

“国标”来了“刷脸”的技术边界在哪里?

4月23日,《信息安全技术 人脸识别数据安全要求》国家标准(以下简称“国标”)的征求意见稿的面向社会公开征求意见。

人脸识别是近年来的热议话题,现实中未告知情况下获取人脸识别数据、“强制”人脸识别等乱象时有发生。此次拟出台的国标主要为解决人脸数据滥采、泄露或丢失,以及过度存储、使用等问题,对于《个人信息保护法》草案中人脸识别相关的规定也有一定的体现和细化。

需示同意 只用于身份识别

编制说明指出,人脸识别在金融、交通、人社、医疗等各行业均得到广泛的落地应用,创造了巨大的社会以及经济价值。但同时,人脸识别信息不易改变,一旦丢失可能永远失去,是个人敏感信息的一种。“由于相关标准规范缺失,人脸识别数据滥采、存储,使方面没有明确的安全要求,造成安全防护措施薄弱,未经用户明确授权或超范围使用人脸信息的情况普遍存在挑战。”

因此,国标的制定主要为解决人脸数据滥采、泄露或丢失,以及过度存储、使用等问题,适用于数据控制者安全开展人脸识别相关业务。

事实上,人脸识别一直是社会关注而热议的话题,人脸识别数据被违规采

“丢脸”会遭遇多大的安全风险?

是否会因此流失呢?负责崇庆里小区加装电梯的销售经理林根义告诉记者,市场上提供人脸识别功能的设备,比如电梯,以本地化储存数据为主:“用户信息都存储在当前的人脸识别设备中,有可能在前期信息采集环节泄露,但这种情况比较有限。”

低风险不等于零风险

不论是政府参与,还是引入第三方公司,人脸信息似乎都处于不易流失的低风险状态,我们是否可以放松警惕呢?

比起背后稍显遥远的风险,人们通常更在意眼前的方便。有人出于无奈:“刷脸场景如此普遍,想回避也不可能。”有人怀着无畏之心:“我不做亏心事,不怕被拍。”更多人则是抱着从众心理:“大家都在用,怎么会正好就是我的信息泄露呢?”

然而,低风险并不意味着零风险。

金卫清告诉记者,小区改造的过程中,有极少数人拒绝提交自己的头像和信息,转而选择磁卡、手机等其他开门方式:“确实有一些业主担心自己的隐私权被侵犯,但这部分人很少。”

国内“人脸识别第一案”主诉人郭兵就是这样的少数派。2019年10月,他将强制游客刷脸的杭州野生动物世界告上法庭。该案被视为国内消费者起诉商家的“人脸识别第一案”,郭兵因此成为舆论的焦点。然而鲜有人知的是,该案仍在审理时,他与其他人脸识别滥用的“死磕”又开始了。2020年8月,郭兵所在的杭州市钱塘区白杨街道某社区业主群中弹出一条消息,要求业主带上身份证去物业录入个人信息,以尽快使用小区门口的人脸识别系统。

作为浙江理工大学的特聘副教授,郭兵近年来主要从事网络安全、个人信息

集及滥用的情况曾被多次曝出。如在售楼处安装人脸识别系统,今年的“3·15”晚会上揭露的多家商户在未告知或征得同意的情况下,通过人脸识别系统偷偷获取客户的人脸识别信息等。

《个人信息保护法》草案第27条规定:“对人脸识别进行专门规定,要求在公共场所安装图像采集、个人信息识别设备,应当为维护公共安全所必需,遵守国家有关规定,并设置显著的提示标识。所收集的个人图像、个人信息特征信息只能用于维护公共安全的目的,不得公开或者向他人提供;取得个人单独同意或者法律、行政法规另有规定的除外。”

国标针对于上述乱象做出了一定回应,同时对于《个人信息保护法》草案中的相关规定也有体现和细化。

如,国标要求收集人脸识别数据时,应向数据主体告知收集目的、数据类型和数量、处理方式、存储时间等规则,并征得数据主体的明示同意。只有在非人脸识别方式安全性或便捷性显著低于人脸识别方式(如机场、火车站进行人证比对等)情况下,方可开展人脸验证或人脸识别;人脸识别数据不应用于除身份识别之外的其他目的,如评估或预测数据主体工作表现、经济状况、健康状况、偏好、兴趣等情况。

此外,国标规定在公共场合收集人脸识别数据时,应设置数据主体主动配合的数据主体选择使用,不应因数据

主体不同意收集人脸识别数据而拒绝数据主体使用基本业务功能等。

即使数据主体授权了人脸识别,依据国标规定,仍能在明示停止使用功能、服务,或撤回授权等情况下,要求数据控制者删除人脸识别数据或进行匿名化处理。人脸识别数据原则上不应共享、转让,若因业务确需如此,则应按照相关法律规定开展安全评估,并单独告知数据主体共享或转让的目的,按双方身份、接收方数据安全能力、数据类别,可能产生的影响等信息,征得数据主体的书面授权。

而针对人脸图像,国标要求应在完成验证或辨识后立即删除,如果开发商希望存储人脸图像,同样要经过数据主体单独书面授权同意。

值得注意的是,国标中还特别提到了“原则上不应用人脸识别方式对不满十四周岁的未成年人进行身份识别”。

此前,为防止未成年人沉迷游戏,应部分政协委员、人大代表及家长的呼吁,游戏厂商拟引入人脸识别验证,然而随着未成年人个人信息保护日趋重要,这些举措的实施也将变得困难。

