面产生了不容忽视的消极影响,而且这种影响反过来也会妨碍或抑制手机行业、智能产业以及数字经济的健康发展。”金善明说。

有关主体已关注到手机厂商拦截可能存在的垄断、不正当竞争等问题。2017年11月7日,中国互联网协会牵头制定发布的《移动智能终端应用软件分发服务协议公约》倡导,企业在下载、安装、升级、使用、卸载应用软件时,不得滥用自身优势干扰或阻碍其他应用软件开发;不得滥用用户提示的方式干扰或阻碍其他应用软件开发服务。

2023年2月,针对这种手机厂商“割据为地”获取流量利益的行为,工信部下发的《工业和信息化部关于进一步提升移动互联网应用服务能力的通知》明确要求,确保知情同意安装,向用户推荐下载App应遵循公开、透明原则,真实、准确、完整地明示开发运营者、产品功能、隐私政策、权限列表等必要信息,并同步提供明显的取消选项,经用户确认同意后方可下载安装,切实保障用户知情权、选择权。不得通过“偷梁换柱”等方式欺骗诱导用户下载安装;实现便捷卸载。

今年3月17日,最高人民法院发布司法解释(以下简称《解释》),通过细化互联网不正当竞争等行为的具體情形,基于《解释》对反不正当竞争法第12条中的“未经其他经营者同意,在其合法提供的网络产品或服务中,插入链接,强制进行目标跳转”“误导、欺骗、强迫用户修改、关闭、卸载其他经营者合法提供的网络产品或服务”的具体认定作出了规定。

朱杰认为,手机厂商恶意拦截行为应当受到规制。他建议,可由行业协会或公权力机关制定标准,限制手机厂商拦截行为,即可不拦截外部合规应用,也不能限制外部软件的权限获取,对上述排除限制第三方公平竞争的行为予以治理。

“面对数字经济领域出现的新型不正当竞争行为,只有通过法律的完善和实施,才能促进行业生态健康发展,保护企业创新积极性,激发市场主体活力。”朱杰说。

漫画/李晓军

□ 本报记者 潘从武 □ 本报通讯员 赵书城 龚彦晨

厚厚的灰尘,干瘪的轮胎,无论风吹雨打日晒,一动也不动,这就是传说中的“僵尸车”。“僵尸车”外观老化,积满灰尘,长期停放在某处,不仅占用公共资源,还具有一定的安全隐患。

“僵尸车”是如何产生的?治理有哪些难题?近日,《法治日报》记者对此在新疆维吾尔自治区展开调查。

影响环境存在风险

乌鲁木齐市市民丽丽每天下班都会看到几辆“僵尸车”。“相关部门怎么不清理呢?这太影响环境了。”她很理解。

4月20日,记者来到王丽丽下班必经的乌鲁木齐高新技术产业开发区(新市区)某小区外,发现街边停放着数辆颜色不同的“僵尸车”,车上遍布灰尘,雨刷器和车身都有不同程度的损坏,其中一辆黑色轿车车胎瘪了,车座破烂不堪,方向盘裸露电线。另一辆银灰色轿车更为破旧,通过敞开的车窗,记者看到车内堆满了收音机、炒锅、衣服等杂物,且散发着一股酸臭味。

“这些车辆长期无人使用,有的已经无法行驶。”该小区物业公司负责人王博说。

随着汽车保有量不断上升,新疆各地“僵尸车”数量也持续增加,不仅侵占公共停车资源,还存在安全隐患。

今年年初,库尔勒市公安局交警大队副大队长孙威峰带队巡逻至一小区内的停车场时,发现一辆“僵尸车”下出现一堆油渍。经查,原来是该车的机油泄漏,他赶忙呼叫救援力量妥善处理。

“车辆长期不使用,会产生油料泄漏。”孙威峰告诉记者,车内的电瓶在高温下还可能发生爆炸,情况严重的会引发车辆自燃。同时,停放在小区道路上还可能影响消防车、救护车等特种车辆通行。

产生原因多样复杂

“僵尸车”是怎么产生的?

周晓彤是和田市的一辆“僵尸车”车主,2020年,她更换了新车,想将原有的轿车售卖,可二手车车商的出价无法达到她的心理价位,就将车辆停放在小区外的公共停车位上闲置至今。

家住阿克苏市的李梦泽有一辆轿车达到强制报废标准,但因强制报废补贴太少,车在停车场“僵”了2年。其间,他将轿车当成储物空间,将一些废旧物品塞进车里,堆在车旁。有一次,其堆放在车旁的物品砸坏经过的车辆,为此他赔偿对方1000元。

阿克苏市公安局交警大队大队长谢炎告诉记者,车辆报废,达到强制报废标准是产生“僵尸车”的主要原因。“这两种类型的‘僵尸车’只能强制报废,但强制报废补贴的金额较少,对车主缺乏吸引力,有的车主嫌麻烦,就将车长期闲置。”谢炎说。

昌吉回族自治州呼图壁县公安局交警大队副大队长张焕福介绍,产生“僵尸车”的原因还有:车辆被盗抢后,犯罪分子随意将车遗弃;车主失踪或死亡后车辆被遗忘等。

缺乏法律定性和处罚依据是“僵尸车”治理难的原因之一。

“目前对‘僵尸车’的处理没有一个官方的明确界定。”张焕福说,根据民法典规定,所有权人对自己的不动产或者动产,依法享有占有、使用、收益和处分的权利。私家车是私人财产,尽管“僵尸车”长期停放无人管理,但是贸然处理会侵犯公民的财产权。

