上传“自拍照”或泄露个人隐私

专家提醒:面对生物特征识别技术应用要多长个“心眼”

□本报综合新华社等报道

上传“自拍照”也可能会泄露个人隐私，这可不是危言耸听。随着生物特征识别技术在生活中的广泛使用，人脸、声纹、虹膜、指纹，甚至是步态都已经成为重要的个人身份信息，同时也有可能成为个人隐私的泄露方式。

【事件】

“秀自拍”有“泄密风险”

风险要比盗刷严重得多

“扫一扫二维码，上传一张自己的照片，来看看你过去的样子。”不久前，一场网络互动活动火了一把。它让网友上传自己的照片，并在朋友圈中分享“自己过去的样子”。随后，有人质疑这样的活动存在泄漏网友生物特征信息的风险，尽管活动主办方迅速澄清，表示不会保存用户照片和其他个人信息，但依旧引发了人们的关注。

从一张照片中可以提取到用户的哪些信息？上世纪八十年代，某杂志一张封面照片《阿富汗少女》吸引了众多读者的目光。十多年后，为找寻照片中当年那个神秘少女，技术人员通过虹膜识别技术，在上千个自称是照片主角的人中找到了她。北京理工大学光电学院副教授何玉青向记者讲述了这一故事。

“那是用 30 多年前的相机拍摄的照片，以现在的摄影技术，想要获取某个人的虹膜信息并非难事。”何玉青说。

当前，人脸识别技术更加普及，随意上传自己的照片是否存在安全风险？记者向多位技术专家求证，多位给出了肯定答复。

“尽管不少互联网企业都声称有自己的人脸识别算法，并能够通过机器深度交互学习来甄别是活体还是照片，”360 视觉技术专家邱学侃表示，“但是任何人脸识别技术都无法保证 100%不被照片等影像骗过去。”

上海市信息安全行业协会会长谈剑峰表示：“生物认证最大的共性是唯一性，每个人都有独一无二的脸、指纹和虹膜等，正是这种唯一性让大家认为生物认证是安全的。但生物特征数据库一旦被攻破，大量带有唯一性的生物特征数据被盗取，这带来的风险要比盗刷严重得多。”

“如果你的邮箱密码被盗用，你可以重新设置密码来弥补损害。但如果你的虹膜或者指纹等信息被盗用，你是不可能重新设置虹膜或者指纹的。”英特尔公司软件工程师郭向阳说。

把“我”变成“你”很简单

“复刻”他人指纹非难事

除了人脸信息之外，虹膜、声纹、指纹、掌纹、手指静脉甚至步态都可以作为身份识别的重要生物特征。一旦这些信息被他人盗取利用，轻则造成个人财产损失，重则危及国家安全。

今年春节期间，一些机构通过社交软件发布了“口令红包”的小游戏。在此类游戏中，用户需要根据文字提示的内容录制一段绕口令，随后系统会根据用户发送的音频来判断该段绕口令是否标准，并派发一定数额的红包。有专家指出，若上述活动被不法分子控制利用，极有可能泄露用户的声纹信息。

科大讯飞声纹识别技术负责人李晋表示，从目前的技术手段来看，声纹解析并不复杂，“当用户的声纹信息被不法分子获取，有可能会被解析，进而根据其特性合成与该用户音色相同的声音，或者把其他人的声音转换成该用户的，用于电话诈骗等犯罪活动。”

在一些视频网站上，甚至还出现了利用指模工具复制他人指纹的教学视频。何玉青表示，“复刻”他人指纹并非难事，一些人出于指纹考勤需要，将自己的指纹信息提供给他人用来制作指纹倒模，从而给自己的生物特征信息泄露埋下了隐患。

资料图片

【专家】

用户需谨慎监管要加强

“一张没有其他附加信息的照片泄露隐私的可能性不大，但应该防范他人恶意将照片与其他个人信息串联后做非法用途。”安全专家提醒，对于一些要求上传手持身份证照片或视频的服务，用户应保持警惕。

戴美瞳能避免被复制虹膜信息吗？何玉青的团队通过实验证明，目前市面上销售的美瞳或隐形眼镜等产品均无法完全遮挡虹膜信息，“虹膜信息主要处在靠近瞳孔的边缘部分，由于瞳孔大小会随光照变化而发生改变，因此即便是花纹多的美瞳也只是能遮挡住极少部分的虹膜信息。因此我们建议，使用虹膜验证身份的敏感人群不要随意上传照片到网络，也不要轻易接受他人拍摄照片的要求。”

