将文字转成照片或将音频转为文字 网络工具教程“秒”出“伪原创”

网络作品“伪原创”现象调查

调查动机

互联网内容生产市场的拼杀日趋白热化,优质原创内容可谓互联网上的“兵家必争之地”。在此背景下,不少平台推出网络作品申请原创功能,此举既可以保护原创作者的合法权益,也推动优质内容不断出现。然而,有不少人却瞄准了原创市场,炮制出“伪原创”作品。“伪原创”手段有哪些?《法制日报》记者展开了调查。

独家调查

□ 本报记者 张昊

内容生产无疑是当前互联网经济的一大“风口”。不管是传统媒体的转型者,还是自媒体人,都将内容生产视作互联网经济的一个富矿,文字、视频、音频等产品不断出现在各种网络平台。

既然是内容生产,就涉及到内容的版权问题,衍生出了网络作品盗版侵权现象。不过,与传统的盗版侵权相比,网络原创作品还面临一种新的侵权形式——“伪原创”,即通过各种手段将原作者的原创作品变成侵权者的“原创”。

“伪原创”手段花样百出

刘思含目前在北京一家视频新媒体公司市场部工作,主要业务是负责公司生产内容的版权保护。

“我们是做科普、知识类视频的新媒体公司,在微信、微博等很多平台上投放医学、汽车等多个领域的内容。我们制作的每一个原创内容由三个部分组成,视频和详细的画外音讲解,还有相对精简的文字。”刘思含说。

一个原创内容包含视频、音频、文字三部分,按理说是不容易被他人直接“拿走”的,但刘思含恰恰遇到了这种情况。

2016年12月27日,刘思含所在的公司上传了一篇关于汽车外观的原创内容。“今年2月中旬,某微信公众号发出一篇文章,用了我们原创视频的截图,复制粘贴了文字版,把画外音整理成文字。在这个基础上,剽窃者给文章加了个开头和从网上扒来的图片。就这样,对方把我们的原创内容变成了他的原创作品。”刘思含说。

刘思含在微信后台与对方交涉,对方不承认。之后,刘思含所在的公司向平台投诉,并要求对方把稿子删掉,对方回复,“既然你们都投诉了,那就交给平台方处理吧”。

“被抄袭的不仅是我们的汽车公众号,我们制作的其他领域的视频,每周会发现并举报几次剽窃行为。”刘思含说。

记者调查发现,目前网上的“伪原创”抄袭方法还有不少。例如“洗稿”,就是把类似的几篇文章拼在一起,之后申请“原创”。

目前,常见的平台审查机制主要由机器完成,即按文字内容的比例来判断是否存在抄袭。不过,机器审查存在一个弱点,就是很难识别视频和漫画。

“我们公司以创作漫画或视频为主,抄袭者直接对视频进行截屏,将原创文章中的文字内容转换成图片,不使用文字,机器就很难识别出抄袭。”刘思含说,“我们与粉丝的互动是问答式的。在读者留言中会有一些提问,我们在互动中作出相应解答。我了解到,有的公号甚至抄袭我们和读者互动的内容,将这些问答内容搬到自己的文章中。”

在线自动生成“伪原创”

记者在调查中发现,除了刘思含提到的各种“伪原创”手法,还有一种模式——在线自动生成“伪原创”。

记者通过阅读多个“伪原创”工具的说明并试用,梳理出其制作过程和原理。“伪原创”的目标是通过同义词替换的方式,让搜索引擎认为是一篇原创文章,从而提高在搜索结果中的排名。“伪原创”工具或在线生成网站都有自己的同义词库,有的通过免费模式向用户开放一部分,另一部分更大的同义词库则要用户付费后才可以使用。

“用‘伪原创’工具可以把在互联网上复制的文章瞬间变成您自己的原创文章。”一个“伪原创”网站的说明这样写到。此类“伪原创”工具还可以在文章中随意植入想被读者看到的关键词或网址,以达到宣传作用。

