國立臺灣大學法律學院法律學研究所

碩士論文

Department of Law

College of Law

National Taiwan University

Master Thesis

個人資料去識別化困境新解—「資料財產權」進路

A New Way to Solve the Problems of Personal Data in the Process of De-identification: "Data Property Right" Approach

嚴治翔

Chih-Hsiang Yen

指導教授：李建良 博士

Advisor: Chien-Liang Lee Ph.D.

中華民國 112 年 6 月

June 2023

doi:10.6342/NTU202301113

謝詞

本篇論文的完成尤其感謝李建良老師的悉心指導，從碩一下學期受老師指導以來，無論在基本人權課堂報告上、公法論壇的文章投稿上、還是後來一年的論文寫作上，老師總能在百忙公務中，以短短數語即點出我在論文思考架構上的核心矛盾及不足。老師從初始的決定題目、形成問題意識、到後續論文的發展，無不密切地指導，每次與老師討論完論文，總是會感到如沐春風，覺得對未來文獻查閱方向更加確定，或是發現更多論述途徑能使論文益臻完善。

此外，非常感謝口試委員吳全峰老師及何之行老師，以其等在醫療法、資訊隱私法的多年專業，於繁雜公務中仍撥冗審閱本篇論文，並在口試時就本篇論文格式、架構、實體核心問題意識等方向上提出極具建設性的批評及指教，尤其特別感謝兩位老師在美國案例法上提供的指導，讓我在後續論文修正上有了更明確的方向。

另外，在三年研究生活的面向上，我想特別感謝李建良老師、邱文聰老師、劉靜怡老師、蘇凱平老師及 Rob Leflar 老師，讓我能以研究或教學助理的方式學習，並獲得經濟上的支持。感謝李建良老師除了幫我撰寫推薦信讓我得以遠赴荷蘭萊頓大學進修外，更讓我加入台灣人工智慧行動網的文章編輯工作，讓我在整理摘要文章的同時，學到很多跟論文研究有關的知識；感謝邱文聰老師從我大四時起就聘我為獎補助生，讓我協助其職災因果關係研究文章的整理，在我進入研究所後，更繼續讓我參與個資權利管理系統及疫苗緊急授權法制的比較法研究，並提供我在中研院資訊法讀書會旁聽學習的機會，邱老師治學嚴謹又深具人文關懷，在學術研究及職涯發展方向上影響我至深；感謝劉靜怡老師讓我參與人工智慧相關法制研究，協助文章摘要使我的英文能力及資訊法知識大幅提升；感謝蘇凱平老師在法實證研究課程上對我的肯定，不但引介我認識邱老師，更邀請我加入司法院刑事量刑系統更新計畫，讓我得以進一步學習法實證研究。蘇老師時常關心研究生生活狀況，著實令人感到窩心；感謝 Rob Leflar 老師，一位美籍客座

doi:10.6342/NTU202301113

教授，除了在醫療法上指導我甚多，透過全英文的美式教學讓我對海外留學有更多想像，更讓我有榮幸擔任其教學助理得以向其學習更多。

至於在其他研究生活面向上，我想感謝黃詩淳老師對我在法實證研究上的指導，並協助我、林泉苗、及李芯發表文章於月旦裁判時報上；感謝邵軒磊老師教導我許多社會科學中機器學習、統計分析的技術，使我面對法實證問題時，能有更多工具去分析它；感謝榮譽導師李念祖老師，引介我受李劍非律師指導，編修案例憲法教科書，讓我得以在逐一審閱釋字的時候，重新認識憲法；也感謝老師總是於導生聚時分享司法軼聞、針砭時事，增廣我對律師執業的認識。

還有，感謝同門的翔安學長、毓庭學姊給我許多同門的建議與幫助；感謝德威擔任我的口試紀錄；感謝所有在公法論壇、論文發表上給我建議的夥伴，特別是國祐學長與詠綺；感謝冠宇學長幫我審閱論文；感謝存恩學長提供關於資料可攜權的文獻；感謝家妤學姊、昱廷學長、宏仁學長、熙哲學長、仁祥、宇宏、茵茵、靖庭曾與我一同討論本篇論文。另外，在論文之外，也感謝千豪學長、士程學長、京翰學長、能得學長在實習、語言學習上給我的幫助；感謝其叡、偉翔、庚翰與我一同參加法庭辯論賽豐富碩士生活；感謝鴻恩、紹誠讓我得以脫離台北租房地獄；感謝亭霖、青儒、子儀每週一起在壽司郎解悶；感謝世賢、承緯、宜軒、志剛等高中同學給我支持；感謝所有在律訓、農化系、及柔道隊相識的朋友給我的陪伴與鼓勵，特別是柔道隊及其指導老師黃國恩老師跟蘇玫尹老師，若沒有柔道作為運動及調劑，我是不可能完成這篇論文的。

最後，我想感謝我的父母及家人們願意在經濟上、心靈上支持我唸完碩士學位，讓我沒有其他後顧之憂。

嚴治翔 謹致

112 年 6 月

doi:10.6342/NTU202301113

摘要

本文首先聚焦於我國近年來各類政府主導的大型資料庫蒐集案例，歸納出其等多以去識別化為由規避取得個資主體的同意，本文因此分別從去識別化於於定義、技術、定位上的困境討論。

首先當前法律定義上內國定義混亂、比較法上因歷史脈絡無法同一比較，且運作上也不足以賦予個人足夠的控制；再者技術層面上也面臨類型化困難、欠缺統一量化標準等困境；最後於定位上，當前 GDPR 將「匿名化」概念跟其他個資同意、組織、程序保障掛鉤，也愈趨無法解決再識別技術所造成的威脅。

為了因應日漸升高的再識別風險，本文認為（1）應限縮當前歐盟 GDPR 中的「匿名化」概念，使其與其他個資同意、組織、程序保障脫鉤。（2）應將去識別化處理單純理解為資安風控手段，而非影響個資保護規範適用範圍的前提影響因子。（3）應統一目前「去識別化」於法律上及技術定義上的不同。（4）應立法區分不同利用目的、不同資料類型、不同個資主體，以適用不同的同意授權模式。另外，也應使個體就該模式下需面臨再識別風險有更清楚的認知。

最後，為了使個人就其個資的控制，無論如何皆不因去識別化處理而喪失，本文從病歷、基因資訊的利用案例出發，探討美國法上「資料財產權」的理論是否得以透過談判交易、市場手段、限制授權、金錢賠補償等方式，增加個人對零碎、去識別個資的控制。結論上，本文認為美國法的資料財產權理論，基於人對財產具有控制的素樸想像，應有助於建立個人在資料關係中持續性的控制，進而有機會在理論上解決前述如何就去識別化資料賦予個人控制的難題。只不過從功能性、實用性角度而言，此一理論可能並非唯一解答，具體仍須仰賴立法解決。

關鍵字：個人資料；隱私；去識別化；匿名化；財產權；人格權；所有權

doi:10.6342/NTU202301113

Abstract

This thesis focuses on the trend of government claiming that there's no need to obtain consents from data subjects, since the personal data has already gone through de-identification. However, this could cause harm to data subjects. To analyze, this thesis then discusses the three dangers of the over-reliance on de-identification which includes that there's no single definition on de-identification and anonymization; there're also difficulties in categorizing, or generalizing different standards on the de-identification techniques; further, there's no general standard to measure or quantify how high the risk of re-identification is; lastly, present GDPR adopts the concept of anonymous information and uses it to distinguish whether GDPR applies, which makes the regulation itself incapable of dealing with the threat of re-identification.

This thesis suggest that: (1) the concept of anonymous information should be disconnected with the application of GDPR, (2) the process of de-identification should be simply taken as a measure to safeguard the information security rather than the distinguisher of whether the information concerned applies to GDPR, (3) a single, generalized standard on the techniques of de-identification should be established, though it may be difficult, (4) different kind of purpose of data utilizations, genres, and data subjects should apply to different de-identification models, and different consent models. In addition, data subject should be clearly informed about the risk of re-identification under different models.

Lastly, in order to enhance data subjects' control over their personal information, not to let this control weaken by the process of de-identification, this thesis refers to the past disputes between ownership and privacy in the cases of medical records and genetic information. Some suggested to use 'privacy as property' theory in these cases, which aimed to solve the problems by adopting the concept of information market, negotiation, transaction, monetary compensation, and restraints on PII alienation.

In essence, this theory considers the instinct of thinking personal information as one's property help enhance data subjects' control over their information. Though there may be some downsides of this theory, it's a good reference to solve the difficulties of people losing control in the process of de-identification. The theory may not be the only answer to the problem, while it does provide a great insight to the dilemma brought by the big data and the new re-identification techniques. The ultimate solution still has to rely on the legislation.

Keywords: personal identifiable information, data property right, de-identification, anonymous information, restraints on PII alienation, genetic information, data ownership

doi:10.6342/NTU202301113

簡目

doi:10.6342/NTU202301113

詳目

doi:10.6342/NTU202301113

doi:10.6342/NTU202301113

doi:10.6342/NTU202301113

第一章　　緒論

第一節　　問題意識

到底何謂資料？何謂隱私？這些都是近年來資訊社會下每天都聽得到詞彙，然而就其定義卻鮮少能有明確的共識，至於其性質則更是眾說紛紜。

傳統的文獻多著重於探討何謂隱私？其內涵為何？其近年發展態樣為何？如何透過目的限制原則、告知後同意原則、去識別化處理等方式處理資料。但上述這些解決方法無不碰到瓶頸，就目的限制原則而言，資料蒐集目的難以於蒐集初即特定，資料的累積效果使得資料的用途會隨著時間而改變，資料聚匯也使得可利用方向亦趨難以預測，因此就蒐集方就面臨了是否要再次尋求同意、同意成本是否過大的問題；至於對於資料主體方也不容易，個人並不容易於資料蒐集之初就了解蒐集可能對其造成之影響，故因而導致大多數人僅是對空泛或難以理解的告知條款進行同意，導致喪失尋求告知後同意的意義，更甚者乃是就算了解了條款的意義，多數人也無從做出選擇，畢竟消費者所面臨的乃是「全有全無」的選擇，選擇拒絕隱私條款進而拒絕享受服務，或者是選擇放棄隱私投向業者所提供的服務，在如此二選一的難題裡，多數人選擇了後者。

在這樣的情形下，現行的個資保護變得十分扭曲，資料蒐集方會優先傾向將資料去識別化以規避取得同意的麻煩，畢竟只要不是個人資料就不受個資法保護。再者蒐集方會用晦澀的告知同意條款廣泛性的取得同意，這部分對於資料主體來說也意義不大，因此現行體制下，有許多人認為這些基於個資保護所要求的程序是一種不效率[1]。

[1] 現實中的例子舉凡金融領域的集團公司資料共享、進行金融業務前繁複的個資告知同意規定、醫療領域的健保資料庫利用、國民數位身分證發行或是近一年來每天生活必需掃瞄的簡訊實聯制 QRCODE，都未見資料主體對這些議題的重視。

doi:10.6342/NTU202301113

近年來各國開始出現有一些媒體、政治人物、學者開始使用資料財產權或與其相類似的用語來討論個人資料，詞彙上像資料探勘（Data Mining）、資料乃資訊社會下的新石油（Data as Oil）等用語出現，此在在顯示了人們對於資料已經不再是僅從傳統人格權角度去思考，關於資料的財產權等利用面向已經開始被重視。也就是說在企業開始著重資料利用、資料分析的同時，人們也開始反向思考自己的個人資料（如年齡、性別、健康資料、行動軌跡）、非個人資料（購買物品種類、數量、企業資料）是否具有金錢上的價值。而此類主張者大多抱持著與其事後才對資料外洩或是目的外利用撤回同意、請求損害賠償，不如事前就對資料定價來保障資料，不過當然這些主張也面對了不少批評。

本文的問題意識在於，在現行個資保護法制面臨的瓶頸下，我們究竟應該如何分類資料、如何對不同資料定性？所謂個資的定義是否在大數據發展下而擴張至原先不被認為屬於個資之資料？在這樣的情形下，我們是否該不再堅持資料與個人間必須具備可識別性？而是轉向從財產權角度，不論是否經去識別化的角度，去談個資隱私保護？又，我們該如何區分不同資料類型以適用不同保護手段？到底怎麼定性資料才能更促進隱私權的保護？本文將重新爬梳資料權跟隱私權兩者重合及得以互相借鑑之處，從保護目的出發，探討究竟應從何種憲法上權利（人格權？財產權？或兩者？）去保護資料，較足以在當事人自主權的貫徹與資料有效利用間取得平衡。

第二節　　研究範圍

隱私的分類中，Anita Allen 將隱私權依其內容分為以下四種：(1)資訊隱私權、(2)身體隱私權、(3)自主決定隱私權、(4)具財產價值之隱私權[2]。雖然曾有國

[2] Anita L. Allen, *Genetic Privacy: Emerging Concepts and Values, in* GENETIC SECRETS: PROTECTING PRIVACY AND CONFIDENTIALITY IN THE GENETIC ERA 31, 33 (Mark A. Rothstein ed., 1997).

doi:10.6342/NTU202301113

內學者指出[3]，該四種分類未必妥適，未必皆屬於隱私自主權的內涵，而且具財產價值之隱私權應在財產權的範圍下討論即可，不必在隱私權的脈絡下討論。

惟本文認為分類(1)、(4)間其實有定義重合的地方。在大數據分析盛行的今日，純粹的資訊隱私跟具財產權性質的隱私權之間界線已經越來越模糊。資訊隱私權係指涉個人對於個人資訊公開的對象、時間、方式，得以自行決定的權利，應屬較無爭議的定義及類型，其內涵亦受到釋字 603 號解釋所使用，其謂：「……隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障（本院釋字第五八五號解釋參照）。其中就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權……」。本文基於資訊隱私權受到我國憲法明確肯認，故以下將會把有關資料權、隱私權的討論聚焦在資訊隱私權的面向上，另外關於具財產價值之隱私權於此部分多少也有點重疊的部分，因為其正好就牽涉了本文想進行的關於資訊隱私權定性的討論，故也同樣在研究範圍內。

原則上本文將聚焦於討論「得重複利用」、「利用後繼續存在」、「有資料累積聚集效應」、「具有可利用、交換等財產價值」的個人資訊隱私，包含但不限於人類行為特徵受到抽象蒐集再利用所產製的資訊，因此研究範圍並不限縮於與個人相關的個人資料，縱使是傳統上經去識別化而被認為屬於非個人資料者，也會在本文之研究範圍內，不過本文核心的問題意識仍會聚焦在如何以財產權及

[3] 林子儀（2002），〈基因資訊與基因隱私權—從保障隱私的觀點論基因資訊的利用與法的規制〉，Robert Heuser（等著），《當代公法新論（中） ─翁岳生教授七秩誕辰祝壽論文集》，頁 701，台北：元照。

doi:10.6342/NTU202301113

相關保障體系為借鏡，據以保障個資為主體的隱私權法制，因此非個人資料部分僅於理論上無法切割時提及，不會是本文主要探討隱私財產性質的核心。

第三節　　研究方法

本文之研究方法將主要以文獻研究法為主，文獻來源為國內外專書、期刊、論文、以及比較法及相關實務判決等為主，外文文獻上將以英文文獻為主，另外比較法參考上則以美國國內學說、歐盟(General Data Protection Regulation, 2016, GDPR)、等相關個人資料法制為主。

本文主要將以承認資料財產權性質、可交易性的優劣理論分析為主，主要在於透過理論爬梳，建構對資料、數據的最佳定性，目的在據此建構更完善的資料保障體系。

第四節　　論文架構

本文將分成五個章節，於第一章緒論中介紹本文之問題意識、研究範圍、研究方法及本文架構。第二章從歷史脈絡出發，從我國近年幾個重大的政府資料庫建立案例中，重新盤點資訊隱私權於近年來所面臨的挑戰，本文將類型化這些挑戰，歸咎於大數據發展對去識別化產生的定義、技術、定位上的困境，並呈現目前國內外學者對這些挑戰的回應，再聚焦於如何就去識別化個資賦予個人控制此項子議題，最後本文將說明為何認為這些回應並不足以解決當前資料法制所面臨的挑戰，並提出拒斥匿名化概念、類型化去識別化手段，並將之定位為資安手段的解方。另外，為了說明為何個人得以對當前認定屬「匿名化」之個資具有自主控制利益，本文參考了美國的資料財產權理論，並欲以該理論較符合個人直觀為由據以擴張個資定義，增強既有欲強化自主控制的相關理論，就此本文不會對實際上同意機制等隱私設計置喙，僅就理論層面出發，探討何種理論足以在再識別科技發達的今日，使得個人無論就可識別、去識別資料都能取得控制。

doi:10.6342/NTU202301113

第三章，為了探討「資料財產權」理論是否有助於完備「隱私財產權」得加強個人對去識別化資料控制的論述，本文先從「資料財產權」與「隱私財產權」兩個理論的交叉點——病歷資訊隱私及基因資訊隱私的利用爭議為引子出發，繼而引導到「資料究竟應如何定性？」、「資料權屬於人格權還是財產權？還是是什麼權其實並不重要？」等上位概念的重新爬梳。最後第四章則從美國、歐盟、中國等比較法觀點探討「資料是否可以容納財產權的主張？其正反意見為何？」、「具體立法上應定位為哪種財產權？物權？債權？還是智慧財產權？」等更細緻的問題討論上，論述角度上主要從各國比較法，尤其美國法為主的文獻爬梳切入。

對於資料的定性，傳統上採取的是從人格權理論出發，近期則另有資料財產權理論、資料主體相當於投資人理論、智慧財產權理論、資料利用相當於海難救助等千奇百怪的理論出現，本文將逐一介紹這些理論，最後各自點出其優缺之處，並說明本文見解。最後第五章則為結論。

必須特別說明者係，在第三章以降或許會有「資料財產」與「隱私財產」夾敘、混用、混淆，或是覺得本文轉向論述「資料財產」而與第一、二章論述「隱私財產」脫鉤的疑慮，惟本文特此說明，這是由於本文旨在處理「經去識別化處理過後的個資是否仍屬個資？」之故。本文至第二章的結論是認為其等定義上「應該屬於個資」，然而因為在傳統定義上「經去識別化處理過後的個資已非個資」，故本文才退一步去從「資料財產權」的角度去切入，試圖在功能上賦予這些經去識別化處理的「資料」一個類似個資體系，只是從不同理論基礎切入，但賦予主體同樣、甚至更強控制力的機制。簡言之，正是因為「個資」跟「資料」的定義在去識別化技術日新月異的今日不斷被挑戰、模糊化，才形成了本文第一、二章在「個資」體系內論述，第三、四章轉向「資料」體系論述的論文架構。

doi:10.6342/NTU202301113

第二章　　資訊隱私權的當代困境

本文將於本章第一節中介紹三個近年來我國政府建置大型資料庫蒐集個人資料、提供跨資料庫串接可能性的案例，在第二節中歸納說明當代資訊隱私最大的困境分別為去識別化困境，與目的外二次利用困境，在第三節中聚焦於去識別化困境，從定義、技術、與個資定義的關聯等角度分別探討並在援引我國學者見解後，提出本文見解。

第一節　　近期實際案例

以下分別介紹 ETC 案、健保資料庫案及疫情下鑽石公主號之電信追蹤案：

第一項　**ETC 案**

國道 ETC 「國道電子收費系統」（Electronic Toll Collection，ETC），是交通部用以取代國道收費員站崗的新興收費模式，也是現今唯一的國道收費方式。西元 2004 年時，交通部以 BOT 的方式，委託遠東集團旗下的子公司遠通電收，負責 ETC 的建置與維護。遠通電收在 2005 年底完成 ETC 建置，並於 2006 年開始啟用。啟用之初，由於車主仍需自費申裝 ETC 的偵測器，因而安裝率始終低迷不振。低安裝率的狀況，一直要到 2011 年底，遠通改採具有無線射頻辨識（RFID）功能的電子標籤 eTag，並祭出首次免費安裝的方案後，才大幅改善。而到 2016 年時，eTag 的申裝率已超過 94%[4]。

ETC 的運作方式乃在交流道出入口裝設偵測儀器，以計程收費的方式進行。換言之，遠通電收必須蒐集所有國道車輛的路程起迄及收費記錄，才能達成收費目的。由於安裝率高，國道每日的使用者也多，又僅有單一收費方式，因此經年累月下來，即成為一個涵括全時段、全路段、且不同車型的巨量資料庫。

[4] 此部分關於 ETC 案的簡要及運作介紹，摘自何明諠（2016），〈數位時代的隱私邊界：以健保資料庫與 ETC 交通資料庫為例〉，《台灣人權學刊》，3 卷 4 期，頁 146-148。援不一一引註。

doi:10.6342/NTU202301113

此一資料庫由於有受資料探勘等潛在的經濟價值，交通部甚至在 2015 年六月時，舉辦「高速公路 ETC 資料在交通管理之應用創意競賽」，更同時將資料庫進行去識別化後，做成開放資料，並以每日更新的方式，供全國或全世界的人民使用，至今皆是如此[5]。根據何明諠的整理，交通部高速公路管理局建置該資料庫政策背後的理由略為「交通資料蒐集研究及運用亦能運用於大眾運輸規劃或即時交通資訊提供，確有助於增進公共利益。」交通部並進而以公益為由，據以規避個資法關於當事人同意的要件。

然而 ETC 資料庫所可延伸的爭議並不止於去識別化不足，或是「公益」說明不足的抽象問題，交通裁罰實務中即有裁罰機關向遠東電收公司調閱車輛 ETC 相關資料做為訴訟上證明違規的證據[6]，進而延伸的隱私權爭議。案例事實略為原告行經高速公路路肩時遭第三人以行車紀錄器檢舉，原告主張第三人之行車紀錄器是否經校準不無疑義，被告則在訴訟中調取原告之 ETC 相關紀錄佐證。事實審法院略以：「……基於前開司法院釋字第 603 號解釋意旨，本院認政府基於提升高速公路收費效率之特定目的，委託民間設置高速公路電子收費系統，蒐集人民在高速公路行動之資料，其設置目的及功能既在『電子收費』，除有重大事由(如重大犯罪刑事偵防)外，應禁止『法定目的外使用』，即就 ETC 相關資料，除有特定重大事由外，應禁止在電子收費目的外使用。」進而認為該資料不得做為證據，進而撤銷原處分。

然而本件訴訟原告於二審中以及更一審中皆受到逆轉的敗訴判決。二審台北高等行政法院在判決理由中[7]，迂迴地繞過機關以違反個資法的方式取得證據是否得適用的問題，轉而以法院應職權調查證據為由撤銷原判決，認為：「……檢舉人之行車紀錄器是否有定期實施校準或遭人為調整，而致其時間標示發生不準

