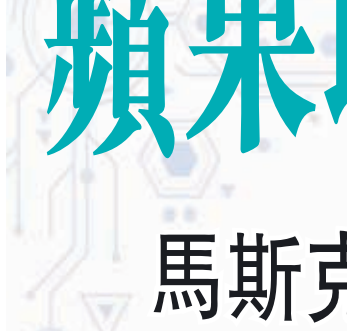
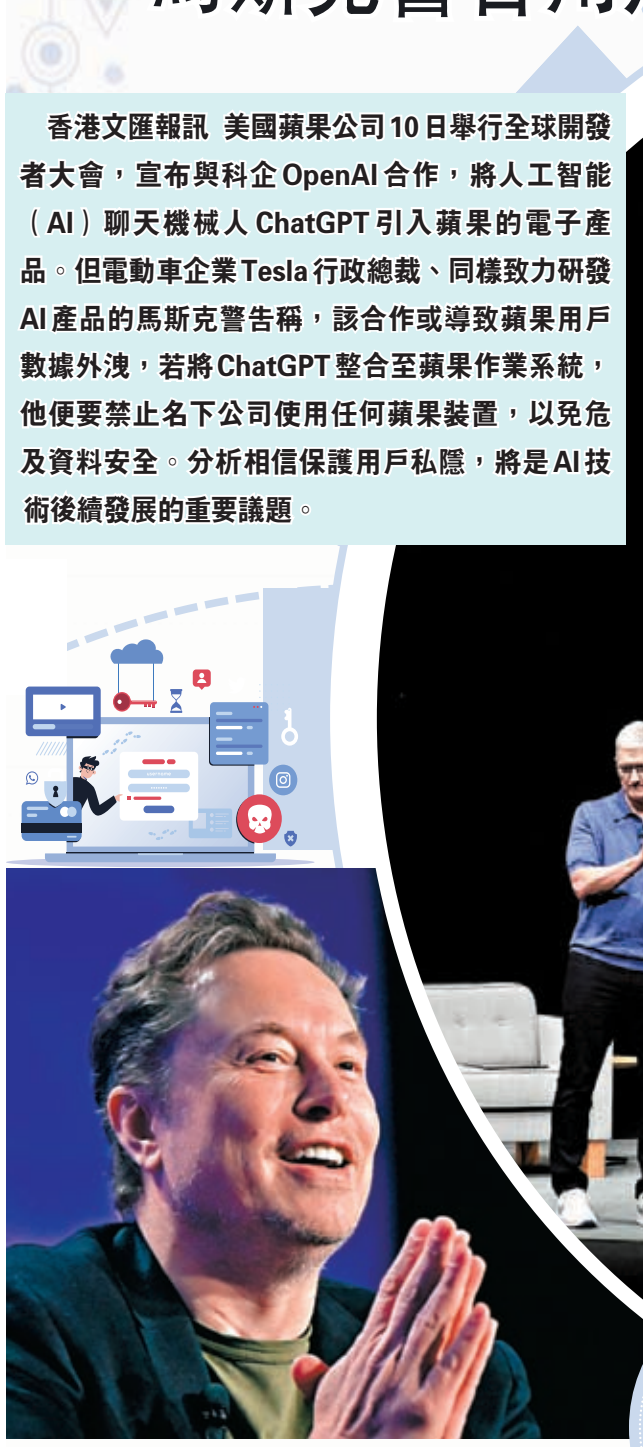
蘋果聯手OpenAI 保護私隱引熱議

