换脸应用：“狂欢”背后的隐忧

有趣的“换脸”App 看似免费，却在暗地里标注了价格。

文 | 范舫诚　廖哲文

2021 年 5 月 7 日，一款名为“Faceapp”的软件登上了苹果应用商店 App Store 免费榜第一名，并且在之后的几天持续“霸榜”，而它的开发者，是一个来自杭州、名不见经传的科技公司。这款换脸应用与 2017 年俄罗斯无限实验室推出的爆款 FaceApp 宛如孪生，仅是名称里有一个字母的大小写不同。2019 年 7 月流行的“变老滤镜”让 FaceApp 的全球下载量累计

脸在人际信息传递过程中起着至关重要的作用，脸部替换就意味着身份的篡改和虚假的信息，出现了“眼见未必为实”的情况。

超过 1 亿次，2020 年 6 月流行的“变性滤镜”，又让 FaceApp 重新爆红。

近年来 AI 换脸软件层出不穷，制造了许多“刷屏级”软件。从 ZAO 到 Avatarify 再到如今的“Faceapp”，换脸“狂欢”并没有退热的迹象，而其背后的 AI 技术，则受到越来越多的关注。

爆红换脸

“AI 换脸”，也称为深度伪造技术，其本质是一种基于人工智能的人体图像合成技术。回归技术本源，实现 AI 换脸的基础技术之一，正是人脸识别技术。人脸识别，是一种生物工程，基于人类面部特征捕捉一幅类似于相机捕获的表情的图像或影像，这些影像会被自动识别与追踪，进而对检测到的人脸进行脸部识别的一系列相关技术，通常也被称为人像识别、面部识别。

换脸技术在美国好莱坞已经存在并应用了 20 多年。在电影《速度与激情 7》中，演员保罗·沃克因车祸意外逝世，剧组利用了换脸技术对其进行面部捕捉，然后用 CG 技术将保罗的脸嫁接到另一位演员面部，使得作品得以完成。可这并不代表 AI 换脸技术就可以被广泛地应用于电影领域，因为 AI 换脸的技术难度大、成本高，并且演员的表演技巧和真情流露都是不能被人工智能完美复刻的，因而其并未在消费级产品中广泛使用。

近年来，GPU 算力的巨大增长使得 AI 换脸技术被推向更广阔的市场，深度学习算法和生成对抗网络算法开始得到广泛应用，进而使得图像处理相关的 AI 技术得到了迅猛发展。

目前的换脸方式可以分为两类：一类是基于面部特征点映射的表情转换，代表性的技术是 Face2Face 和 FaceSwap，这种技术允许实时地将一个人脸换上另一个人的表情，典型的应用是“合成奥巴马”；另一类换脸技术基于学习的方法，代表性技术是 DeepFakes。DeepFakes 采用深度学习的方法，需要较长的训练时间，但替代的效果较好，其制作的 FakeAPP 应用程序图形界面简单易用，可以使用家用级的 CPU 和显卡制作换脸的视频，且经过参数优化后，视频整体的一致性非常高，达到了人眼难以识别的程度。

2018 年 1 月，使用 DeepFakes 技术的简易版 AI 换脸工具 FakeAPP 正式上线。2019 年，ZAO 突然火遍中文互联网，而它们盛行风靡的原因正是因为这个软件可以将视频中的人脸，通过 AI 算法换成另一个人的相貌。用户只需要把照片上传，就能够将相应的脸嵌入心仪的视频中，可以说是“傻瓜操作带来了惊艳的效果”。简单来说，DeepFakes 技术的开源为 AI 换脸视频的流行打下了基础，FakeAPP 的诞生则让 AI 换脸视频成为真正意义上的爆款。而 ZAO 的出现，将 AI 换脸视频的风行推到一个新的高度，此后类似软件才开始如雨后春笋般生长。