记者把原创文章复制粘贴到这样的网站上,一键即可生成同义词替换过的文章,被替换的词通常用不同的字体和颜色标记出来。

在这个过程中,记者发现,专业类文章替换较少;生活类的文章替换掉的词较多;文章越长,替换率越高。在线“伪原创”工具还附带相似度检测、关键词排序、关键词统计、关键词组合工具等在线工具,文章整体替换的比例在10%左右。替换后的文章可读性降低,网站建议对文章进行人工修改提升可读性。一个“伪原创”网站在说明中称,“‘伪原创’文章最好将文章开头和结尾用自己的语言组织,这样的效果更好一些”。

记者使用相似度检测对原创和“伪原创”进行对比发现,机器识别出相似度在85%至98%之间。

记者在网站上看到一个生成记录,内容文本字符长度为734个字的文章,共替换了44个词长度为90个字符,替换比率为12.26%。原文和替换之后的文章相似度为92.6%,如此高的相似度怎么办?这些网站给出了进一步的“解决方案”。

“在线生成文章,将其粘贴入前两步已做好的‘伪原创’文章后一段即可”。记者点击“在线生成文章”发现,生成的并不是可读的文章,而是一段看似是中文的乱码。将这段乱码贴在文章最后,相似度降低到84.3%。

除了用乱码降低相似度,这些网站介绍称还可以在文章中插入图片,建议用户打乱文章顺序等方法。

此外,记者发现,网上还可以搜索到大量关于“如何制作‘伪原创’”的教程。

原创维权依然麻烦

作者的原创内容遭“伪原创”剽窃,将会有哪些损失?

“就商业价值而言,一篇文章招广告,卖价要看这个公众号的粉丝量有多少。大一点儿的公众号,一篇头条文章去年的价格大约是5万元;剽窃我们的公号,估计一篇头条文章的卖价在几千元到两三万元之间。保守估计也可以卖出几千元。”刘思含说。

刘思含告诉记者,从后台数据来看,如果是关于热点问题的原创,剽窃的作品可能在至少一个星期时间内对原创产生影响。对于科普内容而言,大部分都是没有时效性的,剽窃对于原创的影响时间持续更久。

面对“伪原创”侵权,原创者是否想过维权?又该如何维权?

“对原创作者来说,他们需要投入大量精力去制作优质内容,让他们去做维权的事情非常消耗精力。特别对于个人原创者而言,或许这一天或者一个星期特别有灵感,能写一篇特别好的文章,结果被抄袭的事情一闹,可能这一段时间他什么也做不了了。”刘思含说。

据刘思含介绍,对于公司而言,遭遇剽窃后的主要诉求就是让对方把文章删除。“我们会时不时在后台搜一搜关键字,看是否有未经授权的转载。没有经过授权的,就算是有些人标注了来自我们的公号,我们还是会联系对方把文章删掉。大部分抄袭的人都挺心虚,都会删稿。遇到不删除的,效率比较高的做法就是向平台方举报”。

记者调查了解到,不同的平台对原创举报的处理周期不同。有的平台,原创作者当天投诉,过几个小时就会出处理结果,有些平台审核过程会比较麻烦。“尤其是公司机构,需要出示一个企业声明,载明哪篇文章被抄袭,要加盖公章,扫描,上传。整个过程耗时短则两三天,也可能更长。”刘思含说,“走法律途径保护原创获得赔偿的方式,对公司机构而言太耗精力,不划算。”

刘思含所在的公司铺设了“全网”运营渠道,不管在什么平台上发现抄袭,都可以与平台方联系,将抄袭的文章删掉。“但是,对于个人原创者,这个工程则无法完成。一是他们发作品平台非常有限,不可能跟很多平台合作保护自己的原创。二是他们没有精力去沟通。”刘思含说。

近期,有平台推出一个叫做“维权赔付”的功能,意思是通过后台与平台方签订协议,如果遭遇抄袭由平台帮原创者维权。平台方先赔付50元,然后平台再帮原创作者走诉讼途径维权。诉讼成功后,再赔付100元。

“不管被剽窃的是什么内容,不管是视频还是文字,都是同一个价格。签订这个协议,意味着平台按照固定的价格赔付作者。然而,制作漫画和视频的成本高于纯文字的内容,我们认为这个赔付金额太少了。如果不签协议,我们确实不会走诉讼的途径。”刘思含说。

