
大數據和人工智能的危機與挑戰

余創豪 chonghoyu@gmail.com

兩個假設的案例

以下是一個虛構的案例：顧思忍先生經常瀏覽互聯網，但他不喜歡自己的私隱受到侵犯，所以採用瀏覽器的時候，他會慣常啟動「無痕跡視窗」（Incognito window），這樣谷歌便不會收集他瀏覽網頁的數據；基於同樣道理，每次在 YouTube 觀看完電影之後，他都會刪除所有觀看影片的歷史紀錄，他知道當自己這樣做的時候，YouTube 便無法根據他的口味向他推薦電影，但他不想自己的資料被濫用；最近，他用 Signal 替換了自己的 Whatsapp 帳戶，並用 MeWe 取代了臉書（Facebook），因為他不想自己的生活受到科技霸權操控。此外，他參加了一個民間志願團體，遊說國會去立法禁止科技公司收集互聯網上的活動數據。

有一天，他忽然發現到自己多個帳戶被黑客入侵，不但資料被盜用，而且黑客冒充他的身份，在互聯網上散播假消息和仇恨言論，他花了很多唇舌向人解釋自己是清白的，最後決定聘請律師控告多間科技公司疏忽職守，他所提出的論據是：「科技公司有責任保障網路安全，任何網上活動都應該留下能夠被追蹤的記錄，那些公司應該找出黑客入侵的渠道和假消息的來源。」你覺得顧思忍先生以上兩種要求是否有點矛盾呢？

在以下的假設情況中，你會很輕易找出矛盾的地方：毛仁見是活躍的政治活動家，去年她參加了至少十次街頭示威，每一次她都會破壞安裝在街道每一個角落的監控攝像鏡頭，她擔心攝像機會記錄她和同伴的臉，然後警察會使用面部識別軟件和大數據來將他們起底，如果警察知道他們的身份，他們可能會受到警察的監視，甚至騷擾。

在今年毛仁見參加了另一場街頭抗議活動，在活動進行期間他們遇上了反示威團體，那是一個名為「謙卑男孩」的極右團體，「謙卑男孩」在街道的暗角放冷槍，殺死了兩名示威者，並且打傷了十多人。毛仁見十分憤怒，她強烈要求警方採用人面識別系統和大數據去追查兇徒，並將他們繩之於法。

大數據和人工智能的偏見

現在我們處於一個大數據和人工智能的時代，大數據和人工智能是兩樣不同的東西，但兩者相輔相成，互聯網和不同的科技產品收集了人類活動的大量數據，人工智能其中一個範疇是機械學習（Machine learning），跟從前不一樣，現在電腦工程師再不會將所有規則寫入程式裏面，而是向電腦灌注大量的數據，這樣人工智能便可以通過學習無數個例子而變得越來越「聰明」，人面識別技術就是機械學習其中一種應用。

使用大數據和人工智能的道德問題一直存在爭議，最近，一部名為《編碼偏見》（Coded Bias）的紀錄片再次掀起了這個熱門話題，這部電影可以在很多地方觀看，有趣的是，我在「統計分析系統」公司（SAS）組織的一次會議上觀看了這部電影，SAS 是全球最大的統計和數據科學軟件公司。隨後，這部電影亦會在「洛杉磯數據科學會議」（DataCon LA）上放映。



這部電影的開頭講述一位麻省理工學院的黑人女學生試用面部識別技術，但是，無論她怎樣調整角度和室內光線，該系統都無法運作。但是，在她戴上一副白色面具之後，該軟件即可發揮功能。她發現，許多面部識別技術都可以正確地識別白人的臉部特徵，卻不能識別膚色較深的人。紀錄片指出了人工智能的許多偏見和錯誤，例如在英格蘭，警方的面部識別系統將一名黑人誤認為罪犯，他被警察攔住和受到盤問，最後警方發現他是無辜的，於是讓他離開。在德克薩斯州侯斯頓市，一位表現優良的老師幾乎被辭退，因為績效評估電腦程式認為該老師無法為學校增加價值。此外，亞馬遜公司自動檢查求職人士履歷表的軟件發生嚴重偏差，將大部分女性申請者篩走。還有，大數據嚴重地侵犯了個人私隱，令這個世界變成了奧威爾小說《一九八四》所描述的極權社會。影片記錄了該名麻省理工學院的學生和一群同路人發起了反對人工智能技術的運動，最後，三藩市和奧克蘭等幾個主要城市都禁止使用面部識別技術。