对此,浙江大学光华法学院互联网法律研究中心主任高艳东曾建议企业进行更多创新,从心理成熟度方向出发,在游戏准入阶段设计相应“测试”,在区别是否心智成熟的同时,加强未成年人的成就感与自我约束”。(张雅婷 郭美婷)



息保护领域的研究,对于物业强制搜集数据的做法本能地感到不安。他去物业和社区交涉,拒绝提供信息,并提出诸多人脸识别存在的安全和法律风险。谁料两个月后,他偶然发现,自己几年前办理门禁卡时拍摄的照片未经同意已被物业递交给第三方公司。大门开启只需花几秒钟,但担心数据泄露带来的焦虑感,已在郭兵心里持续了一年。

这份焦虑与越来越多的犯罪活动转移到线上有关。网络犯罪案件量及占比这几年呈逐年上升趋势,其中“和“丢脸”相关的案子也是越来越多。据郭兵所知,目前已有一些人脸信息泄露案件与百姓的日常生活息息相关。2018年8月,浙江一个犯罪团伙通过软件将非法购买的公民证件照制作成3D头像,“骗”过支付宝的人脸认证技术,非法获利4万余元,被查扣的个人信息近两千万条;

(钱弘慧)

“护脸计划”启动 可信人脸识别行业标准呼之欲出

日前,中国信息通信研究院云计算与大数据研究所发起的“可信人脸识别守护计划”(以下简称“护脸计划”)正式启动。

针对“护脸计划”的启动背景,云计算与大数据研究所所长何宝宏表示,近年来人脸识别技术落地势头迅猛,被广泛应用于公共安全、金融支付、交通出行等领域,落地应用过程中,也暴露出侵犯隐私、安全风险、过度收集等问题,屡屡成为社会焦点。之所以倡议发起“护脸计划”,是希望站在产业的视角,通过标准制定、测试评估、行业自律、威胁共治等手段,有效回应用户的信任问题,增进行业和社会共识,促进产业链健康发展。

“护脸计划”联络人石霖告诉记者,“护脸计划”已形成《可信人脸识别操作指引》草稿,近期通过广泛征集行业意见以及内部研讨后,不久后将推出正式版指引(标准),为人脸识别技术产业链的运营企业提供参考依据。

为人脸识别技术“正名”

有目共睹,人脸识别使用在社会及

个人生活中越来越普及,由此公众对技术滥用、信息泄露的担忧与恐慌也与日俱增。无论是居民社区“刷脸”门禁、售楼处的人脸识别摄像头,还是号称“中国人脸识别第一案”的郭兵诉杭州野生动物园一案,都引发了广泛的社会关注与讨论,今年央视“3·15”晚会还曝光了人脸识别摄像头滥用,海量人脸信息被违规收集存储,作为设备及技术服务商的苏州万店掌、上海悠客、广州雅量、厦门端为等公司更是被推上舆论的风口浪尖,一时之间,商业零售品牌“人人自危”。

根据公开介绍,“护脸计划”主要工作内容集中在四个方面,一是制定人脸识别技术与应用的可信标准,二是开展人脸识别测试评估并发布结果,积极回应社会关切,三是跟踪监测人脸识别安全、信任问题,成员间共享威胁情报,四是举办产业交流活动。

目前,“护脸计划”已形成了《可信人脸识别操作指引》草稿,目前推进的思路是梳理人脸识别应用核心问题,提炼关键要素,打造人脸识别的可信范式,推动产业健康发展。简单来说,在可信AI操作指引的基础上,针对人脸应用就可靠可控、保护隐私、明确责任、多元包容、透明可释这五个原则进行细化,其中“明确责任”指要明确产业链参与主体的责任,同时明确保险机制,“多元包容”是指产品需求多样化,比如老年人群的智能化需求也要考虑到。

除此之外,2020年10月21日,全国人大公布了《个人信息保护法(草案)》,更细化地明确了公共场所安装图像采集、个人信息识别设备的用途限制。目前该草案仍在立法推进过程中,对于提升全社会对包括人脸在内的个人信息的

安全感具有深远而重要的意义。与此同时,杭州、天津等多地的法律法规也不同程度地明晰部分适用主体使用人脸识别信息应用的边界与限制。这些信号表明,人脸识别技术普及应用的“配套”法律法规也在逐步完善优化。

在法律法规不断明确底线和原则的同时,应用层面“颗粒”场景中的行业性自律、技术应用标准也在不断地跟进,“护脸计划”便是典型的代表。

“绝大部分的运营主体,当使用了人脸识别技术及相关设备后,事实上其业务层面已经没有办法退回原点了,因为相应的业务量一旦实现了增长,甚至一些业务的商业逻辑也发生了改变,服务的消费者、企业客户往往已经形成了使用习惯,在这种情况下,退不回去只能往前走,那怎么走呢?在这个时候,我们需要通过行业自律、安全保护联盟

新技术绝非法外之地

五项基本原则

五项基本原则

五项基本原则

五项基本原则

五项基本原则