制图/高岳

网络原创作品保护应跟上互联网思维

分析

□ 本报记者 张昊

去掉作者名字、修改标题、视频内容截屏、把视频配音转成文字模式……《法制日报》记者调查发现,当前,互联网上的不少内容生产者都遇到了“伪原创”问题,而且侵权方式多种多样。

如何在原创保护中植入更多互联网基因?记者采访了业内专家。

权利人为何很少起诉

“著作权包括人身权和财产权。‘伪原创’的本质就是剽窃,也就是侵害权利人的著作权。”中国政法大学传播法研究中心副主任朱巍说。

中国政法大学知识产权研究中心特约研究员、IT律师赵占领也认为,常见的“伪原创”涉及侵犯原创者多方面权利。未经授权转载,甚至还没有署名,侵犯的是署名权;修改作品名字或者给文章做一些简单的调整、删减,侵害作品的修改权;此外还有侵犯作品的完整权、信息网络传播权、复制权。

“文字作品原创者很少就权利被侵犯到法院起诉。”赵占领说,著作权侵权赔偿的标准有三种:第一,权利人的实际损失;第二,侵权所得;第三,酌情判定,文字作品的赔偿按字数计算,参照每千字几十元的标准。招商收入损失、流量损失、广告收入损失,对方的侵权所得很难举证,一般都是参照每千字几十元的标准酌情判定。考虑到用户的阅读习惯,新媒体平台上发布的文章大多比较短。原创者诉讼维权要支付公证费、诉讼费、律师费,至少要几千元。“对权利人而言不划算”。

赵占领告诉记者,绘画、摄影作品等图片版权被侵权,权利人起诉的较文字作品会多一些,原因是美术作品赔偿标准比文字作品高,赔偿以几千元居多,而且双方和解的多一些。

自媒体出现后,相较以往互联网上的内容由新闻机构、平台自创的方式,转为用户自己生产内容。版权属于用户个人,这种权利主体的变化,也对维权产生影响。

赵占领说,以往版权的权利人是集中的,大部分情况是传统媒体授权给网络媒体,若网络媒体未经授权转载多个内容,传统媒体通过诉讼维权,在成本不变的情况下收益更高。自媒体时代,平台鼓励用户生产内容,权利主体分散。发生版权侵权时,每一个权利人自己去维权就可能遇到取证难、成本高而赔偿低等困难。因此很多人放弃维权。“过去,机构版权保护意识、能力都比较强。权利主体变化后,权利人法律意识相对较弱,维权能力低”。

平台应积极履行责任

“‘互联网+’时代保护原创的核心目的没有变。保护的思路不是限制传播,而是要在发挥传播功能的同时保护原创,让更多人的作品被更多人看到。”朱巍说。

原创内容该如何保护?两位专家都认为应将网络平台责任放在最前面。

朱巍认为,微信平台的原创申请保护机制,比较侧重保护原创者的人身权。微博利用社区的自律机制,只要举报证明在先发布,也可以马上删掉。现在各大平台都有一些原创保护机制,各有特点。

“识别‘伪原创’不难,问题在于平台是否积极履行主体责任。”朱巍说,平台用互联网技术发现真正的原创者是很容易的,只不过有的平台懒于去做。用户也并不太喜欢,嫌麻烦。网络平台具有“双重身份”,既有可能是内容提供者也有可能是服务提供者,几乎所有原创、“伪原创”都是通过平台传播的;用户发现侵权之后依法通知删除、维权要求都是发给平台的。所以,平台应该承担一个主体责任。平台应该积极履行避风港规则,接到权利人通知,必须要采取必要措施。

赵占领则将网络平台的原创保护责任分为三个维度,首先应该建立原创保护机制。第二,现在大的平台都有侵权处理机制,但有的效率低,有的处罚轻。例如投诉一次删除一次,下次再侵权还是做删除处理,处罚力度太轻。第三,平台建立的维权机制,应进一步降低权利人的成本。