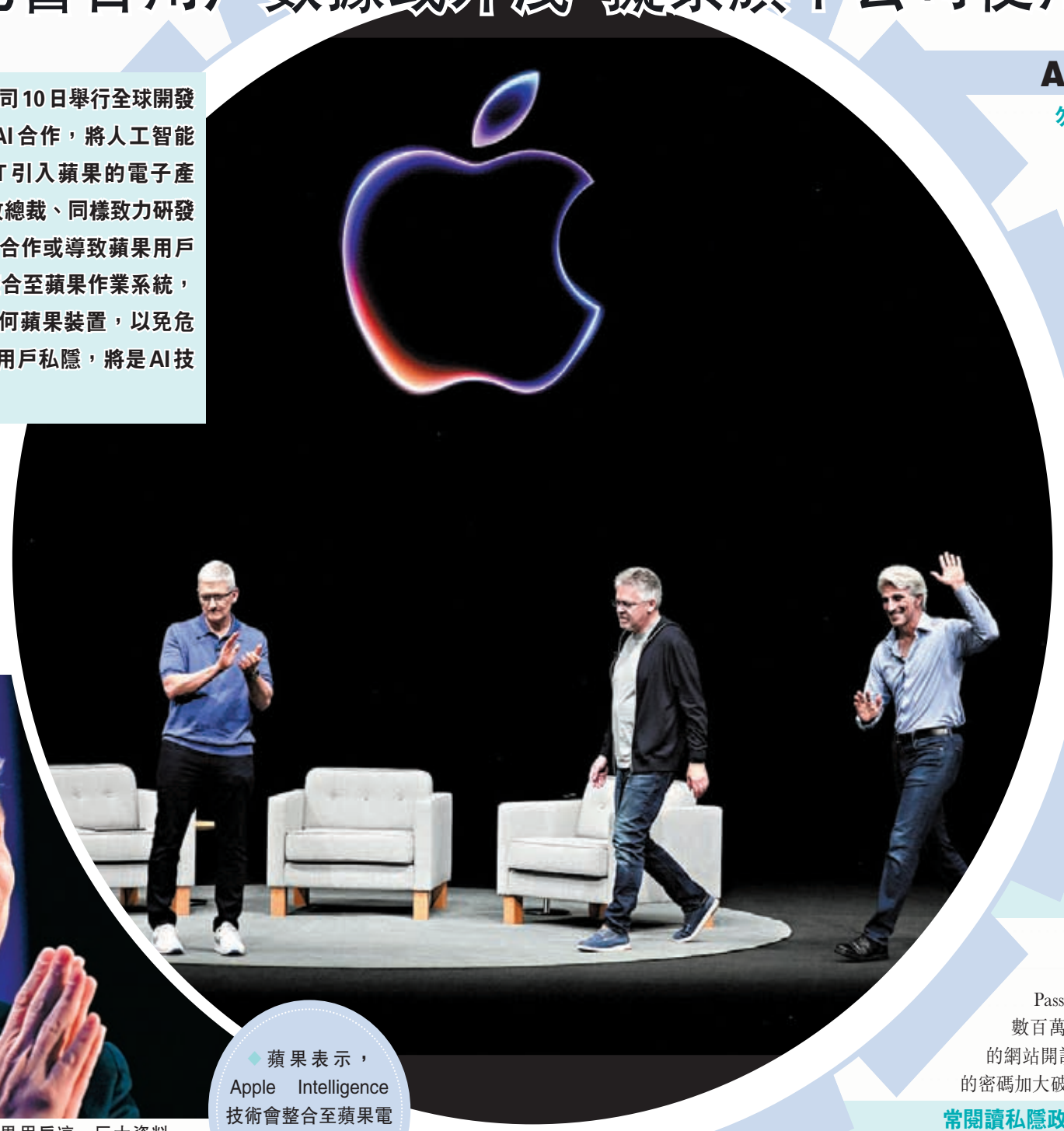
馬斯克警告用戶數據或外洩 擬禁旗下公司使用蘋果設備

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，都不會被長期保存。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，例如黑客可以冒用受害人身份使用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。」

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。

◆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

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，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數據，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。

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。

◆民眾在OpenAI總部抗議，要求安全建設AI。 網上圖片

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工具時保證未成年人安全。

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還提出一項法案，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。

維納稱，新法案會將安全測試限定在企業投資超過1億美元開發的大型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。」

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26日更新私隱政策，默許其名下所有社媒使用其用戶的帖文、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。

◆示威人士在歐洲議會大樓前放置朱克伯格的人形紙牌。 網上圖片

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數據保護權之上，「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%。施姆雷斯稱，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。