[5] 關於今年的比賽請參見高速公路局網站，https://www.freeway.gov.tw/Publish.aspx?cnid=2863（最後瀏覽日：02/17/2021）。
[6] 臺灣新竹地方法院 105 年度交字第 119 號判決
[7] 臺北高等行政法院 106 年度交上字第 82 號判決

doi:10.6342/NTU202301113

確之疑義，並非不能命檢舉人以證人身分具結作證，或對其行車紀錄器加以檢驗等調查方法予以釐清，且檢舉人若願提供其 ETC 相關資料，似亦非不能佐證檢舉人於 105 年 4 月 30 日駕車行經國道 1 號高速公路南下 88.1 公里處之時點，並非欠缺調查管道，原審法院仍應依職權查明為裁判基礎之事實關係，不受當事人主張之拘束。」

此處法院的論理凸顯了該資料庫另一爭議。即縱使不論「機關得否以公共利益為由」調取 ETC 相關資料，裁罰機關仍可以徵詢檢舉人是否願意同意提供 ETC 相關資料去做舉證，此時第一層次的問題乃「第三人所擁有的 ETC 資料是否與被檢舉人的資訊隱私權完全無關？」，第二層次的問題則係「被檢舉人的資訊隱私是否因此被再識別而受侵害？」因此，本文認為台北高等行政法院之論理是否符合個資法的要求，並非無疑。

至於本件最後的更審判決[8]則認為：「……惟本件被告向遠通公司調閱系爭車輛 105 年 4 月 30 日之 ETC 通行錄，係在已知特定交通違規行為之狀態下，佐證證明行為人即原告有違反道路交通管理處罰條例之行為，以維護道路交通安全，應認係為防止他人權益之重大危害，為增進公共利益所必要，仍得為特定目的外之利用。是本件被告調閱原告車輛之 ETC 通行紀錄，並未違反個人資料保護法相關規定，該 ETC 相關資料，當可作為本件違規行為之證據使用。」本判決雖正面處理該資料庫調取是否符合個資法的爭議，然而卻對於公共利益模糊帶過，論述不清，且疑似倒果為因地去論證公共利益的存在，先以有檢舉人的檢舉在先，因此對違規事實的確定性較高，裁罰機關即有公共利益去調取，然而調取 ETC 資料的目的即在證明檢舉人的檢附資料是否屬實，檢舉人的檢附資料能否作為公益的基礎並非無疑，更審判決如此論述公益的方式無疑顯得怪異且忽略個人隱私在公益價值衡量中的角色。

[8] 臺灣新竹地方法院 107 年度交更一字第 1 號判決

doi:10.6342/NTU202301113

上述關於 ETC 相關資料的調取爭議並未停止，根據公路總局[9]，為有效降低超速可能造成較嚴重之交通事故，該局將於台 61 線沿線與桃園市、苗栗縣、臺中市、彰化縣及雲林縣政府警察局合作，設置區間測速執法設備，以執行速度管理。目前該設備均已建置中或已完成正進行宣導中，預計將於 109 年春節前陸續開始執法。區間平均速率科技執法重點，主要目的在於維持路線整體車流效率及降低肇事率，蓋以往取締超速都採固定式測速照相或由警方現場拍照，其所偵測皆為單點瞬間速度，駕駛人常常於測速地點減速至規定速限內，然離開測速地點後又恢復原超速狀態，對於行車速度之控制非常有限。區間測速係將速度控制範圍由點擴大至線，不採偵測單點速度，而以車輛行駛時間與距離加以換算平均速度作為執法依。對於駕駛人而言，在測速範圍內即使稍有超速，只要後續將速度降低，尚能符合規定速限，相較於固定測速方式更具調整之空間與彈性[10]。

為計算平均速率，現行已實施多年之 ETC 系統成為最容易且最快速建置區間平均速率執法系統的工具，隨之則引發諸多質疑，如該執法方式是否合乎法源依據、ETC 系統是否會侵犯個人隱私等。

目前對此似尚無司法案件可資參考，然依據新北市政府警察局交通警察大隊針對萬里隧道執行區間平均速率科技執法的公告說明[11]，其指出「道路交通管理處罰條例（以下簡稱道交條例）第 40 條規定對於現行法令就超速之認定，並無限制僅能以雷達或雷射等設備偵測，換言之，以區間平均速率認定超速亦符合法令規定」；至於偵測系統有無侵犯個資，該大隊則說明「車輛號牌係依交通法規公開之資訊，屬個資法第 2 條第 1 款『其他得以直接或間接方式識別該個人之資料』，但車牌號碼在未有其他資訊（車籍資料）輔助下，尚不足以指向特定個人，

[9] 以台中市施行區間測速為例，參考交通部公路總局網站，https://www.thb.gov.tw/sites/ch/modules/news/news_details?node=eeb33aa6-58a1-4d5d-b6aa-28dd4d5270b0&id=0393a5b4-649f-45d6-9549-3927b7b35fe7（最後瀏覽日：02/17/2021）。

[10] 吳侑霖、張育瑋、呂佩玲（2019），〈科技執法於易肇事路段之應用－以台 2 線萬里隧道為例〉，《臺灣公路工程》， 45 卷 2 期，頁 14-25。

[11] 新北市政府警察局(2019)。《平均速率科技執法》，載於：https://www.traffic.police.ntpc.gov.tw/cp-2772-44747-27.html（最後瀏覽日：02/17/2021）。

doi:10.6342/NTU202301113

屬間接個資。警察機關實施區間測速執法所蒐集車牌號碼資訊或處理係執法所必須，符合個人資料保護法第 15 條第 1 項第 1 款『公務機關對個人資料之蒐集或處理，應有特定目的』，並符合執行法定職務必要範圍內之規定。」

簡言之，又是一件以公益之名，輔以間接個資不足以識別個人，非屬個資而不因受到保護的論理。然而普設區間測速所取得的資料絕非僅限於車輛號牌，路徑速度、車輛外觀、行經時間的紀錄皆在其內，以上綜合的取得下是否仍為個資法下的間接個資？新北市政府警察局交通警察大隊的說明無疑顯得避重就輕。

第二項　健保資料庫案

本件乃進入經終局判決確定，幾年前由台灣人權促進會提出釋憲聲請[12]，並於近日於憲法法庭完成言詞辯論的程序[13]，其原因案件為最高行政法院 106 年度判字第 54 號判決，其乃近年來國內討論最熱烈的實務爭議，為數不少的研究隱私權的學者都有對本案表示意見，其重要性不言而喻。

本件起於中央健康保險署（當時為健保局）原為辦理全民健保業務，依全民健康保險法蒐集個人就醫與健康保險資料，卻自 1998 年起，在未告知個資當事人（自亦未得其同意）的情況下，即經初步加密，逕將所蒐集之健保資料委託國家衛生研究院建置「全民健康保險研究資料庫」，再提供或販售予學術界與非學術界用於健保業務以外之目的，又自 2011 年起，直接將完整可識別之健保個資，提供予第三人，即衛福部（當時為衛生署）建置大型資料庫，由衛福部自行以代碼取代姓名與身分證字號後，提供使用者做跨資料庫（包括其他衛福資料，以及衛福部以外之其他公務機關蒐集之資料）間之連結比對，用於學術研究及生醫產業研發目的。原告為被蒐集個資之人民，其等分別於 2012 年五月、六月間，請

[12] 台權會網站，https://www.tahr.org.tw/cases/NHID（最後瀏覽日：02/17/2021）。
[13] 司法院網站，《健保資料庫案言詞辯論新聞稿》，https://www.judicial.gov.tw/tw/cp-1887-629970-b76ca-1.html，（最後瀏覽日：05/10/2022）。

doi:10.6342/NTU202301113

求健保署停止繼續將原告個人之全民健康保險資料用於保險相關業務以外之目的，亦即請求退出健保署或第三人在保險目的外所建置之資料庫。

最高行政法院最後判決原告敗訴，其背後理由的一項重點在於法院的一個核心想法，即個資如果可以通過「去識別化特定個人」之檢驗標準，即可確定上訴人等之隱私權不會受到侵犯，其核心的觀點就是個人資料的「去識別化」乃權衡個人資訊隱私權與健保資料庫公共利益衝突現象最有效率之手段[14]。法院進而以此作為拒絕原告行使事後退出權的理由之一，認定健保署拒絕原告行使事後退出權的決定，並未違反比例原則，駁回原告之訴。對此最高行政法院將去識別化的程度綁定是否構成隱私權侵害的內在邏輯，學者多以法務部於民國 101 年 7 月 30 日針對個資法第 16 條第 5 款及第 20 條第 5 款規定所做之函釋的第 4 點說明為例，認為此一邏輯乃機關所慣用[15]。此一批評絕非憑空而出，觀前述 2020 年執法機關針對 ETC 資料作為區間測速證據是否侵害隱私權的回應，亦可映證此點。

然而在質疑去識別化的資料是否仍受隱私權保障後，究應如何有效率地以告知後同意落實隱私權保障？學者張陳弘認為由於健保資料庫的資訊數量龐大，且嗣後常見不同於原蒐集目的以外的事後使用需求，因而倘若就人民的同意模式採取空白授權的同意模式將會不夠完善，然而倘若每次都需要逐一履行告知後同意，現實上無疑是窒礙難行。故主張透過分層同意的方式，藉由獨立委員會審查數個同意模式給予人民選擇，再配合例外除法律或法院命令另有規定，或是為了超越資訊隱私利益的公益時，始賦予人民得主張退出的制度去因應[16]。

---

[14] 張陳弘（2018），〈國家建置全民健康保險資料庫之資訊隱私保護爭議－評最高行政法院 106 年度判字第 54 號判決〉，《中原財經法學》，40 期，頁 246；最高行政法院 106 年度判字第 54 號判決，旁碼 1411-1415。「……而本案適用新個資法第 16 條但書第 5 款許可規定為檢驗後，如果得以通過「去識別化」之檢驗標準，即可終局確定上訴人等之隱私權不會受到侵犯，而其以「隱私權有受侵犯之虞」為基礎所提起之本案請求，亦可確定於法無據，原判決之最終判斷結論即可維持……」

[15] 法務部（101）年法律字第 10103106010 號函。其甚至認為個人資料經提供者處理後或蒐集者依其揭露方式無從再識別特定當事人後，則該筆去識別化之資料已非個資法第 2 條第 1 款所定之個資，即無個資法之適用。

[16] 張陳弘，前揭註 14，頁 214-219。

doi:10.6342/NTU202301113

對此一判決，學者邱文聰從另一角度分析[17]，認為根據 GDPR 第 21 條第 1 項規定，以「執行公益任務或公務」作為蒐集、處理或利用個資之合法基礎時，不僅應額外賦予個資當事人「反對權」，更應由公務機關負擔證明其資訊作為具有超越當事人自由權利保護必要之極重要公共利益的義務。套用在本件的話，也就是認為關於公共利益的舉證責任應由蒐集機關負擔。然而其認為本件爭議更根本的問題在於立法論上，個資法 16 條但書第 5 款上關於目的外利用之「去識別化」標準，究竟能否正當化個資的強制蒐集、處理或利用？關於這點的質疑其實與學者張陳弘之質疑相類。學者邱文聰的理由在於「徹底切斷資料與主體連結」後的資料，並非完全沒有統計或學術研究上的利用價值。其主張不應單以資料是否去識別化為審查標準，而應參考職業自由的三階段審查理論，並立基於釋字 603 號所隱含的類型化、不同密度的比例原則去決定審查標準。涵攝上其認為既然釋字 603 號在傳統大規模、建立資料庫的資訊作為採取中度審查，要求應「基於特定重大公益之目的」，並以法律明定，且「其蒐集應與重大公益目的之達成，具有密切之必要性與關聯性」。則在本件健保資料庫的情形，既然相較於釋字 603 號解釋的單純指紋蒐集有更進一步發展創造、描繪群體圖像的能力，即應採取最嚴格的審查基準。蓋資料庫建置後將會有後續決策、國家管制干預、給付或社會監控的可能，因此應該從人性尊嚴與尊重人格自由的角度去採取有別於釋字 603 號的審查標準。

結論上學者邱文聰認為個資法第十六條但書第五款僅以籠統的「學術研究」目的，甚而允許公務機關以「追求資料更高使用效率」，作為「強制徵收」「非真正去識別化」個人健保資料之理由，顯然不能通過「追求極為重要之公益目的」與「直接密切關聯之手段」的檢驗。

第三項　**疫情電信追蹤案**

[17] 邱文聰（2018），〈被淘空的法律保留與變質的資訊隱私憲法保障──評最高行政法院一○六年度判字第五四號判決與相關個資法條文〉，《月旦法學教室》，272 期，頁 38-43。

doi:10.6342/NTU202301113

2020 年 2 月 5 日我國接獲日本通報鑽石公主號郵輪發現武漢肺炎確診案例，回溯發現該郵輪曾於 2020 年 1 月 31 日停靠基隆港並有遊客下船觀光。由於武漢肺炎傳染力極強，必須及時掌握與該郵輪遊客接觸之人員，以免疫情失控，惟郵輪業已離開基隆港，無法進行遊客面對面訪視以瞭解實際旅遊景點與接觸民眾。因時間緊迫，為調查可能接觸對象，嚴重特殊傳染性肺炎中央流行疫情指揮中心（下稱中央流行疫情指揮中心）分析可能之調查方式包括調閱監視器與車牌辨識系統、刷卡紀錄、遊覽車行車紀錄 GPS、高速公路 eTag 紀錄等，惟前述資料都有其侷限性，首先關於監視器，不但可能有需要調取票的門檻問題，且重點在於其調閱耗費勞力時間過距，對於隔離的即時性而言不足。而就刷卡紀錄、行車紀錄、GPS 等紀錄而言，其等過於特定且記錄面向過於狹隘，蓋手機 GPS 功能可手動關閉，刷卡紀錄跟行車紀錄亦有不能完全透露遊客去向的缺點。最後，關於高速公路 eTag 記錄，其無法顯示目標遊客到底在其行程中接觸了哪些人，涵蓋不夠廣，故也不妥適。最後中央流行疫情指揮中心基於綜合上述考量，決定透過「手機漫遊定位紀錄」確認下船遊客行蹤及可能接觸之民眾。

其餘更細緻的理由有四，一乃基於風險管理的角度必須匡列的範圍可以寬泛一些，故相比於 GPS 或三角定位，基地台定為較為妥適；二乃使用便利，蓋 GPS 易受天氣及人為影響，不夠全面；三乃隱私平衡，蓋三角定位多用於犯罪偵防，而疫情管制所需知道的可能接觸族群，並不需要特定到那麼細；末則是資訊的易取得性，此乃本文認為最主要的理由，蓋 GPS 不會自動上傳到國內電信業者的系統中，三角定位的資料電信業者也不會就每一筆資料儲存，然而基地台定位的資料只要手機開啟電源，郵輪於入境時就會有訊號儲存在基地台，因此主管機關得藉由與航海圖的時間比對，得以區分並確定遊客使用的門號，進而以遊客所在位置直徑 500 公尺的範圍為篩選範圍，圈定 62 萬人，以細胞簡訊的方式發布通知提醒民眾自主隔離。

doi:10.6342/NTU202301113

關於隱私權的可能爭議上，政府部門相關文獻指出[18]鑽石公主號郵輪事件所使用之手機定位資訊，僅有手機訊號出現之地點，並不知悉該手機門號之持有人，無法直接識別該個人資料之當事人，惟如透過電信公司之資料，則可查得該手機門號之所有人，故係屬個資法下可間接識別個人之資料[19]。關於政府向電信業者請求該資料的行為，因屬中央流行疫情指揮中心為蒐集手機定位資訊以供疫情監測資訊研判的必要，係屬執行法定職務必要範圍內之蒐集，故符合個資法 15 條[20]，而其利用也未逾越蒐集的目的，故亦未違反個資法 16 條[21]。至於電信業者蒐集該定位資料的行為，該篇文章則指出電信公司係因與電信用戶間有契約關係而取得用戶手機定位資訊，符合個資法第 19 條 1 項 2 款[22]，且後續利用資訊轉交於中央流行疫情指揮中心之行為亦因符合法律明文規定、為增進公益等理由而符合個資法 20 條 1 項但書第一、二款[23]。最後除了上述定位資訊外，中央流行疫情指揮中心更將上述資訊與健保資料庫結合[24]，一方面標記被隔離者方便其識別，

[18] 簡宏偉等著（2020），〈大數據運用與隱私保護－手機定位資訊於防疫應用之法律問題研析〉，《國土及公共治理季刊》，8 卷 3 期，頁 69。

[19] 個人資料保護法第 2 條第 1 款：「個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。」

[20] 個人資料保護法第 15 條規定：「公務機關對個人資料之蒐集或處理，除第 6 條第 1 項所規定資料外，應有特定目的，並符合下列情形之一者：一、執行法定職務必要範圍內。二、經當事人同意。三、對當事人權益無侵害。」；中央流行疫情指揮中心實施辦法第 3 條規定：「本中心任務如下：一、疫情監測資訊之研判、防疫應變政策之制訂及其推動。二、防疫應變所需之資源、設備及相關機關（構）人員等之統籌與整合。三、防疫應變所需之新聞發布、教育宣導、傳播媒體優先使用、入出國（境）管制、居家檢疫、國際組織聯繫與合作、機場與港口管制、運輸工具徵用、公共環境清消、勞動安全衛生、人畜共通傳染病防治及其他流行疫情防治必要措施。」

[21] 個人資料保護法第 16 條規定：「公務機關對個人資料之利用，除第 6 條第 1 項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。」

[22] 個人資料保護法第 19 條第 1 項第 2 款規定：「非公務機關對個人資料之蒐集或處理，除第 6 條第 1 項所規定資料外，應有特定目的，並符合下列情形之一者：…二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。」

[23] 個人資料保護法第 20 條第 1 項但書第 1、2 款規定：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為增進公共利益所必要。……」

[24] CHI-MAI CHEN ET AL., *Containing COVID-19 Among 627,386 Persons in Contact With the Diamond Princess Cruise Ship Passengers Who Disembarked in Taiwan: Big Data Analytics*, 22(5) J MED INTERNET RES, e19540 (2020).

doi:10.6342/NTU202301113

一方面也在透過結合病史、旅遊史[25]，避免未主動通報症狀，但有實際就醫的患者成為制度外漏洞。

關於此案件雖亦有學者為文批評，惟似仍著重於法律保留或是法制上應完整化、體系化建構的面向[26]、或僅強調相關機關必須謹慎，然而未對政府關於比例原則的運用提出嚴正質疑者[27]。

至於中央流行疫情指揮中心則於 2020 年 5 月 28 日針對社會上對於隱私權侵害疑慮回應：「鑒於國內 COVID-19(武漢肺炎)疫情風險低，其將鬆綁民眾生活防疫措施。為讓民眾生活及產業經濟在一定的安全條件下，逐步恢復正常運作，其在考量實務作業、諮詢專家並與相關部會研商後，公布『COVID-19(武漢肺炎)』因應指引：實聯制措施指引[28]」，供各界參考運用。

指引中第五點略謂，為確保個資保護，各場域所蒐集的民眾個人資料，均要指定專人辦理並善盡資料保護責任，且最多存放 28 天，之後即必須刪除或銷毀。這些資料只能在配合疫調時使用，不可用於其他目的，蒐集方式可採用紙本或電子，如使用電子方式蒐集，必須採行資安防護措施。此外，蒐集民眾個人資料時，應明確告知當事人包含蒐集機關、目的、個人資料項目、利用期間、利用對象及方式、當事人依個資法可請求的權益及不同意提供時的影響等 7 項資訊。然而該指引的性質究為行政規則？還是行政指導？有無法律授權依據？人民得如何監督並確認相關機關已經確實刪除或銷毀系爭個資？人民或第三人如何對相關機

[25] 衛生福利部中央健康保健署網站（2020），《防疫再升級 健保雲端系統提供高風險地區旅遊史》。載於：https://www.nhi.gov.tw/News_Content.aspx?n=FC05EB85BD57C709&s=012016EE70C9A226（最後瀏覽日：02/17/2021）。

[26] 李崇僖（2020），〈在瘟疫蔓延中檢視個資保護法制〉，《台灣法學雜誌》，387 期，頁 39-43。

[27] 何建志（2020），〈COVID-19 疫情期間防疫與隱私之平衡：相關法律議題分析與社會正義觀點〉，《台灣法學雜誌》，387 期，頁 23-32。

[28] 衛生福利部疾病管制署網站（2020），《「COVID-19(武漢肺炎)」防疫新生活運動：實聯制措施指引》。載於：https://www.cdc.gov.tw/File/Get/t-_Xs5DDee2qzBFC1fRXJA（最後瀏覽日：02/17/2021）。

doi:10.6342/NTU202301113

關的不作為救濟？此類問題似皆屬待解之問題，因而系爭指引的效力是否僅為虛晃的回應，實不無疑問。

第二節　大型資料庫對資訊隱私權的挑戰

由上述三件案子約略可見我國隱私權發展近年來所面臨的挑戰大約是「目的外利用風險」以及「去識別化作為工具性保護提供的失能」，分述如下：

第一項　目的外利用風險

首先是第一點：大型資料庫的建置存在不可逆的隱私風險且容易逸脫建置時所設定的目的。

在 ETC 案中，機關雖先以該資料庫建置能運用於大眾運輸規劃或即時交通資訊提供，有助於公共利益，並以此為由建置了該資料庫，然該資料庫的建置嗣後卻產生了外溢的效果。在前述提及的判決中，即外溢到行政罰的檢舉證據資料上，此資訊原非裁罰機關或被檢舉人所能取得或預期被蒐集者，然而關於該證據資料是否侵犯隱私而不得利用的討論，卻在終審法院模糊的公共利益論證中被輕描淡寫的帶過。而在近年的「全民健康保險資料人工智慧應用服務試辦要點」中，也是逸脫原先健保資料庫的公共目的，不管個人是否同意地將敏感健康資料供「產業應用」[29]。

無獨有偶地在疫情電信追蹤案中，政府於疫情管制上透過出入境資料庫、健保資料庫、ETC 資料庫、電信業者基地台訊號資料庫等串聯的方式，讓過往於前揭資料庫推行時所強調並承諾保障的目的外利用限制、告知後同意要求、終止、退出權等隱私權保障內涵，在至高的公共利益名下，蕩然無存。此無疑也逾越了那些資料庫建置原先設定的公益目的範圍。

[29] 參考吳全峰（2019），《不用你同意，政府做莊賣個資？》。載於：https://infolaw.iias.sinica.edu.tw/?p=984（最後瀏覽日：02/17/2021）。

doi:10.6342/NTU202301113

至此似可發現一旦此類資料庫的建置完成，其蒐集的結果是以近乎如不可逆的化學反應般「再也回不去了！」這也明顯說明了大規模資料庫的建置有更深層於「資料是否去識別化」、「利用是否於蒐集目的內利用」、「事前嗣後是否真摯同意」的問題存在。蓋一旦資料庫建置完成，即幾乎確定於未來某時點，當公共利益被群眾恐慌過分放大時，遲早會受到目的外利用[30]。而倘若上開情形發生，所有隱私權的保護面向很可能都很難在比例原則下發揮作用。此情形在我國在人民面對疫情的恐慌，相對風險受到社會輿論放大時顯得格外明顯。