“目前各大平台的原创保护机制,往往只在自己的平台上起作用。如果是跨平台抄袭,这些保护机制就不好用了。”朱巍说。

“如果不保护原创,每个人的原创力量得不到保护,那么就不会有人搞原创,复制粘贴就行了。这样,互联网特别是创作领域就会变成荒漠。”朱巍说,网络平台下一步应该想一想,如何在鼓励传播的过程中保障权利人的权利。渠道就是从人身权再到财产权的保护,财产权更多的是从经济补偿的角度来说。

原创保护思路待升级

朱巍通过理论研究发现,对于网络上的侵害版权问题,英美法系更强调财产权的保护,大陆法系更强调人身权的保护。

朱巍告诉记者,互联网的创作保护之路才刚刚开始。在“互联网+”的背景下,关注度经济占了上风,这种新型的业态还处于起步阶段。著作权保护的程度、保护的方法需要怎样跟进技术的发展、补偿应该怎样做,这些问题学者们也还在研究当中。

朱巍说,著作权法的体系是Web1.0、2.0时代的产物,互联网版权的保护办法比较落后,只是靠付稿酬的方式,没有特别好的保护办法。互联网经济时代,原创者的财产权已经和流量、关注度经济、大数据等结合起来,应该用Web3.0、4.0的思维看待原创保护。他认为,特别是分享经济出现后,应更多探讨著作权中的补偿机制。作品一旦发表之后,付费方式可以考虑更多使用靠广告分成、转流量或者商议好的其他方式。用其他方式来保护作品、作者的权利,是可行的,是一种前进。

对于平台原创保护机制的创新,朱巍认为,平台要多创新技术手段,保护原创者的人身权;保护原创者的财产权利则可以使用流量奖励、积分奖励、广告分成、广告联盟、专栏转载分成等方式,把版权人作为“老板”角色参与分成。平台与原创者强强结合,让原创者不单纯卖自己的作品,同时也可以卖自己的影响力。

赵占领认为,著作权法修改后,针对著作权侵权规定了惩罚性赔偿,文字作品的赔偿标准提高了,但总体来说赔偿标准还是比较低。司法实践中对著作权侵权赔偿的标准应该提高。

针对自然人权利人维权难的情况,赵占领提出另一个解决思路——进一步完善我国的著作权集体管理制度。著作权集体管理组织,对于侵犯协会管理的文字作品著作权的行为,依法采取维权行动。著作权集体管理组织目前存在的问题是收取的费用过高、分配机制不透明等。如果著作权集体管理组织能够建立更有效的机制,更好地发挥它的作用,由专业机构来维权,也能在一定程度上解决自然人维权困境。

智能网联汽车上路前需做好法律防护

车辆或驾驶员信息泄露均产生威胁 『黑客』远程操控或致车毁人亡

法 智能网联汽车虽然是新兴事物,但是“黑客”攻击的行为性质和过去类似,无论是刑事处罚还是民事赔偿都有依据。在立法上应该是没问题的,主要还在于执行方面。对于针对智能网联汽车的高科技犯罪,执法、司法机关需要拿出较强的技术手段去应对

视点关注

□ 本报记者 杜晓
□ 本报实习生 张佳欣

近日,工业和信息化部、国家发展和改革委员会、科技部印发了《汽车产业中长期发展规划》。“规划”提出,到2020年,要培育形成若干家进入世界前十的新能源汽车企业,智能网联汽车与国际同步发展;到2025年,新能源汽车骨干企业在全球的影响力和市场份额进一步提升,智能网联汽车进入世界先进行列。

智能网联汽车,专业描述是搭载先进的车载传感器、控制器、执行器等装置,并融合现代通信与网络技术,实现车与车、车与人、车与云等智能信息交换、共享,具备复杂环境感知、智能决策、协同控制等功能,可实现“高效、安全、舒适、节能”行驶,并最终实现代替人来操作的新一代汽车。

简单理解,智能网联汽车有两层技术含义:其一为智能汽车,即可以实现无人驾驶功能的汽车;其二为联入网络,可以实现相互通讯的汽车。

三部委印发的规划让企业看到了智能网联汽车的政策利好。

另一方面,不少公众从一部电影感受到了智能网联汽车发展过程中的隐患——在新近上映的热门大片《速度与激情8》中,有一幕给人们留下深刻印象:大量汽车被“黑客”控制,胡乱冲撞。

