

蘋果聯手 OpenAI 保護私隱引熱議

馬斯克警告用戶數據或外洩 擬禁旗下公司使用蘋果設備

香港文匯報訊 美國蘋果公司周一（6月10日）舉行全球開發者大會，宣布與科企 OpenAI 合作，將人工智能（AI）聊天機械人 ChatGPT 引入蘋果的電子產品。但電動車企業 Tesla 行政總裁、同樣致力研發 AI 產品的馬斯克警告稱，該合作或導致蘋果用戶數據外洩，若將 ChatGPT 整合至蘋果作業系統，他便要禁止名下公司使用任何蘋果裝置，以免危及資料安全。分析相信保護用戶私隱，將是 AI 技術後續發展的重要議題。



◆馬斯克質疑 OpenAI 可能利用蘋果用戶這一巨大資料庫獲利。 法新社



◆蘋果表示，Apple Intelligence 技術會整合至蘋果電子產品的各個系統。 路透社

今屆開發者大會上，最受外界關注的 AI 技術 Apple Intelligence 壓軸登場。蘋果表示，這款 AI 技術會整合至蘋果電子產品的各個系統，用戶可以在撰寫稿件、校對內容、日常生活時使用各類 AI 功能，發送短訊時還可以用文字生成圖片。蘋果還宣布與 OpenAI 合作後，用戶可以在喚起數碼助理 Siri 時，免費使用 ChatGPT。

蘋果私有雲保護數據

向來倡導私隱保護的蘋果，今次宣布利用新技術私有雲（PCC）保護用戶數據，意味蘋果不會將用戶所有數據都傳送到雲端，而是僅上傳用戶查詢時所需要的基本數據。負責收集用戶數據的蘋果雲端服務器，則不設永久儲存能力，蘋果用戶透過設備發送到 ChatGPT 的所有內容，都不會長期保存。加上蘋果沒有為 PCC 設置繞開私隱保護通道的特權接口，黑客必須攻破整個 PCC 系統的防火牆，才能嘗試尋找特定使用者的資料。

不過馬斯克指出，現有的數據分享用戶條款及協議非常複雜，用戶很可能在無意間，同意分享了自己的私隱數據。他亦質疑 OpenAI 可能利用蘋果用戶這一巨大資料庫獲利，「蘋果無法自主研發 AI，卻稱能確保 OpenAI 保護用戶私隱，這是荒謬的。」

訪客亦需交出設備

馬斯克又稱，他會規定日後進入其名下公司

的訪客，必須將蘋果設備交出，放在屏蔽訊號的法拉第籠（Faraday cage）當中，暗指他警惕蘋果設備有洩密風險。

美國科技網站 VentureBeat 專欄作家、硅谷私隱安全分析師托馬森指出，PCC 並非萬無一失，一旦其加密演算法的弱點暴露，不論是內部破壞還是外部攻擊，攻破 PCC 防火牆的風險都很高。托馬森也強調，私隱外洩最大的風險正是設備本身，例如黑客可以冒充受害人身份使用 PCC，或是利用釣魚軟件等方式，令用戶在無意間落入私隱外洩陷阱。

托馬森認為，在 AI 時代保護用戶私隱，既需要先進的技術，也需要不斷彌補電子設備作業系統、應用程式和網絡協定中的潛在漏洞，「PCC 是發展 AI 技術與保護私隱共存的美好願景，但人們需要從根本上改變處理個人資料的方式，以及確定處理敏感資訊人員的責任。」

美多州立法監管 不得擅用聲音肖像

香港文匯報訊 美國國會一直未有提出全面監管人工智能（AI）技術的法案，但多個州份開始自行立法，推出嚴格監管措施。《紐約時報》引述科技行業游說團體 TechNet 稱，今年以來，全美各州的立法者提出近 400 項監管 AI 的新法案，單是硅谷所在的加州便有約 50 項，內容涵蓋保護用戶私隱、保護用戶肖像權，對 AI 模型進行安全測試等。

加州州議會上月提出約 30 項監管 AI 的新法案，作為當地 2020 年通過的法案延伸，進一步限制 AI 科企收集用戶資料，並避免 AI 工具應用在住宅和醫療保健服務等領域時，或因分析用戶個人資料出現歧視問題。報道指出，加州 2022 年還通過一項兒童安全法案，要求科企研發 AI 工具時保護未成年安全。

田納西州今年 3 月通過「人聲及肖像安全法案」，明確規定未經藝術家明確授權同意，科企不得在 AI 生成的內容中，使用他們的聲音和肖像等。科羅拉多州亦頒布消費者保護法案，要求 AI 企業在研發新技術時，就保護個人私隱問題保持「合理謹慎」。

對 AI 進行安全測試

加州民主黨參議員維納爾提出一項法案，要求科企日後推出的生成式 AI 模型，必須進行安全測試，並賦予州總檢察長就消費者權益及私隱受到 AI 軟件侵害後，由州檢察部門直接對科企提出訴訟的權力。維納爾稱，新法案將安全測試限定在企業投資超過 1 億美元（約 7.8 億港元）開發的大型 AI 模型，法案已得到科技業界普遍支持，「我確實希望美國國會採取行動，但我對此並不樂觀。」



