

收集主体多、安全保障弱、亟须强立法——

谁来保护我们的生物特征信息？

近日,杭州野生动物园规定,不录入人脸信息将影响该公园年卡正常使用,引起社会关注。

当前,公民的指纹、面部特征等生物特征信息是否面临被过度采集的风险?哪些主体正在获取我们的生物特征信息?相关信息保护在哪些方面亟须补强?记者就此展开调查。

公众生物特征信息屡遭过度收集

记者从北京大学法学院副院长薛军教授处了解到,当前,人脸、指纹等个人生物特征信息已经成为身份证号码、手机号码等信息之外,过度搜集公民信息案件中新的“重灾区”。

同时,由于生物特征信息与个人财产、人格权益之间的联系日趋紧密,信息一旦丢失或失控,将给信息所有者造成巨大且难以挽回的损失。

这并非杞人忧天。2019年2月深圳某人脸识别企业被证实发生数据泄露事件,超过250万人的核心数据可被获取,680万条记录泄露,其中包括身份证信息、人脸识别图像及GPS位置记录等。

一些软件也涉嫌过度采集用户的生物特征信息。此前,中国消费者协会曾发布《100款App个人信息收集与隐私政策测评报告》。报告显示测评的100款App中,10款App涉嫌过度收集个人生物特征信息。一度成为互联网热门应用的某换脸软件开发企业,也在今年9月因涉嫌未依法依规收集使用用户个人信息被工信部约谈。

有国内知名互联网企业视频识别安全专家向记者透露,当前存在为数不少的不法分子、数据黑灰产从业者通过通过实名认证,达到注册虚假账号或者直接侵犯他人账号的目的,需要相应的人脸信息,甚至在国内已催生出一定规模的“过脸产业”。

记者搜索互联网,发现网络论坛中存在大量针对电商平台、特定设备的

“过脸”技术解答,甚至有完整“过脸”技术教程,包括软件选择、脚本设置等。一些网站上还有“过脸软件”代码链接,随意供人下载。

我们的生物特征信息流入何处?是否安全?

那么在日常生活中,究竟是谁热衷于记录和储存我们的生物特征信息呢?奇安信网络安全研究中心主任裴智勇告诉记者,当前大致有三类主体。

首先是部分视频监控的运营主体。比如通过商场酒店、会议场馆等公共场所视频设备采集信息。

其次是一些公共职能部门、大型互联网企业、商业机构等,经过用户授权,采集包含用户个人生物特征的数据信息。

第三是科研机构因为科研需要收集使用,如存储一定规模的样本供人工智能进行学习、训练。

浙江大学计算机学院人工智能研究所教授李玺表示,目前公民生物特征信息的主要采集储存主体提供信息安全保护的能力水平参差不齐,信息公开透明度也不够,容易导致海量信息面临安全风险。

与此同时,业内人士透露,目前在授权采集过程中,大量商业主体为降低自身成本,通过格式条款或单方告知的形式“逼”处于弱势地位的公众出让生物特征信息,甚至在合同约定中暗含自我免责条款。这些都不利于相关信息保护。

“未来也不排除根据收集来的数据重建个人生物识别特征的可能,比如3D打印技术‘复刻’人脸。到那时我们



所面临的风险就不仅仅是虚拟世界被入侵,而是现实生活中被冒充。”奇安信集团副总裁左英男说。

正、邪技术力量仍将缠斗 法律空白亟须填补

受访网络安全专家认为,人脸、指纹、虹膜甚至基因,生物特征信息因其随身性、唯一性,将被愈加广泛地应用于金融、购物、安全等生活场景的趋势不可逆转。但其可复制性则同样决定了围绕信息安全技术所展开的“道魔之争”将长期持续。

记者了解到,目前针对“换脸”潜在的风险,技术层面主要可以通过“活体检测+人脸比对识别”应对,同时通过翻拍、3D结构光、多维度生物特征信息等辅助技术,也能够一定程度上增加相关技术的安全性。

有专家认为,当前相关法律规范层面的缺位同样亟须填补。

据浙江浙杭律师事务所高级合伙人姜海斌律师介绍,我国网络安全法规定了“谁收集、谁负责”的原则,并规定收集个人信息须经被收集者同意,其中包括个人生物特征信息。但对于收集相关信息主体需要提供何种程度的保护力

量、如何评估与公开、公民个人敏感信息的保护层级、具体保护措施等关键问题,目前均尚未制定具强制力的法律规范。

2018年5月,全国信息安全标准化技术委员会颁布实施《信息安全技术个人信息安全规范》,作为推荐性国家标准,其中将生物识别信息明确归为“一旦泄露、非法提供或滥用可能危害人身和财产安全,极易导致个人名誉、身心健康受到损害或歧视性待遇等”的个人敏感信息。

北京航空航天大学法学院院长龙卫球认为,该标准针对个人信息收集、保存、使用、委托处理等环节提出要求,落地网络安全法的原则性规定,填补国内个人信息保护在实践标准上的空白,为企业进行个人信息保护合规提供具体指引。

目前,我国正加快推进个人信息保护法立法进程。对此,薛军也建议,应在立法层面需区分普通个人信息和敏感个人信息。“针对个人敏感信息,或可建立特许制度,就是说,如无法律法规授权,即使在公民个人同意的情况下,一般商家、私人机构等也不得收集包含个人生物特征的敏感信息。”

(据新华网)