隱私 AI 發展 應受重視

黃光彩（臺灣量自安全協會理事長）

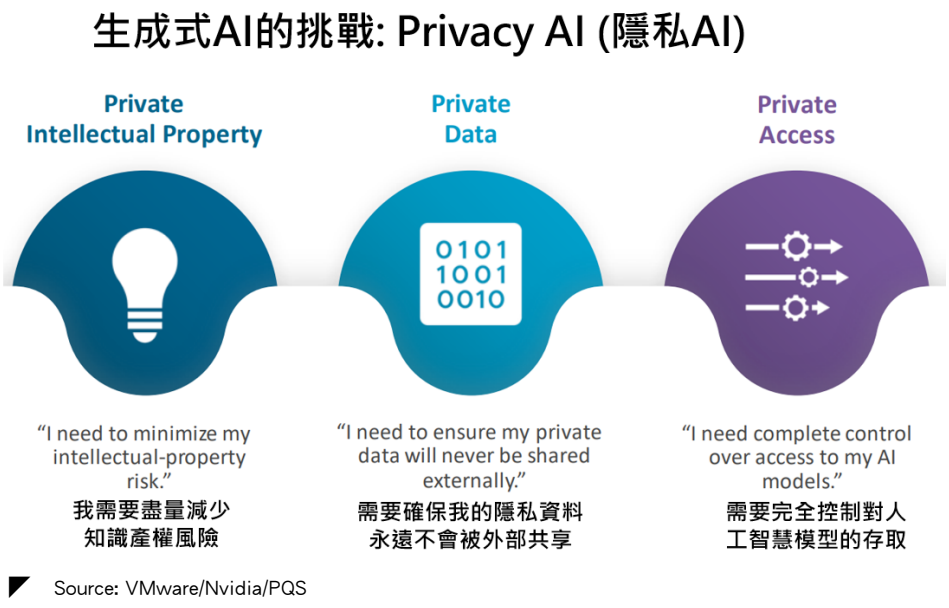
根據 NIST 的報告，人工智慧（AI）系統主要可分為**預測性 AI（Pred AI）和生成式 AI（Gen AI）**，這兩種類型在技術手段和應用場景上有所不同，因此在規範和使用上也應該有所區分。

生成式 AI 技術的出現為 AI 帶來了新的突破，它不僅可以觀測、分類和分析數據，還可以生成全新的內容。Pred AI 是利用複雜的演算法和機器學習技術，來分析大量的資料，找出模式，並做出未來可能發生的預測或決策。在網路安全領域，這種技術可以幫助辨識潛在的安全漏洞，預測新的攻擊手法，並主動防禦網路威脅。

企業領導者對於生成式 AI 的應用充滿期待，隨著 5G／6G／LEO、AI、大數據等新技術的快速發展和創新應用，各類數據海量聚集，呈現指數級增長。數據安全也已經成為事關國家安全與經濟社會發展的重大問題。他們認識到這一技術將為業務帶來巨大的商機，同時也意識到可能面臨的風險和挑戰。通過各行業的應用測試，產業必須要更好地評估生成式 AI 的建置，並制定相應的應對策略，以確保生成式 AI 的負責使用。全球各地的企業都在積極將生成式 AI 整合到自己的業務中，希望以此加速業務發展並提高效率。然而，在這一過程中，如何保護客戶的數據隱私、確保數據安全成為一個新的挑戰。

生成式 AI 將能夠為金融服務、醫療保健、製造等領域的成千上萬客戶提供其所需的全棧式軟體和運算，使其能夠使用基於自身資料定制的應用，充分挖掘生成式 AI 的潛力。隨著生成式 AI 爆發，企業紛紛想投入自家的機密資料訓練「專屬大腦」，根

Vision



據市調機構麥肯錫估計，生成式 AI 每年可能為全球經濟增加多達 4.4 兆美元的價值。

Privacy AI（隱私AI）

數字經濟時代的特徵是將數據視為關鍵的生產要素，通過跨領域、跨行業、跨地域的機構間的數據流通來釋放要素價值，但是在面臨數據融合需求的同時，如何防止數據的泄露、盜用、濫用，仍是機構參與數據流通時面臨的難題。隱私 AI 主要關注在利用 AI 技術的同時，保護個人隱私。

Private AI 是一種架構方案，可解鎖 AI 商業效益並滿足企業實際隱私與合規需求。它的核心價值是保護用戶的隱私。它致力於為開發人員提供可靠的隱私保護解決方案，並確保數據的安全和保密。它還提供可以自定義和控制的 Access Control，以確保數據只能被授權人士使用，同時會涉及到 AI 開發或使用單位、政府是否有良好的資料治理（data governance）政策。它的重點包括：

- **隱私保護的技術應用：**隱私 AI 技術致力於在不暴露個人敏感信息的情況下，進行數據分析和處理。這包括使用如同態加密（Homomorphic Encryption）、差分隱私（Differential Privacy）等技術來保護數據在使用過程中的隱私。
- **解決的問題：**隱私 AI 要解決的問題是如何在大數據時代中，實現數據的有效利用與個人隱私的保護之間的平衡。特別是在稅務、醫療、金融等敏感數據領域，這一問題尤為重要。
- **領域推動者：**推動隱私 AI 領域的領導者包括一些專注於 AI 安全和隱私研究的個人、公司和學術機構。例如 OpenAI 就是在 AI 倫理和安全性方面做出貢獻的組織之一。
- **保護的資料：**PII（personal identifiable information）、PHI（personal health information），和 PCI（personal card Information）均屬於隱私資訊治理類別。治理被定義為組織必須遵守的安全法規，以保護敏感的客戶資訊並對其使用保持透明。

Private AI 應用案例：供應鏈金融

供應鏈金融是企業經營的一個關鍵領域，它涉

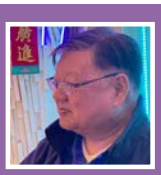
及到企業之間的資金流動、資金調配和風險管理。使用 Private AI 在供應鏈金融中有其必要，因為：

- **數據隱私保護：**供應鏈金融涉及大量數據，包括交易記錄、供應商信息和金融數據。使用 Private AI 可以確保這些數據的隱私和安全，防止未經授權的訪問或數據泄露。
- **增強的效率和準確性：**Private AI 可以自動分析和修改策略、計劃和資源分配，並生成各種形式的內容，從而實現更快的響應時間。這有助於提高供應鏈金融的效率和準確性。
- **風險評估和管理：**Private AI 可以幫助企業對供應商進行風險評估，並制定可管理的供應鏈金融解決方案。通過使用 AI 分割供應商，可以更好地評估其支付風險。

Private AI 可以使供應鏈金融更加安全、高效且具有彈性，並為企業提供更好的數據隱私保護和風險管理. 最近，VMware 宣告攜手數家公司如 NVIDIA、Intel、IBM 等，抓緊商機攻進企業私有 AI 領域，能夠讓企業把 AI 建立在自己的資料中心或伺服器中，不需要經手其他大型雲端公司，或者擔心被餵給通用的 AI 模型訓練。它的技術能夠協助企業做到：

向上擴展（Scale-up）：GPU 使用效率提升、共享資源效率。

向外擴展（Scale-out）：部署在更多環境，應用更多元。



作者黃光彩博士，現為臺灣量子安全協會理事長，亞洲大學講座教授，曾是台師大校長、IBM 全球副總、企業董事。專長為 AI、知識管理、供應鏈金融、企業轉型等。專注於量子計算、後量子資安、高速運算的散熱系統從晶片到資料中心。