# 資訊研究中的去識別化問題

吳全峰
副研究員
中央研究院法律學研究所



Institutum Jurisprudentiae
Academia Sinica
中央研究院 法律學研究所
Institutum Jurisprudentiae
Academia Sinica

# 資訊隱私保護之利益

- 個人資料不得任意去識別
  - *Whalen v. Roe* 法院對於資訊隱私之保護，認為實際上應包含兩種不同之利益(Helen L. Gilbert, Minors' *Constitutional Right to Informational Privacy*, 74 U. CHI. L. REV. 1375 (2007))
    - 資訊隱私/資訊安全（security of personal information），亦即避免個人資料之外流
    - 資訊自主（autonomy in making important decisions），亦即對個人資訊獨立決定之權利
  - 比例原則之利用
    - 除非具正當理由，否則資訊自主不應受到限制（亦即不得在無正當理由下任意去識別/去連結）
    - 即使資訊自主因正當理由受到限制，亦應將相關資訊提供個人，以將限制資訊自主之傷害降到最低

# 不滿裸照被挪用 女秀出「2顆痣」告贏名醫

2014-11-25 08:23

〔即時新聞／綜合報導〕一名林姓女子前年至名媛診所整形，術後竟發現自己的胸部「裸照」被「整形風」網站做為宣傳用途，氣得向整形醫生蔡豐州提告，法官經比對林女身上「2顆痣」位置，認定蔡男刊登的確實為林女胸部，判蔡男和唐姓負責人應賠償林女20萬元。

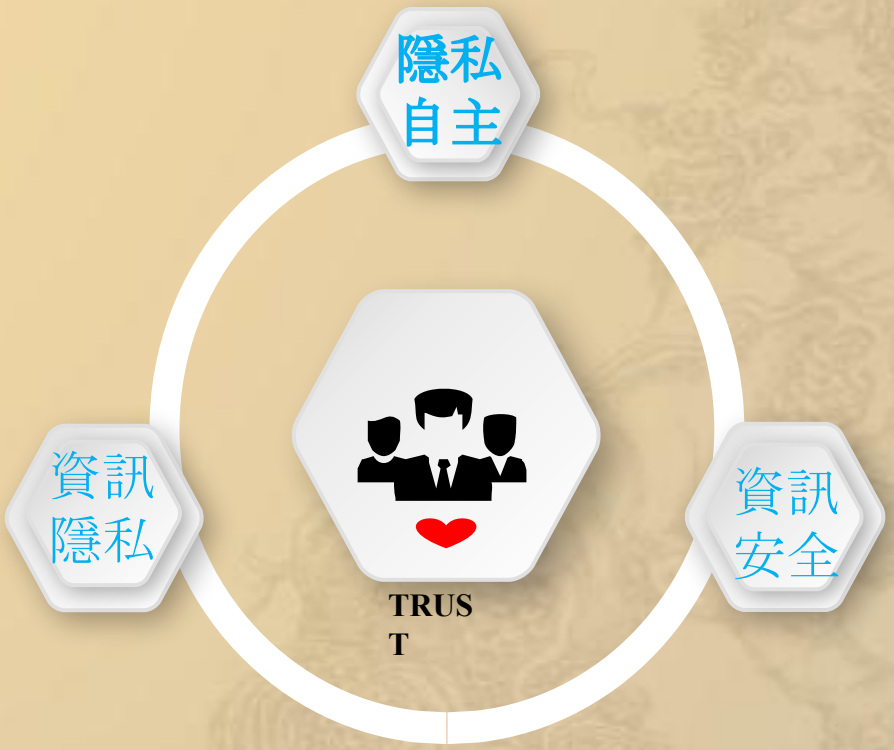
一名女子整形術後發現自己的胸部「裸照」被網站做為宣傳用途，氣得提告。示意圖，與本新聞無關。（資料照）

《蘋果日報》報導，北市林姓女子控告名媛診所名醫蔡豐州侵害隱私權，指出自己前年至該診所整形，而蔡男事後竟擅自將她手術前後的胸部裸照放在「整形風」網站，照片中清楚拍攝林女頸部至肚臍間的部位，還附註「蔡豐州醫師」、「版權所有」等字樣。

