AI技術與隱私

台大電機系 于天立

tianliyu@ntu.edu.tw

技術及法令

- 人工智慧/機器學習/資料探勘/資料科學
- 希望從大量資料中找出有用的資訊與知識，而非利用資料分析特定個體。

- 歐盟資料保護指令 (95/46/EC)
- 亞洲太平洋經濟合作會議 (APED) 的隱私架構
- 經濟合作暨發展組織 (OECD) 的隱私原則
- 2003 美國參議院通過一項法令，禁止國防部利用資料探勘方法蒐集、分析一般民眾的資料

案例

- 2006 AOL → 650k user search records with anonymous IDs. Recovered by NY times, 5 million USD.
- 2006 Netflix Prize 100 million data → predicting movie rating. 16 days later, two researchers (U of Taxes) matching the data with IMDB reviews.
- 2009 被告 “To some, renting a movie such as *Brokeback Mountain* or even *The Passion of the Christ* can be a personal issue that they would not want published to the world.” 9 million USD.

注重隱私保護的機制

- 模糊敏感資料的精確度
  - 資料抑制(suppression)
- 隨機修改
- 分散式儲存

技術

- 匿名化 (k-anonymity)
- 多様化 (l-diversity)
- 接近化 (t-closeness)
- 差分穏私 (ε-differential privacy)
- 同態加密（homomorphic encryption）
- 零知識証明（zero-knowledge proof）

零知識證明

- 一種特殊的交互式證明
- 證明者知道問題的答案，他需要向驗證者證明「他知道答案」這一事實，但是要求驗證者不能獲得答案的任何信息。
- 數獨例子

法規面期許

- 腳步常常太慢
- 責任分擔常有技術進入門檻問題
- 技術本身並不危險，危險的是使用它的人
- 一知半解的使用技術是危險的