◆民衆在 OpenAI 總部抗議，要求安全建設 AI。 網上圖片



◆示威人士在歐洲議會大樓前放置克伯格的人形紙牌。 網上圖片

AI 時代加強私隱保護方法

勿與聊天機械人分享敏感數據

使用 ChatGPT 等 AI 軟件時，盡量避開涉及個人私隱和敏感數據的議題，例如向其詢問如何設置密碼、討論自身或他人的健康情況，甚至用於起草工作中的機密文件等。

謹慎在網上公開內容

網絡用戶在網上撰寫的文字、社媒分享的圖片，各類影片和語音筆記，都可能被利用。例如利用公開的影像和音頻，AI 軟件可以模擬特定對象的聲音或容貌，用戶過多分享類似的個人資料，會增加身份被盜用的風險。

小心處理網絡活動

AI 演算法可以整合並且分析用戶的動向，需要用戶留意，例如用戶在與 AI 聊天機械人溝通時，傳遞出負面情緒，部分 AI 軟件可能會因此放大傳送給用戶的負面信息。

盡可能保持匿名

AI 系統可能透過用戶在網上留下的少量數據，整合出準確的個人資料，或進行完善的性格分析等。匿名使用網絡可以一定程度減少個人資料外洩風險，相關方法包括使用匿名網絡瀏覽器、使用不同的賬號名稱，嘗試一次性電郵等。

使用更複雜密碼

部分 AI 軟件可用於破譯密碼，例如一款名為 PassGAN 的軟件，會使用從外洩的資料庫中獲取的數百萬個真實密碼，進行破譯密碼訓練。用戶在不同的網站開設賬號時，可以使用不同的密碼，也可設置更長的密碼加大破解難度。

常閱讀私隱政策

使用網絡服務、分享任何類型的個人資料前，用戶應留意閱讀私隱政策，了解相關企業、網站和平台會如何處理公開的資料。若條款和政策對用戶保護私隱不利，用戶應設法避免使用相關服務，或盡可能避免公開分享自己的資料。

科技界研多種方法訓練 AI 並保護私隱

香港文匯報訊 人工智能（AI）技術發展，需要使用大量資料補充大型語言模型（LLM）數據庫，發展 AI 技術與保護個人私隱維持平衡，成為科技業界一大挑戰。《福布斯》雜誌引述美國科企 YData 創辦人、AI 技術專家克萊門特分析稱，研發團隊補充 LLM 數據庫時，可使用自動化個人資料識別技術、差分私隱和合成資料等方法，作為抹除數據中的個人資料、保護個人私隱的方法。

使用合成資料

克萊門特指出，自動化個人資料識別技術是利用特定演算法，篩選除收集的數據中所有個人資料，自動將當中的敏感資訊和數據匿名化，再輸入數據庫中。完善的自動化技術可以快速篩選數據、節約成本，提升利用大型數據庫訓練 AI 系統的效率，也可以最大限度避免對個人資料處理不當可能帶來的後果。

差分私隱則是一種共享數據方式，在處理數據時，差分私隱方法會利用演算法，



◆發展 AI 技術與保護個人私隱維持平衡，成為科技業界一大挑戰。 網上圖片

為所有數據添加一組隨機代碼，令系統無法準確識別特定對象的個人資料，但不會影響對目標群體的統計學分析。將差分私隱方法應用到訓練 AI 模型的資料中，可以保證 AI 模型的整體訓練效果，同時降低特定對象的資料被識別利用的風險。

克萊門特還提到，另一種訓練 AI 模型的方法是利用合成資料，這些看似關乎「真實人物」、包括詳細地址和電話等信息的資料，實則是完全用自動化演算法創建的假資料，不包含任何真實的個人資料和私隱。使用合成資料訓練 AI 系統，不會直接接觸用戶的真實數據，可以滿足多地個人資料保護法的要求。加上這些資料屬於人工產物，即使發生意外事故，這些假數據外洩也不會影響用戶的安全。

擬收集用戶數據訓練 Meta 在歐盟 11 國收投訴

香港文匯報訊 科企 Meta 將於 6 月 26 日更新私隱政策，默許其名下所有社媒用戶的帖子、私人照片和網絡跟蹤數據，用於訓練 Meta 的人工智能

（AI）系統。歐洲私隱權倡議組織 NOYB 就 Meta 此舉涉嫌違反歐盟《通用數據保護條例》，在歐盟 11 個國家發起投訴，呼籲當局叫停 Meta 的做法。

路透社報道，Meta 上月 22 日發布訊息稱，公司會使用名下社媒平台用戶在網上公開分享、獲得用戶許可的信息，用作訓練 AI 系統。然而 Meta 發送給名下社媒 Facebook 用戶的信息稱，即使沒有使用 Meta 的產品和服務，沒有 Meta 名下社媒賬號的人，他們的圖像若出現在其他用戶公開分享的影像或帖文中，Meta 仍可能收集並處理這些資料。

NOYB 稱，該組織已呼籲法國和德

國等 11 個歐盟國家的執法部門採取行動。組織創辦人施雷姆斯表示，歐洲法院 2021 年已裁定在廣告事務上，Meta 沒有合法權益凌駕於用戶的個人資料保護權之上，「Meta 試圖用同樣的方法訓練其 AI 系統，公然無視歐盟法院的裁決。」

最高罰 4% 營業額

依照歐盟《通用數據保護條例》，涉嫌違規的企業可被罰款，最高達全球總營業額的 4%。施雷姆斯稱，歐洲現行法例要求 Meta 允許用戶自行選擇，是否將公開的資料給予該公司作 AI 軟件訓練用途，而非默認公司可使用相關資料，要求用戶申請退出。