商场天花板上探头密布 识别芯片公开买卖

人脸识别时代 谁来保护我的脸

据《北京晚报》报道，从上班打卡的考勤门禁，到回家开门的智能门锁，再到售卖日用品的便利店……随着科技发展，越来越多的生活场景正用上人脸识别技术。

记者调查发现，目前大量物联网设备用上了基于AI的人脸识别技术，价格低廉的人脸识别芯片、高清摄像头模组等硬件也纷纷涌入市场，大有泛滥之嫌。对此，安全专家呼吁，生物识别是个人信息安全最后一道防线，行业亟待划出法律准入红线，避免厂家以“新科技”为噱头，过度使用人脸识别，引发系统安全风险。

（本版均为资料图片）

【市场乱象】 上班考勤、逛商场统统“被刷脸”

“最近公司换了新的门禁系统，上班进公司从刷指纹变成了刷脸。”在北京望京上班的白女士表示，公司的这套门禁系统拥有无感人脸防假功能，用照片或者视频来验证人脸都没用，“明显感觉科技正在渗入生活方方面面”。

记者注意到，除了人脸识别门禁，目前北京一些写字楼里还用上了人脸识别考勤摄像头，在出入口区域，人员无须停留，就能自动开关办公室玻璃门，后台系统也能无感监测员工的考勤情况。

不断更新迭代的智能门锁，也用上了人脸识别功能。在居然之家北四环店，记者看到德施曼、三星等各种品牌的智能门锁都支持人脸识别解锁功能。“用人脸识别刷脸进门多方便，不用掏钥匙，也不用输密码。”一位销售人员大力推荐。不过，对于这些智能门锁在人脸识别上的安全性，销售人员仅简单回应称：“大品牌自然有保证。”

一些商场、便利店也装上了人脸识别高清摄像头用于人脸抓拍，方便做客流分析。“相比传统的红外线客流监测，人脸识别摄像头可以去重统计访客数，更加精准，还能分析客户群的性别、年龄，记录会员个人信息和历史到访时间点，方便做新老客户管理。”一位卖家告诉记者，目前在珠宝店I DO、努比亚门店、华为门店等都有基于人脸识别摄像头的会员管理系统。

【潜在问题】 低价人脸识别芯片公开售卖

尽管接入人脸识别功能的物联网设备各式各样，但原理大都相同：安装了人脸识别芯片和高清摄像头模组。记者在调查中发现，目前价格低廉的人脸识别芯片在电商网站上大量销售。“超清人脸识别芯片，如果是工业级别的星光级低照度，价格是399元。”京东上某电脑办公专营店的客服对记者表示，星光级夜视是指夜间无任何辅助光源也能实现清晰的彩色监控，“芯片采用USB接口，免驱动即插即用，最远可捕捉50米”。

除了即插即用的USB接口芯片，记者发现，还有大量可定制的芯片模组在电商平台上售卖，价格十分低廉，几十到几百元就能买到。

“300万高清像素的人脸识别摄像头模组只要38元，支持高速摄像，适用于监控设备、智能家居可视门铃、考勤机等设备。”某微视电子的淘宝客服告诉记者，目前市面上有不少硬件厂商和自己的代工厂都有合作，批量购买价格更低。“30万像素、100万像素、200万像素、500万像素乃至800万像素的摄像头芯片模组都有。放到各类智能设备里内置即可，可定做，也都支持二次开发。”

采集人脸信息，涉及隐私安全，这样的芯片模组真的能公开售卖吗？记者了解到，目前在法律层面上并无相关管理规定。此外，芯片研发也无明确准入门槛。相反，业内为了降低计算机视觉技术准入门槛，不少公司决定主动开放视觉人工智能开放平台。“目前虹软的视觉人工智能开放平台完全免费，没有使用限制和使用约束条例，新增了活体监测、人证比对等全面升级的人脸识别软件开发工具包。”虹软副总裁祝丽蓉介绍。

