T-Road與個人隱私保障

中央研究院資訊科學研究所

王柏堯

安全與隱私

- 安全與隱私是類似但不同之問題。簡要地說
  - 安全泛指保護資料，不讓資料洩漏給未經授權的對象。
  - 隱私泛指在給予經授權資料後，對個人資訊還需有所保障。
- 舉例而言
  - 確保我的資料從未外流，是安全問題。
  - 確保他人無法自授權後的資料中，推論我其他的資訊，是隱私問題。
- 安全是一個非常古老的問題，經過數千年的努力，目前仍未解決。
  - Caesar cipher (Julius Caesar, 100-44BC)
- 隱私是一個非常年輕的問題，目前連問題都還沒有弄清楚。
  - The Right to Privacy (Warren and Brandeis, 1890)

隱私保障的困難

- 隱私的意義，隨著文化、族群、時代、個體的不同，而有不同的解釋。
- 在哲學、法學、及社會科學中，對隱私有很多的探討。
  - 研討會中有許多專家，請勿錯過他們的演講。
- 由於隱私尚未有普遍且精確的定義，隱私保障便需要符合社會及法律的要求，不會只是一個技術問題。
- 就算把隱私保障簡化爲一個技術問題，過去二十年的經驗，也指出隱私保障是一個非常複雜的技術問題。
- 相較於安全，我們對隱私的瞭解實在太少。

隱私保障的條件

- 在問題和目標並不明確的情形下，其實不容易進行技術面的討論。
- 爲了便於討論，以下列出一些關於隱私保障的條件：
  1. 隱私保障不應基於他人之善意。
     - ★ Amazon Alexa, Apple Siri, Facebook and Cambridge Analytica, Google DeepMind, PRISM, ...
  2. 隱私保障需符合法律要求。
     - ★ 法律是社會規範的底線，任何隱私保障機制必須符合法律要求。
  3. 隱私保障應滿足個人期望。
     - ★ 每個人對其隱私有不同的定義，一個好的隱私保障機制應客制化，以滿足個人不同的要求。
- 以下，我將根據這些條件，討論T-Road目前及未來可能要面對的隱私問題。

MyData I

- 以下來自MyData網站中〔關於MyData〕:
  - 「MyData數位服務個人化」平臺（以下簡稱本平臺）以「民眾隨心同意、資料隨手可得」爲核心理念，提供民眾多元化資料下載及線上服務，讓原本就屬於民眾的資料，重新回歸於民，透過您當次的同意，便可在MyData 平臺中取得政府機關單位所保存您的個人資料，並可當次將這些資料提供給政府機關或您信賴的企業使用。
- 任何個人資料的電子傳輸，都有安全與隱私的風險；個人資料自行保存，又必須承擔更多的安全與隱私風險。
- 另外，我相信最後幾句話事實上應該是：

  透過您當次的同意，便可在MyData 平臺中取得政府機關單位所保存您的個人資料，並可當次將這些資料提供給政府機關或您信賴的企業重覆使用。

MyData II

- 以下來自「MyData數位服務個人化」首頁→資料下載→財稅→財產資料→我要下載

  三、 資料保管及使用

  1. 當您使用本平臺取得個人資料後請妥善保管，其下載資料後續的保管、使用方式及其所造成之影響，本平臺不負任何保管、管理及損害賠償責任。

- 某甲自MyData下載個人資料後，MyData明確地告知不負任何保管、管理及損害賠償責任。
- 問：某甲要如何妥善保管其個人資料？
  - 定期更新系統及軟體、安裝並定期使用防毒工具、定期變更密碼、不使用可疑的軟體、不流覽可疑網頁等等
  - 有多少人覺得各位的手機或電腦從來沒有、將來也不會外洩資料？
- 民眾隨心同意、資料隨手可得、後果自行承擔。
  - 隱私保障沒有滿足個人期望。

MyData III

- 數位個人資料非常容易複製。
- 假設某乙授權A機構自MyData下載其個人資料。
- 若是該資料以電子檔傳送，A機構可以複製並重覆使用。
  - 當A機構重覆使用或是洩露某乙的個人資料，某乙能知道隱私受侵犯嗎？
  - 隱私保障基於他人之善意。
- 理論上，A機構必須在個人資料保護法的規範下，蒐集、利用、處理某乙的個人資料。
- 我們可以更具體地看A機構如何保障某乙的隱私。

MyData IV

- 以下是與MyData合作的兩家機構，申辦同一業務時，其網頁法定告知事項中的「特定目的」：
  - 機構一所列舉之特定目的：
    022 外匯業務；040 行銷(包含金控共同行銷或合作推廣業務)；059 金融服務業依法令規定及金融監理需要，所爲之蒐集處理及利用；060 金融爭議處理；061 金融監督、管理與檢查；063 非公務機關依法定義務所進行個人資料之蒐集處理及利用；065 保險經紀、代理、公證業務；067 信用卡、現金卡、轉帳卡或電子票證業務；069 契約、類似契約或其他法律關係管理之事務；082 借款户與存款户存借作業綜合管理；088 核貸與授信業務；090 消費者、客户管理與服務；091 消費者保護；093 財產保險；098 商業與技術資訊；104 帳務管理及債權交易業務；129 會計與相關服務；135 資(通)訊服務；136 資(通)訊與資料庫管理；137 資通安全與管理；148 網路購物及其他電子商務服務；106 授信業務(含事後管理)；111 票券業務；126 債權整貼現及收買業務；154 徵信；157 調查、統計與研究分析；177 其他金融管理業務；181 其他經營合於營業登記項目或組織章程所定之業務；182 其他諮詢與顧問服務。
  - 機構二所列舉之特定目的：
    001 人身保險；022 外匯業務；036 存款與匯款；040 行銷；059 金融服務業依法令規定及金融監理需要，所爲之蒐集處理及利用；060 金融爭議處理；063 非公務機關依法定義務所進行個人資料之蒐集處理及利用；065 保險代理業務；067 轉帳卡業務；068 信託業務；069 契約、類似契約或其他法律關係管理之事務；082 借款户與存款户存借作業綜合管理；088 核貸與授信業務；090 消費者、客户管理與服務；091 消費者保護；093 財產保險；098 商業與技術資訊；104 帳務管理及債權交易業務；106 授信業務；111 票券業務；112 票據交換業務；126 債權整貼現及收買業務；135 資(通)訊服務；136 資(通)訊與資料庫管理；137 資通安全與管理；154 徵信；157 調查、統計與研究分析；177 其他金融管理業務；181 其他經營合於營業登記項目或組織章程所定之業務；182 其他諮詢與顧問服務。
- 「特定目的」可以包含行銷、網路購物及其他電子商務服務、其他金融管理業務、其他經營合於營業登記項目或組織章程所定之業務、其他諮詢與顧問服務。

