你的“脸”安全吗？

“刷脸”真的靠谱吗？

面部识别技术越来越先进，并不断渗透我们的日常生活。一些人乐观地认为，“刷脸”时代正在向我们走来。可是，“刷脸”真的靠谱吗？例如刷脸支付设备能否识别双胞胎、或者非真人的照片和视频呢？会否泄漏隐私？

准确度还有欠缺

人脸识别的准确率究竟有多高？香港中文大学教授杨晓鸥曾经给出过一组数据：计算机识别人脸的准确率可达 99.15% ，而肉眼识别的准确率大概在 97.52% 。在美国，有机构使用亚马逊公司的面部识别系统扫描了535名国会议员的面部照片，并与相关数据库中的2.5万张罪犯照片比对，结果28名议员被系统识别为罪犯。

英国多个城市的警方开始试应用面部识别技术。但其公布的有关数据显示，伦敦警方使用的面部识别系统错误率高达98%，被批评为“几乎完全不准确”。伦敦警察局局长克雷茜达·迪克对此辩护说，她不认为这项技术会带来大量逮捕行动，但公众“期待”执法机构测试使用面部识别技术。

英国警方曾将面部识别技术应用在音乐会、节日庆典或足球赛等场合。据英国媒体报道，在威尔士加的夫举行的2017年欧洲冠军联赛决赛中，警方使用的面部识别系统产生2400多次匹配，其中2200多次是“假阳性”匹配，即把普通人错认为犯罪嫌疑人。

美国麻省理工学院“媒体实验室”研究人员测试了微软、IBM（国际商用机器）和中国旷视科技3家公司的面部识别系统，让3个系统判断1270张图片中人物的性别。结果显示，3个系统对肤色较浅男性的判断错误率都低于1%，识别效果较好；但对肤色较深女性的判断错误率从21%到35%不等，识别效果差。

但总体来说计算机的人脸识别能力是远胜于人脑的，无论是发型变化、常规化妆、胖瘦变化，甚至微整形、长相相似等情况，计算机都能准确识别。

不过，对于长相酷似的双胞胎、多胞胎，以及整容后判若两人的情况，人脸识别可能会失效。但是随着技术的发展，未来在刷脸的使用场景中会逐渐增加指纹、掌纹、虹膜、声纹等生物特征作为辅助密码。

训练数据不理想

对于“媒体实验室”的研究，IBM公司沃森和云平台业务首席架构师鲁奇尔·普里说，人工智能系统深度学习的有效性有赖于训练的基础数据。即使人工智能模型本身设计优异，不理想的训练数据只能导致高错误率及带有偏见的判断。曾有研究显示，在美国广泛使用的一套面部识别系统训练数据中，超过75%的图像为男性，超过80%的人为白人。

英国《自然》杂志在近期一篇评论文章中也指出，无论在学术界还是产业界，开发出复杂算法会广受赞誉，但相对而言，很少有人关注数据如何收集、处理和归类。导致人工智能产生偏见的一个主要因素，就是训练所使用的数据质量不佳。

麻省理工学院人工智能研究人员乔纳森·弗兰克尔认为，很多用于面部识别的图片质量不佳，尤其是那些街头监控摄像头拍下的图片，也是导致面部识别技术在实际应用上经常出错的一个重要原因。

忧心隐私安全

除本身存在技术问题，面部识别大量使用还引发了对个人隐私的担忧。对于用户而言，个人信息安全同样重要，很多人在刷脸时也许会思考“刷脸时我的照片被谁看到了？”美国乔治敦大学法律中心一份关于技术与隐私的报告显示，美国目前有16个州允许美国联邦调查局使用面部识别技术，将犯罪嫌疑人照片与相关数据库中的驾照照片进行比对。

美国数字化权利保护组织电子前沿基金会的詹妮弗·林奇说，很多人并不同意警方在寻找罪犯时比对自己的照片，他们并不知道州政府有这种政策。

出于对隐私和安全的担忧，一些人甚至研制推出了反监测装备。德国人亚当·哈维曾在德国混沌通信大会上介绍了自己研制的“假面”产品，比如在衣服上绘制起迷惑效果的图案，让面部识别系统难以识别真实的脸。

怎样规避可能存在的风险？

尽管“刷脸”技术给人类生活带来很多便捷，但其中暗藏的一些风险也需要我们引起足够的重视。

在网上不要轻易刷脸

“在网上不要轻易‘刷脸’！”网络安全专家提醒大家，尽量不要在网络上使用人脸识别技术，作为唯一的认证方法。

作为人的生物特征，人脸数据是具有唯一性的，一旦丢失便不可再生。而任何一个数据进入到计算机后，都会变成计算机代码，就可能会被截获、被重构、被重放，一旦这些数据被还原，并被黑客等犯罪分子拿到以后，你唯一的身份数据就丢失了，而且永远没办法再生，因此风险很大。

为了降低使用风险，每种技术都应该用在恰当的地方，而人脸识别这种技术，并不适合在互联网和网络支付上，作为唯一的认证方法，这是非常不安全的。专家表示，我们在大脑里设个密码，如果忘了可以改，如果是银行发的动态密码器、U盾等产品，你丢了也可以去换个新的，但是作为生物特征的人脸，却是具有唯一性的。

任何一种新技术，都要在相应的场景使用，才是最合适的。专家认为生物认证技术也是未来的一种发展趋势，但它的使用范围，应该如何使用它，应该是有限制的，不能一味地滥用。

制定个人生物信息安全规范

“生物信息安全是一个庞大的领域，个人生物信息保护是这个领域亟待解决的问题。”有学者提出，目前，个人生物信息的法律保护面临着三个问题：一是个人生物信息权作为具有人格权属性的私权，尚未明确纳入私法保护范围；二是针对个人生物信息在刑事侦查、治安管理、人口治理、医疗卫生等领域的非商业应用，以及政府和相关机构的责权利，特别是个人生物信息权保护边界等急需明确；三是针对个人生物信息商业应用和相关产业侵权风险及不正当竞争，目前缺乏相应的特殊规制，法律救济、行政处罚也无法律依据。

对此，可以立法进一步规范相关内容，诸如虹膜和面部识别的技术可以在什么范围内使用，以及如何使用，包括授权和使用者的等级，都需要在立法中详细规定。这些方面已经零散地体现《民法总则》《网络安全法》等司法解释和规定中，但是并未形成完整体系。2018年5月1日《信息安全技术个人信息安全规范》（GB/T 35273-2017）实施，可以比照这个规范来制定个人生物信息安全规范，或者补充和修改这一法律，把个人生物信息安全作为一个独立的章节加入到《信息安全技术个人信息安全规范》中。

□ 记者 吴承江 整理自新华社、《经济日报》等