在 AI 换脸软件大行其道、全民狂欢的当下，人们开始了对于其侵犯隐私权、肖像权的担忧与讨论。以俄罗斯公司开发的 FaceApp 为例，其在流行的同时，也曝光出了不小的隐私问题。FaceApp 的问题当然并不只有面部信息这么简单，在 FaceApp 的隐私政策里清楚也写着，该应用会获取你的位置信息、IP 地址和日志文件等信息，以便定位目标广告。有了这些数据，FaceApp 的广告客户就能够对特定区域用户投放广告。而该应用的服务条款内容中的规定，也明确了其在为你“服务”的过程中，也能够将你的数据卖得一干二净。

技术风险

脸在人际信息传递过程中起着至关重要的作用，脸部替换就意味着身份的篡改和虚假的

信息，出现了“眼见未必为实”的情况。面部信息作为自然人最重要的生物识别信息，一旦被他人非法使用，损失难以估量。人脸识别技术作为目前市场上商用程度最高的生物识别技术之一，遭受了不少质疑。

对于换脸视频，支付宝安全中心曾在 2019 年作出回应，由于目前金融识别采用的多是三维人脸识别技术，即通过现实人物的动作来多点面地采集识别信息，因此基本不可能被换脸视频突破。

然而随着时间的推演，AI 换脸技术也迎来新的进步，即便是金融级别的人脸识别，也很有可能失手。2020 年年初，浙江衢州抓获一个犯罪团伙，他们运用技术手段骗过某平台人脸识别认证，并使用公民个人信息注册某平台账户，非法获利数万元。值得注意的是，该案件中犯罪嫌疑人使用的技术正是利用 AI 换脸技术，最终成功地欺骗了人脸识别系统。

换脸技术带来的种种风险，本质上是“生物识别信息”的安全问题。生物识别信息，顾名思义，即基于人体固有的生理特性（如指纹、脸像、虹膜等）和行为特征（如笔迹、声音、步态等），可用于个人身份识别和鉴定的信息。显然，个人信息不仅包括传统意义上的姓名、住址、电话、工作单位等物理信息，还包括人脸识别、虹膜技术、指纹、DNA 等个人生物信息。

在金融科技领域，特别是互联网及移动支付等安全验证的过程中，以面部特征、指纹为生物特征的识别技术已经成为重要的验证方式之一，刷脸支付、人脸打卡、视频开户等使用面目特征的各种手机 App 及现实生活场景的应用越发普及，背后的人脸信息泄露、人脸图像滥用、AI 换脸等现象和黑色产业链日渐浮出水面。由全国信息安全标准化技术委员会等成立的 App 专项治理工作组发布的《人脸识别应用公众调查报告 2020》称，有九成受访者使用过人脸识别，其中六成受访者认为人脸识别有滥用趋势，三成受访者表示个人隐私或财产安全已经因此遭受损失。

监管约束

维护相关使用者权益，要从市场监管入手，条款规范则是市场监管的重中之重。还要利用好现行法律，对敢于顶风作案的黑色产业及灰色软件开发公司做出从重处罚、给出典型判例，给行业树立规范和典型，对不法分子形成威慑，使得技术用在正道。

同时，还需要建立严格的行业规范来应对风险。各运营方、技术开发方不能独自成为技术孤岛，只求技术更迭，不注重隐私风险。全行业都需要接受更严格的行业规范和法律监管。其实我国的相关法律法规已经做出规定，参照《民法典》，收集自然人信息应当遵循“告知——同意”原则，征得该自然人的同意，且被采集者也有权撤回。而正在面向社会公开征求意见的《中华人民共和国信息保护法（草案）》提出，在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必须，遵守国家有关规定，并设置显著的提示标识。

AI 应用的数据隐私问题尤其值得警惕，AI 换脸技术作为一项利弊兼具的双刃剑，在为公众带来深度娱乐、为金融行业带来革新便利的同时也带来了诸多安全隐患。为此，行业需要应用开发方、运营方、相关监管部门各司其职，跟上 AI 技术攻防战的步伐，使 AI 换脸技术在法律、道德、技术的多重约束下合理应用，造福人类。

（作者分别系厚朴投资管理有限公司高级投资经理、中国科学院大学经济与管理学院博士研究生）