對此，蔡男表示，「整形風」屬於學術性網站，自己不清楚照片來源，且強調裸照「沒拍到臉」、「看不出是誰」。林女氣憤、痛罵蔡男推卸責任，為證明網站中胸部確實為己所有，林女自拍裸體供法官比對，由於2照片中皆出現「2顆痣」、且位置一致，法官認定照片為林女本人，判定蔡男與名媛診所負責人唐書榮應連帶賠償林女20萬元。

# 資訊隱私保護之利益

- 去識別化之建立
  - 個人資料隱私(隱私自主、資訊隱私)、資訊安全之平衡
  - 正當程序保障
  - 標準、機制與作業流程



# 去除個人資訊(identifiers)之方式:台灣(I)

- 台灣對於資料去除個人資料後提供再利用之概念架構並不明確
  - 人體研究法第4條第3款規定「去連結:指將研究對象之人體檢體、自然人資料及其他有關之資料、資訊(以下簡稱研究材料)**編碼**或以其他方式處理後,使其與可供辨識研究對象之個人資料、資訊,**永久不能以任何方式連結、比對之作業**」
  - 人體生物資料庫管理條例採類似之相同規定,第3條第7款規定「去連結:指於生物檢體、資料、資訊**編碼**後,使其與可供辨識參與者之個人資料、資訊,**永久無法以任何方式連結、比對之作業**」
  - 人體生物資料庫管理條例18條第1項規定「設置者就其所有之生物檢體及相關資料、資訊為儲存、運用、揭露時,**應以編碼、加密、去連結或其他無法辨識參與者身分之方式為之**。」
  - 個人資料保護法僅有「依其揭露方式無從[直接或間接]識別當事人」之用語,其概念上殆與「去連結」相當
    - 個人資料保護法施行細則第2條:**本法第二條第一款所稱得以間接方式識別,指保有該資料之公務或非公務機關僅以該資料不能直接識別,須與其他資料對照、組合、連結等,始能識別該特定之個人。**
    - 個人資料保護法第17條:...**所稱無從識別特定當事人,指個人資料以代碼、匿名、隱藏部分資料或其他方式,無從辨識該特定個人者。**
- 資料處理程度:經濟部標準檢驗局「個人資料去識別化過程驗證要求及控制措施」技術文件(CN29100及CN29191)

# 去除個人資訊(identifiers)之方式:各國比較

- 美國與歐盟對於隱私(包括資訊自主與資訊安全)之基本價值並不相同，導致其對去除個人資訊之方式，與相對應之管制模式出現差異
  - 美國:以個人自主保障為主，因此限制之要件(去除個人資訊之範圍與再識別化之可能性)較為寬鬆 → 當事人同意不必然成為正當化之要件
  - 歐盟:以人性尊嚴為主，因此限制之要件(去除個人資訊之範圍與再識別化之可能性)較為嚴格 → 當事人同意為正當化之要件

# 去除個人資訊之方式：去識別化（de-identification）

- 美國HIPAA所發展出之概念，指去除**個人資訊**（identifiers）之健康資訊，無法據以識別特定個人或基於合理確信該資訊將無法作為識別特定個人之資訊：
  - 透過統計學家或具有相當經驗之專家，判斷該資料無法識別當事人
  - 透過刪除18項列舉的辨識項目以達成去識別化的效果
- 某種程度認為去識別化即可以達成永久無法直接或間接辨識特定個人之目的，因此美國法便認為在此情形下直接提供去識別化之資料供研究使用並對個人資訊自主加以限制，應具有正當性
  - 但在科技進步與運算成本降低之情形下，再**識別**（re-identification）**之**風險大幅增加，美國學界對於單純去識別化是否足以正當化健康資訊之再利用，亦有所批評

