AI 人工智慧-人臉辨識

臉部辨識技術背後，有什麼「骯髒的小秘密」？

eiphone 大壯旅

臉部辨識技術，成為整個 AI 行業最為常見的技術應用之一；不過，在辨識效率越來越高的同時，人們也開始擔心臉部辨識技術，發展過程中的隱私安全問題。

比如說最近 IBM 利用 Flickr 下載的圖片來進行臉部辨識訓練，就引起了人們的質疑；NBC News 針對此事進行了詳細的報道，媒體對這篇報導，進行了不改變原意的編譯。

近些年來，臉部辨識技術得到了長足發展，除了幫你解鎖 iPhone，還能讓執法機關在人山人海中，「一眼」就認出犯罪分子，商店甚至用它來辨識自己的「死忠」客戶。不過，法律專家卻警告稱，大量未經允許濫用網路照片，最終會畫地為牢，反過來成為監控你的「幫凶」。

現在的臉部辨識技術還不完美，它工作時靠的是算法，目標則很簡單——認出那張獨一無二的臉。

想把這個任務完成好，技術人員就必須提前「餵給」算法「養分」，即天量的臉部照片。那麼這些照片從哪來呢？當然是網路。

起初，算法學習的照片，都會按照不同的標準進行分類，比如年齡、性別、膚色等，但經過一段時間的學習後，它的能力開始變得有些嚇人了，於是法律和人權專家開始大聲疾呼，他們擔心技術人員，對普通人照片的濫用，會帶來「反噬」效果。

「這是 AI 訓練數據集背後的骯髒小秘密。技術人員可不管三七二十一，只要能用的照片他們都不放過。」紐約大學法學院教授 Jason Schultz 說道。

最近 IBM 公司也進了「暴風圈」，今年 1 月它們向研究人員，分享了自己的數據集，包含了 Flickr 上近 100 萬張照片，雖然 IBM 號稱，此舉是為了減少臉部辨識的偏差。

瞭解真相後的攝影師們不願意了，因為 IBM 在他們的作品上，加了各種細節注釋，包括臉部幾何結構、膚色等資訊，而這些照片最終，可能會成為臉部辨識算法的「養分」。

「我拍過的人可沒想過，自己的照片居然會被用在臉部辨識算法訓練上。」公關經理 Greg Peverill-Conti 氣憤地說道，他有 700 多張照片，被收錄在了 IBM 的「訓練數據集」中。「IBM 太草率了吧，它們怎麼能不經同意，就使用這些照片」。

IBM 公司 AI 研究主管 John Smith 則表示，公司「致力於保護個人隱私」，如果誰想從數據集中移除照片，儘管聯繫 IBM。

雖然 IBM 信誓旦旦的保證 ，Flickr 用戶可以隨時移除數據集中的照片，但事情哪有那麼簡單，這本就是個有來無回的「不歸路」。因為 IBM 需要拍攝者發送想要移除圖片的鏈接（光靠 Flickr 賬號不管用），而它們卻從沒分享過，到底這個數據集用了誰的 Flickr 照片，所以你大概率會被蒙在鼓裡。

對於這個數據集，IBM 有自己冠冕堂皇的理由——它將用於學術工作，且擔負著讓臉部辨識，變得更加公平的重任。當然，在網絡照片濫用方面，IBM 並不是獨一家，數十家其他研究機構或公司，也在採集網路照片，訓練自己的臉部辨識系統。

一些法律專家認為，這不僅僅是對數百萬人，肖像權和隱私權的侵犯，它還加重了人們對臉部辨識技術的擔憂，也許有一天執法部門會讓它「雙手沾滿鮮血」。

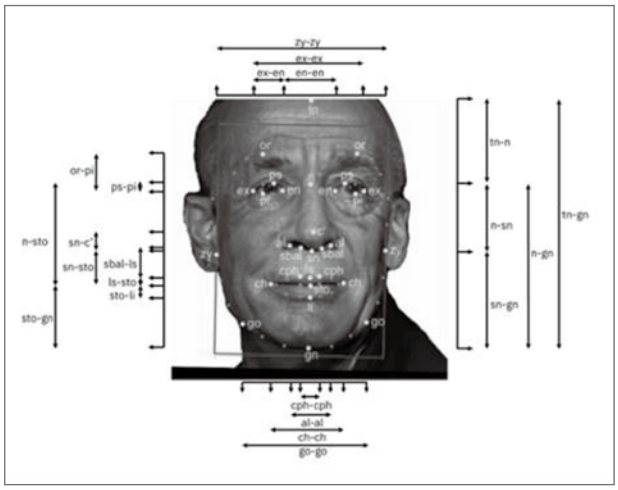
臉部辨識技術的進化歷程

臉部辨識工具剛剛誕生時，研究人員會付錢請人來試驗室「幫忙」，這些人拿錢辦事，將自己不同姿態和光照角度下的照片，留了下來以供研究之用。不過，這樣的方案成本高還浪費時間，因此早期的數據集，往往只有數百個樣本。

進入新世紀後，網路飛速發展，研究人員突然意識到，臉部辨識的好時光來了，因為網上有天量的照片可供使用。

「直接打開搜索引擎，輸入名人的姓名，然後下載各種 360 度無死角的照片既可。」美國國家標準技術局數據集採集人員 P. Jonathon Phillips 說道。

