你社交网站上的照片 也许已经被用来训练人工智能了

人工智能2019-04-23

毫无疑问，这张家庭照片是非常可爱的:照片中的爸爸留着短须，戴着无框眼镜，棕色头发的妈妈咧着嘴笑着。他们正和两个蹒跚学步的女儿一起嬉戏，同时品尝着冰淇淋。但是，这张照片于 2013 年被上传到照片分享网站 Flickr 上时，“可爱”以外的属性引发了争议。对于面部识别系统来说，这张照片有着独特的意义。照片里，人脸出现在了画面的不同位置。这样的照片能够帮助训练人工智能来识别照片和视频中的人脸。

韦斯特于 2013 年拍摄的这张照片被收录在 IBM 的人像数据集（Diversity in Faces）中

IBM 开发了一个名为“人脸多样性”的新项目，并为其准备了上百万张图片，这张其乐融融的照片就是其中之一，该项目旨在提升人脸识别的公平性和准确性。

照片的拍摄者是佛蒙特州农村的一名图书管理员，名叫杰萨姆·韦斯特 Jessamyn West。当她发现这张照片被 IBM 使用了的时候，她感到既惊讶又愤怒，她曾将这张照片上传到 Flickr，并添加了知识共享（Creative Commons）协议，以便让其他人可以使用这张照片。

但是她不知道的是，包括她拍摄的自画像在内的十几张照片，和这张照片一样都包含在了人脸识别数据集中，这让她感到十分不安。她说：“如果当初有人（就使用我的照片）征求过我的同意，我不会如此不安和愤怒。”

多年来，研究人员们通过互联网收集并注释了各类物体的照片，以此来训练电脑，让其可以更好地了解它们周围的世界。通常，他们通过谷歌图片搜索、公共 Instagram 帐户和一些其他的途径(有些合法，有些可能不合法)获取数量巨大的图片。得到的数据集通常被用于学术研究，比如训练或测试人脸识别算法。但随着微软、亚马逊、脸书和谷歌等公司押宝人工智能，人脸识别正走出实验室，进入大型企业的视野中。

随着消费者意识到他们在互联网上留下的数据能够产生的巨大威力，人脸识别数据集正在加剧人们对隐私和监控的担心。因此，一些研究人员正在重新审视这种野蛮收集他人照片的行径。在充满分享精神的互联网中，使用他人照片本应征求别人同意。

照片从哪里来？

由于深度学习的普及，近年来机器学习研究蒸蒸日上，人脸识别技术也得到了极大的改善。在一个典型的用例中，照片、视频或实时流媒体中的人脸会被扫描、分析，接着，它们的特征会被拿来与数据库中注释过的人脸进行比较。

这项技术正被用于打击人口贩运和机场快速安检，同时它也被用于监视音乐会、体育赛事。

然而，面部识别的准确性仍是一个问题。研究人员开始担心人工智能系统中存在的歧视和偏见。该技术在正确识别有色人种和女性等方面还存在着重大缺陷。造成这一问题的原因之一，是数据集里男性相对于女性、白人相对有色人种的悬殊比例。

对机器训练来说，数据多样性很重要，但数据的体量大小也同样重要。人脸识别系统的训练和测试需要在数千万甚至数百万张人脸上进行。

多年来，研究人员一直通过 IBM 的人脸识别数据集来进行相关研究。这个包含图片链接的数据集都是从 Flickr 和雅虎发布一百万张图片的资源包中整理生成。该资源包被称为 YFCC100M，它被用于各种各样的科学项目研究，包括在不使用地理坐标的情况下估算照片和视频的拍摄地点的研究。

许多公司、研究机构和个人都为面部识别编制了数据集，IBM 只是其中之一。其中一些数据集由实际的图像组成，还有一些类似 IBM 的数据集，是由图像链接组成的。有时，数据集也是可以通过拍摄模特得到的。

这些人像属于英伟达用于训练 GAN 系统的数据集

通常情况下，这些数据集是知识共享的，但它们必须用于非商业目的，比如算法研究。但 CNN 发现，大量的类似数据集可以从 Github 等网站免费下载。

David A. Shamma 在雅虎实验室担任研究主管时，帮助整理了 Flickr 的数据集。他认为，近些年来学术界为了机器视觉和识别研究，正从他们能接触到的任何地方，想方设法地搜集数据，“在这个一个学术领域里，人们经常说，‘没有造成伤害，就不算犯规’”。

Shamma 认为，他和他的同事发布的 Flickr 大数据集，通过将大量授权的图片交给研究人员，可以帮助学术界以此为基础进行研究。

这些被上传到 Flickr 上的图片来源于像韦斯特这样的普通人和一些专业人士。这些图片拥有的知识共享协议是一种特殊类型的版权许可，?它明确规定了图像可以在何种条件下被他人使用和共享。