而這並非僅在我國發生，參諸美國法，相同情形發生得比我國更早。依據學者林昕璇的分析[31]，美國 1978 年國會以保護國家安全為由，制定《涉外情報控法》，經史諾登揭密後顯現當局對於不論是否為美國公民，亦不論公民是否涉及不法行為而達合理懷疑門檻，皆進行無差別和大規模的蒐集，其一即為大規模蒐集電話的 metadata 計畫，藉由大規模的資料庫串聯勾稽，監控通訊紀錄。聯邦法院對相關爭議在 Clapper v. Amnesty International USA、 ACLU v.Clapper、Klayman v. Obama 等案件中，以第三人理論及其衍伸之自願揭露法則，傾向認為一旦資料係屬人民主動提供予第三人，或放置到公開空間，即不得主張有合理隱私期待，另外也常以原告欠缺當事人適格、未具體說明損害、監控手段仍在法規目的授權的寬泛授權範圍內等理由，判決原告敗訴。此類見解使得資訊隱私所得以保障的範圍大為限縮，同時也忽略了此類資料庫建立後，後續可能延伸的目的外儲存分析、重新組合的風險，會完全脫離於當初資料被蒐集人同意的合理期待內。這無疑就是本文所欲強調的大型資料庫建置的不可逆風險，而這樣的風險似乎在可以想像的未來中並不會止歇。現在正受激烈論戰的區間測速設置爭議，未來極有可能會延伸出行車軌跡、停留時間全面描繪的爭議。

[30] 翁清坤（2020），〈大數據對於個人資料保護之挑戰與因應之道〉，《東吳法律學報》，31 卷 3 期，頁 34。其舉出許多目的外利用案例，像是二戰時荷蘭建立的人口普查資料被納粹用於搜尋猶太人、報稅資料被移轉制追討積欠保費的健保主管機關等。

[31] 林昕璇（2020），〈論大規模政府監控之資訊隱私保障—評析美國聯邦法院相關裁判〉，《台灣民主季刊》，17 卷 2 期，頁 59-71。

doi:10.6342/NTU202301113

第二項　去識別化的失能

再者是第二點：去識別化容易淪為蒐集利用機關的免死金牌。

在前述提到的區間測速案例中，新北市警察大隊的官方回復認為區間測速只會擷取車牌，故僅屬於間接個資，得以在法定職務必要範圍內蒐集利用。然而此忽略了普設區間測速所取得的資料並非僅限於車輛號牌！縱使沒有特別去歸檔，但是路徑速度、車輛外觀、行經時間的紀錄皆不難由該數據延伸得到，以上綜合的取得下是否仍為個資法下的間接個資？新北市政府警察局交通警察大隊的說明無疑顯得避重就輕。同樣的爭議在健保資料庫案中亦同，最高行政法院在終局判決中的立場同樣也是認為只須把去識別化的程度跟公共利益做衡量即足，此無疑如學者張陳弘所批評[32]，是過於狹隘的化約，很容易造成個資一旦脫離個資主體控制後，個資主體喪失的不僅是控制利益的合理隱私保護期待，而是連同秘密性與親密性利益的合理隱私保護期待，一併失去。

此類政府機關傾向倚賴去識別化作為正當化蒐集、利用事由的情形似乎是非常普遍的。在前述疫情電信監控案中相關機關公務員所發表的文章中[33]即可以發現，其等認為手機漫遊定位紀錄因為相較於三角定位跟 GPS 而言更不精確，因此延伸的隱私風險較小，屬於較可行之方案。然而這樣的說法不免啟人疑竇，原因在於機關最後還是特定到了一些個人，或者甚至可以說那些模糊的群體正是機關的目標客體，因此在機關可以說是完全命中的情況下，若說以手機漫遊定位紀錄特定個人是對隱私侵害較小的方法，似乎僅是穿鑿附會的巧合而已。倘機關欲正面回應隱私爭議，應該更著重於為何政府得以勾稽前揭數個資料庫進而特定出個人？法源何在？手機漫遊定位紀錄是否為個資？若勾稽得以輕易達成，則政府

[32] 張陳弘，前揭註 14，頁 240；張陳弘（2018），〈新興科技下的資訊隱私保護：「告知後同意原則」的侷限性與修正方法之提出〉，《臺大法學論叢》，47 卷 1 期，頁 215-217。
[33] 簡宏偉等著，前揭註 18。

doi:10.6342/NTU202301113

是否仍得宣稱手機漫遊定位紀錄係對隱私侵害較小的手段？這些問題始為資料庫建置後利用問題的核心。綜上，本文認為上述案例皆凸顯了政府機關傾向把資料去識別化作為其後續蒐集、利用而不告知被蒐集人或可能受影響人的擋箭牌。

第三項　小結

在前面幾個部分中，本文整理了大型資料庫建置所延伸的爭議，鳥瞰後似可見其共通特色在於皆是在公共資訊與私人資訊的界線逐漸模糊下、以模糊的公共目的為名、輔以去識別化或是以宣稱蒐集間接個資為手段、大規模地抽象蒐集並利用人類社群產生的個人資訊，其結果乃幾乎不可避免地造成未來高機率的蒐集目的外利用以及所生的不可預期侵害結果。

針對此一全面監控的挑戰，本文如前述認為有兩大共通問題，即目的外利用風險、及去識別化的掩飾。對於此二問題，翁清坤認為就目的外利用困境而言，其乃肇因於大數據利用模式本身即是在追求不同資料集之間的連結，因此容易跟目的明確原則產生衝突，其認為重點在於後續利用與原先同意目的間的「相容性」評估，其援引英國資訊委員辦公室見解指出，新目的與原始目的間必須考量新目的如何影響當事人隱私，以及資料再利用方式是否還在當事人合理期待範圍內，若已經超過就應該另行取得當事人之告知後同意[34]。

學者邱文聰也有提出相關對應，認為應該透過舉證責任反置以及更細緻架構的比例原則去迫使機關把模糊的公共利益說明清楚，並應命行政機關說明具體到為何可以透過去識別化正當化蒐集與目的外利用[35]。本文認同此一看法，但本文認為這樣的方法僅能解決前者關於機關是否將資料作目的外利用的問題，對於後

[34] 翁清坤（2020），前揭註 30，頁 114。然而其也指出，當新目的出現時，有時難以事後再找到所有當事人一一通知，再者，大數據得以由非個資創造出個資，此也會產生應於何時及如何通知當事人的挑戰。

[35] 邱文聰（2018），前揭註 17，頁 38-43。

doi:10.6342/NTU202301113

者問題，至多只能使得機關不得再以去識別化作為蒐集利用唯一的正當化理由爾，然本文認為所謂的去識別化，在現在科技的日新月異下，或許在不遠的未來，這樣的技術將很容易被第三方再識別，使得該技術能提供給隱私的保護將會非常有限。不僅於此，在法律定義上而言，本文也認為，實然面的發展過快，也會使得規範面上就其字面定義有所顛覆，使得不同族群產生不同的理解，而這樣的理解落差，本文認為即有高度可能使得利用前的告知說明不夠完整，使得「去識別化」成為蒐集方虛妄的一招，並產生虛妄的保護效果，本文對此深感疑慮，故將在下一個部分著重於去識別化的困境，試著回答去識別化作為隱私保護手段之一到底遇到了怎麼樣的困境？隱私權保障的問題是否仍適合繼續在去識別化的層面討論？並暫時將資料庫建置後的目的外利用風險暫且擱置。

第三節　細論去識別化的挑戰

在前述的三個政府建立資料庫的案例中，常見機關將去識別化作為運用個資的單一要件，也就是只要將個資經去識別化處理，對於此一已去識別化個資的任何使用行為，就不會是侵害資訊隱私的結果，當然也不需要取得個資主體的同意。如此不以個別立法授權強制蒐集、處理、利用等方式合比例限制當事人權利，轉而以資料去識別化確保資料機密性，據以「補充單純以個案中的資料利用價值作為資料取得合法基礎的正當性」的手段[36]，常被學者批評：

（一）去識別化手段並未完全切斷與個人資料的連結可能性，只達到非真正去識別化的「假名化」，在現今人工智慧學習發達的科技環境下仍有與不同資料交互勾稽、拼湊、再識別出個人的可能[37]。

[36] 邱文聰（2018），〈初探人工智慧中的個資保護發展趨勢與潛在的反歧視難題〉，收於：劉靜怡編，《人工智慧相關法律議題芻議》，頁 161，元照。
[37] 邱文聰（2018），前揭註 36，頁 161；翁清坤（2020），前揭註 30，頁 119。後者也指出大數據分析技術使得個資的匿名化、去識別化狀態越來越難以維持，由於 AI 擅長在不相干的資料間

doi:10.6342/NTU202301113

（二）邱文聰認為去識別化不能作為資料蒐集單獨的合法基礎[38]，像是歐盟即認為「假名化」處理後之個資，仍屬於 GDPR 所規範的可識別資料[39]，「假名化」僅是作為「目的相容性」判斷[40]與一般資料處理[41]時的一種必要或補充的資訊安全手段，經「假名化」處理並不會取得蒐集、處理或利用的合法基礎。

（三）張陳弘同樣認為去識別化不能作為資料蒐集單獨的合法基礎。蓋隱私保護利益切分成三個各自獨立的面向，分別是「控制利益」、「秘密性利益」與「親密性利益」，雖然去識別化個資的利用可能不會對「秘密性或親密性利益」造成傷害，然而只要該去識別化後的個資仍屬個資，仍有還原連結特定個人的可能，就必須保障該個人之「控制利益」。如果要犧牲或剝奪該個人的控制權，就要有其他足以壓過該個資主體控制利益的其他正當化理由，個資的去識別化處理並非足夠理由[42]。

由上可見，所謂去識別化的困境有二，一是去識別化的功能究竟是否能達到完全不可再識別的「匿名化」程度受到質疑，二是在這樣的基礎下如果個人仍與該「有再識別風險之匿名化」或是「假名化」個資存有連結，自然就必須保障個人的控制利益，不能單以資料已經去識別化為理由，排除個人的同意或是更細緻的公益正當性與立法要求。

以下本文將把前者拆成定義上的困境、以及技術上能否達到匿名化的困境分別探討，再延伸至此一爭議所造成的個資定義困境，最後總結此一「去識別化困境」並介紹當前學者對此提出的解方，以及本文見解。

建立關聯性，使得不可逆轉的匿名化難以達成，甚至是不可能的，匿名化是否充分也難以於事前評估。不過翁氏在結論上仍然認為「匿名化」得以減緩個資遭濫用。

[38] 邱文聰（2018），前揭註 36，頁 172。

[39] GDPR, Recital 26.

[40] GDPR Article 5(1)(b), 6(4)(e), 89(1)

[41] GDPR Article 32(1)(a)

[42] 張陳弘（2018），前揭註 32，頁 264-265。

doi:10.6342/NTU202301113

第一項　定義上的困境

首先在切入去識別化做為正當化個資蒐集的理由是否妥當之前，應先理解究竟何謂去識別化。如果白話一點的說，去識別化就是在刪去或留存兩個二元選項中找出一個平衡，因此實就是一個程度上高低的概念。根據美國知名隱私權暢銷書作者麥爾荀伯格所提出的「數位生鏽」概念[43]，資訊的部分刪除且繼而減低資訊的準確性，是他認為可以緩和刪除、留存二元性的方法之一，並讓科技的運作更接近人類記憶的運作方式。本文認為其想法跟去識別化的內涵其實非常相似，都是為了在刪除與留存間取得一個平衡，然這樣的平衡是否能清楚界定，其實不無疑問。

關於去識別化的內涵，各國規範皆不一致，為了避免混淆，本文姑且先不介紹名詞定性，僅以刪除到留存之間的功能性區分，區分出幾個可能的概念。首先：（一）離留存最接近者，是指可以透過該資料內涵直接辨識出特定個人。舉例而言，身分證字號、姓名即為適例。（二）次之者，是指客觀上或對一般資訊接受者而言，無法透過合理方式勾稽比對辨識出特定個人的情形，此種方式通常採用加密、編碼等去連結等方式處理資料，資料處理者通常仍保有回復資料原型的能力。（三）再者，是指以銷毀密碼或編碼簿的方式使得資料永久與個人去連結，高機率無法再識別出個人。（四）末者則是自蒐集資料之初，該資料即不含可辨識個人的資料，其跟（三）的差別在於其不須經過一個去連結的過程，身高、年齡、性別為適例。

目前文獻中常見使用去識別化(de-identification)跟匿名化(anonymization)兩個名詞，就後者而言，較無爭議通常指的是前述的（三），亦即以原則上不可回復的方式(irreversibly)，將資料與特定個人之間的連結關係全面切斷。然就前者而

[43] Viktor Mayer-Schönberger（著），林俊宏（譯）（2015）。《大數據:隱私篇：數位時代，「刪去」是必要的美德》，第一版。台北市：天下遠見。頁 264。

doi:10.6342/NTU202301113

言在定義上就較為分歧，如果僅是以代碼或隱藏部分資料的方式，則在學理上稱作「假名化」（pseudonymization），在這樣的情形，仍有與特定個人勾稽連結的可能性存在。

第一款 美國法

以美國為例[44]，其並不存在匿名化跟去識別化的明確區分，蓋兩者皆僅是在描述再識別風險降低的過程，以健康保險可攜與責任法案(Health Insurance Portability and Accountability Act, “HIPAA”)為例，該法對於決定特定健康資料是否屬於可識別特定個人資訊（Personally Identifiable Information, “PII”）的標準有二。一係統計標準：由具有專業知識與經驗的專家以書面文件決定，標準乃如果一個具有一般統計和科學相關知識經驗的人員，不能單獨從該資料辨識特定個人時，該資料就可被認定為非可識別個資；二係安全港方法：刪除表列的 18 項可識別資訊作為安全港。原則上只要去除姓名、詳細地理位址、與個人連結的日期、電話、電郵、社會安全碼等獨特可識別的特徵共 18 項，且無其他明知可藉由單獨使用或合併其他資訊加以再識別的資訊存在時，即屬去識別化、不可識別特定個人資訊（Non-PII），不受隱私規則規範。不過應注意者係統計標準跟安全港方法並非互斥，在依安全港方法去除 18 項可識別特徵後，專家仍可以另外基於風險考量去增加第 19 或第 20 項的要求。

然而該法下仍有若干例外情形可以在健康個資未達上述標準時，得以不須獲得資料主體授權逕用於研究，像是「有限資料組」不要求刪除達 18 項特徵，只要接收者願意簽署資料使用協議，並遵守相關規定即可；其他情形還有進行研究前的審閱準備、過世者資訊的研究、已經獲得組織審查委員會（IRB）或隱私委員會（Privacy Board）的批准等情形，也可以無需獲得資料主體的同意[45]。

---

[44] 程法彰（2020），〈我國資通訊產業的個資去識別化運用爭議〉，《萬國法律》，230 期，頁 75-76；張陳弘、莊植寧(2019)，《新時代之個人資料保護法制：歐盟 GDPR 與台灣個人資料保護法的比較說明》，頁 156-9，台北：新學林。

[45] 張陳弘、莊植寧，前揭註 44，頁 159-159。

doi:10.6342/NTU202301113

第二款 歐盟法

至於歐盟的規定，GDPR 於第 4 條第一項謂：「『個人資料』係指有關識別或可得識別自然人（資料主體）之任何資訊；可得識別自然人係指得以直接或間接地識別該自然人，特別是參考諸如姓名、身分證統一編號、位置資料、網路識別碼或一個或多個該自然人之身體、生理、基因、心理、經濟、文化或社會認同等具體因素之識別工具。」根據學者張陳弘所指出[46]，歐盟資料保護工作小組（Article 29 Data Protection Working Party）為了釐清個人資料概念於 2007 年間做成的意見書，更進一步區分「可識別性」跟「去識別性」乃兩個不同的概念。

前者決定隱私保護的範圍，後者則在於決定隱私保護的強度。就可識別性的概念採取「不論是資料控制者或任何其他人，透過所有可能、合理的方式，得以識別出特定個人。」的寬鬆標準寬認資料受到法律保護。至於去識別化作為保障隱私權的手段之一，則必須透過法益權衡的方式衡量去識別化的程度是否足夠。而其標準又可分成主觀標準跟客觀標準，在主觀標準下，係以具動機的侵害者的觀點去判斷，至於是否該假設該動機侵害者有無合理能力或先驗知識，仍有不同的看法存在。而客觀標準說則以侵害人從已持有的可識別性或去識別性個資，與去識別化資料庫的個資比對產生再識別結果的機率高低，據以判斷去識別化的程度高低。而倘若去識別化的程度已經達到事實上、制度上不可逆的程度，且永久除去識別特定個人的可能性時，此時該資料即已非屬個人資料[47]。

第三款 我國法

至於我國個資法對於所謂的去識別化，並沒有明確的定義，僅能藉由個資法及其施行細則的規定大略窺見其貌。關於個資的定義在個資法第 2 條第一款內，其區分為可直接識別者與可間接識別者，而個資法施行細則第 3 條則闡釋所謂可

[46] 張陳弘，前揭註 14，頁 41-48。

[47] Working Party Article 29, *Opinion 4/2007 on the Concept of Personal Data*, 01248/07/EN WP 136 (June 20, 2007), https://www.Clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf.

doi:10.6342/NTU202301113

間接識別性乃指「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。」

其他意義上接近「去識別化」的條文用語為「資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人」，此類用語分別見於敏感個資的蒐集、處理、利用（第 6 條 1 項但書 4 款）；告知義務的免除（第 9 條 2 項 4 款）；公務機關目的外利用（第 16 條但書 5 款）；非公務機關蒐集、處理個資（第 19 條 1 項 4 款）；非公務機關目的外利用（第 20 條 1 項但書 5 款）。另外依據個資法施行細則第 17 條，所謂無從識別特定當事人，是指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者。

由此可知現行個資法並無「去識別化」這樣的用語或相關定義，而所謂的「代碼、匿名、隱藏部分資料」的方式，「代碼」跟「隱藏部分資料」部分，似屬前述實質功能上的（二）僅達到假名化的程度，而不到完全無法再識別的程度，然而施行細則又混用「匿名」的文字，導致法條究竟係指匿名化？還是假名化？即產生模糊空間[48]。這樣的概念是否足夠清楚明白且足以當作資料蒐集的正當化理由，實有再思考的餘地。

如學者吳全峰即指出個資法施行細則第 3 條的無從「直接」識別其實比較接近美國之去識別化（de-identification），亦即將與個人可識別因素（identifiers）排除即可，故假名化（pseudonymization，指處理後資料仍可透過與其他資料對照以識別特定個人，編碼即屬之）亦屬「去識別化」工具；但歐盟之匿名化（anonymization）概念卻必須達到不得直接及間接識別的程度，因此由於假名化資料仍可對照回推，故被認仍屬可識別個資（GDPR 前言第 26 段）。結論上其認為個資法就「無從識別當事人」的概念，在法條用語、法務部函釋、法院判決中無統一定義與內涵，甚至直接橫向移植並混用美歐法規用語（如假名、匿名、

[48] 吳全峰、許慧瑩（2018），〈健保資料目的外利用之法律爭議：從去識別化作業工具談起〉，《月旦法學雜誌》，第 272 期，頁 48-49。

doi:10.6342/NTU202301113

編碼、代碼、隱藏部分資料、去識別、去連結），未考慮概念差異，遂導致衝突不斷[49]。

除了用語混亂外，另一個從條文可見之處在於，我國個資法中的去識別化功能上大多與「公益、統計或學術研究目的」結合，作為公務機關與非公務機關蒐集、處理個資、目的外利用的例外規定，並據以免除資料控制者的告知義務。在敏感性個資的情形，又進一步限縮僅公務機關得以醫療、衛生或犯罪預防之目的，在去識別處理下蒐集、處理、利用敏感性個資。由上可見我國法就去識別化在個資法中的定位與意義，是將其做為資料控制者於學術、統計目的蒐集、處理、利用個資時的「條件」，其邏輯極有可能是為了「公益」目的，將去識別化當作「風險管制手段」，取代目的外利用需額外取得的告知後同意。

這樣的邏輯有幾點值得質疑，首先是「為何以公益統計或學術研究目的為限」？統計及學術目的固然可能相較於其他目的具備更高的正當性，然而縱使如此，難道就不需要更細緻地考量研究目的與資料蒐集範圍的目的相容性，以及是否符合最小蒐集？再者，如果去識別化只是風險管制手段，何以能取代「同意」？又，當資料蒐集非出於公益目的時，此時「去識別化」的功能又為何？去識別化將如何影響資料主體同意權的行使？如何使資料控制者的組織、程序義務減輕？此類質疑似乎皆尚無法透過現行個資法回應。

第二項　**技術上的困境**

在說明了去識別化在定義上、法規上的模糊之外，有一更重要的問題浮現，亦即科技上的發展是否能真的做到完全去識別而讓再識別的風險極低？如果用前述功能性去識別化的理解來看的話，就是指即使是在（三）刪除密碼或銷毀編

[49] 吳全峰（2018），《個資保護再思考》，載於：https://tw.appledaily.com/forum/20180625/D43MRQWXCC7AX5KKKDBGTFKKF4/（最後瀏覽日：04/27/2021）。

doi:10.6342/NTU202301113

碼的去識別化的資料，是否仍有可能透過跟不同資料庫的勾稽去重新再識別到足以特定個人的程度？也就是說，所謂的去識別化的工具的成效是否會因為其他再識別工具的發展而式微，使得去識別化的保護宣稱逐漸被架空？更甚者，縱使是蒐集當初不被認為屬於足以特定個人或與個人相關而不適用個資法的資料，是否也會因為技術的發展而逐漸無法撇除與個人的關係，進而形成保護漏洞？

以下本文將先整理當前法律學者對於去識別化技術處理後，再識別可能性的討論，釐清其等所質疑的重點。接著，為免討論趨於單純的科技懷疑論，本文將探究現行的去識別化技術與模型實務上究竟為何？最後則試圖回應及重新整理「去識別化技術困境」究竟為何。

第一款 再識別風險的質疑

關於去識別化對隱私保護在當前科技上面臨的困境，依據論者何琳潔所整理的外國文獻所示[50][51]，倫敦帝國學院及比利時魯汶大學（Université catholique de Louvain）日前開發出一種演算法，只要給予至少 15 項的屬性特徵（attributes），如性別、郵遞區號、婚姻狀況等，則可以從幾乎是任一資料集中辨識出 99.98%的美國人。更精確講法是「在任一即使是不完全的資料庫中，只要有至少 15 個特徵描述，就有 99.8%機率可以辨識出特定人；而特徵數量減少，也只是機率降低而已。」

該篇研究認為即使是在人口異質性不高的地區，已經嚴格隨機取樣、不完整的資料庫，在缺乏外在資料庫的情形下，依然可以在該演算法下有一定的再識別可能性，且該再識別正確性非常高，這樣的結果將導致原先所認為的去識別化難

[50] 何琳潔（2019），《你的個資真的已經匿名化了嗎？》。載於：https://infolaw.iias.sinica.edu.tw/?p=1831（最後瀏覽日：04/27/2021）。

[51] 除此之外，就美國生物資料庫再識別風險的整理可以參考 Mark A Rothstein, *Is deidentification sufficient to protect health privacy in research?*, 10(9) AM J BIOETH 3, 5-6(2010)。其同樣提到僅用性別、地區碼、生日三項特徵就有 63~87%機率可以特定出個人；如果只利用有限的人口統計資料，在符合 HIPAA 規範的情形下，仍有 0.04%再識別機率。

doi:10.6342/NTU202301113

以符合歐盟 GDPR 所定義的匿名化，這嚴重衝擊了去識別化在科學上、法律上的意義[52]。

與此一研究相類似的研究領域稱為復原識別科學，Paul Ohm 認為專家可以透過再識別（re-identify）或去匿名化（de-anonymize）的方法實現個人身份的再識別，傳統的刪除姓名跟社會保險號碼的匿名化技術將不再有用，即使是非敏感性、不被視為具有個人識別性的資訊，交互比對仍有高度破解匿名化的可能[53]。

此非唯一示例，另一個例子乃是 2016 年的一項德國研究[54]，其發現三百萬德國人民可以從其網路瀏覽紀錄被辨識出來。Svea Eckert 一位北德廣播公司的臥底記者，跟 Andreas Dewes 另一位資料科學家合作成立一家虛擬公司向資料處理商（data brokers）嘗試免費地要了一個月份的關於三百萬德國人的瀏覽紀錄(URLs)跟瀏覽的時間記錄，藉由這份資料庫他們發現只需要極少數、約十份左右的瀏覽紀錄，即足以如指紋般辨識出個人的瀏覽歷史紀錄。這在政客或公眾人物的特定與辨認上更為容易，只需從該政客或公眾人物推特的發文時間跟網站資料與資料庫中的瀏覽紀錄交叉比對，即可進而特定出個人的其他瀏覽歷史。Ecker 跟 Dewes 指出這些資料處理商事實上是有在販售這些資料庫的，而雖然業者宣稱這些資料庫乃匿名化資料庫，然他們的研究結果顯示在該「匿名化」中再辨識出特定個人並非如想像中困難。

其他零零星星還有一些評論像是 Peter Bittner 說到：「非個人資料的累積、對大數據的強大關聯的演算法將會有可能得以關聯到個人，進而將非個人資料轉

---

[52] Thomas Brewster, *120 Million American Households Exposed In 'Massive' ConsumerView Database Leak*, (Dec. 19, 2017), https://www.forbes.com/sites/thomasbrewster/2017/12/19/120m-american-households-exposed-in-massive-consumerview-database-leak/?sh=72dbdffb7961; Luc Rocher et al., *Estimating the success of re-identifications in incomplete datasets using generative models*, 10 NAT COMMUN. 3069 (2019).