北京大成(乌鲁木齐)律师事务所律师谷雨说,目前有关“僵尸车”的治理没有专门立法,只是在一些法律法规里有和“僵尸车”相关的法律条文。“例如,根据道路交通安全法和《机动车强制报废标准规定》,达到报废标准的机动车不得上道路行驶,对于公共道路范围内的‘僵尸车’可以视作违停车辆,直接予以拖移。”谷雨说。

形成合力主动作为

事实上,针对停放在公共道路范围内的“僵尸车”,新疆公安交警部门已采取多种措施进行清理。库尔勒市公安局加大巡查执法力度,协助城市管理部门清理路边“僵尸车”;阿克苏市公安局交警大队采用“统一停放、集中公示”的方法,将停放在道路上的“僵尸车”集中清理至专用停车场;和田市公安局交警大队组织多次“僵尸车”专项治理行动,累计清理“僵尸车”100多辆。

据了解,非公共道路上“僵尸车”的处置较为复杂。“僵尸车”大多是车主的合法财产,不管是业委会、物业公司还是社区都没有执法权,如果遇到“僵尸车”不存在违法行为,车主不配合或联系不上车主的情况,通过法律途径解决问题也会困难重重。

“可以通过立法或者修订相关法律法规,让治理‘僵尸车’有法可依。”谷雨认为,首先应通过立法明确界定“僵尸车”,其次,要厘清执法主体,明确不属于公安交警部门管理范围内的“僵尸车”由谁管理。

“让治理‘僵尸车’有法可依只是第一步,这项工作绝非一个单位或部门就能完成,需要社会各方主动作为,形成合力。”谷雨表示,治理“僵尸车”还需要更多相关机制的完善和政策的支持,例如完善机动车报废规定和流程,鼓励车主通过“以旧换新”的方式淘汰旧车等。今年3月13日,国务院印发《推动大规模设备更新和消费品以旧换新行动方案》的通知,其中明确提到“开展汽车以旧换新”,这为从源头治理“僵尸车”提供了新方向。

“法治保障,多方发力,完善制度设计,健全工作机制,方能找出解决‘僵尸车’问题的最优解。”谷雨说。

一停多年无人管的「僵尸车」咋整

专家:须依法治理找出问题的最优解

做医美打的16支针有11支已过期

□ 本报记者 唐荣 李文茜 □ 本报通讯员 彭梓涛

做一次医美打16针花了25万元,事后发现这16针中大多数都过期了,该如何维权?近日,广东省深圳市南山区人民法院依法审理了一起医疗美容服务合同纠纷案,判令被告退一赔三共52万元。

据了解,A门诊部为B公司成立的法人独资有限责任公司,许可经营项目包括医疗美容。2022年3月,王女士在B公司产品加盟商周经理的推荐、陪同下,前往A门诊部参观、听讲座,并于当天支付预付款5万元。几天后,王女士与B公司签订《形象设计协议书》,约定由

B公司对王女士进行综合形象设计,费用5万元且可抵消消费项目款。同日,王女士又与A门诊部签订《医疗美容服务协议书》,约定王女士接受A门诊部玻尿酸注射下巴、额头、唇珠等美容项目,共计25.78万元。合同签订后,王女士现场支付8万元,由周经理代为支付5.78万元,并向A门诊部出具一份7万元的欠条。当晚,王女士即在A门诊部接受了全部的美容项目服务,共注射16支透明质酸钠凝胶。

注射后,王女士发现自己容貌几乎毫无变化,她进一步追问美容项目详细信息并索要手术记录后,发现注射的产品大多已过保质期,王女士认为自己遭遇欺诈,遂将B公司、A门诊部和周经理诉至南山法院,

要求撤销签订的《医疗美容服务协议书》与欠条,退还已付款项并赔偿三倍损失。

南山法院审理认为,案涉医疗美容是王女士为改善自身容貌及健康状况,满足更高审美需求而选择的服务项目,符合生活消费特征;A门诊部、B公司亦有别于非营利性医疗机构,故本案纠纷属于医疗服务合同纠纷。

A门诊部作为提供医疗美容服务的经营者,应当确保消费者的身体健康和生命安全。A门诊部向王女士高价销售医美产品,但案涉16支产品中有11支已过保质期,进行操作医师虽具有美容外科专业执业医师资质,但在操作当时,尚未完成在该

门诊部的执业备案,而A门诊部亦未对医师资质等情况事先披露,相关行为均明显有悖于诚实信用原则。

因此,南山法院依法认定A门诊部在为王女士提供案涉医疗美容服务中存在欺诈,遂判决撤销《医疗美容服务协议书》、欠条,判令A门诊部退还王女士已实际支付款项13万元,并赔偿三倍价款39万元。B公司作为A门诊部的独资法人股东,因未就两公司财产相互独立提交任何证据,应对A门诊部上述款项承担连带清偿责任。王女士以周经理为A门诊部、B公司招揽客户为由,要求周经理承担连带责任的主张于法无据,法院不予支持,该判决已生效。