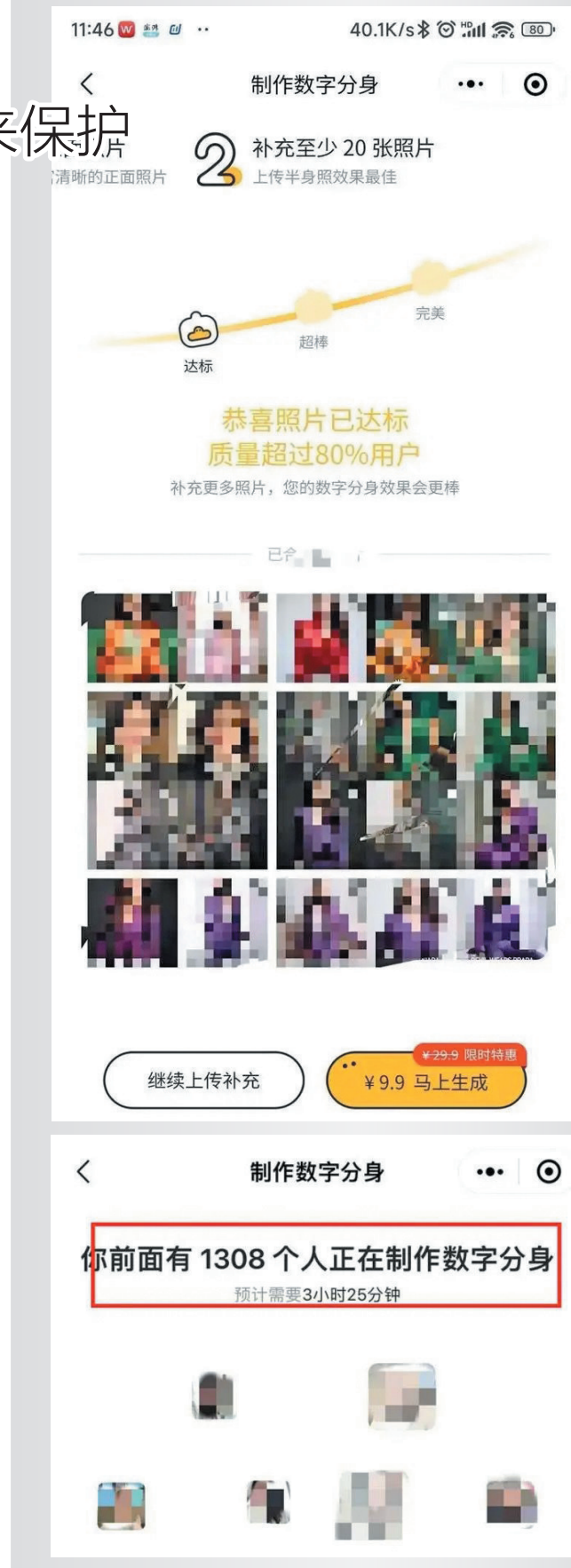
2023.7.26 星期三
责编 薛亮 | 美编 郑宙 | 校对 小缪
江南晚报

9.9元拥有AI写真?

小程序走红背后,用户人脸隐私谁来保护

“制作数字分身,只需上传20张以上包含人脸的合格照片,限时特惠9.9元。”刚刚过去的周末,一个名为“妙鸭相机”的微信小程序火了。为用户打造“专属AI摄影师”,妙鸭相机在其官方公众号如此介绍。数字分身是吸引用户的第一步,之后是选择不同模板,生成写真,最后便是提示用户可以选择付费进行精修写真,用户可以生成一套可媲美天真蓝、海马体的AI写真,并可将图片上传微信朋友圈、微博等社交平台。

据官方介绍,该产品自6月30日开启邀请制内测,背后的AI模型名为“提香”(Tiziano),至今为用户提供了30多个可选择的写真模板。火速蹿红之后,妙鸭相机遭遇“隐私”争议,争议背后,是网民对于个人隐私安全的担忧:用户上传的照片如何处理?应用方是否会将用户照片挪作他用?若上传的照片被用于AI模型训练,用户的一些面部特征是否会被用于生成其他图片?而这些不仅仅是妙鸭相机,也是更多需要上传照片的相机应用所面临的问题。



收费9.9元,数千人排队

看到朋友圈刷屏的“AI写真”后,刘森觉得“效果不错,才9.9元。”她被吸引着登录小程序体验起来。参考流程,上传一张正面照片后,为了效果好,“认认真真选了20张不同角度的照片”,一番操作下来,她得到的提示是“等5个多小时,完成后会通知。”

时隔一晚,刘森才看到生成的不同风格肖像照、艺术照、证件照,“有2套效果还不错”,她选出3张满意的照片发到了朋友圈,配文“9.9元的AI写真,真香。”

近半年来,以ChatGPT为代表的大模型产品甚嚣尘上,国内企业也掀起“百模大战”,在此背景下,妙鸭相机于6月开始内测,打出的口号是“让每个人拥有一个属于自己的AI摄影师”。