腾讯玄武实验室负责人于□表示，生物识别信息的存储应遵循最小化原则，特别是应禁止存储生物识别信息的原始数据。因为人的生物特征只有一套，所以将生物识别技术用于身份验证，实际上就相当于在不同网站上使用相同的密码。一旦攻击者窃取了这些生物识别信息的原始数据，用户在其他网站上的账号也就危险了。

“我国对个人信息保护的基本要求都有了，但是制度设计中还没有明确哪个部门来履行监督管理职责，一些法律中对‘有关主管部门’的指向也还不够具体。”中国信息安全研究院副院长左晓栋说。

“《个人信息安全规范》已经发布，要考虑如何进一步提升规范标准的约束力，进而提升个人生物特征信息的保护效果。”左晓栋建议，相关法律法规、政策要积极引用《个人信息安全规范》，在特定领域强化国标的约束力。

从源头上防范信息泄露

一些网友可能觉得上传一张图片不会给自己带来多大风险。但有网络专家指出，互联网公司在收集用户照片的同时，也收集了照片中的时间、位置等信息，这能够对用户进行定位。而且照片中还可能携带手机信息，比如用户用的是什么类型的手机。更严重的是，后台数据库可将用户的位置信息、照片、姓名以及手机号等对应起来，拼凑出更加精准的个人信息。

在浙江垦丁律师事务所联合创始人律师麻策看来，类似产品本身不具备数据安全意识和技术配备，一旦数据被内部人泄露或者被黑客攻击，后果会非常严重。

因此，互联网企业在收集、使用公民个人信息时，必须遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经被收集者同意；不得违反法律、法规，并采取合理可行的措施，保护用户个人信息。而用户在玩类似互动游戏的时候，一定要提高风险防范意识，不要只顾好玩而随意提供个人信息。当然，主管部门也要加强对相关企业的监管，并及时发布风险提示。如此，才能从源头上防范个人信息的泄露。

【提醒】

把自拍照放网上会不会泄露个人隐私？在网络上秀孩子的照片会带来什么样的危害？重庆市沙坪坝区人民检察院的助理检察员向晓玲与网友分享网络聊天时应遵循的规矩。

◆自拍照易泄露个人隐私

自拍照的主体是自己的容貌，并不会泄露什么个人隐私。这样的想法真的是正确的吗？向晓玲说，在别有用心的人看来，每张自拍照都会泄露照片主体的个人隐私。向晓玲说，自拍照一般都是在静态环境中完成，这样的环境大多是在家里或者照片主人经常去的场合。因此，网友除了可以看见照片主人的样貌外，还可以从照片的背景得知照片主人的家庭和经济情况。

“如果这些照片被别有用心的人看到，他们会从你照片的背景里，比如家里的装修情况，得知你家境如何，从你常去的场合，判断你自身的经济状况，从你经常出现的固定场合，判断你的生活作息规律，甚至得知你的工作单位和家庭住址。这些都是自拍照无意中泄露的个人隐私。”向晓玲说。

同时，向晓玲提醒市民，不要在与陌生人或者不熟悉的朋友网络聊天时，轻易告诉对方自己的工作单位和家庭住址。“从我们最近办理的案件来看，有些网络聊天软件甚至已成为毒品销售的工具，个人信息泄露所带来的危害远超你的想象。”

◆网上秀孩子萌照很危险

孩子在生活里的萌照、自己和孩子的亲子游照、孩子在学校获奖的照片……很多家长喜欢将自己孩子的照片放上网络与人分享其中的苦与乐。但你知道吗？这样的照片极容易将你的孩子带入危险之中。

向晓玲说，这些照片会给别有用心的人提供包括孩子爱好、性格、家庭情况、就读学校等在内的大量信息，甚至犯罪分子还可以通过照片推断出孩子的上学放学时间和常去地点，找到适合犯案的时间。

大量信息的泄露，还会让犯罪分子通过推断出的信息，和孩子第一时间建立亲密感，让孩子误认为犯罪分子是自己父母熟悉的朋友。

向晓玲说，除微博与 QQ 空间外，一些亲子 QQ 群也成为隐私泄露的高危区。因为加入 QQ 群时，群主多会要求新成员添加个人信息，而且一些家长在聊天时，因为感觉同是孩子家长就放松警惕，常有意无意谈及孩子的情况。

根据拐卖儿童案件分析，犯罪嫌疑人为取得孩子信任，都会通过聊天、与家长或邻居套近乎的方式套取孩子的相关信息。