[53] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1704 (2010).

[54] Alex Hern, *Anonymous' Browsing Data Can Be Easily Exposed, Researchers Reveal*, The Guardian, (Aug. 2, 2017), https://www.theguardian.com/technology/2017/aug/01/data-browsing-habits-brokers; Daniel Oberhaus, *Your 'Anonymous' Browsing Data Isn't Actually Anonymous*, (Aug. 3, 2017), https://www.vice.com/en/article/gygx7y/your-anonymous-browsing-data-isnt-actually-anonymous.

doi:10.6342/NTU202301113

換成個人資料[55]。」Viktor Mayer- Schönberger 跟 Kenneth Cukier 提到：「只要夠多資料，不管再怎麼努力，完美匿名化是不可能存在的[56]。」WP29 歐盟資料保護工作小組強調新興科技已經使得匿名化越來越難以達成[57]。國內學者張兆恬亦曾以《科學》雜誌之文章為例指出各資料庫之間的網絡連接已經使得匿名化的保護程度更加薄弱[58]。結論上顯見，即使資料控制者已近乎讓個資主體被再識別的機率看似不可能，證據顯示再識別風險依然存在[59]。

第二款 去識別化技術與模型

為了具體描繪前述提到之再識別風險，以下將簡略得說明五類「去識別化技術」與融合貫通該五類技術所延伸出的三種「去識別化施行模型」，本文將分析資料處理者在選擇去識別化方法時可能考量的因素，包含如何以最小蒐集原則達到研究目的、如何平衡資料蒐集同意所需的成本、以及如何評估不同去識別化技術分別蘊含的再識別風險等因素。

第一目　去識別化技術

就去識別化技術部分，大致有抑制法、擬匿名化、泛化、隨機、彙集等五種：

---

[55] Peter Bittner, *Intellectual Property Management Challenges Arising from Persuasive Digitalisation: The effect of the Digital Transformation on Daily Life*, in INTELLECTUAL PROPERTY AND DIGITAL TRADE IN THE AGE OF ARTIFICIAL INTELLIGENCE AND BIG DATA, 67, 71(Xavier Seuba et al. eds., 2018); *See also* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 65 (2018)。其提到任何單一片段的資訊或許並非特別「個人」或別具親暱性，但其累積總和卻可以描繪更細緻的個人。

[56] VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 155 (2013). 其提到在有足夠資料的前提下，即使再努力完美的匿名化仍是不可能的。

[57] Working Party Article 29, *Opinion 05/2014 on Anonymisation Techniques*, 0829/14/EN WP216 (Apr. 10, 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[58] 張兆恬（2016），〈人體生物資料庫之隱私權爭議：美國法的啟示〉，《法律與生命科學》，5 卷 1 期，頁 38。

[59] Michael Veale, Reuben Binns and Jef Ausloos, *When Data Protection by Design and Data Subject Rights Clash*, 8 INTERNATIONAL DATA PRIVACY LAW 105 (2018).

doi:10.6342/NTU202301113

（一）抑制法（Suppression）

抑制法簡單來說就是「移除部分資料，以降低資料集的準確性[60]」，在前述 HIPAA 隱私規則的「安全港法」中，把規則所列的十八個項目資料移除後再釋出，即可歸類為抑制法之一。

抑制法又可以細分成「紀錄抑制（Record suppression）」、「區域抑制（Field suppression）」和「遮罩（Masking）」三個類型。紀錄抑制指的是在從原資料中去除部分離群值[61]，或是進行次取樣（Subsampling）[62]、挑選出較無隱私風險的資料；區域抑制，即刪除敏感的欄位類別[63]，例如出生年月日等；最後，遮罩指的是將所有唯一識別符（unique identifiers）的資料欄位刪除[64]，舉例來說像是身份證字號。

（二）擬匿名化（Pseudonymization）

擬匿名化，有稱為「虛擬假名技術」也有稱為「假名化」者，即是將資料集中的所有唯一識別符（例如姓名、身分證資料、病歷號碼等）以虛擬假名或代碼取代[65]。此一方法保留不同資料庫之間的連結，但去除個人資料被識別的可能性，例如前揭健保資料庫中即是將不同筆健保資料賦予不同代碼予以假名化，此時雖

---

[60] 蔡昀臻、樊國楨（2016），〈大數據之資料去識別的標準化實作初探：根基於 ISO/IEC 2nd WD 20889：2016-05-30〉，《資訊安全通訊》，22 卷第 4 期，頁 8。

[61] IGI Global, *What is Attribute and Record Suppression*, https://www.igi-global.com/dictionary/attribute-and-record-suppression/72012.

[62] WILLIAM J. SCHROEDER & KENNETH M. MARTIN, VISUALIZATION HANDBOOK 32 (2005).

[63] 蔡昀臻、樊國楨，前揭註 60，頁 8。

[64] 祝亞琪、魏銪志（2016），〈行動支付之個人資料去識別化方法〉，《電腦稽核》，34 期，頁 20。其等指出唯一識別符(Unique identifier)，又稱直接識別符，係指「在資料集中的屬性其只須單獨存在即可唯一識別資料集內的資料主體」。

[65] 蔡昀臻、樊國楨，前揭註 60，頁 8。補充說明：此處「擬匿名化」及「假名化」泛指所有將識別符以假名或代碼取代的方法，實務上法務部曾於 105 年 4 月 8 日法律字第 10503505760 號函檢送「公務機關利用去識別化資料之合理風險控制及法律責任」之研析報告，認為資料以代碼等雙重加密去識別化即屬「可匿之擬匿名化資料」，效果類似匿名化而得以排除個資法適用，就此解釋乃法務部自行創設，本文並不贊同且認為該名詞有混淆之疑慮，蓋本文認為所有以假名或代碼取代識別符的方法，無論單向或雙向加密，因仍有再識別可能性，故皆非等同匿名化。相關批評亦可見吳全峰、許慧瑩，前揭註 48，頁 6。

doi:10.6342/NTU202301113

然難以在未獲得代碼簿的前提下，得知特定筆資料是誰的資料，但藉由假名的連結，仍有機會連結出同一個人的健保資料。

假名化的技術方法有兩個步驟，第一是選擇特定個資特徵進行假名的替換，選定後該類別集合即可安全刪除或是以適當安全方式維護，第二則是分配假名，可以依據成本、重新識別風險等方式分配，像是給予隨機值並留存對照表，或是透過加密或雜湊演算法產生另一數值存於資料集中[66]。

此一作法有兩點需注意，其一是「資料－代碼」間的對照資料保存必須確實，因為如果能得到對照資料，就可以直接得知代碼後的真實身分，因此資料處理者應該要將代碼簿安全的刪除，或是以適當安全的方式加以保存。其二則是代碼如何產生和分配也必須具備一定複雜性，蓋如果分配方式過於規律可循（例如以數字為假名代碼，且第一碼代表性別、第二碼代表戶籍地、第三碼代表出生月等等），將使得要重新識別出假名所代表的特定個人變得容易。對此，有使用隨機產生、分配假名的方式，也有使用加密機制或雜湊演算法來產生假名，就後者而言，就有可能透過原先使用的加密演算法逆推回原先的真實數值。

（三）泛化（Generalization）

泛化技術指的是將資料中所選屬性的精準度降低、修改為較概略的資料，此做一法可以在降低資料的再識別可能性，也可以同時維持資料的真實性，不過在精確性上或多或少會被犧牲。具體的做法包括「捨去」以及「頂部／底部編碼」[67]，前者係指先決定捨去基礎，再依捨去基礎將每個原值捨去到最近經該基礎的值。簡單來說，就是複雜版的四捨五入；而後者係指將資料的最小或最大值轉化成以「超過一萬元」或「少於零元」等方式表示，避免實際數字被揭露，把資料分級距處理也屬於泛化方法之一，不過此類方法仍須與資料利用目的相互權衡。

[66] 祝亞琪、魏銪志，前揭註 64，頁 23-4。
[67] 祝亞琪、魏銪志，前揭註 64，頁 24。

doi:10.6342/NTU202301113

（四）隨機（Randomization）

隨機法指的是透過修改特定屬性資料的值，藉以降低攻擊者在同一份資料集中，藉由一個屬性值來推論另一個屬性值的能力，常見的具體方式包括「添加雜訊（Noise addition）」以及「置換（Permutation）」，前者是在選定的屬性欄中添加隨機值（例如在一個有假名和薪資的資料集中，加入數筆隨機的薪資資料，並且同時替其分配新的假名），但在分配的同時不影響目標所欲得知的資料集統計資訊。後者則是保持原始的資料，但將資料內容彼此交換（例如在前述資料集中，將兩筆屬於不同人的薪資資料交換）[68]。

隨機法的好處是可以維持該屬性資料集的統計上正確性，就「置換」的方法來說，因為只是將資料的排列順序彼此交換，當然不會影響該欄的統計結論（包括統計分布、平均值、中位數值等等）；至於「添加雜訊」的做法，雖然加入了虛假的隨機干擾值，但仍可以透過數學計算的方式，繼續維持該欄統計結果的正確性。在此意義上，運用隨機法有助於經處理後資料的統計分析正確性。

（五）彙集（Aggregation）

彙集法的基礎意義，即將原本一筆筆的資料透過統計的方法，產生各種統計數據（加總、計數、平均值、中位數、最大最小值、相關、分配、圖表等等），並以統計數據替代原資料加以利用。換言之，就是只提供經計算後的統計資料，而不提供原始的各筆資料。在此意義下，統計法應該是各種方法中重新識別可能性最低、最安全的去識別化方式，不過在此方式下處理的資料很可能即去除了個人資料之屬性[69]，且相對的，因為只提供了統計數據，因此資料的可利用性也最低，蓋彙集資料本身欠缺顯著產業利用價值，有價值的依然是彙集前階段的東西。

[68] 蔡昀臻、樊國楨，前揭註 60，頁 8；祝亞琪、魏銘志，前揭註 64，頁 24。

[69] 應注意者係即使經處理後不符合傳統對於個資的定義，這並不代表該統計資料無法對群體或個人產生影響或歧視，學者指出演算法建立的群體群像如果與具體自然人的個人圖像比較配對，仍有可能預測或評估該自然人之特徵、偏好、能力或行為模式。詳參邱文聰，前揭註 36，頁 165。

doi:10.6342/NTU202301113

另外，如果資料利用者仍能夠看到單筆資料的話，就不算純粹的彙集資料，以至於仍有可能導致隱私洩露，以敏感醫療資訊為例，如果窺探者可以搜尋「在前幾 N 筆資料中有幾位曾罹患肺癌」、以及「在前 N+1 筆資料中有幾位曾罹患肺癌」即可得知排序第 N+1 位的病患是否罹患肺癌[70]。

第二目　去識別化模型

就運用前述去識別化技術所建構的去識別化模型有三種，分別是運用「抑制法」、「泛化」的 K 匿名模型、運用「隨機」的差分隱私模型、以及運用「彙集」的亂數回應模型，詳細介紹如下：

（一）K-匿名模型（K-anonymity model）

K 匿名模型是去識別化方法中最重要也時常被提及的模型之一，其透過前述抑制（刪除）或泛化等方式來調整原始資料，並使得調整後的資料能符合「在資料集中的任何一個人，有至少 K-1 名個人擁有相同屬性」。換言之，資料中符合相同條件（例如薪資、郵寄區號、性別等等屬性資料均相同）的個體數量達到 K 個以上，就可以認為該資料符合 K 匿名的要求[71]。由此可知，K 值越大，個別主體就越不容易從整體資料中被辨識出來。又，因為 K 匿名法是透過刪除或泛化原始資料的方式來將個人隱藏在總數為 K 的人群之中，因此若這 K 個人的背景資料越相似，就可以在去識別化的過程刪除或泛化越少的資料，也因此，K 匿名化的操作經常會先進行「分群」，亦即將背景較類似的 K 個人分為一群，再接著進行資料抑制或泛化。

---

[70] 李斯壯、黃彥男（2019），〈數位時代之數位隱私保護〉，《國土與公共治理》，7 卷 4 期，頁 35。

[71] Latanya Sweeney, *Achieving k-anonymity privacy protection using generalization and suppression*, 10(5) INTERNATIONAL JOURNAL ON UNCERTAINTY, FUZZINESS, AND KNOWLEDGE-BASED SYSTEMS 571 (2002)；Google，《GOOGLE 如何匿名處理資料》，載於：https://policies.google.com/technologies/anonymization?hl=zh-HK（最後瀏覽日：2021/05/29）。

doi:10.6342/NTU202301113

不過應注意者係 K 匿名法並不是沒有缺點，如果前述分群所依據的特徵即是第三人（窺探者）想知道的特徵，該分群下的 K 匿名就會喪失意義。此又稱作一致性攻擊[72]。舉例來說，即使在 K 較大的情況下，如果有五筆資料的患病情況一致（例如五人均有患病），則即使有五名相同的人員，第三人雖無法確定其想探知之人是該五人之中何人，但仍可透過上述資料了解該目標已經罹病，此就窺探目的來說即已達成[73]。

另外，經過 K 匿名化後的資料，雖然可以將個人隱藏進以 K 個人為一群的群體中，但有時這 K 個個體中具有特定敏感資料者只是少數，容易受到「單獨挑出」的再識別攻擊。此時，實作上會加上「L-多樣性法」的處理，即透過前述「隨機法」（添加假資料）的方式，使 K 個個體中至少有 L 個個體具有不同的敏感資料，進一步降低被識別的機率[74]。K 匿名法在我國政府機關中也已經有嘗試進行實作，2015 年財政部財政資訊中心即運用 K 匿名法，對稅務資料以處理後對公眾公開為目標進行去識別化處理[75]。

（二）差分隱私模型（Differential privacy model）

差分隱私模型是另一個在實作上十分重要的去識別化模型，操作的方式是在原資料集中，透過數學運算加入雜訊（不存在於原資料集中、但與原先存在的個人相似的資訊），藉此使潛在攻擊者無法確定哪一筆資料屬於其鎖定的真實個人，但盡可能維持統計的精準度[76]。其運作方式和 K 匿名法十分不同，差分隱私模式是透過「加入數學雜訊」的方式來處理資料，後者則是對於原資料進行抑制和泛化處理。

---

[72] 陳泓歷（2017），《基於差分隱私之資料去識別化保護與隱私洩漏風險評估系統》，頁 16，逢甲大學通訊工程學系碩士論文。
[73] 李斯壯、黃彥男，前揭註 70，頁 34。
[74] 蔡昀臻、樊國楨，前揭註 60，頁 20。
[75] 蔡昀臻、樊國楨，前揭註 60，頁 17-20。
[76] 李斯壯、黃彥男，前揭註 70，頁 36-37；王紹睿（2018），〈淺談人工智慧系統的隱私資訊安全保護機制〉，《科儀新知》，215 期，頁 77-78。

doi:10.6342/NTU202301113

差分隱私的一個優點就在於可以正式定義何謂隱私保護，不必因為假設第三方擁有不同的外部資訊，就對現行去識別化處理造成無法避免的再識別風險提升；與此相對的比較對象正是 K 匿名化，K 匿名化的缺點在於，其只能做到分群內無法被再識別，然而如果已知加入兩個外部的資料類別可以造成再識別，K 匿名化並無法藉由在原先資料集處理以避免再識別情形發生[77]。這種難以於事前就預測外部資料庫對去識別化效用影響的缺點，有中文文獻用「無法抵擋背景知識攻擊」來形容[78]。

不過雖然差分隱私模型得以精密的數學計算為基礎，計算出較準確的再識別風險，但也不是沒有缺點，像是有指出差分隱私對於資料釋出及隱私保護沒有一般性的演算法可以套用，而必須個案中建立，且與其他去識別化方法相同，依然必須在隱私保護與統計準確度之間犧牲衡平[79]。

此處若仔細討論可能會超出本文所能掌握的領域，此處僅依本文的理解，簡單說明之。所謂差分隱私具體上係透過隱私參數 ε 值來調節加入雜訊（又稱噪音）的多寡，進而決定資料可用性與去識別化程度之間的平衡，當 ε 值越大，加入的雜訊就越少，此時資料可用性較高，然而相對的就會存在安全性不足的疑慮；反之則可用性較低，安全性較高。不過 ε 值的抉擇並不是一件容易的事，數據集的大小、數據的分佈態樣等統計特性都會影響最佳 ε 值的設定，這也是為何於上述中提及差分隱私必須於個案建立的原因。

最後對於本文關注焦點上，最重要應注意者係，差分隱私其實於數學上的討論仍存在許多定義上、以及效果衡量標準上的分岐。像是究竟該如何選擇「雜訊」？如何定義「安全性」？，易言之，就「如何調整資料可利用性及安全性之間的平

[77] Arvind Narayanan and Vitaly Shmatikov, *Myths and Fallacies of Personally Identifiable Information*, 53 COMMUNICATIONS OF THE ACM 24, 26 (2010).
[78] 陳泓歷，前揭註 72，頁 15。
[79] Narayanan & Shmatikov, *supra* note 77, at 26；陳泓歷，前揭註 72，頁 25, 35。

doi:10.6342/NTU202301113

衡」才算最佳化，學說上目前仍在積極發展，因此若要說有明確定義仍稍嫌過早，不過縱使如此，差分隱私仍為目前學者認為較佳的去識別化技術。

（三）亂數回應模型

亂數回應機制是指從試驗設計的初始就使用無法確定個別受試者個資的試驗設計。舉例來說，如果進行一個是否曾吸毒的調查，在受試者接受調查前，會以亂數決定受試者是否應誠實填寫問卷，如果以丟硬幣決定亂數的話，就是正面的話要據實以答，反面的話，就一概填寫否定。如此一來所得到的吸毒人口比例就只需將最後統計數據依照亂數比例（以硬幣而言是二分之一如實填寫）除以二即可得知，而從頭到尾除了受試者者本人外，無人知悉確切是誰有吸毒[80]。

此一設計的優點其一在於受試者知悉沒有人會知悉其回答，因此沒有造假的動機；其二是大量數據蒐集後即可得知目標數據無需於蒐集後再做去識別化處理，避免了許多人為或是資訊傳遞過程可能的資安風險。然而其最主要的缺點在於其通常只能運用在單一資料欄位，且該欄位可於最後進行簡單統計處理的情況，而無法用於需保留欄位數值相關性的情形，再者收案量也必須足夠，因此使用範圍上相對限縮[81]。

第三款 小結

從上述去識別化技術的相關介紹約略可歸類出三點：

一是去識別化程度與資料可利用性成反比，去識別化程度越高，資料可利用性越低，不過由於很多時候研究也未必需要使用到最完整的資料，因此是否與資料利用目的相符，仍須個案依據「資料分析、利用的精確性需求」和「投入在去識別化的勞力、時間、費用」作為選擇去識別化方法的考量因素。

[80] 李斯壯、黃彥男，前揭註 70，頁 37。
[81] 李斯壯、黃彥男，前揭註 70，頁 38。

doi:10.6342/NTU202301113

二是所謂去識別化不該理解成三段差，也就是不該於概念上僅分成「未經處理」、「經處理仍可再識別」、及「處理後不可再識別」三種情形，而應該將所有去識別化技術理解成係對於再識別風險「量」的調控。易言之，也就是風險光譜的概念。蓋無論是運用「抑制」與「泛化」技術的 K 匿名化模型、運用「隨機」技術的 L 多樣性模型，或是「添加雜訊」的差分隱私模型，只要仍是蒐集資料後才進行資料處理的技術，就皆有一定程度的再識別風險，如上述模型正是用「K 值」、「L 值」、隱私參數「ε值」等量化數值的高低，據以試圖精確描繪去識別程度及再識別風險。

這其實恰好回應了本文在本節、第一款整理學者對去識別化的效用質疑，其等指出所謂去識別化，即使已經處理到當今法律定義下、不可回復、不可再識別的「匿名化」，實然上於未來科技發展、或其他可預見、外部、公開、非公開的資料庫交互比對下，依然難保無再識別風險。此一觀點如果從 K 匿名化的 K 值概念思考即可理解，蓋所謂 K 值高低僅代表特定資料庫內難以特定個體的情形，其並不能保證在存在其他外部公開資料庫存在的情形下，個體能不被再識別。

三，所謂去識別化的技術定義跟去識別化的法律定義不但在各自領域中都存在分歧，再者兩者的討論上也存有層次上的差異，故實際上難以於兩者之間進行對照連結。就法律定義來說，以我國法為例，光是在所謂「無從識別」的標準上，就有「經假名、代碼化而第三人客觀無法推知即符合[82]」、「永久無法逆推出個資主體始符合[83]」等數種情形[84]，遑論其他各國像是歐盟 GDPR、美國 HIPAA 分別就匿名化存有不同法律定義、對去識別化也存有安全港法、專家法等不同定義。

