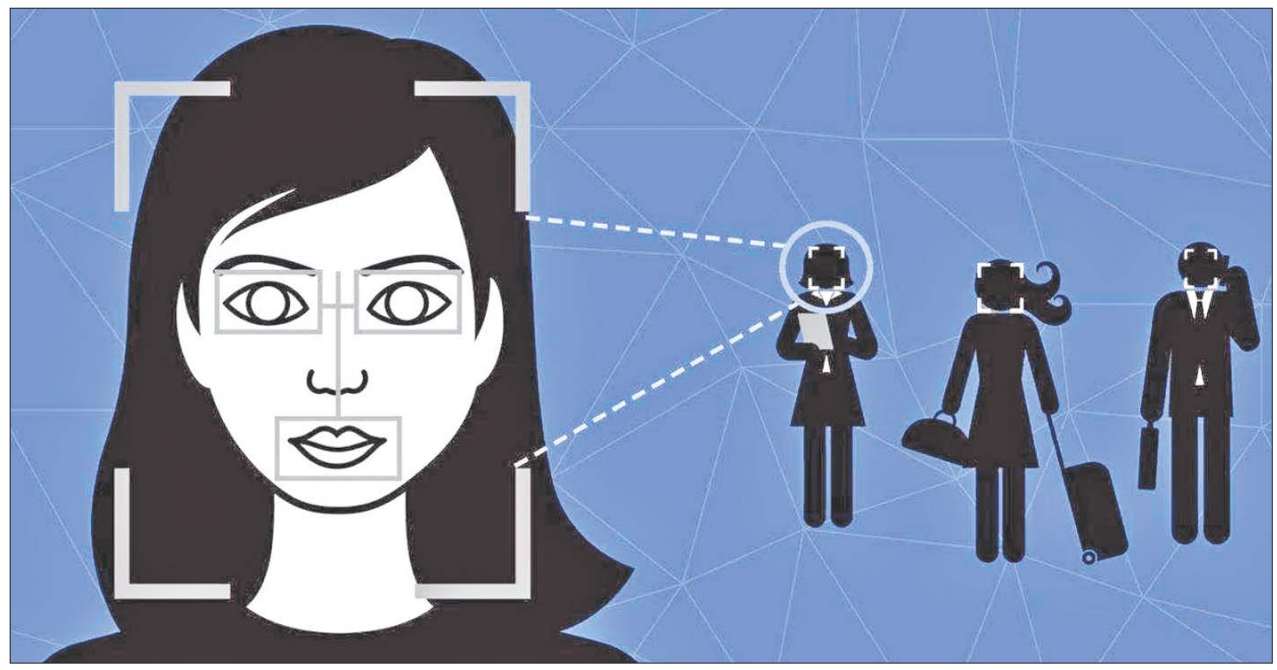
当你的脸变成一串『密码』之后……

面对人脸识别技术存在的照片泄露等风险，我们该如何应对？

伴随着人脸识别技术的发展，其争议始终存在。先是有因不接受动物园将入园方式改成“刷脸”，浙江理工大学副教授郭兵将杭州野生动物世界告上了法庭。而后又发生了清华大学法学院教授劳东燕遇到“不刷脸不让进小区”的情况，对此，劳东燕认为在小区安装人脸识别装置并无必要，并且不经同意收集人脸数据也违反了现行的法律规定，经协商，街道最终同意业主出入小区可以自愿选择门禁卡、手机或人脸识别的方式。

目前，不少人对于人脸识别技术的应用表示担忧，主要认为其有照片泄露的风险。人脸照片泄露就是人脸识别技术的“锅”吗？面对泄露风险，我们要如何应对？



采集：人脸识别相对“温柔”

“在人脸识别技术出现之前，更早的生物特征识别的应用是指纹识别，因为人的指纹具有独一无二的特性以及相应的法律证物价值。从法律意义上讲，摁指纹在古代就已经被较为广泛地应用了。”河北工业大学电子信息系主任、教授邱波表示，其实指纹识别技术应用的历史，一路伴随着更多的反对声音，究其本质，指纹才属于真正的私密性特征，具有法律意义上的信用性。而且指纹需要人配合采集，往往对人心理的冲击力更大。

