AI换脸APP问题太多 火得快凉得更快

8月31日，一个叫ZAO的AI换脸APP一夜之间火爆全网。

代替莱昂纳多给你的Rose来一句深情的“You Jump,I Jump”;一秒钟和“现男友”李现同框,让他给你遮太阳;变身吴彦祖……“仅需一张照片,出演天下好戏”,通过AI换脸技术,你仅需上传一张照片,就可以成为梦寐以求的“戏中人”。由于新奇有趣,又满足了普通用户的小小虚荣心，一夜之间,ZAO便迅速刷屏了朋友圈。

没想到,火得快,凉得更快。ZAO上线的第二天下午,ZAO的默认用户协议就引起了各界对其隐私安全风险的质疑,包括对面部识别的支付安全带来的隐患。国家工信部也表示关注并约谈问询。

由此引出的一系列热点问题,人脸等视频素材是否拥有合法版权？刷脸支付还安全吗？AI骗案会不会因此猖獗……

■新快报记者 郑志辉

■廖木兴/图

一部手机一张自拍就能“做主角”

AI换脸并不是新鲜事。

2017年底,国外一位ID为“deepfakes”的网友,利用业余时间创造了一个AI换脸算法,后来这个算法被广泛称为deepfakes。

deepfakes首先在科技社区中流行起来。一开始只是技术爱好者的随性试玩，后来有人用它将色情作品中的主角换成明星脸，这种做法在科技社区引发大量争议，最后被彻底关掉。但AI换脸技术,一直进化至今。今年年初,B站UP主“换脸哥”，使用这个技术将94版《射雕》里扮演黄蓉的朱茵换成杨幂的脸,看过的人都惊叹“神乎其神”。

ZAO这款APP之所以一夜爆红,正是因为其将“换脸技术”的门槛降得极低。ZAO内含有大量视频素材,用户不必会PS，甚至连美图秀秀级别的美颜都省略了,直接上传头像照片就可以将原视频片段换脸,一键生成就可分享到朋友圈。

其实,ZAO的本质还是满足用户的猎奇与虚荣心。对比之前靠给照片加上贴纸特效的Faceu脸萌、预览你老后模样的FaceApp等简单功能就火爆一时的在线美颜、换脸变装APP,一部手机,一张自拍,ZAO直接把你放入经典大片中做主角,怎能不火？

潜在风险大,易引发“丢钱”“丢清白”

换脸AI功能的强大带来的潜在危险性、威胁性,立即就能被察觉到。像前面提到的“黄蓉”被换脸事件,在一众微博大V的侵权抗议后,UP主“换脸哥”赶紧下架了相关视频,并呼吁大家尊重版权与肖像权,专注于技术本身。

有此先例后，不少用户在玩耍ZAO的时候,就特别关注了其用户服务及隐私保护协议，一下子就揪出了其中的大问题。

“在您上传及/或发布用户内容以前，您同意或者确保实际权利人同意授予ZAO及其关联公司以及ZAO用户全球范围内完全免费、不可撤销、永久、可转授权和可再许可的权利，包括但不限于可以对用户内容进行全部或部分的修改与编辑(如将短视频中的人脸或者声音换成另一个人的人脸或声音等)以及对修改前后的用户内容进行信息网络传播以及著作权人享有的全部著作财产权利及邻接权利。”

该条款直指ZAO及其关联公司将获得用户上传内容的著作权利,包括其中的人脸肖像照，引爆了公众对ZAO的广泛质疑:“ZAO的用户协议太离谱了”“有手机号,有面部画像,通过技术合成,犯罪分子可以替你和你的家人通话了”……

其中的潜在风险不言而喻。首先是正方兴未艾的刷脸支付,“丢脸”会不会导致“丢钱”？当前,大部分银行等金融机构开设了人脸识别登录APP功能,“刷脸”支付、远程签约等场景也越来越多见，例如今年“3·15”晚会上，就演示过用“活”照片成功突破某款手机的“刷脸”登录系统。

此外，通过3D打印等技术,“人脸面具”可以获得较高仿真度,此前也已有人使用3D打印面具通过某知名网络支付平台的面部验证。

除此之外,目前不少网贷机构进行“活体检测”时仍使用人工审核或技术含量偏低的机器审核(如“点点头”“摇摇头”“张张嘴”等),一旦公众的面部识别信息被不法分子掌握,很可能用这些黑科技让用户无辜“被网贷”,背上巨额债务。

另一大风险是“丢脸”可能导致“丢清白”。当前,换脸技术被用在一些涉嫌违法犯罪领域的情况并不少见。一些网站用“AI换脸”“换脸视频”等方式提供用知名艺人“面孔”“嫁接”出的视频，这些视频往往涉嫌色情淫秽,且难辨真假,往往让被害人有口难辩、名誉受损。

问题多多,换脸APP未来成迷

其实,ZAO最初那份用户协议的无赖之处并不仅止于对用户肖像权的无视、侵占。实际上,从之后ZAO运营团队被工信部问询约谈，到之后所做的四点说明来看,ZAO团队以及团队背后的陌陌公司,太急于推出这种技术来引爆市场,根本就没有考虑过新技术可能引发的法律、伦理风险。

用户隐私的保障——用户通过ZAO在平台使用并替换新头像,其图像信息是否留存在服务器中？如何确保这些图像信息不被滥用、被泄露、被贩卖？

北京师范大学法学院网络与智慧社会法治研究中心主任刘德良近日表示,针对人工智能技术的前瞻性立法,未来需要跨过的一个坎是首先要转变观念，从关注个人信息的泄露转到滥用的方向(现在的主流看法都在强调泄露,而不在防止滥用上),现在我们的个人信息已经存在于N个商家和机构中，防止泄露几乎不可能,所以关键在于不能滥用。在观念转变之后,再组织专家商讨、提案,系统地规范什么叫滥用,滥用有哪些类型,如何从民法、行政法、刑法上有效防止滥用。相关法律法规的建立完善要具有可操作性,不能不利于大数据和AI产业的发展。

刷脸支付、设备解锁的安全性——一键换脸技术如此成熟,我们是不是要担心一下钱包安全和智能设备解锁问题？

刘德良表示，从立法上要让进行身份识别的机构或者平台(比如银行、支付平台、电信公司、保险公司)去承担责任。如果法律有这种规定,就会倒逼这些机构、平台认真核查比对,要想方设法开发更新的技术手段,有效避免身份假冒滥用。如果不这样立法,掌握个人信息的机构、平台就会把风险转嫁给被假冒者,让个人承担风险。

监管风险——ZAO让用户自行上传照片或视频,如果用户上传了不符合法律要求的照片或视频,通过网络传播,而ZAO并没有阻止,那么它将面临极大的监管风险。甚至,假如用户利用该平台进行涉嫌犯罪的行为,ZAO又该如何监管？

日前就有外媒报道,今年3月,一群窃贼使用AI语音模仿软件,仿冒某公司高层电话该公司员工,让其把钱打到一个异地账户中,电话中高度仿制了这名高层的音调、停顿甚至是德国口音,最终成功盗走了24万美元。研究者称,这是全球首例公开报道的AI诈骗案。有联合国区域间犯罪与司法研究所负责人就此表示，将机器学习技术应用于欺骗性声音使网络犯罪变得更加容易,“想象一下,以CEO的声音进行视频通话,这是你熟悉的面部表情,这样的话你根本不会有任何疑虑”。

可以说，以上这些问题，短期内都非ZAO能够解决的,因此,就更别谈什么商业模式了。