隨著社交網路的興盛和自媒體的發展，普通人的照片也突然多了起來。研究人員默認這些照片是對所有人開放的，有時他們甚至會從 YouTube 的影片中抓取臉部圖片。



由於工作的非經營性質，學術人員用起照片來，絕對是近水樓台，因為他們能繞過版權問題了，而 Flickr 的性質更是讓它們成了研究人員絕對的安全之選。

為了保證數據集的多樣性，IBM 其實從 Flickr 上 Down 了超過 1 億張照片，隨後又精選了 100 萬張有注釋的臉部照片。為了力求精確，它們甚至為這些照片定了 200 多種分類標準。

谷歌學術指出，這種研究方法在業內幾乎已經是盡人皆知，因為有數百篇學術論文，都在靠照片採集來佐證自己的論點，沒人敢說自己是完全清白的，或者拿到了授權或同意。因此，臉部辨識準確性的提高，和分析工具的進步，主要就是靠這些「野路子」來的照片。

IBM 真沒拿臉部數據集賺錢？

「要想讓臉部辨識系統超常發揮，訓練數據必須足夠多樣化，而且覆蓋範圍足夠廣。」IBM 的 John Smith 說道。

在 IBM 看來，自己的數據集並未將圖片中的人臉，和具體的名字聯繫起來，這就意味著系統不會侵犯人們的隱私。不過，依然有人質疑 IBM 的動機，因為它們可是向政府出售過監控工具。

舉例來說，911 襲擊發生後，IBM 就將臉部辨識技術，賣給了紐約警方，執法部門透過搜索監控錄影，就能辨識出特殊的膚色或發色。IBM 還曾推出過「智慧影像分析」產品，它們能透過監控攝影機，給人們加標籤（亞裔、黑人或白人）。

如今，IBM 則有了 Waston 視覺辨識系統，透過圖片算法，就能辨識出人的年齡和性別。配合正確的訓練算法，客戶就能從圖片或影片中，辨識出特定的人。在被問到 Waston 用了什麼訓練數據時，IBM 稱數據有多個來源，不過卻拒絕披露具體的數據來源，並美其名曰保護知識產權。

一再逼問下，IBM 稱從 Flickr 拿到的像片數據集，僅用於研究，不會用來提升公司的商用臉部辨識工具。不過，有專家指出，類似 IBM 和 Facebook 這樣的公司，其研發和商業營運部門之間的界限非常模糊，而且研發部門的知識產權均歸 IBM 所有。

因此，臉部辨識公司 Kairos 前 CEO Brian Brackeen 斷言，即使學術部門研發的算法，有其非商業化性質，這些算法最終還是會被拿來賺錢。

他還打了個形象的比喻，「你可以把它看做拿臉部辨識技術洗錢，公司將網上的照片，洗成了自己的知識產權。」

「被選中」的攝影師們怎麼想？

澳洲攝影師 Georg Holzer ，將自己的作品上傳 Flickr ，是為了記錄自己聲明中的精彩瞬間，他也簽署了創意認證，只要是非營利性項目，就能免費使用他的照片。不過，他沒想到自己的照片會成為臉部辨識技術的「養分」。

「我瞭解技術能造成的傷害。」Holzer 說道。「當然，臉部辨識技術也有其積極的一面，但如果用得不對，它也能剝奪人的基本權利和隱私。我是無法接受這項技術廣泛應用的。」

「我覺得 IBM 可不是家慈善公司，最終它們還是會用這項技術牟利，所以臉部辨識技術還是會進入商業市場。」Holzer 說道。

Dolan Halbrook 也有 452 張照片，被 IBM 的數據集「侵吞」，他也認為 IBM 在使用這些照片時，應該徵得自己的同意。

當然，也有攝影師覺得自己的照片，能被 IBM 選中，並用在推動臉部辨識發展上是一大幸事。

瑞士的 Guillaume Boppe 就表示：「如果我的照片能幫助 AI 進化，降低探測錯誤率，並最終提升全球安全指數，我舉雙手贊同。」

想從數據集中刪圖？沒那麼容易

如果你不同意 IBM， 將自己的照片當成訓練數據，也可以聯繫它們刪除，但操作起來沒那麼容易。一位被抓取 1000 多張照片的攝影師忙活了半天，也只刪除了 4 張照片，因為他無法找到所有照片的鏈接，而 Flickr 賬號 IBM 可不認。

此外，即使從 IBM 的數據集中刪除了照片，IBM 研究夥伴拿到的數據集也無法一並刪除（已經有 250 多家組織和機構，接入了 IBM 的數據集）。

顯然，IBM 的數據集不是公共場所，沒法想來就來想走就走。

好在，各國對隱私數據的保護正在加強。舉例來說，歐洲就將照片看做「敏感個人數據」，如果 IBM 不按規定刪圖，可能就會被歐盟重罰。在美國，也有一些州有了相關規定，在不徵得當事人同意的情況下採集、儲存和分享生物資訊屬違法行為，而生物資訊包含指紋、虹膜和臉部幾何結構等。

近期，芝加哥的律師 Jay Edelson 就向 Facebook 發起了集體訴訟，稱其臉部辨識工具觸犯了相關法律。

至於典型的法院判例，現在還是一片空白。