本文認為關於法律上就去識別化的定義，除了必須從各國立法過程、比較法參考脈絡下去理解，功能上也必須從「時間上是否指現在、一定期間，還是永久

[82] 臺北高等行政法院 103 年度訴更一字第 120 號判決
[83] 人體生物資料庫管理條例第 3 條第 7 款。
[84] 排列組合上還包括「任何情形（即使屬於該領域專家）通常情形仍無法推知」等情形。

doi:10.6342/NTU202301113

不可再識別？」、「是否考量外部公開或非公開資料庫的勾稽可能？」、「再識別風險是從客觀還是主觀角度出發？」、「主客觀又究竟係指一般人、一般窺探者、還是該領域專家角度？」等角度逐一分析比對，不宜於名詞用語上打轉。

另外就去識別化的技術定義而言，不同模型間有不同的標準，標準間各有優缺點（如下表所示），但因為各模型衡量去識別化程度的標準不同，因此標準之間難以互相比較，似乎難以建立共同標準。舉例而言，K 匿名化係採取K值高低判斷，差分隱私則以隱私參數 ε 值調控雜訊量，再以處理後資料的平均、變異數、標準差、資料洩漏風險、資料消失率等標的，更細緻的去描述去識別化程度跟資料可用性之間的複雜關係。

表一、K 匿名化與差分隱私模型比較[85]

	K 匿名化	差分隱私
定義	1.要求對數據中所有元組進行泛化處理，使其不再對任何人一一對應。 2.泛化後每條紀錄至少與 K-1 條紀錄一致。	對原始數據或是統計結果加入雜訊達到保護效果。
缺點	1.無法抵擋一致性攻擊及背景知識攻擊。 2.默認屬性都有相同重要性。 3. K 匿名模組雖然不斷改進，保障更多細節，但仍需特殊攻擊假設及背景	要滿足保護的抽樣函數和保護條件困難。

[85] 本表摘要自陳泓歷，前揭註 72，頁 8。

doi:10.6342/NTU202301113

	知識，陷入保護模型不斷提出又不斷被攻破的循環。	
優點	匿名效果較佳，但可用性與匿名效果需要取捨，泛化程度會降低可用性。時間空間成本花費最小。	1.攻擊者有背景知識，隱私也不洩漏。 2.嚴謹統計學模型，方便數學工具及定量分析證明。 3.降低風險同時，保證資料可用性。加入的噪音量與數據大小無關。

本文認為若要徹底地解決去識別化困境，就不能只關注數學技術上的定義、或是只關注法律上的定義，而是必須盡量在評量標準上統一二者。此一主張本文理解是知易行難，蓋光是技術上就存在不同模型，且各模型存在定義上的爭執、其分別適用的場合也不同，若要將技術定義與法律定義統合，自然會存在巨大阻力與困難。然而本文認為也正是此一特色才凸顯了現行隱私法制於制度上的不足，蓋技術上之所以需要這麼多模型正是在於社會上存在不同的去識別化需求，這些需求分別是從不同成本、蒐集目的、利用方式、防範對象、外洩容許性等觀點所出發，本文認為這凸顯了現行隱私法制於法律規範上分類過窄、涵蓋不全，甚至最簡單者僅以「未經處理」、「經處理仍可再識別」、及「處理後不可再識別」三種情形就認為已經將去識別化分類窮盡，顯然是對不同資料領域、資料類型、利用目的的理解不足。舉例來說，光是資料類型就可再區分成「外洩不至大幅影

doi:10.6342/NTU202301113

響權益的一般性資料」、「外洩將導致權益嚴重受損的敏感性資料」、以及「外洩將危及公共安全等重大情形的機密性資料」等三種情形[86]。

本文之所以認為技術上的定義與法律上的定義統合或許仍有可能的原因在於，去識別化技術上於定義上存有共通性。蓋無論是 K 匿名化還是差分隱私模型，其等皆是採取「可量化」的再識別風險評估模型。這代表法律上的定義至少也可以比照技術上的定義採取一個將再識別風險量化的觀點，而非採取概念式的三分法，一概排除「匿名化」的個資適用現行隱私法，此一作法無疑是將「再識別風險」過於輕視，而於概念上過早將資料排除於法制外，在許多研究顯示再識別風險提升的今日，著實讓法制顯得缺乏彈性，導致涵蓋過窄。

雖然在法律上對於去識別化也採取量化標準可能存有爭議，不過本文認為這乃是肇因於不同資料類型、不同研究目的，對於再識別風險、資料可利用性、技術花費時間成本，與隱私保護三者之間的平衡（Trade-off）考量的不同。

就此，基於事物本質差異大，需要更細緻規範的緣故，關於「怎樣的去識別化處理應該對應到怎樣的組織、程序上要求」，或許可以給予行政機關較高的裁量空間進行判斷，或是由獨立專家、委員制定更細緻的規範，而不該以立法方式僅一過於簡單、化約、死板的定義侷限。另外，也可參考 HIPAA 的規定，透過另設專家判斷機制等方式，交由第三方監督，使得正當程序要求更加完備。

對此就有學者指出美國無論是聯邦受試者保護規則（The Federal Policy for the Protection of Research Subjects (Common Rule)，美國通用規則）或是 HIPAA 下的隱私保護規則，於法規適用範圍上不但不納入去識別資訊（deidentified information）[87]，且就去識別化的具體處理上，也不要求取得個資主體的授權或同意，甚者，去識別化處理上也欠缺統一的程序、標準規範，其以病歷資訊的去

[86] 參考自 ISO/TS 25237:2008-12-01, Health informatics – Pseudonymization.規範的隱私防護保證層級。轉引自蔡昀臻、樊國楨，前揭註 60，頁 13。
[87] Rothstein, *supr*a note 51, at 2., 45 C.F.R. § 164.502(d)(1)

doi:10.6342/NTU202301113

識別化為例指出，由於去識別化過程通常涉及多步驟處理，而非一鍵完成，因此過程中所產生的個資外洩風險，即在當前不重視去識別化處理的架構下被忽略了[88]。其批評所言甚是。

第三項　延伸個資定義困境

承上，若採用風險光譜的量化概念，統一法律、技術上對去識別化的定義，接著仍會延伸出一個關鍵問題，即何謂「個資」？蓋雖然歐盟將去識別化概念拆成二者，一是可識別性，並盡量寬鬆判定以使得資料適用個資保護法律規範，二是去識別性，據以主、客觀標準判斷是否符合規範，然而後者如果已經達到事實上、制度上不可逆的程度，且永久除去識別特定個人的可能性時，此時該資料即已非屬個人資料，結論上仍會排除個資法的適用。此一結果導致「去識別化」不僅於可識別別性的面向上涉及個資定義、個資法是否適用問題，在去識別性的面向上也同時兼有風險管控的功能。然而在前述關於去識別化的法律、技術上定義的討論下，尚未處理到「何謂個資？」的定義問題。由於兩者可識別性跟去識別性的討論實難以區分，故關於個資定義問題，也必須一併討論。

根據傳統的理解，資料被定性為個資是適用 GDPR 的前提[89]，然而個資的定義於近年來逐漸模糊。GDPR 所指涉之個資係指「有關識別或可得識別自然人（資料主體）之任何資訊」[90]，此處的可識別指的是「資料控制者或第三方可以透過合理方法直接或間接識別該個人」[91]，而所謂的合理方法必須以「彼時的科技條件，客觀評估再識別所需的時間、成本」[92]。在此一框架下學者指出歐盟法院於近年來不斷擴大個資的定義，並整理出兩個趨勢，一是所謂「個資」不需要單獨

---

88 *Id.*, at 5.
89 Working Party Article 29, *supra* note 57, at 5. 匿名化不可識別資料即不再適用歐盟個資法。
90 GDPR, Article. 4 (1).
91 *Id.*, Recital 26.
92 Working Party Article 29, *supra* note 47.

doi:10.6342/NTU202301113

憑其自身即可識別出個資主體，二是能使得再識別個資主體成為可能的資訊，不需要屬於同一實體所有[93]。

另外，也有指出所謂「個人可識別資訊」（Personally Identifiable Information, PII）以及「標準識別符」（quasi-identifier）實難以從技術上定義[94]，並將逐漸喪失意義。蓋試想像一個人所看過的書、衣櫃裡的衣服，這些資料單獨來看或許並無法識別個人，但只要這些因子的數量夠大就會足以識別出個人[95]。易言之，任何資訊都可以用來再識別，只要該資訊在不同人之間有獨特性。

上述總總都將使得「何謂個資？」此一問題變得越來越難以事前預測，而必須仰賴個案分析，而這正是人工智慧下，科技善於將個資與非個資連結的科技發展結果，因此將會很難說哪一個資訊不可能於未來能跟個資產生連結[96]。關於此一個資與非個資間定義越來越趨模糊的趨勢，國內學者也有提及[97]。

這樣的發展也進一步影響了資料去識別化的定位，傳統上 GDPR 或是個資法都不適用於匿名化、無法指向任何已識別、可識別個人之資料，然而現在的情況不一樣了，在匿名化資料跟其他資料結合的時候，兩者有可能導致個人之再識別，這將會導致所謂的匿名化資料將會是相對的，而不再存有單一固定的定義，此時 GDPR 前言所謂的「再識別合理方法必須以彼時的科技條件，客觀評估再識別所需的時間、成本」[98]，就成為了判斷是否屬匿名化資料的一個重要判準。

上述之困境同時是科技，也是法律上的問題，一方面從科技的角度觀察，各類資料的取得越來越多、資料分析技術及硬體技術也越來越成熟，這將會使得資料庫間交互連結、從顯非個人資料推導出個人資料的可能性越來越高；另一方面

---

[93] GIOVANNI DE GREGORIO, DIGITAL CONSTITUTIONALISM IN EUROPE: REFRAMING RIGHTS AND POWERS IN THE ALGORITHMIC SOCIETY 234 -235 (2022).
[94] 所謂標準識別符(Quasi-identifier)係指資料集中的識別符與其他額外在資料集外的屬性結合，可唯一識別其資料主體。相關定義可參：祝亞琪、魏銘志，前揭註 64，頁 20。
[95] Narayanan & Shmatikov, *supra* note 77, at 26.
[96] *Id*., at 236.
[97] 邱文聰，前揭註 36，頁 162。
[98] GDPR, Recital 26.

doi:10.6342/NTU202301113

從法律的角度觀察，這也顯示了當前缺乏一個完善的法律標準得以妥善分類個資[99]。像是就有學者認為當前「匿名化個資」的概念誤導並產生了一種「使人自以為可以透過匿名化個資，絕對、永久清楚切分個資法適用範圍的幻象[100]」。

第四節　　我國學者見解

上述討論了去識別化定義困境、技術困境以及從去識別化困境所延伸的個資定義困境，就此，當代學者分別對此一識別化困境提出看法，其等大概可以分成兩類：（一）從技術層面解決、（二）從強化資料蒐集、處理、利用、甚至是去識別化後，都賦予一定程度的同意授權機制來解決，本文稱之為強化、擴張同意進路。簡要如下：

（一）首先是欲從技術層面來解決者，如宋皇志在經過判決實證研究後發現[101]，我國司法判決仍誤以為刪除部分直接識別標誌即可去識別化，毫無再識別風險之概念。其認為對於大多數研究而言，著實沒有追求資料絕對精準之必要，可用區間模糊數據的精準性，平衡個人資料隱私保護與資料可用性。此即是運用本文於前曾去識別化技術介紹時所提及的「泛化」的例子之一。

另外，其也認為資料提供者應確保去識別化的成效，在交易前對去識別化之效果進行驗證，透過挑選個人已知的幾筆資料，確認是否得由這幾筆資料比對識別出特定人，據以認定再識別風險是否低於一定標準[102]。這樣的作法其實已經於我國踐行，如經濟部標檢局即出版了一系列相關的國家標準，包括 CNS29100 系列以及 CNS29191 等與個資保護和去識別化流程相關的組織參考。其中以「資訊

[99] Michele Finck and Frank Pallas, *They Who Must Not Be Identified – Distinguishing Personal from Non-Personal Data under the GDPR,* 10(1) INTERNATIONAL DATA PRIVACY LAW 11, 11(2020).
[100] Khaled El Emam and Cecilia Alvarez, *A Critical Appraisal of the Article Working Party Opinion 05/2014 on Data Anonymization Techniques*, 5 INTERNATIONAL DATA PRIVACY LAW 73, 81–2 (2015).
[101] 宋皇志（2018），〈巨量資料交易之法律風險與管理意涵—以個人資料再識別化為中心〉，《管理評論》，37 卷 4 期，頁 37-51。
[102] 宋皇志，前揭註，頁 37。

doi:10.6342/NTU202301113

技術-安全技術-個人資訊去識別化過程管理系統-要求事項」為名的 CNS29100-2 國家標準中，即有關於再識別風險檢視的規定[103]，其要求組織進行「資料保護衝擊評鑑」(DPIA)和「重新識別風險評鑑」[104]。

（二）至於從擴張、強化同意的角度解決者：

首先是學者張兆恬即質疑去識別化跟僵化的告知後同意無法充分解決當代資料蒐集問題，而認為應該從賦權參與者的角度去讓參與者重拾資訊自主，其方法是將焦點從告知同意所關注的資料蒐集的那一刻，轉移到資料取得後與參與者間持續性的關係，透過提升透明度或第三方機構的參與與監督以強化參與者的決定基礎[105]。而抱持這類想法的學者並不在少數[106]，像是邱文聰即認為動態同意（Dynamic Consent）或後設同意（Meta consent）機制可使得當事人持續修正自己的同意決定以及隱私偏好，使個人得以透過當代科技對個資的未來利用有持續性的控制。而由於科技使得個人持續行使自主決定的權利行使成本降低，因此去識別化路徑也不該繼續被認為是合理正當、有效率的途徑[107]。

動態同意及後設同意固然是解決單次告知後同意的好方法，不過此一理論未處理的問題乃如果今天資料已經細碎化、甚至去識別化而難以與個人連結時，此時應該透過何種理論基礎來為個資主體「賦權」？以下介紹兩種主張，一是以馬

---

103 經濟部標準檢驗局（2019），《CNS 29100-2:2019 資訊技術-安全技術-個人資訊去識別化過程 管理系統-要求事項》，頁 20。

104 「重新識別風險評鑑」比較好理解，其概念和本文先前提到 HIPAA「專家法」類似，都是對於經處理資料「被重新識別出特定個人」的風險值進行評估。至於 DPIA，則是較廣泛地對於組織經手的個人資料的隱私風險進行評估，比較重要的是此標準指出，並非所有的個資處理都要求相當的保護等級或形式，組織需要透過對其面對的特定風險的認識，決定要在怎麼樣的情況下，採取何種資訊保護措施。就此，隱私風險的管理是此過程的核心方法。詳參經濟部標準檢驗局，前揭註 103，頁 12-14。

105 張兆恬，前揭註 58，頁 42。

106 林其樺（2015），〈一般常見把姓名、身分證字號隱碼的做法，其實並不等於將個人資料「去識別化」〉，《關鍵評論》，載於：https://www.thenewslens.com/article/33049（最後瀏覽日：04/27/2021）。葉志良（2016），〈大數據應用下個人資料定義的檢討：以我國法院判決為例〉，《資訊社會研究》， 31 期，頁 23。林其樺主張應將個資整個生命週期（從隱私權政策、風險評估、去識別化操作、到重新識別評鑑等）都納入關注，葉志良認為應將基於資料安全與課責性原則所採取的去識別化方法視為一種保護措施（protective measure），而不是作為大數據謎題的解方。

107 Chiou Wen-Tsong, *Digital development and privacy: Is there a way to alleviate the uneasy tension?* In THE WAY TO LAW: IIAS'S 10TH ANNIVERSARY, 465-468 (Chien-Liang Lee eds., 2021).

doi:10.6342/NTU202301113

賽克理論賦權，也就是從資料處理過程中如果可以拼湊出個人，即仍將其視為個資；另一則是以接近資料財產權的角度，從資料源頭所有人出發，只要能追溯出原所有人，無論資料是否可識別，仍以此一理論賦權於主體。

（1）首先是主張馬賽克理論的林昕璇，其指出當代數據持有者的能力以及技術的強度已然提升，原先不敏感的資料能透過分析取得其他敏感資料，敏感資料跟不敏感資料的界線更加模糊，甚至到最後可能一切資料都會是敏感資料。面對此一情形，應該藉由「馬賽克理論」的援用，以解決「資料過於片段零碎、無法識別特定人，因此就不需取得令狀、不需獲得同意」的問題，其同時點出當前過度僵化的告知後同意機制，僅著用於「資訊取得階段」，而不涵蓋後續「分析、處理與散布的資訊使用階段」，以致於無法避免系統化、常規化、連結多目的用途的個人資料蒐集與利用，使得人民的隱私利益於逐漸銷蝕殆盡[108]。

此一馬賽克理論具體上應用於細碎、難以直接認定屬於個資的資料。依本文理解，林氏於此處所指的細碎資料（元資料，metadata）可能在現行個資保護法律下，無論是歐盟 GDPR 觀點，或是我國個資法觀點，都係不受個資保護法律規範的「非個資」（匿名化個資）。林氏認為如果該資料經過一定的組合，就可以從細微片段中拼湊出個人生活圖像時，此時就應認為國家對該資訊蒐集、使用的行為該當於「搜索」，需依令狀原則始得為之；反之，若仍存於片段狀態，尚難拼湊出個人時，則繼續適用合理隱私期待與第三人理論[109]。

（2）在去識別化逐漸喪失保護效力的同時，也有認為為了因應再識別化的風險，以及更貼近一般社會大眾直觀上對個人資料的理解，應該擴張個人資料的定義，無論其是否具備可識別性，皆將其納入個資保護的範圍。論者何琳潔即以一張「遮蔽臉部面孔之裸照」為例指出，對於一般人而言，縱使第三人無法直接

[108] 林昕璇，前揭註 31，頁 81。
[109] 林昕璇，前揭註 31，頁 82。

doi:10.6342/NTU202301113

辨識出該照片當事人，一般人仍會認為這是屬於個人的資料[110]。因此無論是否有再識別可能，或甚至是已經到完全匿名的狀態，仍應認為該資料屬個人資料的範疇，據以保障資料主體自主控制的權利。

此一見解相較於學者林欣璇的馬賽克見解或是張兆恬的賦權見解，無疑又更往前推進了一步，蓋其並不在乎零碎的資料是否仍能透過組合拼湊，而形成馬賽克理論的保護客體，其只在乎到底該資料的源頭屬於誰所有，而誰直觀上最有主張該資料的相關權利，且資料是否經去識別化並不會影響權利得否主張的判斷。當然這樣的看法不無反對意見，Ohm 即認為倘若將可識別之個人資訊定義擴大解釋，難免會讓資料使用者放棄去識別化的作為，反而增加隱私與資料安全的風險；更進一步的風險是，隨著解釋的擴張將使得隱私保護架構顯得難以執行[111]。

第五節　本文見解

由上述整理可見，去識別化的困境在於科技上再識別技術的發展導致匿名化變得困難，而由於匿名化與否是區分該資料是否仍屬於個資、是否仍適用個資法的關鍵，因此此一發展也同時導致個資定義漸趨模糊，必須視該資料於一定脈絡下的情境下，是否仍有合理可識別個人的機會而定。

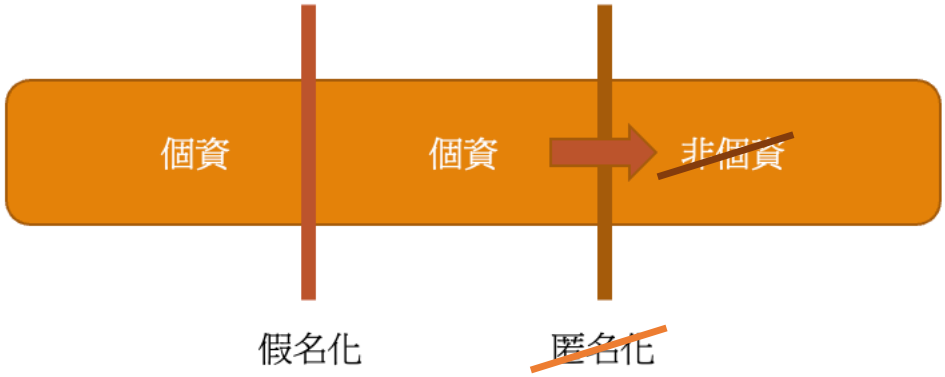
第一項　限縮解釋「匿名化」概念

在歐盟強調「依當時科技水準、一般人努力無法再識別」的「匿名化」概念經前說明可見其並非絕對保障的情形下，本文認為自然就難單以「資料已經去識別化處理」為由，作為資料蒐集、處理、利用的單獨基礎。也就是說如果站在風險耐受度較低、認為資料再識別機率較高的角度，此一匿名化概念將失去規範上

[110] 何琳潔，前揭註 50。
[111] Ohm, *supra* note 53, at 1701-1777.

doi:10.6342/NTU202301113

的意義，換句話說，未來將只存在以量化風險高低區分的假名化，而不存在完全的「匿名化」，如下圖所示：



這將會對隱私權產生的重大影響在於，不宜將匿名化再當作區分是否適用個資法的標準，蓋任何去識別化的行為都將僅被視為是調控個資外洩風險的工具而已（去識別化處理於定位上應屬於資安手段，而非排除同意、授權的條件），誠如經過假名化之資料依然適用 GDPR，歐盟將假名化作為風險管理手段，而非像匿名化資料般從定義上就排除 GDPR 適用[112]，本文認為未來不應該再以資料經「匿名化」為由，過早於前端個資定義就排除個資法的適用，而必須具體於個案探究假名化或是其他前述介紹的去識別化技術的功能與成效，並最好能由立法、行政分就各不同資料類型、利用目的、去識別化手段做出詳細、合理的分類對應要求。易言之，本文認為至少要限縮當前歐盟「匿名化」概念的適用範圍，將該概念跟其他個資的同意、組織、程序保障規範脫鉤，不該再將個資是否「匿名化」作為 GDPR 或個資法適用與否的唯一考量因素。

第二項　類型化、細緻化去識別化處理

在限縮匿名化概念於法規範上的適用定位後，關於去識別化的規範必須更細緻、更清楚。理想上應區分不同公益目的，再基於不同比例原則的操作，配合不同程度的去識別化處理，據以妥善解決數據匯集、儲存整合與分析能力提升後所

[112] GREGORIO, *supra* note 93, at 239.

doi:10.6342/NTU202301113

產生的再識別困境。具體作法上有學者即建議應該更細緻的去討論以下幾點：像是（一）去識別化與其他隱私保護措施的連結、（二）去識別化資訊應於多少程度上適用可識別資訊的規範、（三）去識別化資訊應該透過哪些特定方法保護，如通知、同意管理或選擇退出等方式、（四）去識別化資訊用於研究、公益或其他目的時，應該怎麼被規範、（五）是否所有去識別化資訊都要適用特別保護，還是僅限於健康敏感性資訊[113]。此類具體法律上的管制及倫理上的要求，可能會根據研究種類不同、去識別化程度高低、再識別風險高低、個人或群體不同的脆弱程度不同（vulnerability）等因素，而有差別待遇之必要。

關於其具體作法已經逾越本文所欲處理的範圍，不過本文認同此一方向，只不過應注意者係，雖可透過不同的公益目的操作不同程度的比例原則，再配合不同程度的去識別化處理，以分層適當的保護隱私權。然而誠如本章第三節、第二項、第三款小結所述。關於去識別化程度上量的差異，不同去識別化模型間、不同法域間，甚至是同一國內的法制間都可能存有不同的認識，此差異能否透過清楚定義而彌平、雙方溝通時能否有共同的認識等，實不無疑問。再者，去識別化程度越高，資料可利用性越低、費用成本越高，此一內生限制也應納入考量。

第三項　去識別化作為資安保障工具

本文認為去識別化處理於法制上的定位應該被當做資安手段並做更詳細的規範，而非當作正當化個資蒐集、處理、利用的條件。當前我國個資法於第 27 條第一項[114]以及其施行細則第 12 條第二項[115]，關於資料控管者的安全性義務的

---

[113] Rothstein, *supra* note 51, at 11.