“因为有接触采集具有心理上的侵入性和强迫性，而非接触采集方式则不具有侵入性。指纹必须按压，才能被采集到，原本属于更难推广的技术。”邱波解释道，相对于指纹，人脸是外露的，并不需要如指纹识别的按压等操作，人脸数据即可被监测系统采集，类似的生物特征识别还有虹膜识别、步态识别等。所以从技术角度上看，指纹识别技术的阻力应该更大一些，而人脸识别相对来说是比较“温柔”的一种方式了。

但当今人脸识别技术变成热议话题，争论不断，邱波认为，这可能和现在人脸相关技术的发展有关。比如将一张人脸跟别的身体组合在一起，PS出一张照片，然后通过技术就可以把这张照片跟一个真实的三维人脸模型相结合，从而制造出一个和照片一模一样的虚拟人。这个虚拟人可以说你从来没说过的话，做你没做过的表情。“这种通过人脸技术做了违背本人意愿的事情，是导致人脸信息采集具有了侵入性的原因，与人脸识别技术本身具有侵入性不是一个层面的。从这个角度看，人脸信息被非法盗用的可能性增加，就导致了大家对人脸识别技术具有很强的戒备心理。”

“如果单从技术角度看，这种私密性争议毫无意义，因为我们正常情况下日常都会露脸，那就有人脸随时被‘抓取’到的可能性，脸本身没有秘密可言。”邱波说。

另一方面，让人们对人脸识别技术戒备心强的点在于，人们觉得看到脸的样子就能和个人其他信息关联起来，而指纹则不然，任何人看到一个指纹并不能立刻知道这个指纹属于谁，所以就觉得很安全。“其实这就是人的错觉，和实际技术识别是两回事。现在通过手机号码、身份证号码，甚至一张名片就能泄露出很多个人信息，脸的信息和这些信息目前也没太多区别。”邱波说。

“因此在录入环节，大家没必要过度纠结于人脸识别的侵入性。”邱波说。

存储：人脸识别并非比对原始照片

“其实人脸识别技术从诞生那天起，其技术就基本保证了存储环节的安全性。人脸识别的技术是不需要存储真实人脸照片的，每张人脸照片在存储的时候都会化为一个个经过精心构造的特征数字码。”邱波解释，人脸图像特征被提取后，就可以进行人脸的编码，生成一个人脸特征向量，从而进行存储和比较运算。也就是说在机器那里，人脸特征变成了一串数字，它们可以表示眼睛之间的距离，眼睛和眉毛的距离、耳朵的大小等等，具体是什么根据特征提取方法会有变化，这样每一张脸都存成了一个“密码”。机器在进行人脸识别的时候，就类似于在密码本中查找特定密码的过程，只需要比对这些数字即可。

那这些数字能随时恢复成照片吗？“实事求是地讲，通过技术是可以把数字‘密码’恢复成人脸照片的，目前有很多科研人员在研究这类技术，而且技术水平也越来越好。”邱波表示，但是防范这个问题也并不难。一方面我们未来在对人脸进行编码的时候，可以采用有损压缩和保密特征提取算法，这样就很难进行真实的高清恢复。另一方面，完全可以通过法律、法规的制定，禁止随意使用这种恢复人脸的软件。

“其实包括手机号码、身份证号等都可以以向量的形式存储，把这些个人的隐私信息都编辑成一般人无法识别的代码。”邱波解释，因为经过编码，这些信息已经变成特定的码序列了，即便被泄露给某人，如果他想要拿到这些内容，还必须先进行解码。而解码器是可以从技术源头上进行适当控制的，因为一般人不具有解码能力，这样就能做到隐私信息不会被轻易泄露。这也涉及另外一个领域叫数据安全，就是怎么保证编辑后的码序列不会被轻易破解。

“虽然技术层面上是可以保证人脸识别技术的安全性的，但是也不能排除一些别有用心的机构，不管出于什么目的，私自保存人脸的原始照片。”邱波强调说。

对此中国政法大学知识产权研究中心特约研究员李俊慧表示，按照《民法典》第一千零三十四条规定，“个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。”