# 資訊隱私保護之利益：美國HIPAA

- 原則禁止使用或揭露當事人之健康資訊(protected health information, PHI)，除非有**法律明文規範**之以下目的，可不需當事人授權（authorization）：
  - 提供予資料所有人、係基於診斷、付費及照護措施(treatment, payment, and health care operations, TPO)之目的、有提供當事人表示反對之機會…
  - 透過去除下列 18 種個人資訊達成去識別（de-identified）
    - 姓名
    - 地理資訊
    - 各種日期資訊
    - 電話號碼
    - 傳真號碼
    - 電子郵件地址
    - 社會安全號碼
    - 病歷號碼
    - 醫療計畫或健保號碼
    - 帳號
    - 各種證照編號
    - 車牌、車籍資料
    - 設備編號或序號
    - 網路位址(URLs)
    - IP位址
    - 生物辨識資料（如指紋、聲紋）
    - 臉部照片
    - 其他可識別個人之編號或特徵

但在當事人第一次就醫並使用該機構提供之健康照護服務前，機構有義務以書面（notice letter）通知當事人資料可能之使用方式與對象（換言之，當事人似仍有選擇退出之機會）

# 去除個人資訊之方式：匿名（anonymization）

- 德國聯邦個人資料保護法BDSG規定，「匿名表現(rendering anonymous)」係指修改個人資料使有關私人或具體情況之訊息無法對應至已識別或得識別之個人，或**須耗費過鉅或耗時過久**始得識別者
- 德國並不認為可以藉由**去除個人資訊而達到永久無法識別特定個人之目的**
  - **也因此，此立場可能促成德國採資料主體收集（資料）（collecting from the data subject）原則，亦即資料原則上應從資料所有人處收集並利用，在利用並不允許，除非基於法律另有規定、基於履行行政義務的本質需要從其他人或其他團體處取得資料、或是從資料所有人收集將需要不合乎比例的努力**
  - **即令證明從資料所有人收集將需要不合乎比例的努力，但因其利用與原來收集目的不相同時，故仍需資料所有人之同意**
  - **換言之，資料之再利用仍以當事人同意為原則，而匿名化僅為資料處理之過程，並不足以構成限縮個人資訊自主之正當理由（因永久無法識別為無法想像）**

# 去除個人資訊之方式：匿名（anonymization）

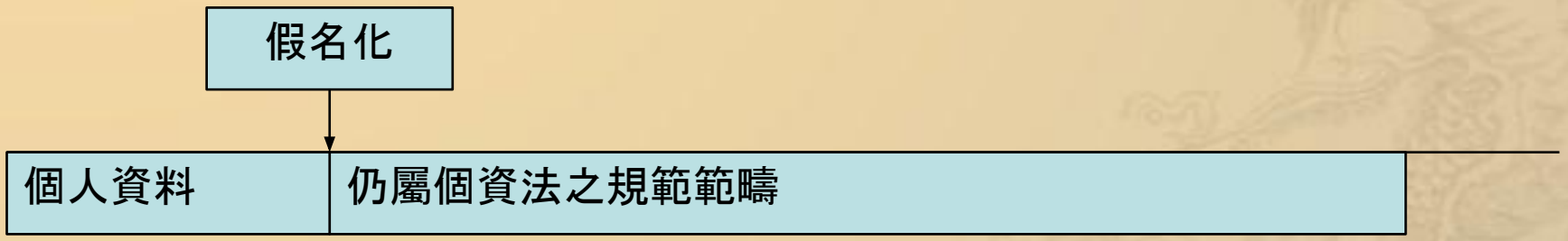
- 歐盟立法例（Directive 95/46/EC, Recital 26）同樣認為者認為匿名須是不可逆的（irreversible），亦即特定個人之資訊在匿名化後將無法透過所有、可能、合理的方式被辨識出來
  - 因此，匿名化僅被視為應用處理個人資料之一項技術，且依目前的技術，將形成如同刪除般的永久效果（as permanent as erasure）；換言之，匿名化將使個人資料不能夠再為處理（Opinion 05/2014 on Anonymisation Techniques）
  - 但既然匿名化僅為一項技術，且無法確認匿名化後即完全不能識別特定個人（It is critical to understand that when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this dataset (for example after removal or masking of identifiable data), the resulting dataset is still personal data），故個人資訊自主仍有其重要性
  - 換言之，雖然經匿名化之資料得排除適用個人資料保護，但資料控制人在將資料進行匿名化時，仍須視為個人資料之處理，亦即仍受個人資料保護之規範並須符合相關規定，並無得豁免適用之情形