[114] 個資法第 27 條第一項:「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人 資料被竊取、竄改、毀損、滅失或洩漏。」

[115] 個資法施行細則第 12 條二項：「.....第二十七條第一項所稱適當之安全措施.....一、配置管理之人員及相當資源。二、界定個人資料之範圍。三、個人資料之風險評估及管理機制。四、事故之預防、通報及應變機制。五、個人資料蒐集、處理及利用之內部管理程序。六、資料安全管理及人員管理。七、認知宣導及教育訓練。八、設備安全管理。九、資料安全稽核機制。十、使用紀錄、軌跡資料及證據保存。十一、個人資料安全維護之整體持續改善。」其所例示的十一款，似乎皆屬於內部管理程序，而無涉去識別化處理，因此尚難將去識別化處理歸類於上述適當安全維護措施內。

doi:10.6342/NTU202301113

例示規範中並未涵蓋去識別化處理，反而最接近「去識別化」的「資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人」用語，僅見於敏感個資的蒐集、處理、利用（第 6 條 1 項但書 4 款）、告知義務的免除（第 9 條 2 項 4 款）、公務機關目的外利用（第 16 條但書 5 款）、非公務機關蒐集、處理個資（第 19 條 1 項 4 款）、及非公務機關目的外利用（第 20 條 1 項但書 5 款）等規範「例外得以蒐集、處理、利用情形」的條款。

此與 GDPR 相當不同，蓋 GDPR 在第 32 條第一項即規定[116]：「考量現有技術、執行成本、處理之本質、範圍、脈絡及目的與對當事人權利及自由之風險變動之可能性與嚴重性，控管者及處理者應執行採取適當之科技化且有組織的措施，以確保對於風險之適當安全程度，包括但不限於適當之如下事項：（a）個人資料之假名化及加密。」（a）款顯然將去識別化處理置於資料控管者的安全性義務定義下，此與前述我國個資法第 27 條一項、施行細則第 12 條二項關於安全性義務的例示規定相比，即可見我國個資法的狹隘與不足。

此一法制上的缺失，導致去識別化處理僅在蒐集、處理、利用的同意例外規定中出現，混淆了去識別化處理作為安全性義務的定位。「去識別化處理」本身就應該被視作個資的「處理」，原則上應取得資料主體的同意，且屬資料控管者的安全性義務的一環，並非「蒐集、處理、利用」排除同意取得的例外規定。

第四項　賦權強化控制

至於就前述學者就去識別化困境提出的解方，本文認為主張賦權予參與者，使得其得以在資料取得後的持續性關係中確保其資訊自主權的作法而言，這無疑是將隱私權保障放在正當法律程序下一個更全面的角度在思考，這種作法或多或少已經將隱私的保障焦點轉移，不再僅關注資料在蒐集當下是否具有可識別性，

[116] 張陳弘、莊植寧，前揭註 44，頁 242。

doi:10.6342/NTU202301113

或是否屬於第一次資料蒐集。蓋在這科技快速成長變動的過程當中，法律或是資料蒐集機關等對去識別化的認知內涵時常會趕不上科技的進步，假如只聚焦於第一次的資料蒐集時點是否取得告知後同意，彼時法律所規定必須提供的說明，很高機率到最後以事後觀點檢視時，會顯得非常不充分。而這並非能單單怪罪於公部門民主制度的運作效率永遠趕不上科技變化的傳統科技監管問題，因為即使是私人間的資料蒐集，雙方也未必對於現在所擬定的契約下的非可識別個資，未來無被再識別可能有清楚明確的認識。

此或許即為隱私侵害與資料利用邏輯下的內生矛盾，蓋資料的利用可能非常難以在蒐集之初就特定、隱私風險也難以在蒐集同意權之初就具體描繪使被蒐集方得以明確理解與知悉，以前述歐盟如何判斷資料已經去識別的主觀說為例，即可見所謂潛在具動機的侵害者，是一個難以預想且很有可能是一種必須透過事後觀點去確認的浮動概念，該標準可能會隨著時間、科技發展或承審法官而有所不同，因此該標準下的去識別化要求以及隨之而形成的告知後同意是否會有一般性的預防隱私侵害的功能即值得存疑。

同理，關於前述新聞所提及的「15 項屬性特徵或是十份網路瀏覽紀錄就可以識別出個人」，這樣的概念是否在資料蒐集者在以去識別化為由進行資料蒐集時，能使被蒐集者對相關概念了然於心？是否能讓資料被蒐集者了解到去識別化只是一個程度上的差異，並非完全無再識別可能？這些問題能否具體的被回答，使被蒐集者得以在腦中能形成一個關於未來資訊外洩風險、再識別風險的具體圖像，將影響個資自主權的討論是否還應該聚焦於當前僵化的告知後同意制度。

前述曾提到學者有提出所謂「賦權予參與者使得其得以在資料取得後的持續性關係中確保其資訊自主權」的作法，即意在解決此一問題，然而雖然其等透過落實資料蒐集前、中、後的正當法律程序，隨時使資訊主體在有目的外利用或第三方利用時，充分了解其資料蒐集目的、可能的用途、可能的洩漏風險，得以解決前述再識別風險隨時間演進而浮動的難題，然而本文認為該理論可能缺漏了一

doi:10.6342/NTU202301113

部分論證，也就是「為何」個人可以在資料屬於「去識別化資料」時，對該資料從蒐集、利用、到處理，皆享有「動態」的同意控制或授權。

本文目前認為可能的理由有二，（一）是像林昕璇一樣透過「馬賽克理論」於再識別風險達一定程度時，就將細碎的資料重新與個人連結，重新賦予個人自主權，然而此一理論無法完整的涵蓋整個資料蒐集、處理、利用過程，如果再識別風險未被凸顯，則動態同意的基礎仍會被動搖、（二）乃是像何琳潔主張般，自始就透過擴張個資定義以加強個人對細碎、被打散個資的控制。兩者的差別在於馬賽克理論並沒有限縮當前歐盟之「匿名化」概念，其就「匿名化」的理解仍是僅於某時點下成立，而非永久不可再識別，因此只要再識別風險上升到足以拼湊出個人圖像，則匿名化又不復存在。相對的，自始擴張個資定義，如果係指無論如何經去識別化處理都仍屬個資，就是進一步去限縮此「匿名化」概念，即無論經哪種去識別方式處理？當下可否再識別？只要從事後觀點個資主體得以證明該片段資料「係從己身所出」或「與自身存在私暱性連結」，該片段資料仍應認定屬於個資。

本文比較贊同後者何琳潔所主張應擴大個資定義、賦權於資料被蒐集方的見解。蓋馬賽克理論於應用上可能存在太多不確定性，像是礙於科技上未知、或是由於其他公開資料庫出現時點的不同，進而導致不確定何時可被再識別？再者，再識別的定義也可能存在分歧，蓋再識別風險是可量化的機率，並沒有一定的閾值可以判斷。末者，最重要者係此一理論依然保留了讓資料蒐集者得以「匿名化即與個人無關」的邏輯，進行資料蒐集、處理、利用的可能，只是個人可以再識別風險已然提升，個人已被拼湊為由，再次取得自主控制而已。

本文認為此一理論忽略了個資分析、處理、利用經常是在不知不覺中進行的現實，當個人理解到個資再識別風險時，通常個資已經外洩，甚至目的外利用已經發生，此時若再賦予個人控制權，礙於隱私權的侵害多半不可逆，此時個資主體至多只有退出權、刪除權、或損害賠償可資選擇而已。相對的，透過限縮與排

doi:10.6342/NTU202301113

拒運用「匿名化」概念，改採擴大個資定義的方法，則可以自始就將所有個資處理，無論是否採取去識別化手段，皆認定是個資的蒐集、處理、利用。除非有法定事由、公益或取得個人同意的情形外，否則原則上不得進行。在此一理論下，甚至所謂的「去識別化處理」本身都會被視作個資的「處理」，而原則上就需要取得同意。此時對於個資的保護就會被推向更前端起步，不必嗣再識別風險明確後始得介入。

不過具體理論上究竟應該如何「擴張」個人對於細碎的個資的控制？如何將看似於當下已難以跟個人連結的資料，認為個人仍對該資料有控制權？是否仍有馬賽克理論以外，其他以個人為出發點進行賦權於個人，並讓個人得以不分資料是否經去識別化與否，皆得以主張資訊自主權的理論？此乃本文於第三章以降的重心。

本文認為美國法上關於資料財產權的主張或許可以作為參考，據以支持本文擴張個資定義的主張，雖然該理論出現的脈絡與「擴張個資定義」稍有不同，惟該理論仍意在賦權予個人，因而或許得以挪用於本文所欲探討的個資定義議題。該理論將個資視作個人的「財產」，應用於本處，可試以「所有權」的角度思考個資，此時直觀上無論該「個資」是否經過多高程度的去識別化處理，仍會係屬個人所有，如同將一塊橡皮擦切得再細，原所有人仍對每個碎屑擁有所有權一般。

此一理論的優點在於其符合個人對個資的直觀想像，如同有調查研究指出，一般人對於個資的想像並不符合可識別、非識別資訊間的法律上保護區別[117]。像是 Hull 及其同事於 2008 年對 1193 名，從五個學術醫療中心的家醫科、胸部外科和腫瘤科招募來的患者所進行的研究顯示。有 72%的患者即使在研究蒐集資料屬於匿名化資料的情形下仍想知道研究結果，而當研究資料係可識別時，有 81%患者想知道研究結果，只有 17%的患者只想知道運用可識別資料所生的研究

[117] *See* Rothstein, *supra* note 51, at 9.

doi:10.6342/NTU202301113

結果，而不想知道運用匿名化資料所生的運用結果。另外，在這些想知道研究結果的患者中，**當被問到「匿名化（Anonymous）」的生物檢體是否可被用於研究使用時，57%認為研究者應該向其尋求同意**，僅 43%認為向其通知就足夠了[118]。

相同的發現也見於 Westin 受美國醫學研究會(institute of medicine, IOM)委託於 2007 針對一般合法利用健康紀錄（health record）所做的問卷研究中，其發現高達 38%的受試者希望研究者於使用其所有的可識別（personally-identified）醫療或健康紀錄時，仍應向其尋求同意；19%認為只要研究不對外揭露個人身份且受機構審查監督，就不需要尋求個人同意；而**有 13%不希望其健康紀錄在任何情況下被利用**；只有 9%認為不需向其聯絡或尋求同意；20%表示不確定[119]。

另有一 2005 年之澳洲問卷研究發現雖然大多數受試者（67%）願意提供其去識別化個人健康資訊供醫生於醫療研究中使用[120]。然而該研究發現有**高達 81%的受試者認為即使是去識別化資料，仍然希望醫生在進行此類研究前，應向其等尋求同意**[121]。

由上可見當代個資主體對於個資的想像，其實完全不符合當前以「可識別個資」、「不可識別個資」作為分野的管制架構。個人對於個資的直觀想像，其實無法被現行「去識別」脈絡的利用管制思維所涵蓋，因此，為了探討更符合個人直觀想像的管制架構，以下將於第三章從病歷資訊、基因資訊的利用爭議出發，探討資料的歸屬與性質，再於第四章透過對美國資料財產權理論的爬梳，探討比較法上的理論參考是否能更符合個人對個資的直觀想像？又該理論是否得以將

---

[118] Sara Chandros Hull et al, *Patients' views on identifiability of samples and informed consent for genetic research*, 8(10) AM J BIOETH. 62 (2008).

[119] Alan Westin, *How the Public Views Privacy and Health Research*, Results of a National Survey Commissioned by the Institute of Medicine Committee on "Health Research and the Privacy of Health Information: The HIPAA Privacy Rule". (Institute of Medicine Committee Meeting, 2006), 21-22, https://www.ftc.gov/sites/default/files/documents/public_comments/health-care-delivery-534908-00001/534908-00001.pdf.

[120] *Id*., 然而有 62%不願提供其去識別化個資健康資訊供商業目的使用。

[121] Australian Medical Association, *AMA Poll Shows Patients Are Concerned About the Privacy and Security of Their Medical Records*, AMA, (July 20, 2005). https://www.ama.com.au/media/ama-poll-shows-patients-are-concerned-about-privacy-and-security-their-medical-records. 若細分用途，則如果供政府使用為 78%者同意、供商業使用為 79%者同意。

doi:10.6342/NTU202301113

個資定義擴張，使得無論可識別個資、不可識別個資，一概都能賦予個人一定程度的自主權利主張以強化個資保護範圍？

第三章　　資料的權利歸屬與性質

為了逐步切入如何賦權個人以保護個資資訊自主權，本章將先從病歷的資料歸屬問題以及基因資訊的性質爭議兩個經典案例出發，探討資料的法律上性質及權利歸屬爭議，再進一步回歸理論源頭重新爬梳個資保護於法制上的定位，也就是隱私權規範究竟應於固有的人格權體系、還是應於財產權體系下討論，才能既符合個人直觀想像，又能兼顧資料利用與個人自主權。

第一節　　從病歷資訊爭議思考資訊財產權

關於是否應該不論資訊是否經去識別化，概皆納入隱私權保障範圍這項爭議，除了前述提及的遮蔽可識別特徵的裸體照片想像實驗可作為一般人對隱私定義的直觀說明外，本文發現這個爭議其實已經具體且徹底地展現在病歷的隱私權保護議題上。蓋病歷資料的歸屬或所有權，縱使經去識別化處理，病人多數會認為病歷屬於自己所有，但在實務上，病歷乃由醫師及醫療團隊紀錄與製作，由醫療機構依法儲存與保管，使得病歷本身之所有權以及其上所載資訊的使用利用不易切割或清楚明確界定，因此在醫院方利用該資訊或資料主體請求利用時，即容易產生爭議，同樣的例證就顯現在前述健保資料庫案的訴訟契機中。

第一項　載體及載體上的資訊

在進入病歷資訊的性質討論前，傳統民法學者有認為必須先清楚區別載體以及其上所載的資訊兩者，並將兩者分開討論。如楊岳平即說明傳統民法學說上認

doi:10.6342/NTU202301113

為，當資料載體的定性為實體物時，屬於動產，一般來說就是由製作者取得所有權應無疑義，而資料載體若為電磁紀錄，雖究屬無體財產還是動產，實務上仍有些許爭議，但基本上仍然應該類推民法動產的規定。而就載體上所載的內容而言，有可能是無體財產權（著作權）、社員權（股東權）、人格權（肖像權、隱私權、姓名權等）、或僅是單純的事實而非法律上權利，究竟為何必須回到個案判斷[122]。

上述乃將法律上之物（權利客體），以及附著於其上的權利本身或事實分論，然而有些時候這個區分未必明顯。載體的所有權、資訊的使用權以及隱私權的保障，三者的權利內容、客體可能共享或重疊。傳統民法學者認為權利之成立有三要素，亦即權利主體、客體、以及標的（內容）。權利客體乃是權利標的成立上不可或缺的對象，例如物權的標的是直接對物的支配，故其客體為一定之物；而人格權之標的，係直接支配權利人本人之人格的利益，故其客體為權利主體之本人[123]。

當在討論病歷上的個人醫療紀錄時，如果觀察的角度是以財產權的角度出發，那麼會有兩種可能，第一是從病歷本身的那張紙作為有體物、權利客體的角度，用民法物權的觀點為其權利歸屬定性；第二則是著重病歷上所載的資訊，由於法律上之物，只要非人之身體，凡能為人類排他的支配之對象，且獨立能使人類滿足其社會生活之需要者，不論其係有體物還是無體物，皆屬之[124]。故姑且可以將抽象的乘載資訊也當作是法律上之「物」。雖然有見解認為若物不限於有體物，將使得權利（尤其債權）之上再有所有權，繼而徒增物權與債權觀念之混亂[125]，

---

122 楊岳平（2021），〈重省我國法下資料的基本法律議題—以資料的法律定性為中心〉，《歐亞研究》，第十七期，頁 35。作者認為電磁紀錄與傳統動產雖有異，特別是電磁紀錄的易複製性導致電磁紀錄的財產法有特別設計 的需求，故最好將電磁紀錄定性為無體財產，然而考量到目前我國針對電磁紀錄尚無如其他無體財產(例如專利、商標、著作權)設有專法，因此建議電磁紀錄原則上還是類推適用我國民法關於動產的規定。

123 洪遜欣（1976），《中國民法總則》，頁 201，自刊。

124 洪遜欣，前揭註 123，頁 202-203。蓋法律上之物與物理上之物不同，重視物之「客體性」，從現代社會經濟生活觀察，像是光、電、熱等，只要人類可以予以支配的自然力，縱然沒有一定型體，亦跟有體物同。

125 洪遜欣，前揭註 123，頁 204。其所援引的依據乃日本民法修正案理由書。

doi:10.6342/NTU202301113

不過若採取法律上之物包含有體物及無體物之觀點，就會形成上述病歷實體本身、所載資訊是兩個物（權利客體）的結論。相對的，如果觀察的角度是由隱私權角度出發，權利客體就是抽象存在病歷上的、與個人人格形塑相關的個人資訊，範圍可能更窄，雖然隱私權也關注這項「物」本身的歸屬，但著重的點在於是否以符合個資法告知後同意等合法方式利用。

第二項　可能形成的爭議

此處可能形成的爭議在於：第一、病歷本身未必具有實體、病歷本身可能只是以電磁紀錄的形式存在於硬碟或網路雲端上而已，此時還會有兩個物的權利客體嗎（電磁紀錄、電磁紀錄上所載的資訊）？還是說此時只有一權利客體（也就是「資訊」本身）？再者，此時若同時從權利觀點觀察，也就是從財產權以及隱私權在病歷資訊利用上的情形觀察，便會發現兩者所關注的焦點緊密的疊合了，權利客體上不再容易區辨載體跟載體所載的資訊兩者，且就權利本身而言，財產權所關注的「歸誰所屬、如何使用、利用、收益、交換」也會跟隱私權所關注的「告知說明後同意、目的內利用、個人自主控制」高程度的重疊[126]。

不僅如此，姑且不論此時的電子病歷是兩個權利客體（電磁紀錄與抽象資訊）還是一個權利客體（抽象資訊），此時該權利客體在財產權、所有權歸屬的討論中，一定程度必然會大幅影響隱私權保障的實踐。舉例來說，如果認為電磁紀錄基於著作權規範於民法上由醫院所有，然隱私權人卻主張電磁紀錄上所載資訊應

[126] 關於人格權與財產權的密切關係可參考黃立（1995），《民法債編總論》，元照，台北：二版，頁 258。其將人格權分成精神人格權與財產人格權，認為兩者有時可能可以併存而不相涉，例如歌星死亡後的肖像權可能喪失可能精神人格權但還具備財產人格權。不過也有可能有併存但利益相互衝突的情形，像是攝影師拍攝個人的照片時，前者就構圖、光線、快門、光圈等設定有勞力、智慧付出而享有著作權，然而在攝影師未獲個人同意，而就其作品販賣盈利時，個人的精神人格權或許沒有受到侵害，但財產人格權卻可能受到侵害。

doi:10.6342/NTU202301113

完全由其所控制使用方式、範圍、內容、是否公開等，此時究應如何調和雙方的權利衝突就會產生爭議。

楊岳平就以資料可攜權為例指出，當我們在病歷資訊談及資料可攜權時，依我國現行個人資料保護法，個人資料主體尚無此權利，亦即無權請求持有其個人資料的控管者將該資料提供予資料主體以外的第三人，因此製作該病歷的醫院依民法就該紀錄就享有所有權，而有權能決定是否將該紀錄提供予第三人。縱使該病患對該紀錄享有個人資料保護法的保護，但因個人資料保護法並未設有資料可攜權的規範，並未賦予該病患請求醫院提供該紀錄予第三人的權利，故醫院基於財產權上的權利就有權拒絕提供。由此即可見，隱私權所能帶來的保障，有時候礙於法律的發展，未必能如同財產權般全面，在隱私權上的規範不足時，此時判斷就會落入財產權的判斷[127]。簡言之，載體的歸屬不是一件不重要的事，更多時候載體的歸屬反而會影響個資權利的實現。在討論上還是宜暫時先將載體跟資訊兩者的性質極其歸屬分開討論會比較清晰。

第三項　國內外文獻介紹

國內文獻上，大多聚焦於資料載體本身的法律定性。如學者蔡甫昌等人[128]即廣列國內學者意見指出，我國學界大致上認為病歷是屬於醫師或醫療機構所有。學者陳聰富即認為[129]，病人不得訴請醫院或醫師交付病歷原本，而僅得對上載之資訊享有影印及閱覽的權利。學者林志六則認為[130]應該區分該資料是否須經醫療人員憑藉專業知識判斷製作，倘否定，如影像紀錄或檢查結果本身，病人得享有

127 本文的觀點是隱私權的內涵不足時，我們是否可以藉由談論該資訊作為財產權的權利客體的角度，透過賦予財產權的方式給予相當於、甚至是更高過於隱私權所能給予的保障？本文見解將於後詳述。

128 蔡甫昌、莊宇真、陳俞璇、葉曉宜（2020），〈病歷與健康資料研究應用之倫理與法律〉，《台灣醫學》，24 卷 5 期，頁 475。

129 陳聰富（2014），《醫療責任的形成與展開》，初版，台北市：台大出版中心，頁 156-158。

130 林志六（2003），〈病歷之所有權、閱覽權與謄寫請求權〉，《醫望雜誌》，21 期，頁 93-95。

doi:10.6342/NTU202301113

全部的使用權限。學者何建志則是進一步指出[131]雖然一般人直覺認為病歷本身為病人所有，但在醫療法欠缺相關規範前，依民法及著作權法規定，病歷應該是屬於醫事人員或醫療機構所有。

