“换脸”APP火了！但你知道“丢脸”的后果吗？

近日，一款基于人工智能技术的“换脸”APP走红网络。使用者只要上传自己的高清照片，即可将本人面孔与大量影视片段中的明星面孔置换。既可以自己过明星瘾，又可与心爱偶像“同框”出演，于是大量年轻用户选择将自己的高清照片上传网络，“换脸”娱乐。

记者发现，如此“换脸”，用户面部生物特征信息被盗或失控的“丢脸”风险不小。该款APP用户协议中载明：用户一旦上传自己的照片进行视频“换脸”，将在全球范围内完全免费、不可撤销地将包括人脸照片在内的肖像资料授权给该公司和其关联公司。虽然此后相关企业在舆论压力下，对其用户协议进行了部分修改，但风险依然存在。

一旦“丢脸”，我们将面临哪些风险？漏洞又该如何堵上？

□新华社记者 颜之宏

漫画 朱慧卿

风险一：“丢脸”能导致“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”支付甚至是远程签约等场景也越来越多见。如果用户的“脸”不安全，“钱”也将面临莫大风险。

企业通过用户协议等手段取得的用户面部识别信息面临被泄露风险。据记者了解，今年2月，国内某面部识别公司的数据库发生信息安全事故，数百万条个人信息被泄露；8月，欧洲一家公司发生大规模信息泄露事件，数百万人面部识别信息被泄露……公众面部信息被滥用风险增大。

记者在一些知名网购平台输入“人脸面具”“硅胶头套”等关键词，发现有不少商户出售“人脸头套式面具”，其中一些甚至可以按客户提供照片定制。记者获知，通过3D打印等技术，“人脸面具”可以获得较高仿真度，且面部识别数据越详实、仿真度越高，对以面部识别信息作为密码账户的突破力就越强。此前已有人使用3D打印面具通过某知名网络支付平台面部验证。

“贸然将自己的清晰正面照上传并授权他人进行存储或另作他用，关乎‘钱袋子’安全。”中央财经大学金融法研究所所长黄震认为，目前法律对“AI换脸技术”规范不足，因此保护好自己的面部信息在当下十分必要。他建议，有关部门应加快推广相关技术规范落地应用。

记者从多家已启用人脸识别功能的金融机构处了解到：当前金融机构设置的人脸识别安全等级高于智能手机相关功能，但由于不少交易场景中识别标准并不统一，因此风险仍在。多名专家建议，用户将面部识别设置为财产账户密码时，应同时设置其他验证办法，减小风险。

风险二：“丢脸”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已不少见。记者发现一些网站用“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。另外，记者在QQ群和百度贴吧中以“换脸”和“换脸视频”为关键词检索发现，有不少社交群组打着“技术交流”幌子兜售此类“明星换脸”视频。

知情人告诉记者，除贩卖“换脸”非法音视频产品牟利外，一些不法分子还利用手中掌握的贷款人人脸信息，以此类技术进行非法催收活动，直接侵害贷款人人格权、名誉权，甚至滋生出敲诈勒索等其他严重犯罪活动。

北京师范大学网络法治国际中心执行主任吴沈括认为，AI“换脸”法律风险点多，从现实案例看，名誉侵权是高发问题。尤其是恶意拼接制作侮辱性、污蔑性视图素材或者予以非法传播、利用的，对受害人造成的伤害难以及时发觉且极难有效救济，需要有关部门高度关注、积极预防。他建议，由于该领域技术性强，相关企业众多，规模大小不一，应强化职能部门监管力度，杜绝选择性事后执法，建立全行业全流程公平监管，依法严惩违法违规主体，打造稳定、良性的可预期市场环境。

风险三：“丢脸”能导致“被贷款”

有过网贷申请经历的人对于“点点头”“摇摇头”“张张嘴”之类的动作也许并不陌生。借贷者在录入身份信息后，网贷机构会对申请人进行“活体检测”，以确保放款对象为本人，把关借贷安全。但记者发现，一些基于相关技术的修图APP能够“起死回生”，让静态面部照片模仿生物活体“动”起来。

记者使用一款知名修图软件，载入一张包含人物面孔的照片后使用其“3D塑颜”的功能，图片中的人物便能按记者需要完成“上下点头”和“左右摇头”等“动作”。

在另一款宣传语为“让你的照片活过来”的APP中，只要载入一张包含人物面孔的照片，就可以一键让照片中的人物“开口说话”。记者发现，使用者还能利用该APP决定说话内容，并可对录入声音进行声线处理，调整音色音调，视听感觉十分逼真。

有业内人士告诉记者，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，一旦公众的面部识别信息被不法分子掌握，用这些黑科技“活”过来的面孔，很可能以假乱真，让不知情者“被网贷”背上巨额债务。此前“3·15”晚会上就有人演示用“活”照片成功突破某款手机的“刷脸”登录系统。记者还发现，在苹果和安卓手机商店中有不少利用AI“换脸”类APP供人挑选。

中国信息安全研究院副院长左晓栋认为，随着AI“换脸”使用场景更丰富，行业和监管部门应当研发相应的“反换脸”检测技术，来筛选相关视频是否由“换脸术”完成。他建议，要加快建立人工智能算法的安全评估制度，对不同场景下AI“换脸”技术进行评估，解决相关技术滥用问题。