# 去除個人資訊之方式：匿名（anonymization）

- 歐盟Art 29 工作小組第216號有關匿名化技術意見書
  - 資料經處理後是否達到匿名化狀態之三項判斷依據(風險):
    - 是否仍可能**識別特定個人**(“single out” an individual?)
    - 是否仍可**連結至個人相關紀錄**(link records “relating” to an individual?)**及**
    - 是否仍得從相關資訊**推斷至個人**(can information be “inferred” concerning an individual?)
- 比較
  - 歐盟相對嚴格，提供資料經匿名處理後須達**一切合理方法無法回復連結**至特定個人之要件之具體規範

# 去除個人資訊之方式：假名（pseudonymization）

- 資料經假名化後，仍得藉由資料控制人掌握之金鑰（key）回溯辨識當事人
  - 德國聯邦個人資料保護法規定「『假名/化名』係指為使資料當事人不可能被辨識或難以辨識，而改以另一識別符號以取代姓名或其他得識別之特徵」
  - 僅得視為「適當安全維護措施」，各國均未把假名化視為可提供二次利用之**去除個人資訊之方式**
  - 一般而言，假名化僅得用來進行**須辨識當事人**之醫學或基因研究（仍被視為可（間接）識別之個人資料）



# 爭取歐盟GDPR適足性認定 台歐盟展開技術性對話

2018-06-04 17:08

陳美伶說，GDPR號稱為史上最嚴格個資法，對於個資的輸出一定要獲得「明確同意」，且除非個資通通去識別化，使用代號或是假名都不符合規範，儘管歐盟沒有要求一定要修改當地法令，但在個資保護上必須符合歐盟要求，台灣個資法與歐盟1995個人資料保護指令大約同時，在個資輸出上並沒有明確規範，未來勢必要進行檢討，甚至不排除修法。


國發會主委陳美伶今日說明與歐盟達成開啟GDPR適足性認定工作（國發會提供）

# 去除個人資訊(identifiers)之方式:台灣(II)

- 最高行政法院106年度判字第54號 (106.01.25)
  - 本院發現**本案去識別化作業模 式，實不足到達「完全切斷資料內容與特定主體間之 連結線索」之程度，因此移轉至輔助參加人衛福部之健保資料，其「個人資料」屬性，尚未被全然排除( 雖然已經大幅度降低)**，因此仍有繼續檢討該資料收 受者輔助參加人衛福部對被上訴人所持有之健保資料 有無蒐集處理職權之必要
  - 從被上訴人與輔助參加人衛福部自承之「去識別化 」作業模式觀之，由輔助參加人衛福部派專人來執 行「加密」作業，再攜回加密之個人資料建置資料 庫。如此作業模式即表示輔助參加**人衛福部本也有 「還原」資料與主體間連結之能力，此等結果顯然與由被上訴人「單方」掌握「還原」能力之「去識 別化」標準不符**。
  - 被上訴人雖抗辯稱「『原始資料』仍然保留在被上 訴人手中」云云，但此等抗辯毫無道理，因為:**資 料實際上是一種訊息，應與訊息載體分離看待。而 所謂「原始資料」其實僅是儲放資料(訊息)之載 體，因此載體即使留在原處，載體內之訊息已透過 轉換載體之方式，而脫逸被上訴人之控管，並為輔 助參加人衛福部所控管，只要輔助參加人衛福部之 內部單位公務員，有「還原」資料與主體連結之可 能，對輔助參加人衛福部而言，該資料仍未「去識別化」，而屬「個人資料」**
  - 因為該等資 料解密鑰匙，仍由輔助參加人衛福部內負責資訊秘 密業務單位之公務員保有，而非輔助參加人衛福部 內之任何成員均可取閱，則該等資料與特定主體連 結之「可識別性」已大幅度降低，**但只要輔助參加 人衛福部內部單位成員，有還原資料與主體連結之能力，即不符合「去識別化」之標準**

