青未了 新知周刊

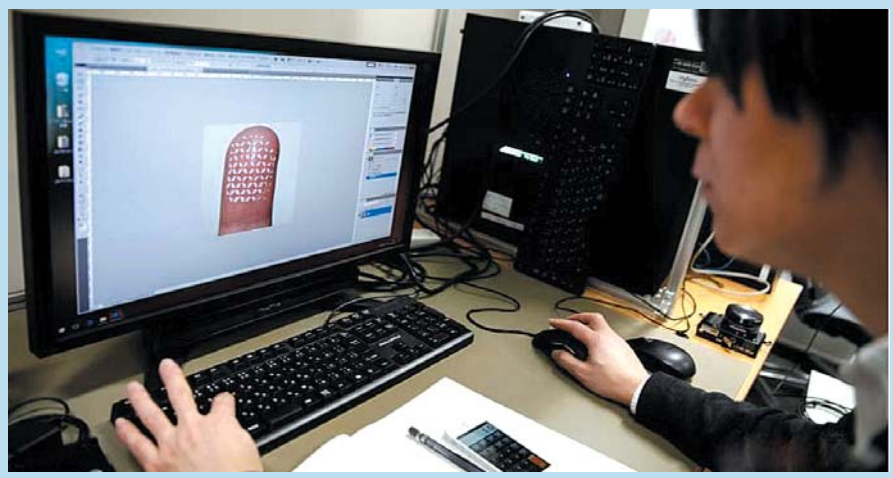
A14—15
齐鲁晚报
2022年6月3日 星期五

主编:任志方 责编:于梅君 美编:继红 组版:侯波

社交媒体时代,很多人会用相机来记录、分享自己生活里的精彩瞬间。但是,你有没有想过,这些照片会无意中泄露自己的隐私?

5月25日,一则“一张照片能暴露多少隐私”和“群聊晒原图有多危险”的话题冲上热搜,讨论次数高达7.3万,不难看出,这个话题备受网民关注。

记者 于梅君



拍照比“剪刀手”需谨慎,此举易泄露指纹信息。

利用制作指纹膜的工具,只需半小时就能做出一个指膜。

一张照片能暴露多少隐私?

网上发原图、拍照比“剪刀手”,都可能让你的信息裸奔

① 群聊中 原图一出天下知

时至今日,不少人的隐私保护意识,可能还仅仅停留在银行卡密码、手机解锁密码、游戏账号等方面,其实,这些只是隐私的基底,在这之上,还有着更多隐私数据,比如个人账号喜好、浏览记录、图片Exif信息(记录数码照片的属性信息和拍摄数据)等,这些隐私数据一旦暴露,我们就仿佛在互联网的大潮中裸泳。

有人做过一个实验,借代购之由,添加一位1800公里外的陌生女性,然后只花了不到半小时,就从她的朋友圈获得了以下信息:她的真实相貌、真实姓名、私家车款式与车牌号码、女儿幼儿园的地址、常去的电影院及餐厅……

我们日常生活中用手机或相机记录的每一张照片,都有自己的“DNA”,即Exif参数,它可以调用GPS全球定位系统数据,在照片中记录下位置、时间等信息。

当你把原始图片发送给他人时,所附带的信息也会一并发出去。无论用微信、短信、邮件或是其他传输工具,都是如此。当对方收到原图后保存图片,选择“显示在地图上”,就可以显示拍摄图片的地理位置。

当然,只有原图才有GPS等相关信息,目前很多软件默认压缩图片时,会抹去相关信息。例如你在朋友圈中发布的照片就是经过压缩的,即使别人下载收藏也无法看到更多信息。

不过,即使没有这些图片与生俱来的“DNA”信息,我们沟通交流、记录生活的每张图片,也传输了很多消息。

比如你在自家窗口拍摄了一张风景图,并发送原图到群里,这就相当于给群里所有人公布了你家GPS位置数据,甚至可以精确到经纬度和海拔,通过拍摄时间与拍摄角度分析,还可能准确推断出你家的楼层和门牌号。