【最新变化】 人脸信息收集越来越隐蔽

“原来商场、专卖店等门口的摄像头，不仅是用于防盗监控，还能收集人脸信息，用来分析会员的各种信息？”记者随机向四位市民出示了连接摄像头的商场人脸识别分析软件，被访市民均表示十分惊讶。“我以为只有刷脸支付、刷脸解锁等APP才会采集人脸信息，完全不知道店铺天花板装的摄像头也能做到。”市民张先生感慨。

“对于集中在金融领域、安防领域的人脸识别应用，安全部门有明确提示，用户有很强烈的感知，也有自我保护意识。但目前人脸识别正从有感知收集趋于无感知收集。”在2019互联网安全与刑事法制高峰论坛上，腾讯安全管理部资深技术专家石追对记者表示，这种无感知的人脸收集是目前人脸识别技术未来最大的隐形威胁之一。

记者了解到，人脸识别的重大安全隐患之一是深度伪造人脸以假乱真。而深度伪造人脸的重要前提是对被伪造者的人脸信息多方位收集。“深度伪造人脸需要大量的人脸进行训练，这很难通过APP拍照大规模搜集，也很难伪造得十分逼真，而家用高清摄像头、长时间在线的智能家居、智能门锁等，可以在用户无感知的情况下收集到大量人脸样本，具有全方位采集人脸的能力。”石追表示，随着5G时代到来，各类智能设备可以万物互联，隐秘采集信息这一趋势将更加明显。

“人脸识别实际上是人工智能的应用之一。”一名业内专家告诉记者，人脸识别过去是数学难题，但随着越来越多开源人脸识别库的出现，比如opencv、face_recognition等，使得这一技术不再是工程师才能解决的难题，应用得到了极大简化，“很多大专生培训一两个月，也能熟练操作这一技术”。

【专家呼吁】 要守住个人信息安全最后防线

“如果一个密码被用于验证多个APP登录，这个密码的安全性将大大降低。同样，如果人脸采集与识别技术被无门槛泛滥使用，人脸识别的安全性也面临极大挑战。”石追告诉记者，“人脸、虹膜等生物特征很难匿名化，发现通用密码在其中一个APP被泄露，还能尽量更改其他APP的密码进行弥补，但人脸信息如果出现被滥采或泄露，对整个物联网、APP甚至金融安全都是灾难。因此，人脸等用户生物信息是个人信息安全一定不能出问题的最后一道防线。”

专家们对人脸识别滥用导致的安全担忧并非空穴来风。今年2月，提供人脸检测和人群分析服务的深圳深网视界因人脸识别数据库缺乏密码保护，导致大规模的数据泄露。据称，该数据库包含了超过256万用户的记录，包括身份证号码、地址、出生日期、照片、工作单位、能识别用户身份的位置信息等高度敏感的隐私信息。

石追表示，随着科技不断发展，技术试错的成本也在不断攀升，建议行业要有自律，不能为突出产品的“智能化”，而过度使用人脸识别技术。“一定要对生物特征信息的运用场景加以区分，在可使用密码、刷卡等方式替代的场景，应有所节制。办法总比问题多，整个行业亟待法律划出准入红线。”他表示。

（袁璐）

【他山之石】 美国旧金山推出人脸识别禁令

事实上，全球已经有不少国家行动起来规范人脸识别技术的使用，保护个人的通用隐私数据。

今年5月，美国旧金山成为全球首个推出人脸识别禁令的城市，禁止该市所有单位使用人脸识别技术。欧洲也已开始考虑对人脸识别等人工智能（AI）技术进行立法，限制公司和公共机构“不加区分地使用人脸识别技术”。今年8月，瑞典数据监管机构则对当地一所高中开出第一张基于欧盟《通用数据保护条例》（GDPR）的罚单，金额为20万瑞典克朗（约合人民币14.8万元），理由是该校使用人脸识别系统记录学生的出勤率。