# 擬匿名化

- 去識別化資料意義與類型
  - 意義--所謂「去識別化」，即指透過一定程序的加工處理，使個 人資料不再具有直接或間接識別性
  - 類型--依其去識別化之加工程度不同，有以下「匿名化資料」及「擬匿名化資料」之類型：
    - **匿名化資料（anonymised data）**：對任何人而言，均無法採取任何合理可能之方法識別特定個人，亦即資料經加工後，毫無保留連結之 可能性
    - **擬匿名化資料（pseudonymised data）**：擬匿名化資料乃是以編碼或 別名取代識別符（例如姓名、國民身分證統一編號等），使研究或統 計人員得以針對個體資訊進行分析而無須識別個體身分，可再細分為2 種態樣：
      - **不可逆（non-retraceable/irreversible）**：以非專屬編碼、單向演算加 密或其他技術處理，使任何人皆無重識別特定人
      - **可逆（retraceable/reversible）**：以專屬編碼、雙向演算加密或其 他技術處理，使其他人無重識別特定人，但原始資料保有者，仍得 透過代碼與原始識別資料對照表或解密工具（鑰匙）還原為識別資 料。此多用於依法允許重新識別之領域，例如：進行醫療實驗研究 時，為能適時回溯追蹤調整對受試病患之醫療處置。

# 去除個人資訊(identifiers)之方式:台灣(III)

- 台北高等行政法院103年訴更一字第120號判決
  - 認為「可逆之擬匿名化資料」(如專屬代碼或雙向加密等保留代碼與原始識別資料對照表或解密工具之方式)亦屬去識別化
  - 若係供公務機關或學術研究機構個別申請使用之資料，因資料提供對象有所限縮,除能對資料接收者之身分、使用目的、其他可能取得資料之管道 、安全管理措施等先為必要之審查外，並得與資料使用 者約定禁止重新識別資料之義務及其他資料利用之限制等，較有利於風險之控管，風險檻值相對較低，其資料去識別化之程度可相對放寬，可提供含有個體性、敏感 性之擬匿名化資料,亦即可採取「可逆之擬匿名化資料 」方式進行去識別化(即以專屬代碼、雙向加密或其他 技術處理，使處理後之編碼資料無從識別特定個人，惟原資料保有者保留代碼與原始識別資料對照表或解密工具〈鑰匙〉之方式)
- 最高行政法院106年度判字第54號判決
  - 無法解決「無法識別當事人」內涵之矛盾
    - 去識別化需「到達『完全切斷資料內容與特定主體間之連結線索』之程度
    - 去識別化「【毋需】徹底排除特定主體之個人資料……【以免】有礙於公益之實踐」