可以说,你无心拍的照片,在有心人挖掘下,可能会让个人信息无处遁形。

② 拍照比“剪刀手” 有泄密风险

拍照还在比“剪刀手”?这个姿势不但已经过时,还很容易泄露个人信息。

在2019年国家网络安全宣传周中,就有专家科普说,在距单反相机1.5米范围内拍摄的“剪刀手”照片,通过照片放大技术和人工智能增强技术,可以完整还原出被摄者指纹信息并制成指纹膜,手机、考勤机、指纹锁等都有被破解的风险。

上海市信息安全行业协会副理事长张伟表示,基本上,在1.5米范围内拍摄的剪刀手照片,可以恢复受试者100%的指纹,1.5米到3米可恢复50%的指纹,3米以上则需要提取指纹。通过照片提取出的指纹,利用专业工具,只需半小时就能制作出一个指模,它可以被不法分子通过指纹技术在各种身份识别渠道使用,如指纹门锁、指纹支付等。

这种黑科技真的存在吗?日本国立信息学研究所科研人员指出,如果拍照时光线明亮,恰巧焦点对准指纹,就可以通过照片复原其指纹信息。据实验,采用市面销售的2040万像素数码相机所拍摄的照片,经过图像处理后,就会得到指纹数据。距镜头1.5米拍摄的照片,指纹可以清晰地呈现出来。

如何保护你的指纹信息?上海信息安全行业协会副主任张威提醒,除了不向陌生人提供自己的指纹,不在不可信的设备上输入自己的指纹外,3米以内不要拍“剪刀手”照片,也不要在网上发送带有自己指纹信息的照片。另外,如果家里有指纹门锁,尽量采用设置指纹+密码的方式打开,以确保安全。

要学会给个人信息“加把锁”。

③ 你的照片可能 被“偷喂”给了人工智能

你可能压根没想到,自己发送到社交平台上的肖像数据,可能会被个别技术公司收集,“偷喂”给人工智能神经网络,成为人脸识别技术迭代升级的“粮食”。

2019年,IBM(国际商用机器公司)就被指在未经用户同意的情况下,在图片分享网站上获取了大约100万张照片,用于训练其人脸识别算法。

IBM研究人员在一篇公开的论文中,详细描述了使用这些照片进行人脸分析的步骤,包括测量人脸五官的距离等。据称,通过使用头部和面部的47个标记点,可以对人的面部照片进行很多可靠的测量。对于技术公司而言,这些照片的价值不言而喻。庞大的图片数据有助于将人脸识别算法训练得更加精确,从而可以快速地从不同照片或不同场景中识别出某个用户。

《麻省理工技术评论》官网发表文章说,人工智能研发人员一直在从互联网的各个角落搜集大量数据,来“喂”那些饥饿的机器学习算法,因为这些算法的训练需要以大数据为支撑。社交平台上的照片,常常成为技术公司获取图片数据的来源。

随着人工智能技术应用越来越广泛,个人隐私被不当利用的担忧同样存在于其他场景。比如,消费者在刷脸支付的同时,面部肖像也会被人脸识别系统所获取。这些照片会不会被技术公司利用,变成训练人工智能神经网络的数据?甚至再次被提供给其他商家,用于其他用途?这些都值得追问。

其实,可能被侵犯的个人隐私,也不仅仅限于面部肖像。现在多种应用软件都可以在语音识别技术的支持下,允许用户进行语音输入。但声纹是重要的个人生物信息,一旦声纹数据被泄露,不法分子有可能利用当前的语音技术,合成难辨真伪的声音,用于电话诈骗等不良企图。

此外,虹膜识别、指纹支付、文字识别等人工智能技术,在应用时也可能涉及个人隐私问题。

④ 如何避免照片 “出卖”你

为了防止在群聊中因发送照片暴露隐私,我们可以做些什么?