可以说,智能网联汽车契合科技发展大趋势,但是也面临着较高的信息安全风险。

七大信息安全隐患

2015年7月,“白帽黑客”查理·米勒以及克里斯·瓦拉塞克入侵一辆Jeep自由光行驶过程的经典案例曝光,大家对智能网联汽车的安全性能提出了大大的问号。两名“黑客”侵入克莱斯勒公司出品的Uconnect车载系统,远程通过软件向该系统发送指令,启动车上的各种功能。

此外,在宝马ConnectedDrive数字服务系统遭入侵事件中,“黑客”利用漏洞以远程无线的方式侵入车辆内部,并打开车门。在特斯拉Model S遭入侵事件中,研究人员通过Model S存在的漏洞打开车门并将车开走,同时还能向Model S发送“自杀”命令,在车辆正常行驶中突然关闭系统引擎。此外,奥迪、保时捷、宾利和兰博基尼等品牌的MegamosCrypto防护系统也遭到攻破。因此,一旦别有用心的人攻击了私人车辆,不仅仅是造成车内财物丢失或者车辆被盗,还极有可能危及到司机和乘客的生命安全。

近日由360智能网联汽车信息安全实验室发布的《2016智能网联汽车信息安全年度报告》认为,智能网联汽车在信息安全方面的威胁包括,TSP安全威胁、App安全威胁、T-Box安全威胁、IVI安全威胁、Can-bus总线安全威胁、ECU安全威胁、车间通信安全威胁七个方面。

以TSP威胁为例,TSP是指汽车远程服务提供商。TSP作为车联网产业链核心环节之一,为汽车和手机提供内容和流量转发的服务。TSP平台漏洞可能来自软件系统设计时的缺陷或编码时产生的错误,也可能来自业务在交互处理过程中的设计缺陷或逻辑流程上的不合理之处。这些都可能被有意或无意地利用,对整个车联网的运行造成不利影响。例如系统被攻击或控制、重要资料被窃取、用户数据被篡改,甚至冒充合法用户对车辆进行控制等。

再以App安全威胁为例,App安全威胁是指“黑客”通过root用户的手机端或者诱导用户下载安装恶意程序,利用这些远程控制App窃取用户个人信息及车辆的控制权,从而控制车辆开锁落锁。早在2015年,安全人员Samy Kamkar就向公众演示了通过在车内安置一个小硬件来入侵车辆的远程控制App的手法,实现车主信息窃取及车辆控制权窃取。

其他如Can-bus总线安全威胁,汽车电子元器件是通过CAN网络连接的,电子元器件之间通过CAN包进行通信。Can-bus总线安全威胁通过逆向工程、模糊测试等方法获得其通信矩阵并破解汽车的应用层总线协议,在不增加汽车执行器的情况下实现对汽车的自动控制功能。也就是说,只要抓住了CAN总线,就相当于是抓住了汽车的神经,就能对汽车进行控制。电影中令人惊呼“僵尸车队”就是这么产生的。

汽车数据也需保护

报告称,以前,汽车是孤立的,物理隔离的,因此“黑客”很难远程入侵汽车内部控制器,除非进行物理入侵,而这个需要很高的犯罪成本。随着互联网的进化,当TSP这样的车联网产品通过T-Box与汽车内部网络联网之后,汽车受到的远程网络攻击就不再是猜想。可以预见,一旦车联网产品普及,关于汽车被攻击的现实案例就会出现并越来越多。

报告分析了一个相关案例:

就在日产于MWC 2016(世界移动通讯大会)上发布聆风电动车最新手机App后不久,澳大利亚网络安全研究专家Troy Hunt发现,软件开发者借助任何一辆日产聆风前挡风玻璃上的VIN码,便可通过Nissan Connect(日产车载系统)手机客户端的身份验证,获取车主身份及车辆充电量信息,并获得车内空调的操控权。虽然这一网络安全漏洞还未涉及油门、刹车等车辆控制关键功能模块,但对续驶里程本已相对有限的纯电动汽车来说,仅远程开启空调这一潜在威胁危害也十分巨大。