人工智能「咸濕」嗎？

驟眼看來，SAS 和 DataCon LA 播放這齣電影的做法好像是跟自己「倒米」，但想深一層，這是值得欣賞的胸襟。在發展大數據和人工智能的過程中，高科技公司和工程師都應該聆聽反對的聲音，並且將倫理元素放入考慮之列。事實上，大數據和人工智能出錯的新聞是無日無之的，以下是一宗《編碼偏見》沒有收錄的新聞：在本年 1 月底，一個研究小組發表的報告中指出，有時候人工智能用來填補缺失的信息，當人工智能分析只有頭部的人像時，軟件將 52.5% 女性照片的身體配上比基尼泳衣或者低胸上衣，但只有 7.5% 的男性肖像變成了光著膀子或穿著低胸上衣，42.5% 的男人變成了穿著西服或其他專業服裝。為什麼會這樣呢？是不是人工智能本身有點「咸濕」呢？



說穿了，電腦工程師將自己的喜好和偏見放入了電腦裏面。相信喜愛科幻電影的讀者已經觀賞過《生化危機》

（Resident Evil），《生化危機》有真人版和電腦動漫版，兩者都有一個名叫 Ada Wong 的角色，電腦動漫遊戲版也有很多版本，在大多數版本中，Ada Wong 都穿著性感服裝，例如比基尼，當 Ada Wong 出場時，男主角里昂·肯尼迪（Leon Kennedy）問她是誰，Ada Wong 出示聯邦

調查員（FBI）的證件。我不禁啼笑皆非，我心想：有那一個女警會在執行任務時穿三點式泳衣呢？我在 YouTube 觀賞《生化危機》動漫版，一位用家留言說：「Ada Wong 穿著比堅尼，她從那裏掏出聯邦密探隊的證件呢？」

修補缺憾還是自毀長城？

事實上，嶄新的技術出現漏洞是不足為奇的，但人們卻忽略了在每個失敗的例子後面，還有千千萬萬個成功的例子，例如大企業採用大數據和人工智能大幅度地減低生產過程中的錯誤和降低成本；筆者用大數據進行研究，得出來的結論比起細小樣本的研究更堅實可靠；我還可以利用人工智能軟件去修改攝影作品，化腐臭為神奇，化東施為西施。

令筆者感到不安的是：每當出現問題時，有些激烈人士便要求全盤廢棄或者禁止這些技術，而不是想出辦法去改善它。平心而論，任何科技在發展過程中都會出現問題，例如幾十年前的汽車是非常不安全的，1965 年，一位 31 歲的律師拉爾夫·納德（Ralph

Nader) 出版了一本書，題為《任何速度下都不安全：美國汽車的危險設計》，但納德並沒有要求禁用汽車，他的訴求是增加汽車的安全設施。

更加重要的是，大數據和人工智能的倫理問題並不只是當地政府、科技公司、人民的三邊關係，外國勢力在大數據社會中亦扮演了重要的角色。美聯社與華府智庫「大西洋理事會」(Atlantic Council) 數位取證研究實驗室 (Digital Forensic Research Lab) 費了九個月時間，分析了推特 (Twitter)、臉書、俄羅斯的 VK、微博、WeChat、YouTube、Telegram 等社交媒體上數以百萬計的貼文，最近他們發表報告，指出許多互聯網上的假消息都是由某幾個外國勢力發出的。現在讓我們回到文章開頭提及的假設例子，若果科技公司沒有收集數據，追查網軍根本是沒有可能做到的。亞當·達拉 (Adam Darrah) 是一家網絡安全公司的董事，最近在亞利桑那州立大學舉辦的一次研討會上，他指出了一個有趣的現象：「美國人不想自己的政府閱覽自己的私隱，但他們並不關注俄羅斯對他們的所作所為。」

美國社會的分化撕裂，是變相的自毀長城！

2021 年 2 月 16 日

[更多資訊](#)