T-Road

- 以下來自國家發展委員會「智慧政府推動策略計畫(核定本)」(行政院108年1月10日核定)：
  爲加速串連政府業務資料庫，建立安全可信賴的政府資料交換機制爲智慧政府優先重點工作。
- MyData允許機關或機構，經個人授權，獲得單筆個人資料。
- T-Road允許機關之間，傳遞多筆個人資料。
- 當大眾個人資料外洩時，如何究責？
  - 是傳送個人資料之機關，未妥善保管所蒐集之個人資料，應當負責？
  - 還是接收個人資料之機關，未妥善使用個人資料，應當負責？
  - 或是T-Road，未妥善處理個人資料的傳遞，應當負責？
  - 系統是否保留詳細的記錄，以利究責？
    - ★ 機關是否希望保留詳細記錄，以利究責？

隱私保障眞歷史 I

- 美國麻州州政府團體保險委員會（Group Insurance Commission）負責爲州政府員工購買健康保險。
- 團保委員會也蒐集135,000政府員工及其家屬之保險資料，經去識別化後，提供給研究人員及賣給產業界。
- 去識別化後的資料，約有一百個欄位。包含：性別、種族、出生年月日、五碼郵遞區號、就診日、診斷、處方、給付總額等。
- 1997年，有好事者分析公開的保險資料，發現只要性別、出生年月日、五碼郵遞區號，即可分辨不同個人。
- 於是好事者花了20美元，買了本麻州選舉人名冊。名冊中包含具選舉權人之姓名、地址、性別、出生年月日、五碼郵遞區號、註冊日期、政黨、上次投票日等。
- 好事者從選舉人名冊之公開資料，找到州長的出生年月日及五碼郵遞區號。又根據公開的保險資料之性別、出生年月日、五碼郵遞區號，找出州長的保險資料，並將保險資料寄給州長。
- Sweeney爲保障隱私，提出了k-匿名機制，現今仍被廣爲使用。

隱私保障眞歷史 II

- 然而k-匿名並無法完美地保障隱私，許多不同的隱私保障機制陸續被提出，也一一被修正。
  - k-anonymity （k-匿名）, multiR k-anonymity, ℓ-diversity, confidence bounding, (a, k)-anonymity, (X, Y)-anonymity, (k, e)-anonymity, (ϵ, m)-anonymity, personalized privacy, t-closedness, δ-presence, (c, t)-isolation, ϵ-differential privacy, (d, γ)-privacy, distributional privacy, ϵ-Pufferfish privacy
- 經過二十年的努力，我們還是沒有找到一個完美的隱私保障機制。每個機制都有不足之處。
- 更不幸的是，不同的資料有不同的特性，而不同的特性需要不同的隱私保障機制，沒有一個機制適用於各種不同特性的資料庫。
- 就算把隱私保障視爲技術問題，二十年的研究只告訴我們，隱私保障是一個非常複雜的技術問題，至今仍然無解。

未來T-Road之建議

- 在differential privacy及其衍生的框架下，個人隱私與資料價值只能求得平衡，無法兩者兼得。當具有價值之個人資料在機關間傳遞，必須承擔相對之隱私風險。
- 不同機關所蒐集之個人資料，具有不同之特性。故其隱私風險及對應之隱私保障機制也不同，必須各自評估。
- 當不同機關之資料互相串連後，便成爲另一個具不同特性之資料庫。這個串連後的資料庫，也必須重新評估隱私風險及設計其隱私保障機制。
- 若是機關所蒐集之個人資料開放給非公務機關使用，隱私風險評估、隱私保障機制、以及究責機制也需重新考量，以符合法律規範。

結語

- 隱私保障同時牽涉法律與技術，比安全問題複雜。
- 如同安全，誠實地面對問題才能眞正地保護個人隱私。

參考文獻

- Sweeney. *k*-Anonymity: A model for protecting privacy. Int. J. Uncertainty, Fuzziness, Knowledge-Based Systems. 10, 557–570. 2002.
- Fung, Wang, Chen, Yu. Privacy-Preserving Data Publishing: A Survey of Recent Developments. ACM Computing Survey. 42(4), 14:1–14:53. 2010.
- Dwork. Differential Privacy. ICALP. LNVS 4052. 1–12. 2006.
- Kifer, Machanavajjhala. Pufferfish: A Framework for Mathematical Privacy Definitions. ACMT Transaction on Database Systems. 39(1), 3:1–3:36. 2014.