首先,可以关闭相机的位置信息。照片分享前打开相册,点击左下角的“分享按钮”弹出分享界面后,点击顶部的“位置”选项,取消默认开启,之后发出的图片将不包含位置信息。

第二,不要轻易给陌生人发送原图。在朋友圈或者微博晒照,因为会被服务器压缩,相关信息会被删除,相对来说比较安全。切记,要建立陌生人群聊中隐私防范意识,尽量不发实拍照片,发送时也尽量不去勾选原图。

第三,验明正身。在微信“设置——隐私”里,将“加我为朋友时需要验证”设为开启,杜绝被陌生人随意加为好友。不要嫌麻烦,将家人、朋友、同事分组,信息选择性发布,真的是在保护自己。

第四,和陌生人说拜拜。每个人的微信列表里都躺着很多不知道怎么加上,但又从来没聊过天的人,建议一律删除。担心误删时,可提前发朋友圈提醒大家。

第五,慎重发布。车票、飞机票、车牌号等,包含大量信息,最好不要晒。另外,老人和孩子的照片也一样,如果实在想在朋友圈展示,可以选择用贴纸打上马赛克。在照片分享过程中,如果发现含有他人的隐私信息,也要培养打马赛克意识,避免引来法律纠纷。

第六,很多手机厂家关注到隐私泄露的风险,在操作系统层面就提供隐私安全抹除的功能,比如,在图库内分享照片时,就有隐私保护功能,开启后可以抹掉位置信息、拍摄数据。

人工智能时代,让每个置身其中的人都变得越来越透明。不过,解决问题的方法其实也不难,总结起来就是:1、避免发原图;2、实在必须发,那就关掉手机定位;3、绝杀招:P图后再发;4、拍照时不比“剪刀手”;5、获取用户个人隐私信息,应保证用户的知情权,要给予用户选择不拿个人隐私“喂”人工智能的权利。专家认为,要实现这一目标,仅依靠行业自觉恐怕远远不够。依靠相关法律对人工智能技术的应用加以规范才是硬道理。

知多一点

“AI换脸”以假乱真?一招识别假脸

一视频网站曾流传出一段视频:《射雕英雄传》朱茵主演的黄蓉被视频制作者通过“AI换脸术”处理成了杨幂的脸,神态表情毫无违和感,一度引发网民热议。

所谓AI换脸术,是基于人工智能的人体图像合成技术生成的假脸。“AI换脸术”强调“以假乱真”,简单说,就是将目标人物各个角度的人脸照片一帧帧贴在被换对象的视频画面上,生成假脸视频。

“从技术层面讲,首先要进行数据采集,捕捉不同姿态、表情、角度和光照的人脸图片;再进行数据处理,包括采集数据标准化及分割算法处理等;制作需要几个小时甚至数十小时,但现在已有许多插件可以辅助。”为央视网络春晚提供虚拟主持人技术支持的偶邦公司创始人郑毅介绍。

如何辨别“AI换脸术”?科学界正在应对这个问题,而主要“杀手锏”是运用AI技术假里辨真。纽约州立大学科研团队发现了伪造视频的漏洞:假脸极少甚至不会眨眼,因为它们多是使用睁眼的照片进行训练的。

研究人员表示,伪造视频往往忽略了“自发的、无意识的生理活动,例如呼吸、脉搏和眼球运动。因此,缺少眨眼是判断一个视频真假的好方法之一。”

这种“反AI变脸”技术通过有效预测眼睛的状态,准确率达到99%。“在伪造视频的后期处理中手动添加眨眼,其实并非一个巨大挑战,而且一些伪造视频已包含眨眼。从长远来看,实际上这是一场通过AI制作假视频和检测假视频之间的持续战斗。”研究人员说。

对此,郑毅提出,“通过强制记录照片和视频拍摄的时间、地点,既在区块链上记录照片和视频不可篡改的时空戳方法,也可进行鉴别”。