打开妙鸭相机小程序,首先需要上传一张正面照片,随后补充至少20张照片,在该步骤,系统会提示照片是否达标,已上传照片的质量超过多少百分比的用户,用户可以选择补充更多照片,让“数字分身”效果更棒。上传照片后,用户需关注妙鸭相机公众号,完成付费流程,标准价是29.9元,限时特惠9.9元,一旦购买成功,不支持退款。

从用户的分享来看,上传照片后,用户可以得到不同风格的写真,如商务写真、时尚海报、证件照、旅游大片等,生成的照片均带有水印,想要下载高清照片或照片原图需支付额外费用。而当记者试用该程序后,发现生成照片预计需要3小时25分钟,前面有1308人。

随着使用用户的增多,等待时间较长被付费用户诟病,用户对需上传21张照片、模板效果不是很好也略有不满。有网友指出在晚上高峰期间,曾碰到4000至5000人排队,等待时间需十几个小时,另有网友表示:“美颜美到不像本人,但又依稀有本人的影子。”

针对网友的声音,妙鸭相机曾在7月17日表示,写真的效果还远没达到团队的理想状态,会继续优化“提香”的能力;妙鸭相机并不是摄影师的敌人,将很快开启对摄影师邀请制的内测合作,通过妙鸭,摄影师可以将自己的风格和审美制作成模板,从而让更多人享受到他们的创意。

用户隐私和数据安全引争议

就在很多用户分享着这份“9.9元带来的快乐”时,也有人担忧“隐私安全问题”,刘森更是在照片生成后产生了顾虑,毕竟此前利用AI换脸进行诈骗的事件频频发生。于是,伴随妙鸭相机产品热度上升,越来越多的用户也对其提出了质疑。

在该产品的原始协议中对AI生成内容有如下描述,用户授予妙鸭相机“在全世界(包括元宇宙等虚拟空间)范围内享有永久的、不可撤销的、可转让的、可转授权的、免费的和非独家的许可”等。

一位业内分析人士看来,本月《生成式人工智能服务管理暂行办法》发出,其中规定“不得非法留存能够推断出用户身份的输入信息,不得根据用户输入信息和使用情况进行画像,不得向他人提供用户输入信息”,而妙鸭相机对AI生成内容的使用协议显然有误。

面对质疑与错误,妙鸭相机于7月20日在其官方公众号发出致歉声明,并对协议内容进行更改,“用户上传的照片只会用于数字分身制作,不会提取也不会用于识别和其他用途,且分身制作完成后自动删除。”

有安全研究员表示,类似AI软件从用户处获得的信息主要是肖像图片,从技术角度而言,它并不比其他上传照片的App有更多风险,但若该类软件向用户索取了更多的肖像使用授权,这意味着用户会暴露更多的风险。看一项应用是否正规,可以从两个方面来看,一是用户上传的照片是否会被存储、存储多久、照片和用户信息在传输和存储过程中,是否存在泄露风险;二是上传的照片是否会被用于AI模型训练。“第一种情况,一旦由于外部攻击或内部不法人员导致泄露,那么用户的照片与相关的用户信息可能流入‘黑产’,被用于针对性的诈骗,或者其他犯罪行为。第二种情况,如果用户的照片在用户不知情的情况下,被用于模型训练,那么用户的一些面部特征可能会出现在其他地方的生成图片中,这可能是用户不希望发生的。”

记者查看妙鸭相机的隐私政策发现,对于储存期限,隐私政策并没有直接给出明确的时间期限,而是“我们只会在达成本政策所述目的所需的期限内保留您的个人信息,除非法律有强制的留存要求”。

一位不愿具名的安全人士向记者表示:“我在使用中发现,首先要上传的图片要求是五官清晰的正面,这几乎是证件照的要求水平,社交媒体上,我们都没有上传过如此高清的照片;其次,未来,AI技术会越来越强大,你不知道以后一张照片会被利用到什么程度。我对这种应用持非常谨慎的态度。”

法律条文

据了解,对于互联网应用在用户隐私保护、用户信息保存方面已有诸多规定。

《中华人民共和国网络安全法》:网络产品、服务具有收集用户信息功能的,其提供者应当向用户明示并取得同意;涉及用户个人信息的,还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

《中华人民共和国个人信息保护法(草案)》:明确个人信息处理者的合规管理和保障个人信息安全等义务,要求其按照规定制定内部管理制度和操作规程,采取相应的安全技术措施,并指定负责人对其个人信息处理活动进行监督。

《中华人民共和国消费者权益保护法》:经营者及其工作人员对收集的消费者个人信息必须严格保密,不得泄露、出售或者非法向他人提供。经营者应当采取技术措施和其他必要措施,确保信息安全,防止消费者个人信息泄露、丢失。

《生成式人工智能服务管理暂行办法》(2023年8月15日起施行):明确生成式人工智能服务提供者应当依法开展预训练、优化训练等训练数据处理活动,使用具有合法来源的数据和基础模型;涉及知识产权的,不得侵害他人依法享有的知识产权;涉及个人信息的,应当取得个人同意或者符合法律、行政法规规定的其他情形。

(澎湃)