知识共享协议于 2002 年首次发布，远远早于当前的人工智能热潮。

尽管研究人员在 Flickr 等网站上免费使用图片，但他们也承认，许多上传这些照片的人可能会对照片被用于训练人工智能的事实感到惊讶。

Shamma 说:“我认为人们对自己的照片用途有一定的预计，但是当被告知具体的人工智能用途时，他们仍会感到意外。”

不满在升级

不论人工智能的从业者们如何解释，韦斯特在得知自己照片被用作机器学习后大吃一惊。今年 3 月，她在阅读了一篇 NBC 新闻报道后，搜索了自己的 Flickr 账户。结果发现她为朋友的家人拍的照片和其他许多照片一样，都是数据集的一部分时，她很沮丧。她认为人工智能的未来很明朗，但自己的照片在不知情的情况下被用来训练人工智能使她忧心重重。

Twitter 上相关的帖子充斥着普通网民的抗议。很多人也沮丧地发现，他们在网上分享的照片(通常是很久以前的照片)成为了训练人工智能的素材。

韦斯特要求 IBM 从数据集中删除她的照片，但这只能通过发邮件来完成。她还必须授权 IBM 使用她的社交账号，以便其能够找到并删除每一张照片。

IBM 表示，它“致力于保护隐私权”，数据集中涉及到的人随时都可以选择退出。不过，它并没有提供工具来帮助确认数据集是否包含了特定的图像，因此人们必须通过 NBC 构建的搜寻工具来查找。

与此同时，芯片制造商英伟达的研究人员正在研究 IBM 的经验教训，并考虑改变自己的做法。

今年 3 月,英伟达发布一个在线工具，帮助人们了解他们的照片是否被包含在用于训练 StyleGAN 的数据集里。StyleGAN 是今年 2 月英伟达公布的一个人工智能系统，善于创造实际上并不存在的逼真人脸，它的数据集包含 70,000 张高质量的 Flickr 授权图片。

在 NBC 揭露了私人图片被用作机器训练后，英伟达的在线工具才出现在网络上。然而英伟达负责图形研究的副总裁 David Luebke 辩称，这项工具已经开发了一段时间了。

他说:“当人们慢慢意识到这一点的同时，我们也一直在为之努力。只要有人（对搜集自己的图片）提出反对，我们也希望能赢得他们尊重。”

如果用户想从数据集中删除自己的照片，或避免其用于未来的计算机视觉研究，该公司还列出了一系列预防措施对用户进行指导。

这些建议包括将照片设为私有、更改其附带的使用许可,以及在照片上添加一个标签，以表明他们不希望将其用于计算机视觉研究。

Luebke 说:“我认为很多人要么不在乎，要么会很乐意他们的照片被用在 StyleGAN 这样的研究上。但如果有人不喜欢这样，那也有办法退出。”

这张韦斯特的自拍照和其他的照片一起被编入 IBM 的数据集中

一些研究人员认为，人们应该通过授权，自己决定图片是否可以用于计算机视觉或人工智能研究。

对此，知识共享协议并不能帮上大忙。只要遵循相关的条款，这个来自非营利组织的许可协议并不限制任何形式的人工智能开发。

知识共享组织首席执行官 Ryan Merkley 称:“这些协议并不是为了保护隐私或研究伦理而设计的。”

等待立法

近年来，人工智能发展之快，以至于相关法规几乎还没有来得及制定，更不用说实施了。法律上，在收集和使用图像进行面部识别时，公司并没有告知义务。

目前还没有相关的联邦法规出台。在各州，情况则有所不同:例如，伊利诺斯州有一项法律，要求公司在收集生物特征信息之前必须得到客户的同意；亚马逊和微软总部所在地华盛顿州的州参议院最近通过了一项限制面部识别使用的法案，该法案仍需在该州众议院获得通过。

Merkley 和其他人认为应该考虑立法来规范数据收集。今年 3 月，参议院提出了一项法案，要求企业在收集和共享识别数据之前必须征得消费者的同意。它还要求公司进行外部测试，以确保算法在实施前是公平的。

数字版权组织电子前沿基金会(Electronic Frontier Foundation)技术政策主管 Jeremy Gillula 则表示，即使没有严格的法律限制私人照片用于人工智能训练，企业和研究团体也应该注意遵守道德规范。

在他看来，这意味着使用照片就要得到照片中人物的明确同意。即便这很难做到，它也是企业必须面对的现实。

- END -