人脸识别有哪些风险？

随着技术的发展，人脸识别已经达到可实用的精度，成为便捷的身份认证工具，广泛应用在高铁安检、小区入户、银行取款，手机转账等各个场景。然而，人脸识别也存在很高的风险，需要提高警惕。

首先，人脸直接暴露在外，极易取得，仿冒风险很高。虽然通过一些技术措施可以降低这一风险（如通过眨眼、转头等动作进行活体检测或与手机验证码结合进行多重校验），但是因为目标样本获取容易，识别系统很容易被仿冒攻击。

第二，人脸可能是最重要的个人信息之一，如果发生大规模泄露事故，可能产生非常恶劣的影响。例如，犯罪份子拿到受害人的人脸照片后，可以方便跟踪，甚至合成各种虚假视频，进行诈骗或勒索。

第三，人脸识别系统被不当利用或被黑客攻击，可能泄露个人行踪，暴露个人隐私。最近，源自美国纽约的“抵制扫描（Ban the Scan）”行动形成声势浩大的反人脸识别浪潮[1]。该行动的网站声称，人脸识别技术正在用来被跟踪和记录每个公民的行为，严重侵犯了公民的自由。同时，人脸识别还有可能对有色人种产生更高的误识别率，间接导致了种族歧视。

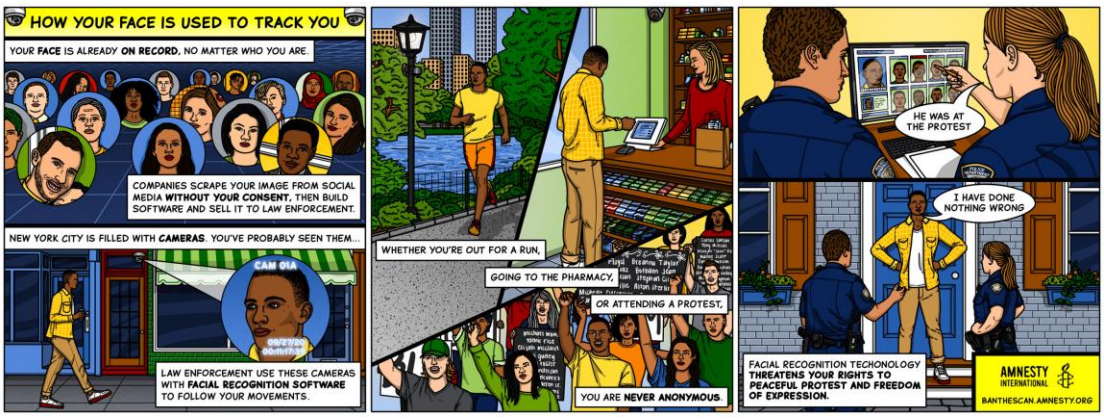

图 1：“抵制扫描”行动认为无所不在的摄像头侵犯了公民权利。

事实上，不论哪种物生认证技术，仿冒、信息泄露和隐私侵犯都是需要谨慎对待的问题，只不过人脸信息太过直接，因此更加敏感。意识到问题的严重性，世界各国都在对人脸识别的使用进行规范，确保人脸信息在采集和使用过程中的合规性；另一方面，人们也在研究低隐私的身份认证方案，如声纹识别、指静脉识别等。不论如何，人们越来越意识到生物信息是一种公共资源，必须交由公共权力机关来统一管理。可以想见，未来对影像的采集会更加严格，在便利店里随意架设摄像头的日子可能要一去不复返了。

[1]https://banthescan.amnesty.org/