另外，關於國外文獻的部分則比較著重於資料本身而非載體的部分，如 Koskinen 等認為[132]基於洛克的思想，應將可識別病歷資訊視為個人人格的一部分，不應由他人主宰，然為了避免將人視為財產而成為客體，應該不要使用 Ownership 或是 Property 等聚焦於經濟層面的用語，而應該採取如 Datenherrschaft（德文：指對資料的絕對或主要掌控權）等名詞，來描述對病歷資料的控制。而 Hall 和 Schulman 則認為[133]，縱然有論者主張不討論病歷資訊所有權的問題，直接聚焦在病歷資料如何保護與控制的議題，然而在電子病歷網絡的普遍廣泛影響下，關於病歷資料財產權的歸屬問題是不可迴避的。其等進一步指出關於物品的掌控或責任未必僅限於財產權法上的理解，其他法律也可能在不同法律基礎上賦予類似財產權的權利，典型範例就是從侵權行為發展出來的隱私權相關法律，賦予了病人對病歷的資訊自主控制權，然隱私權相較於財產權的狹隘之處在於，前者的保護範圍僅限於醫師與病患間的隱私保護約定、或涉及此醫病關係的隱私相關法律，而並不及於其他任何可能擁有這些資訊的第三方。再者，隱私權的面向在於限制資料的取用，而不在於藉資訊銷售獲利的面向。相對而言，財產權的理解因為財產權的保障具有對世效，因此保障範圍並不僅限於醫師與病患間，而及於所有人。另外，財產權同時也著重使用、交換、利用的面向，以及肩負社會經濟發展的目標，當個人主張財產權的方式可能阻礙社會利益時，該財產可能因公共財（public good）的概念而在一定程度被限制。

[131] 何建志（2016），《醫療法律與醫學倫理》，三版，台北市：元照，頁 191-194。
[132] Jani Simo Sakari Koskinen et al., *The concept of Datenherrschaft of patient information from a Lockean perspective*. 14(1) J INF COMMUN ETHICS SOC 70 (2016).
[133] Mark A Hall and Kevin A Schulman, *Ownership of Medical Information*, 301(12) JAMA 1282 (2009).

doi:10.6342/NTU202301113

雖然 Hall 和 Schulman 看似認為財產權的保護比隱私權詳盡，但其等在結論上卻不是採取資訊財產權化的角度去解決此一問題，蓋其等認為病歷資訊跟我們呼吸的空氣一樣，無耗盡的問題，因此原則上不符合財產有限的性質，且若要與無體財產權類比又不具備與之相當的實用性與創新性。再者，賦予個人資訊財產權將有機會導致權利的過度分散，形成反公共財困境 (anti-commons)[134]，進而形成社會經濟的不效率。因此雖然病歷資訊的財產化買賣並不若器官買賣般具備高度倫理爭議性，其等仍然不採取從財產權的角度去解決病歷資訊有效利用的問題。通篇文章雖然看似沒有舉出一個解決問題的方案，但依其脈絡似乎比較贊同藉由契約或隱私權相關法律讓病患取得一個大過於病歷實體物持有方（如：醫院）的資訊控制、取用、販賣權，讓病患自己決定是否販售該資訊並終局地保有撤回、限期、修正、監督、複製的權限。另一方面，關於醫生參與病歷製作的付出，則透過付錢買資訊之一方給予醫生適當補償。其等認為此類將控制權賦予病患的作法得以減輕原先複雜的隱私權規範或病歷財產權歸屬，使得資訊得以在社會上發揮最大效用。

第四項　小結

本文認為到底是否應該依照民法學者的見解，將資料載體跟資訊兩者分開討論其實是可以爭論的議題，從上述國內外文獻的比較就可以發現，國內文獻才將載體跟資訊兩者分論，而國外資訊反而是踩在區分載體所有權跟資訊使用權兩者的意義不大的立場。正是因為病歷電子化的傾象，資訊跟資訊的載體都漸趨於無形，載體頂多只能說是 0 與 1 的電磁紀錄，而資訊則是某種無形的知識而已。在兩者都可以被輕易複製，容易被第三人做其他用途使用時，這樣的區別確實看似意義不大。

---

[134] 典型範例如社會上泛稱的「釘子戶」藉由客觀價值低的土地財產談判獲得不合比例的補償金。同樣認為資訊財產權化會造成權利歸屬不確定的見解可參考 Mark MacCarthy, *Privacy Is Not A Property Right In Personal Information*, Forbes, Nov. 2, 2018, https://www.forbes.com/sites/washingtonbytes/2018/11/02/privacy-is-not-a-property-right-in-personal-information/?sh=36ec02c2280f.

doi:10.6342/NTU202301113

載體所有權跟資訊本身的控制權歸屬這項分類，雖然可以使得討論相關議題的時候，可以參考民法的相關規定，然而割裂所有權議題在載體部分討論，控制權議題在隱私權下討論，卻未必能讓法律關係變得更清楚，因為重點還是在於誰得轉讓？複製？抄閱？更正？盈利？是否需要他方的同意？而這些其實都是隱私權的核心，而非載體所有權的核心。

以病歷資訊為例，若依照我國民法通說將病歷載體的所有權歸屬於醫院，醫院雖然掌握那張紙或相關影像、電磁紀錄的所有權，但結論上，在病歷還是敏感性個資的前提下時，隱私權層次的管制必然會壓過所有權所賦予的權能，讓醫院就病歷資訊的利用變得綁手綁腳。

目前本文所能想到財產權或所有權能發揮作用的情形，除了前述曾提及的隱私權人請求資料移轉，但現行隱私權規範欠缺資料可攜權規範的情形。另一個情形則是病歷資訊已經受到去識別化處理達到「匿名化」，而不再屬於個資的情形，此時醫院在少了隱私權法體系所賦予的限制下，就會得以依照所有權的規定取得完整的控制權。從這個觀點下觀察的話，就會發現載體所有權的歸屬規範壓過了載體上的資訊控制權歸屬的規範。這樣的結論是否妥適？一般認為當財產權的規範適用時，代表隱私權的規範於此不適用或是此時的爭議並非隱私權所關注的焦點，因此並不會認為不妥適，然而本文認為此乃因為當前隱私權並不夠著重於人格權的財產用益面向之故。

舉例而言[135]，就一張結婚照片而言，新郎新娘為被拍攝的對象，並成為該照片之內容，是以新郎新娘分別享有一個肖像權；而攝影師作為拍攝之人，決定照片之構圖、光圈等，對於照片之內容有所創作，是以其就該照片享有著作權，此時當攝影師主張依著作權權法，就其所創作之照片享有公開發表或公開展示的權利，在未經被拍攝者同意時，將該照片公開用於營利時，被拍攝者是否可以對攝

[135] 此一例子出自謝銘洋（1999），〈論人格權之經濟利益〉，《智慧財產權基本問題研究》，頁 13，翰蘆，台北：初版。

doi:10.6342/NTU202301113

影師有所請求？此時如果認為肖像權僅具有人格利益之內涵，則只要上述攝影無不當利用，對拍攝者之名譽或人格未造成損害，此時拍攝者欲主張其受侵害而有所請求，便有困難。但這個例子顯然凸顯了當攝影師將該照片大量印製銷售圖利或做其他營利使用時，被拍攝者只要人格不受侵害就不能有任何主張的荒謬結果，此一結果顯然過度保護著作權人的利益，而忽視肖像權人作為人格權人之利益[136]。

如果套用在病歷資訊的案例上的話就是，假設今天有一醫院利用病患之個人健康資訊進行研究獲有金錢上利益，照傳統隱私權的理解就是只要符合法定例外，且沒有對外不當公開外洩的情形，基本上沒有隱私權的爭議，然而本文認為此時若要說個人不能對該個人健康資訊有更高強度的主張是不合理的。即使現行隱私權規範不納入資料可攜權規範，或是將去識別化的病歷排除了個人的掌控，然而在該資訊來源仍是個人時，本文認為仍應藉由強調個人隱私人格財產權下的權益，也就是強調用益面的權益來重新為個人賦權，雖然此一作法具體上仍會跟「資料可攜權」的內涵稍有不同，像是通用格式轉出等規範就無法單靠強調隱私的用益面向、進而透過立法將個資納入財產權體系據以賦予個人此一權利。不過強調人格權的用益面向的確可以在人格利益外為個資主體增添另一權利主張手段，某種程度也提高了個人對其資料之控制。美國法上目前有相關主張，詳於第四章第二節介紹之。

目前就載體本身的權利歸屬而言，依照我國民法、著作權法的規定，應該屬醫院方所有並無太大的疑義，學者間的主張也不大衝突。至於載體上所載的資訊，

136 我國最近類似判決可參考 110 年度民著訴字第 129 號（鏡週刊訴雞排妹案），案例事實略為雞排妹戴口罩於街上與緋聞對象行走時遭鏡週刊拍攝，雞排妹後將該週刊照片截圖至於個人社群軟體頁面，利用該截圖以自嘈方式幫贊助廠商打廣告，後被鏡週刊起訴侵害攝影著作之再製與姓名表示權。法院認為（1）新聞照片仍有原創性受著作權保障、（2）照片僅拍攝到被告之背影，並無正面之五官，自無從認為系爭照片有侵害原告之肖像權。

本案中法院雖然是認為連肖像權此一人格權都不成立，故更無庸討論其用益權，但本文認為本案的啟示在於如果將「不可辨認五官的照片」之於「肖像權」套用在本文脈絡，其實就相當於「去識別化個資」之於「隱私權」，如果週刊於拍攝及報導時都仍然可以推敲、連結到雞排人本人，何以雞排妹不能對該「模糊」照片主張肖像權？如果個人知悉某研究成果源自其去識別化個資，何以個人不能對該「去識別化個資」利用主張人格權下精神或財產上利益？

doi:10.6342/NTU202301113

Hall 和 Schulman 則指出該資訊確實有可能被認定為是財產權，其等精確地分析隱私權跟跟財產權的相類、及相異之處，在結論上不採取賦予病歷資訊本身財產權性格的做法，本文認為還有幾點值得注意：

首先，第一點，Hall 和 Schulman 的論述基調是建立於以最大效益利用病歷資訊的前提上，然而卻鮮少談到這樣的前提是建立在怎樣的隱私成本上，因此其所提出的反公共財困境，如果在個人隱私過度犧牲的情形下可能不會成立，正如同畸零地土地所有權人的財產權主張，未必可以一概說成是反公共財困境一般，賦予個人對於個資的財產權控制所造成的交易成本未必能一概指為是不效率；相反地，這樣情形的發生可能反而彰顯了一個社會對於個人自主決定財產權或是對隱私權利用的尊重，因此在討論是否賦予資訊本身財產權的時候，必須先對資料利用跟個資保護的立法目的上定位，如果不以最大資料流通為考量，即不能以「賦予資訊財產權地位會造成交易成本過鉅」為理由駁斥。

再者，第二點，在 Hall 和 Schulman 的討論中約略可見病歷資訊存在定位成人格權（隱私權）？還是定位成（財產權）？的困難，本文認為在回答資訊本身是否有財產權性質時，必須先回答的問題是何謂人格權？何謂財產權？差異為何？區分實益為何？這些問題必須先予以釐清，否則無異是淪於概念法學而欠缺實質助益。雖然此一問題乃大哉問，然而此乃回應是否應賦予資料財產權性質論述上所不可或缺的一塊，關於此一問題本文將於本章第三節詳述比較說明。

最後第三點，Hall 和 Schulman 討論了資訊隱私跟無體財產權的可類比性，在論述層次上，必須先說明資料是財產權才討論資料是哪種財產權？哪種無體財產權？因此就此討論必須列後於前一點，當然，本文認為此兩者可類比性的討論必須更細緻的去處理（學說上不無反對見解，詳第四章第三節後述）。

在當代大數據、資料分析大盛其道的趨勢下，資訊隱私的有價性或可利用性逐漸顯現，其商業性可能會不下目前受承認的無體財產權。誠如近年備受討論的

doi:10.6342/NTU202301113

新書《監控資本主義時代》所述[137]，人類行為本身也成為了一種自然資源進而受到大企業如谷歌或臉書等榨取行為剩餘，這正是資訊隱私財產權性格被凸顯的例證之一。事實上，個資早已出現交易市場，其金錢價值也並非無法衡量，舉例而言就可以從以下六種方式去衡量個資的金錢價值[138]，像是：（1）主觀定價：也就是促使資料主體放棄其個資，業者所需支付的價格，此一價格會因個人對隱私態度而異；（2）客觀定價：資料主體為了保護個資所願意支付之保費，如資料仲介業者 Experian 以每月收費 19.99 美元提供防止身分遭竊之服務[139]；（3）個資之市場淨值：如 2012 年間 Facebook 每一用戶之價值介於 90 至 120 美元[140]；（4）個資之淨利，如 Facebook 及 Experian 等資訊公司可從每一用戶或檔案每年獲取的淨利；（5）個資買賣價格：如地址、生日、駕照號碼等駭客於網路上交易可取得的用戶個資；及（6）個資外洩之經濟成本，如 2011 年 PlayStation 有 7700 萬用戶檔案外洩，Sony 公司花 245 億美元成本處理[141]。顯見個資的有價性、可交易屬性早已顯現。

雖然有些學者的確認為隱私以不公開為目的，而無體財產權中除營業祕密外皆以公開為目的，因此拿無體財產權去類比資訊隱私權的財產權性格有些不妥[142]，然而正如同本文在前述章節挑戰去識別化具體上所尚存的效用以及是否應該繼續在去識別化的保護脈絡下去談論隱私權的質疑一樣，本文無疑是站在新資訊時代部分隱私期待早已不復的角度去思考，站在這個觀點上，將資訊本身財產權化是否才是一個更務實的觀點？我們是否更應該關注資訊本身的財產權化是否得

[137] 肖莎娜．祖博夫（著），溫澤元、林怡婷、陳思穎（譯）（2020）。《監控資本主義時代（上卷）：基礎與演進》，初版。台北市：時報文化，頁 158。
[138] Org. for Econ. Co-Operation & Dev. [OECD], *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, 220 OECD 4, 4-5 (2013).
[139] EXPERIAN OFFICIAL WEBSITE, https://www.experian.com/consumer-products/identity-theft-and-credit-protection.html (last visited June 15, 2022).
[140] Christine Bauer et al., On the Value of Information: What Facebook Users are Willing to Pay, (European Conference on Information Systems, Proceedings of the 20th European Conference on Information Systems, 2012), https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1196&context=ecis2012.
[141] 自由時報，(04/04/2022)，〈Sony 公司恐 7700 萬名用戶個資外洩〉，https://news.ltn.com.tw/news/life/breakingnews/490213。
[142] Pamela Samuelson, *Privacy As Intellectual Property?*, 52 STAN. L. REV. 1125, 1148, (2000).

doi:10.6342/NTU202301113

以使得個人重新取回資訊隱私的控制權？縱使是採取一個怎樣賣的有價，怎樣有效利用的非傳統保護隱私權的觀點，這是否從結果論來看是更好的「賦權」手段？正如同《敞開與遮蔽:新媒介時代的隱私問題研究》的作者向淑君所述[143]：「隱私權從消極維護的人格權，轉化為以人格權為主兼具財產權的特點的複合權利，這已經是網絡時代的必然。」是時候該重新思考 Anita Allen 四種分類下的隱私財產權面向。

第二節　　從基因資訊爭議思考資訊財產權

另一個關於個人資料究竟為財產權、還是人格權的性質爭議是針對基因資訊法律地位的討論，以下簡單介紹之，在文獻的討論脈絡上，與前述病歷資訊相同，本文姑且仍先區辨載體以及其上所載的資訊分開討論。

第一項　Moore vs. Regents of the University of California 案

基因法律地位的討論於 Moore vs. Regents of the University of California 案最興盛[144]，此乃美國加州最高法院於 1990 年所做的判決，事實大略是醫生基於治療目的摘除病患之組織，然而後續卻藉由切除之組織進行研究獲利。原告因故提訴強佔(Conversion)。法院於判決中認為醫生應該在建議病人進行某項切除手術前，就告知病人相關於切除該組織的一切利益，即使醫生對該組織的利用與該病人的健康無關。然而關於強佔部分，由於法院認為病人對於切除的組織或細胞並未擁有法律所保障的財產利益(legally protected property interests)，因此不能主張強佔。

[143] 向淑君（2011）。《敞開與遮蔽:新媒介時代的隱私問題研究》，初版。中國：知識產權。頁35。
[144] Moore v. Regents of the University of California, 793 P. 2d 479 (Cal. 1990).

doi:10.6342/NTU202301113

第二項　國內外文獻介紹

關於這則判決，國內學者有從「身體權」、「健康權」切入，認為「人格的自主決定在一定要件下應延長存在於與身體分離的部分，而予以適當必要的保護」[145]。也有從財產權觀點，討論細胞部分（也就是資訊的載體）是否為動產者[146]。這顯現了基因作為資訊載體，同樣具有與隱私權一樣的多面性。甚至說，正是因為基因資訊的權利標的不是基因本身，而是其上所載的「資訊」[147]，因此跟個人資料隱私權的保護非常類似，兩者都是著重附著於某有體物上的「資訊」。

至於學說上分成兩派，一派認為基因附著於物質，因此其隱含的資訊權利也取決於物質，此可稱財產理論，此也是前述 Moore 案中加州最高法院所採取的立場，其認為基因的物理成分包含了該資訊；然而另一派則認為，基因除了物質的附著外，還有全人格法益的附著，因此需看討論的面向，分別適用基因人格權、基因財產權，如果著重於精神的、人格的非物質性存在，則以前者稱呼；然而若以強調交易性、市場價格性的角度，則以後者稱呼。此一理論比較接近智慧財產權的理論[148]。

就一般常人的直觀下，大概會覺得智慧財產論相較於財產理論有道理。蓋一般人對於自己的廢棄組織，即使物理上不在屬於自己，其內涵的基因資訊常人仍會認為自己應該要有某種程度的控制權，學者顏厥安所提出的一種解釋乃：

「我們之所以會認為那些研究單位『沒有權利』或『不應該』將他們藉由我們的基因物質所發現的基因結構申請專利，與其說我們認為那是我們的基因，他們侵害了我的權利，不如說是因為我們覺得『那些基因不屬於他們』，而那些基

---

145 王澤鑑（1998），《侵權行為法第一冊，基本理論：一般侵權行為》，頁 125。
146 陳文吟（1997），〈探討美國 Moore vs. Regents of the University of California 對生化科技的影響〉，載於《智慧財產權與國際私法—曾陳明汝教授六秩誕辰祝壽論文集》，曾陳明汝教授祝壽論文集編輯委員會，頁 230 以下。
147 顏厥安（2002），〈財產、人格，還是資訊？論人類基因的法律地位〉，《台大法學論叢》，31 卷 1 期，頁 23。
148 顏厥安，前揭註 147，頁 24-26。

doi:10.6342/NTU202301113

因與我們（基因物質提供者）有密切的關係。簡單說，認為那些基因『並非研究者之權利』（否定面）的意義，要強過於認為基因『是我自己的權利』（肯定面）[149]。」

然而學者顏厥安也不完全贊同採取智慧財產權理論，蓋採取智慧財產權理論必須面對的挑戰在於「為何基因上附著了人的全人格？」，基因附著了全人格的主張無疑是一種過強的化約，這樣的主張等同是認為基因不只決定了一個人的生理組成、特色與健康，更決定了社會關係、行為、成就、情感、偏好等高度人格屬性的特質[150]。這也就造成了如果我們真要說基因資訊是智慧財產權，就必須認同「基因之上附著有我們的人格」的道德形上學強烈主張。

除了上述討論之外，國外學者方面 Jeffery Lawrence Weeden 不同於顏厥安，其主張基因資訊內容具有永續性，且是最私密個資，應在財產權或類財產權（quasi property, quasi in rem property）的概念下以擴張無體財產權的概念加以保護，而非僅以隱私保護體系保護[151]。

其立論基礎部分源自於當前美國憲法上對隱私權欠缺明文規範。現行美國隱私權討論實源自 Warren 跟 Brandies 提到的不被打擾的權利“the right to be let alone”[152]，後續的隱私權學者多半認為隱私權的憲法基礎乃源自於美國憲法第一、三、四、五、九條修正案共同投射的半影（penumbras）。Weeden 認為現行隱私權的無數保護原則乃處於危險之中，因為他們是被錨定在新建立、定義不清和不斷動搖的原則上，而非像財產權是立基於久經考驗的原則上。擴張隱私權的保護範圍或是將隱私權明文列入美國憲法保障雖然可以是一種保護基因資訊的方式，但它仍然缺少了個人行使財產權的面向，也就是禁止他人利用其資訊獲取

149 顏厥安，前揭註 147，頁 33-34。這樣的說法其實跟本文在前述第二章第三節第三項所提到的去識別化的裸照案例相同，同樣是「覺得不屬於他們所有」大過於「屬於自己所有」，也就是覺得該資料的連結性應該跟自己較高，而應享有更多控制權。

150 顏厥安，前揭註 147，頁 28。

151 Jeffery Lawrence Weeden, *Genetic Liberty, Genetic Property: Protecting Genetic Information*, 4 AVE MARIA L. REV. 613, 616 (2006).

152 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*,4 HARV. L. REV. 193, 195 (1890).

doi:10.6342/NTU202301113

商業利益或以其他方式傷害個人[153]，這樣的說法無獨有偶的跟 Hall 和 Schulman 在前述病歷資訊究屬財產權抑或人格權的比較雷同。

Weeden 認為基因財產權不是源自於個人自主權的發散（emanations）或半影(penumbras)，而是源自於「它」是屬於「我們的」的直觀想像[154]。其認為隱私雖有必要存在，然而其並不夠全面，無法完整保障基因資訊。其用了一個比喻去形容隱私權保障體系的不足，也就是傳統上我們會認為房屋內部是個人的隱私，但如果有天現代科技讓不透明的房屋變成透明的房屋，在隱私權架構下透明的房屋內的人將會喪失合理隱私期待，因而不受隱私權保護，然而若以財產權角度思考，所有財產權利仍會存在，也就是說財產權利才能給予人更完整的控制[155]。

但也有持反對基因財產權者如 Suter 認為雖然財產權通常會跟高度控制連結、且隱私權的發展在美國法制史上部分與財產權重合，然而 Suter 認為基因隱私的授權利用不僅是個人與個人之間的關係，多數時候會涉及家庭成員、醫生、研究者、雇主以及保險人，且分享隱私資訊會造成個人的脆弱與依賴，而此時信任關係（Trust）以及信任授權（Entrustment）才是揭露這些資訊的核心基礎[156]，財產權理論將會使我們將隱私誤認為是一種財產，僅以市場價值及財產上損失衡量損害，窄化其他隱私涉及人格尊嚴的面向的關係破壞損失及對個人的信任破壞傷害，Suter 認為在隱私權保障體系上，以傷害人格尊嚴、違反信賴關係的精神性、非

153 Weeden, *supra* note 151,at 659.

154 類似見解可參考 Catherine M. Valerio Barrad, *Genetic Information and Property Theory*, 87 NW. U.L. REV. 1037, 1062-63 (1993). Barrad 提到自然權利理論足以正當化個人對其基因序列所應有的財產權，因為該資訊是個人自我認同、自我實現所必要，且若任何法律意圖剝奪個人對該資訊的控制所有權，也會是違反自然法的。

155 *Id.*, at 660. 其他贊同基因資訊應該擁有財產權者還有 Ad Hoc Committee on DNA Technology, American Society of Human Genetics, *DNA Banking and DNA Analysis: Points to Consider,* 42 AM. J. HUM. GENETICS 781, 782 (1988)其認為除非另有規定，否則儲存的 DNA 屬於存入者所有; Allen, *supra* note 2, at 49-51.同樣認為基因隱私跟財產有所重疊；George J. Annas, *Genetic Privacy: There Ought to Be a Law*, 4 TEX. REV. L. & POL. 9, 13 (1999); Thomas E. Colonna, *Protection of Privacy in Personal Genetic Information*, 2 W.VA. J.L. & TECH. 2, 47 (1998); Michael M.J. Lin, *Conferring a Federal Property Right in Genetic Material: Stepping into the Future with the Genetic Privacy Act*, 22 AM. J.L. & MED. 109 (1996).