在上述过程中,Hunt的学生Jan通过聆风的手机App Carwings查看到车辆的基本信息,包括预测的剩余可行驶里程、电池充电状态,充满电所需时间等。并且Jan发现充电与空调控制相关,可以远程控制空调的开启,并设定时间。Jan先后向汽车发送了三次指令,最终达到了控制车载空调的目的。

报告认为,防止智能网联汽车受到网络攻击并非易事,应该小心保护汽车和驾驶者的数据,如驾驶者的住所、驾驶习惯、行为、喜好和兴趣等,确保信息的隐私性,决定信息的使用对象和用途。事实上,对驾驶者和汽车公司而言都存在相当的风险。事故、数据泄露和个人信息滥用,任何一个问题都可能对整个自动驾驶汽车的发展构成威胁。若要自动驾驶汽车能针对人们的所有需求提供定制化服务,并与外界紧密连接,也需要人们具备高度的信任和灵活度来接受该项技术。

立法足以应对新事物

尽管智能网联汽车存在不少安全风险,但从技术发展趋势来看,未来,智能网联汽车将占据重要地位。

早在2015年5月,国务院印发的《中国制造2025》中,就首次涉及智能网联汽车的发展。

据报告介绍,智能网联汽车的发展的第一阶段是基于自车感知与控制的驾驶辅助系统(ADAS),这是智能网联汽车发展的基础阶段;第二阶段是应用信息通信(ICT)技术实现车-X之间的信息共享与控制协同,即网联化技术的应用;第三阶段是自动驾驶和无人驾驶的实现,这是智能汽车发展的最终目标。

北京师范大学法学院教授、亚太网络法律研究中心主任刘德良认为,从理论上来说,智能网联汽车是可以被远程控制的。不仅智能汽车,无人机也是一样,都是可以被远程控制的。从更广的范围来看,智能机器人也是可能被控制的。不管是智能网联汽车、无人机还是智能机器人,这些都属于一种智能终端,既然是依靠程序来运行的,那就都有可能成为“黑客”攻击的目标,道理都是一样的。

“只要是依靠程序运行,都面临着安全性这个问题,都会面临非法侵入、非法控制。技术永远都有风险,所谓的化解安全隐患就是一个和‘黑客’斗争的问题,难以从根本上化解,属于一个无限博弈的过程。比如当某个设备貌似处于安全的状态之下,但随后又被‘黑客’破解,接下来技术人员又对相关系统和程序进行修复提高,过段时间可能又出现漏洞,这也是技术发展的客观过程。”刘德良说。

对于智能网联汽车被攻击之后引发的法律问题,中国政法大学知识产权研究中心特约研究员、IT律师赵占领认为,这样的行为可能会涉及刑事犯罪,就是非法侵入信息系统罪。此外,侵入系统、控制系统还可能会造成安全方面的问题,而且不排除一些极端的情况,比如像电影里面造成汽车失控,导致严重的安全事故,出现车祸或者造成人身伤害甚至死亡,这就有可能构成故意伤害罪、故意杀人罪。

“民事方面的法律问题在于,‘黑客’的攻击行为可能会给车主或者用户造成一定的财产损失,这是民事财产侵权。还要看智能汽车的生产商有没有过错,比如‘黑客’攻击系统造成用户人身或者财产损害,生产商是否需要承担一定的民事赔偿责任,这就要看生产商生产的计算机系统本身有没有必要的安全措施,是否有明显的技术漏洞,当然所有技术都不能保障绝对的安全,但是至少要在当时的技术条件下不能存在在一般的专业人士看来明显的技术漏洞,如果有的话,生产商也要承担部分责任。”赵占领说。

赵占领认为,智能网联汽车虽然是新兴事物,但是“黑客”攻击的行为性质和过去类似,无论是刑事处罚还是民事赔偿都有依据。在立法上应该是没问题的,主要还在于执行方面。对于针对智能网联汽车的高科技犯罪,执法、司法机关需要拿出较强的技术手段去应对。“如果车主发现智能网联汽车被攻击并造成了损失之后,首先需要报案,以尽量挽回损失。如果车主想要追究生产商的责任,就要留下相应证据来证明系统存在漏洞,但这实际上是比较困难的”。