其中，个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。

按照《个人信息保护法（草案）》第四条规定，个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

此外，在《网络安全法》中也有个人信息收集、存储及使用等方面的规定。“对于这些个人信息，只要是依法收集，获得授权，在授权范围内就可以使用。”

泄露：现阶段技术无能为力

“2元钱可买上千张脸的照片”类似事件经常见诸媒体报道，也加剧了人们对人脸识别技术的争议。

“不能一看到私人照片在网络流出，就认为是通过人脸识别采集上来的照片。”邱波表示，人脸照片的流出有多种途径，其中有一个很重要的途径就是“网络爬虫”。这种类似于搜索引擎之类的软件，通过编写好的网络程序，到各类网站上抓取想要的照片信息，并保存下来。“这些照片很多都是我们自己传到网上去的，因此我们在上网过程中也要注重自我的隐私保护。”

此外，目前许多手机APP在超出产品功能目的范围之外大量收集用户个人信息，有的甚至是在未明确告知用户的情况下偷偷收集。“可能在无意间，我们照片就被别人所收集下来了。”邱波说。

李俊慧表示，目前《个人信息保护法》专门立法进程也在加快。2020年10月21日，全国人大法工委公开《个人信息保护法（草案）》，面向社会征求意见，目前还在征求意见阶段。

除了在法律法规上加以约束外，在技术层面上能否防止非法采集或者“网络爬虫”呢？

“我们无法阻止拍照，也无法阻止大家把照片上传到网上，更不知道这些采集人脸照片的机构是否偷偷保存了原始照片。”邱波说，但目前来说还不具备相应的技术手段防止这些情况的发生。如果强行阻止拍照的话，可以尝试在相机端想办法，比如把所有销售出去的数码相机软件做特殊化处理，以保护照片没有授权不被传播出去等。当然这也是设想，现阶段，还是得通过法律法规来保护我们的个人信息不被泄露。

据《科技日报》

相关链接

专家：人脸识别亟待完善法律防止滥用

近日，有媒体报道称，在某些网络交易平台上，只要花两元钱就能买到上千张人脸照片，而5000多张人脸照片标价还不到10元。

中国传媒大学文化产业管理学院法律系主任郑宁认为，人脸信息作为个人信息中最为敏感的一类“个人生物识别信息”，更应该成为重点关注和保护的对象。值得注意的是，《个人信息保护法（草案）》已把个人生物特征列入敏感个人信息，处理敏感个人信息应当取得个人的单独同意，个人信息处理者应当告知处理的必要性及对个人的影响。草案还拟规定公共场所安装图像采集、个人身份识别设备，应该为维护公共安全所必需，且只能用于维护公共安全的目的。

中国传媒大学人类命运共同体研究院副院长王四新认为，“人脸识别的滥用在实践中是肯定存在的，是否需要急刹车主要取决于人脸识别的使用者和被使用者之间的博弈，公共机构一般不易介入这样问题的决策。”

“如果不是法定强制人脸识别的场景，应提供其他替代性的验证机制，赋予公众选择权。”郑宁说。

“人脸识别主要需要防止被滥用，而不是规定哪些信息可以用、哪些信息不可用。对个人信息的滥用要作出科学的界定，明确有哪些类型，然后通过法律来对滥用进行规制。”在北京师范大学法学院教授刘德良看来，人们现在都在强调保护、防止泄露个人隐私信息，而没有做到有效防止滥用，结果导致我们越强调保护，现实中出现的问题越多。

据人民网

人脸识别技术应用越来越广泛。（网络图片）

报料电话：(0531)85193700 13869196706 欢迎扫描上方二维码下载齐鲁壹点 600多位在线记者等你报料

报纸发行：(0531)85196329 85196361 报纸广告：(0531)85196150 85196552 85196557 差错投诉：(0531)85193700 发行投诉：4001176556 (0531)85196527 邮政投递投诉：11185 全省统一零售价：1元

刊号：CN37-0003 邮发：23-55 广告许可证：鲁工商广字01081号 地址：济南泺源大街2号 大众传媒大厦 邮编：250014 大众华泰印务公司(大众日报印刷厂)印刷