9.9元“拍写真”？别随便把“脸”交出去

用户上传一张清晰的正面照，再补充至少20张照片，花费9.9元，就能获得精美的AI写真。近段时间，“妙鸭相机”AI相机小程序引发关注，然而隐私及个人信息安全方面的争议也随之而来。这些AI写真软件的用户协议和隐私协议是怎么规定的？用户的照片素材是否会被用到其他地方？记者就其中的风险问题进行了调查。

部分AI写真软件用户及隐私协议并不规范

“妙鸭相机”走红后，有网友发现，该软件的最初版本用户协议中，用户需授权“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、可授权的、免费的和非独家的许可，使得“妙鸭相机”可以任何形式、在任何媒体或用任何技术（无论现在已知或以后开发）使用用户的内容。

有网友认为，上述条款是“霸王条款”。7月20日，“妙鸭相机”发布声明称，原协议内容有误，已第一时间进行了修改。声明表示，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。

除了“妙鸭相机”，市场上还有一些AI写真软件。记者发现，此类软件一般要求在登录前，勾选“阅读并同意”用户协议和隐私协议，才能继续使用。使用方法通常为上传清晰、无面部遮挡的照片，照片数量要求数张至数十张不等。

部分AI写真软件在用户上传照片时会给用户提供选项，即是否需要“生成完成后删除我上传的照片”。然而，该页面还有一则小提示：保留照片将减少不必要的二次上传的麻烦，也将提高下一次生成的速度，减少排队时间。

上述软件的用户隐私协议提及，用户上传的人物肖像仅被用于数字形象、AI肖像生成服务，且相关数字形象、AI形象生成完毕后将自动删除所上传的内容。另一AI写真软件的隐私协议也写明，该平台仅提供个人AI模型生成的图像信息处理服务，不会提取识别信息，不会用于其他用途。用户可以随时选择在系统上删除上传的信息、不予留存。

记者发现，虽然这些软件制定的用户协议和隐私协议条款看起来较为完备，但有些协议的呈现似乎并不怎么用心，并未注明协议的具体更新时间，甚至还有多处错别字，沟通渠道联系方式（包括邮箱和电话）部分更出现空缺。

律师 软件每次收集敏感信息时都应单独告知

一般情况下，软件的用户协议和隐私协议的条款内容较多，部分用户不会仔细看，实际上其中可能暗含隐私风险。

泰和泰律师事务所律师冯沁涓表示，民法典规定，公民享有肖像权和隐私权等权利。消费者在面对AI写真软件提供方自行制定的提示条款时，要特别注意协议中有关肖像权使用范围、期限和使用方式的约定。“有些协议约定，软件提供方可以在全世界永久使用用户肖像，而无需用户同意。一旦用户签署该协议，意味着软件提供方有权在未经用户同意下使用用户肖像用于其他用途，而用户却不能对此追究软件提供方责任，这可能导致自身肖像被滥用。”冯沁涓说，一些提示条款还会约定软件程序可以随时收集用户行程、声像等信息，用户一旦同意，软件提供方则可以通过程序搜集用户的个人行程、语音等，导致个人隐私泄露。

瑞莱智慧AI治理研究院院长张伟强认为，消费者在软件用户协议上可重点关注以下要点，以防止个人信息被滥用：一是协议应明确收集个人信息的目的、用途。二是是否针对特殊人群进行有效保护。三是个人信息的依法依规回收方式。个人信息处理者应当按照相关法律法规要求，在适用情形下主动删除个人信息，不得非法留存或向他人提供能够识别使用者身份的输入信息和使用记录等。

广东南方福瑞德律师事务所律师梁宇麒表示，此类小程序、APP在收集个人敏感信息时，应明确告知收集个人信息的目的、方式、范围，而且每一次收集时都应单独告知，“并非在用户协议、隐私协议已经约定，以后的收集就不用告知。”梁宇麒称，在实践中要结合具体场景形成规范，才算真正的合规。比如用户每次使用某功能时，软件要提示收集哪些信息或者弹出隐私政策，用户点击确认后再继续使用。

规范 目前已有多部法律规范AI技术使用

现在利用“人脸”进行违法犯罪的情况已不少见，犯罪手段也是花样百出。即使软件提供明确的协议、做好提醒规范，但如何保障用户个人隐私不被泄露，仍令消费者担忧。

梁宇麒说，目前各方对于AI数据处理处于适应的过程，处理细则也需要逐渐完善。“平台应主动提高风险意识，制定数据合规和信息保护的制度，并对制度加以公开，将数据处理的流程明细化、透明化，这样用户才比较放心。”

冯沁涓表示，用户使用这些软件得知被侵犯肖像权、隐私权，往往具有滞后性。这要求软件提供方不断提升用户数据保护技术水平，避免数据信息被窃取；同时加强行业自律，强化员工培训，提高法律意识，避免主动泄露用户数据。“应强化行业监管，对数据类软件企业的数据使用情况进行监督检查。如果侵犯隐私或者公民个人信息达到相对严重情形，已涉嫌犯罪的，应移送公安机关侦查处理。”冯沁涓说。

记者了解到，目前已有多部法律逐步对AI技术的使用进行限制。

今年1月10日施行的《互联网信息服务深度合成管理规定》为包括“AI换脸”在内的深度合成服务划定了“底线”。其中第六条规定，任何组织和个人不得利用深度合成服务制作、复制、发布、传播法律、行政法规禁止的信息，不得利用深度合成服务从事危害国家安全和利益、损害国家形象、侵害社会公共利益、扰乱经济和社会秩序、侵犯他人合法权益等法律、行政法规禁止的活动。

今年7月13日，国家网信办等七部门联合公布，于今年8月15日起施行的《生成式人工智能服务管理暂行办法》会对小程序、平台方起到一定的监管作用。

防范 强化个人信息保护意识，认真阅读隐私政策

AI时代已来，如何才能更好地保证用户的个人隐私安全？

律师彭艳军表示，使用类似软件前要谨慎识别，对于来源不明、假冒的软件、小程序要特别警惕。

梁宇麒提醒，消费者自身应该提高风险意识，尤其是遇到软件平台收集姓名、地址、身份证号码、人脸、指纹等个人信息，一定要认真阅读用户协议和隐私政策，要重点关注“是否已超出本来使用该软件功能需要的范围”，若存在风险，应坚决拒绝使用。

张伟强表示，消费者应着重从两个层面提高个人隐私信息的安全性。一是强化个人信息保护意识，注意关注平台对个人信息收集和处理的全生命周期安全风险。它包括对个人信息的收集、存储、使用等各个环节，消费者应重点关注信息收集是否符合最小必要原则、信息处理是否合法合规、信息使用是否存在泄露风险等关键点。

二是提升反AI欺诈风险认知，高度警惕个人信息被非法平台运用最新AI技术进行滥用风险。深度合成等新技术新应用正在改变信息内容信任链的底层逻辑和复杂程度，信息造假门槛明显降低、欺诈风险明显扩大。

本报综合北京日报客户端、《南方都市报》