# 去除個人資訊之方式：台灣經驗之反省(I)

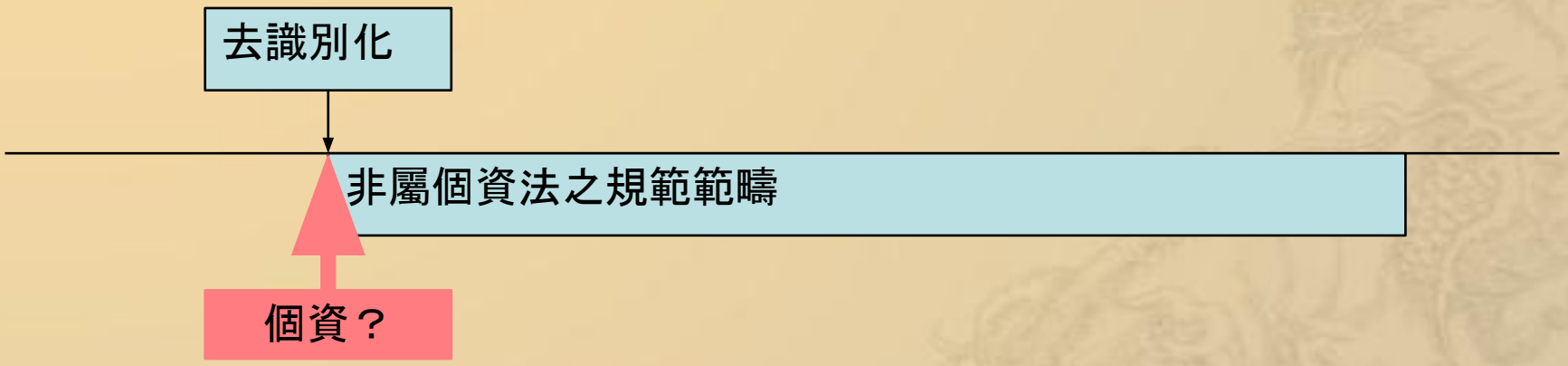
個人資料去識別化後即非個人資料，不受個人資料保護法之規範而得以任意使用？

歐盟對可識別之定義，應考慮所有可以被資料控制者或其他人採用之合理可能方法，判斷是否得用以識別特定個人；故去識別化似乎可被視為非屬個人資料而不受個人資料保護之規範，但此推論建立在以下三個前提：

- 政府不得任意將個人資料去識別後，便宣稱其不受個人資料保護；去識別仍需經當事人同意
- 假名化並非不可識別
- 刪除個人資訊變項並非真正不可識別
  - 因為現況無論資料做如何之處理，可能均無法達成永久無法識別特定人之目的(均有再識別之可能性)，因此需有適當之配套措施
    - 對於去識別之定義與操作應更為明確(各國採取之折衷方式，已非單純去除有關個人資訊之特定變項，而是以是否需耗費大量資源始能識別特定個人作為標準，並在此條件下例外允許使用)
    - 資訊之干擾或其他電腦技術之配合
    - 去識別之過程仍需以資訊自主作為正當性基礎
    - 適當且透明之資訊回饋機制

# 去除個人資訊之方式:台灣經驗之反省(II)

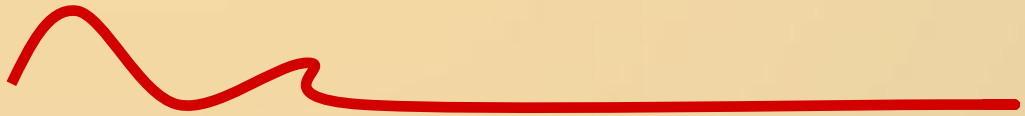
- 已去識別化即非屬個資法之規範範疇(法律字第10303513040號)
  - 如將公務機關保有的個人資料運用技術去識別化而呈現方式已無從直接或間接識別特定個人，即非屬個人資料，公務機關主動公開或被動受理人民請求提供上述政府資訊，除考量有無特別法限制外，分別依檔案法第 18 條或政府資訊公開法第18條相關規定決定是否公開或提供即可



# 去除個人資訊之方式：台灣經驗之反省(III)

- 即令以美國HIPAA較為寬鬆之標準觀察，台灣釋出健保資料所刪除之個人變項(identifiers)仍不完整
  - 以全民健保承保檔為例
    1. 組別
    2. 單位屬性
    3. **地區代號(縣市、區)**
    4. 個人身份證字號(加密處理)
    5. 個人身份證字號檢誤
    6. 個人身份證字號性別
    7. 被保險人身份證字號
    8. 被保險人身份證字號檢誤
    9. 被保險人個人身份證字號性別
    10. **出生年月**
    11. 眷屬稱謂
    12. 投保金額
    13. 異動別
    14. 身份屬性
    15. 保費計費年月
    16. 投保狀態
    17. 被保險人註記
    18. 應繳眷口數
    19. 免繳眷口數
  - 以全民健保低收入戶及中低收入戶檔為例
    1. 低收入戶列冊人口身份證字號(加密處理)
    2. 低收入戶列冊人口性別
    3. 低收入戶列冊人口身份證字號檢誤
    4. 低收入戶列冊款別
    5. **低收入戶列冊起始年月**
    6. **低收入戶列冊迄止年月**
    7. **縣市別**
    8. **鄉鎮市區**
    9. 低收入戶戶長身份證字號(加密處理)
    10. 低收入戶戶長性別
    11. 低收入戶戶長人口身份證字號檢誤

# THANK YOU



Institutum Jurisprudentiae
Academia Sinica
中央研究院 法律學研究所
Institutum Jurisprudentiae
Academia Sinica