156 Sonia M. Suter, *Disentangling Privacy from Property: toward a Deeper Understanding of Genetic Privacy*, 72 GEO.WASH. L. REV. 737, 748-50 (2004).

doi:10.6342/NTU202301113

財產性的損害賠償，會好過於使用財產權體系所建構的市場規則，而僅以市場價值衡量資訊洩漏的損失[157]。以前述 Moore v. Regents 的案例來說，Suter 認為個人可以行使歸入權，將研究者應用原告基因、組織而獲得的經濟收益歸入於本人，但應注意者係，權利主張依據應該是基於信賴關係違反，而非基於個人對於資訊本身具有財產價值[158]。

第三項　小結

本文認為上述基因資訊的爭議，以及學者顏厥安對此基因法律定性的批評，不但與前一小節的病歷資訊所有權、控制權爭議類似，且完全可以作為本文所欲討論的個人資訊人格權、財產權雙面性爭議的參考。

其中有幾點值得注意，首先顏厥安提到其並不贊同以智慧財產權理論處理基因資訊的定性，原因是該理論有基因化約論的影子，蓋若說基因上有全人格的附著，等於是在說基因就決定了一個人的人格發展，這樣的主張無疑比較接近一種神學上信仰的主張。本文認為此處的推論稍嫌過速，原因在於使用智慧財產權理論未必需要有「全人格附著」，著作有著作人格權並不代表著作就決定、完全代表了個人，著作僅是個人部分生活經驗的體現而已，不需過分強調著作的人格屬性。

再者，關於 Weeden 的主張，其主張採用財產權體系來保障基因資訊的理由一部分乃基於財產權體系在美國發展較為完善，就此本文認為於我國隱私權受到大法官以憲法 22 條概括基本權、及多號憲法解釋發展不同於美國的發展脈絡而論，未必能有跟美國法一樣的理由去支持資訊的財產權主張，不過就 Weeden 所

157 *Id.,* at 811-813.

158 關於信賴關係違反所必須賠償的非財產、精神上損失，相較於財產上損失，通常並沒有一定的衡量、量化標準。參考 Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*,39 N.Y.U. L. REV. 962, 973 (1971). 有認為這樣的精神上損失計算上未必要奠基於經濟上損失，或以洩露的資訊市場價值為損害認定基礎，而應該以該資訊對個人的重要性意義為主要考量。參考 Randall R. Bovbjerg et al., *Valuing Life and Limb in Tort: Scheduling "Pain and Suffering"*, 83 NW. U. L. REV. 908, 912 (1989).

doi:10.6342/NTU202301113

提到個人對基因資訊主觀上「那屬於我的」的素樸想像，以及其主張財產權還包含利用、防止不當利用的面向比隱私權體系來得完整等主張，依然是很有說服力。

至於 Suter 所主張的大約可以簡單化約為財產權概念會過度簡化個資作為人格權的複雜、與尊嚴。本文認為財產跟人格並非相斥的概念，況且承認現行人格權有用益面向其實充其量也只是把早已暗潮洶湧的個資交易市場明文化受法律規範而已，如果說基於此一理由拒斥承認個資市場或是個資財產權用益性格的展現，還是有些掩耳盜鈴。

最後一點，從病歷跟基因資訊的案例中，可見無論是病歷資訊或是基因資訊，皆是屬於個人資料的一種[159]，與個人緊密相關、且屬於必須存在於某個實體載體上的抽象資訊，其於理論發展上也出現同樣的人格權、財產權定位分歧，因此若要討論資料的性質歸屬，必定須先處理人格權及財產權各自定義為何？區分實益為何？此部分將於後下一節展開。

第三節　隱私於人格權、財產權間的重新爬梳

前述曾提及 Anita Allen 將隱私權依其內容分為以下四種：(1)資訊隱私權(Informational privacy)：關切個人資訊之取得問題、(2)身體隱私權(Physical privacy)：關切接觸個人身體或生活空間之問題、(3)自主決定隱私權(Decisional privacy)：關切政府或其他第三者干預個人自主決定或選擇的問題、(4)具財產價值之隱私權(Proprietary privacy)：關切個人人格利益的取得與擁有（所有權）[160]。從其敘述可以發現這四個領域剛好可以對應到：資訊、身體、自主、財產。前三者一般而言可以被人格法益所涵括，尤其是個人資訊的保密與自主，然而隱私財產權在我國法中卻是一個異類觀念[161]。蓋雖然非財產權之侵害（絆倒別人所造成

[159] 個人資料保護法第 2 條一款參照。
[160] Allen, *supra* note 2.
[161] 顏厥安，前揭註 147，頁 19。

doi:10.6342/NTU202301113

健康權之侵害），也有可能發生財產上損害（請求醫療費、勞動減損之工作報酬等支出），因而可以請求財產上損害賠償，但是這並不會因而讓「健康權」成為一種我國法意義下的「財產權」。那到底「隱私權」是一種「人格權」還是「財產權」呢，又抑或是兩者皆包含？這個問題必須先釐清什麼是「人格權」？什麼又是「財產權」？才可以回答。

以下第一項討論人格權之內涵，第二項討論財產權之內涵，最後於第三項再重新為隱私權定位。

第一項　人格權的多面性

學者顏厥安認為財產權及人格權差別在美國法的討論脈絡下沒有很大的差異，蓋美國侵權行為法以保障「利益」為核心，不需要有嚴格的財產權與非財產權區別，即使是大陸法系下，非財產損害中最常提及的「生理或心理的痛苦」，在美國法上仍屬財產權的利益[162]。不過顏厥安此一論述可能忽略了民事上侵權責任分成損害成立及損害範圍的兩層次，美國上的不區分非財產損害及財產損害應該是指在損害範圍的層次，損害成立上美國法其實有針對財產權跟人格權做出明確區分的。誠如論者王瑋所提及[163]，美國多數州對於人格特徵的商業利用上的財產權益其實另設有名為「公開權」（Right of Publicity）的財產權加以保護，茲以跟保護精神上人格法益、具一身專屬性的傳統隱私權區別，公開權具有可讓與及可繼承性質，就此部分就跟德國法上的人格權一元論相當不同。德國法是在人格權下討論其財產法益，也就是將人格權的保護法益自精神上的人格法益擴張到財產法益，並對後者打破一身專屬性限制，雖然相當程度認為人格權可讓與、繼承，但還是是在人格權的角度下論述。

[162] 顏厥安，前揭註 147，頁 19。
[163] 王瑋（2020），《人格特徵商業利用之研究》，頁 3，國立台灣大學法律學研究所碩士論文。

doi:10.6342/NTU202301113

以著作權為例，德國於著作權法上的主流學說採取限制讓與的一元論立場，認為人格權所保護的精神利益與財產利益乃緊密相連原則上無法分離，德國著作權法 29 條之一即規定著作權不得讓與，而同法 31 條則規定著作權得授予他人用益權。此一限制性讓與理論是經由約定內容讓與母權利的部分權利，被授權人行使權利時，必須顧及授權人之利益，如果被授權人的商業利用有損授權人之名譽，授權人可本於保有之權利禁止被授權人為該使用[164]。

德國內雖然有少數採取二元論者，如 Beuthien 及 Schmölz，然而並未被主流見解接納。其等認為人格是指內在的精神生活，包括生命、身體完整性、身體活動自由及人格自由發展，與人格相關的客體（如姓名、肖像、言語及個人資訊）並不相同，蓋後者外在於個人而非人格之一部，因而得成為支配權的客體。以個人資訊為例，個人除享有排他權能外，亦享有用益權能，此一對個資的支配權，相當於無體財產權，得讓與，其侵害也可以透過不當得利救濟。

我國對於著作權的理論實際上較接近德國的少數說，蓋我國就此所採取的乃二元論的立場，將著作權區分為著作人格權、以及著作財產權，也就是說在同一標的上存在有人格權與財產權兩種法益，而財產權得以完全移轉於他人。不過也有認為這並不表示我國人格權的理解亦應採取二元論，原因在於著作的利用必須透過著作的「物」本身，但是對於其他人格特徵的利用多數是直接涉及個人人格本身，也就是人格特徵的財產價值得直接連結至個人之人格，包括外界評價、聲譽、形象等[165]。

一元論者認為人格權如同樹的莖幹，精神利益跟財產利益分別為樹根[166]，自主決定是人格權內涵，也是人格權可以涵蓋人格特徵商業利用上財產法益的根據，蓋當個人對其人格特徵如姓名、肖像享有一定控制權限時，才能維護其人格自由

164 黃松茂（2008），《人格權之財產性質以人格特徵之商業利用為中心》，頁 216-218，國立台灣大學法律學研究所碩士論文。
165 黃松茂，前揭註 164，頁 149。
166 王澤鑑（2012），《人格權法》，頁 356，臺北：自刊。

doi:10.6342/NTU202301113

[167]。其等也援釋字 603 號解釋強調隱私權作為人格權的雙面性，擁有「不受他人侵犯」的消極自由，以及「自主控制」的積極自由[168]。

釋字 603 號解釋節錄如下：「隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障 (本院釋字第五八五號解釋參照) 。其中就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。」

人格權不但存在「防禦權」的面向，同時在科技經濟發展下，「利用權」的面向也逐漸被凸顯。更有論者認為人格權上財產法益的內涵應該依個別具體人格權涉及「人格權核心」的程度，而做出不同認定，舉例來說，在生命權、身體健康權等涉及人身完整性的權益，應該就沒有容許財產法益存在的餘地，但若是與社會經濟社會活動有關，非涉及人身完整性的權益，如姓名權、肖像權、名譽權、隱私權、著作人格權、個人資料保護權等就有較大的財產法益肯認空間[169]。

二元論者多認為，我國人格權規範，仍不足以保障人格特徵的商業利用，因此應該另創一獨立財產權，據以突破傳統人格權的一身專屬性限制，在可讓與性、可繼承性等議題上更進一步被承認[170]。

[167] 黃松茂，前揭註 164，頁 146-149。
[168] 王瑋，前揭註 163，頁 66。
[169] 謝銘洋，前揭註 135，頁 58。本處雖然提及隱私權應有較大的財產法益容認空間，但是於內文上僅介紹姓名權及肖像權的財產法益，對於隱私權財產法益的部分欠約更多著墨。
[170] 謝銘洋，前揭註 135，頁 46。

doi:10.6342/NTU202301113

中國方面的文獻對此有一些著墨，像是有學者就持較接近二元論的立場認為，人格標識商品化權是與具體人格權、一般人格權相並列的一種權利，並非僅屬人格權下的財產利益[171]。相似見解有認為[172]：

「『人格商品化權』是獨立於既有人格權的一項民事權利。首先，某項法益是否成為權利，並非天然正當或不正當，而是法政策的必要性和法技術的可能性的結合，『商品化權』原本並不存在，現今卻為各國法律及國際公約所普遍確認，正是由於原有權利（人格權或知識產權）體系不能為此項利益提供充分保護，而其構造（主體、客體及內容）又是清晰的，『人格商品化權』也是如此。其次，正如有學者所指出的那樣，基於同一人格要素，可以同時存在不同的權利並實現不同的功能。肖像、姓名等人格要素之上可以在存在肖像權、姓名權等具體人格權的同時，存在商品化權。具體人格權的功能重在維護人格獨立及人的自由發展的精神利益，同時也保障人格利益中的財產性利益。而商品化權是允許他人使用、開發自己的人格利益並獲得報酬的權利，其主要功能是保障、促進人格利益的商業化利用，既促進市場經濟發展，又使民事主體在其中獲益。」

由上可見此一學者無疑是採取比較實證主義的觀點，認為權利乃是法律所形成的，當既有體系規範不足時，就應承認新的權利。不過中國的文獻上也有持接近一元論立場者認為「人格商品化權」僅是一種特殊的人格權而已，不能因有此一經濟利益就將該權利劃入財產權體系[173]。

關於二元論下的公開權，雖然著重商業利用的保護，然而還是以具有「人格要素」者為限，因此不無學者認為二元論跟一元論之間其實是有整合餘地的，甚

[171] 楊立新，林旭霞（2006）·〈論人格標識商品化權及其民法保護〉，《福建師範大學學報（哲學社會科學版）》，136 期，頁 74。
[172] 溫世揚（2013），〈析「人格權商品化」與「人格商品化權」〉，《法學論壇》，149 期，頁 109。
[173] 馬俊駒（2016），〈人格與人格權立法模式探討〉，《重慶大學學報(社會科學版)》，22 卷 1 期，頁 187。

doi:10.6342/NTU202301113

至說兩者保護模式其實是殊途同歸的[174]。不論是一元論者還是二元論者，就人格商業特徵利用的保護，可謂皆以取得防禦面人格法益，與用益面財產法益之間的平衡為宗旨，兩者實質上對法益保護範圍其實沒有太大的不同，二元論也不因為賦予人格特徵在特定情形下財產權能，而犧牲了人格尊嚴與自主。毋寧說兩說的目的都在於想在不侵害人格尊嚴的同時，透過賦予一定程度的財產權益來貫徹個人自主，因此與其拘泥於一元論在人格權下談人格權限制轉讓的鬆綁，或是二元論中另外成立有限制的財產權來解除形式上的鬆綁，不如直接了當的去回應具體上的問題，像是可否轉讓、可否繼承、可否市場交易等實質爭議點。

具體上這些問題其實更需要被細分探討，像是關於可否轉讓、繼承的爭點，根據主體是法人或自然人的不同，就可能需要不同的規範，蓋法人人格法益屬性的色彩較為淡薄，財產利益色彩則較為顯著，法人沒有感到精神痛苦的可能，只有在組織設立目的下行社會經濟活動的可能。因此規範上對於賦予其人格特徵財產權能的界線可能就會較寬，但非財產上的損失就相對的不應受到肯認。另外，不同的人格權也可能需要不同的財產化界線，像是前述提及的生命、身體完整性部分，由於涉及高度人格屬性，關於可交易性、可轉讓、繼承的屬性就難以被承認；相對的，如果是姓名、肖像、甚至是本文重點討論的個人資料部分，其人格屬性就沒有生命、身體那麼高，因此也多了一些討論可否交易、轉讓、繼承的空間。

第二項　財產概念的多面性

財產權（Property）到底為何？是事實上的物？還是權利？法律實證主義認為只要法律規定，它就可以是財產權[175]，如同邊沁認為：「財產跟法律共存亡，在法律制定前沒有財產，拿掉法律，財產消逝[176]。」撇除此一看法之外，Blackstone

[174] 王瑋，前揭註 163，頁 67, 92。
[175] JOHN G. SPRANKLING ET AL., GLOBAL. ISSUES IN PROPERTY LAW 3 (2006).
[176] Jeremy Bentham, *The Theory of Legislation* 69 (Oceana Publ'ns, Inc. 1975) (1690), Quoted in SPRANKLING, *supra* note 175, at 2.

doi:10.6342/NTU202301113

的定義是“Sole and despotic dominion…over the external things of the world.[177]”一般學者如 Schwarz 給出了一般性的定義，其認為所謂財產權（property right）指的是物體上存在任何無形、有形的經濟利益，且具有對世效、可透過公權力執行保護[178]。亦有類似論點如 Purtova 更廣泛的認為財產權的核心從未改變，也就是必須具備經濟價值、稀缺性、以及可被人類掌控的特性[179]。從客體的角度觀察，財產權的內涵實際上是隨著時間在演變的，早期僅包含有體物，然而到無體物也被涵蓋，像是股份、智慧財產、甚至是近年來歐盟討論的機器產生的資料所有權（data ownership）皆然[180]。

誠如 Radin 所言，任何客體是否於其上存在財產權概念，姑且不論這個財產權是正在被創造還是正在消逝中，在討論的過程中，客體本身所處的法律環境脈絡並不能被忽略，像是不同社會下的契約秩序、競爭及言論自由等都會有所影響。財產權化是社會中一個動態的過程，其**內涵是關於一項有體物或無體物是否及被何財產權主體控制、以及該主體又在多大程度上享有該控制**（從與其他社會成員的互動上評量該控制的程度）[181]。簡言之，其認為資訊的財產權化也同樣是社會性的過程，資料主體、蒐集人等會共同決定「財產權」的權利內涵[182]。

在認定屬於財產權後，財產權所表徵的效力也同樣重要，從效力的角度而言，財產權的內涵無疑是具有高度不確定性的[183]，財產權有可能僅意味一個暫時、可

177 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAW OF ENGLAND (facsimile ed. 1979) (1766).
178 Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056, 2058 (2004). "this article defines property as any interest in an object, whether tangible or intangible, that is enforceable against the world."
179 Nadezda Purtova, *Property in Personal Data: A European Perspective on the Instrumentalist Theory of Propertisation*, 2 EUROPEAN JOURNAL OF LEGAL STUDY 3 (2010).
180 P. Bernt Hugenholtz, *Data Property in the System of Intellectual Property Law: Welcome Guest or Misfit?* In TRADING DATA IN THE DIGITAL ECONOMY: LEGAL CONCEPTS AND TOOLS: MÜNSTER COLLOQUIA ON EU LAW AND THE DIGITAL ECONOMY III, 75 (Stefan Lohsse et al. eds. 2017).
181 Margaret Jane Radin, *A Comment on Information Propertization and Its Legal Milieu*, 54 CLEV. ST. L. REV. 23, 23-24 (2006). 其對物是否有財產權提出了五個特徵，(1)財產由社會定義、(2)（去）財產權化是動態過程、(3)成為財產權是一個過程、(4)一個物在成為財產的過程中是連續性的擁有更多財產權利或擁有更少的財產權利、(5)財產跟非財產的定義間可能存有爭議。
182 *Id.,* at 25-26.
183 LAURA S. UNDERKUFFLER, THE IDEA OF PROPERTY: ITS MEANING AND POWER 4 (2003).

doi:10.6342/NTU202301113

撤銷、隨時可變動的、由公權力賦予的授權[184]，也可能是強大的、近乎完全的對物、土地、思想、資訊的掌控[185]，不過無論如何核心的概念仍是「控制」與「排除」，差別只是在期間長短跟程度高低而已[186]。

至於怎樣的控制與排除才稱得上是「財產權」？其實充滿爭議。有提出觀察發現雖然所謂的「私有」財產權原則上必須具備競爭性，也就是一人的使用會排除他人的同時使用，然而在財產權中完全具備競爭性或完全不具備者都屬少數[187]，也有認為「排除他人使用」是財產權重要、但非充分的要件，排除是使用、用益、拋棄等權利相對應必然具備的財產權能[188]。

具體從「可轉讓性」而言，從前述談及著作財產權的限制讓與性即可見，財產權未必要具備完全的「可轉讓性」，著作權人於有重大事由時，仍得以隨時終止契約，讓分離的子權利消滅。基因資訊亦然，美國法上認為其是不可轉讓但仍具有經濟利益的，於此部分，承認有限制轉讓的財產權反而可以緩解部分看法對於財產權有損人格的擔憂。

綜上所述，財產權的內涵相較於人格權來說較不容易輕易的劃定範圍，不過基本上仍不脫「不拘形式的經濟利益（價值）」、「可控制持有佔有、限定使用方式（控制）」、「具有對世性受到公權力保障（排除）」。

---

[184] Kevin Gray & Susan Francis Gray, *The Idea of Property in Land, in* LAND LAW: THEMES AND PERSPECTIVES 41-43 (Susan Bright & John Dewar, eds. 1998).

[185] Mark A. Lamley, *The Modern Lanham Act and the Death of Common Sense*, 108 YALE L. J. 1687, 1697 (1999); Mark A. Lamley, *Romantic Authorship and the Rhetoric of Property*, 75 TEX. L. REV. 873, 895-904 (1997).

[186] Harold Demsetz, *Toward a Theory of Property Right*, 57 AM. ECON. REV. 347, 354 (1967). 其指出所有權意味著社群承認所有權人擁有排除他人行使所有權人得行使的權利；LAWRENCE C. BECKER, PROPERTY RIGHT: PHILOSOPHIC FOUNDATIONS 18-23 (1970). 其指出所有權的內涵為使用、移轉、與排除他人用益。

[187] David D, Haddock & Lynne Kiesling, *The Black Death and Property Rights*, 31 J. LEGAL STUD. 545, 558-61 (2002).

[188] Adam Mossoff, *What is Property? Putting the Pieces Back Together*, 45 ARIZ. L. REV. 372, 377-92 (2003).

doi:10.6342/NTU202301113

第三項　隱私權的權利定位

首先，針對究竟應該對人格權的經濟利益，採取在人格權底下論述的一元論，還是採取二元論的立場，另外肯認如公開權般的財產權加以保護的爭議，本文認同前述王瑋的見解，關於此一爭議不該流於概念法學的過份區分，應該具體區分不同人格權、不同人格權主體，在不同人格權利用、控制的面向上去做討論，會比在抽象的人格權大概念下討論一元論、二元論來得實際，也不會因此淪入法學概念的過多無意義區分。

因此我國若要針對隱私權作為人格權逐漸被去識別化再經公益、商業化利用的趨勢做出回應，重點不在於以二元論還是一元論去規範資料隱私的財產權性質，而是應該著重在「隱私權跟其他人格權的差異之處為何？」、「權利主體為何？」、「可利用對象、範圍、方式為何？」、「可轉讓（授權）對象、範圍、方式為何？」以及「可繼承對象、範圍、方式為何？」等具體問題的回答上。

而在我國法脈絡下，隱私權基本上是被認為係人格權，因此為了免除麻煩，似不需要硬將隱私權下的財產利益另外認為是財產權的一類，隱私權雖然在資訊時代下面臨商品化的困境，但在本質上此類經濟利益仍是人格權在商品經濟中的延伸，其內涵在於人格權人運用自己的人格特徵，使其人格權內容擴張。法律賦予權利人此項權利，就是保障權利人的人格特徵在延伸到商品領域時，不被他人非法運用，從而賦予權利人支配或者維護自己人格價值的權利。對於人格權人而言，人格特徵是本，而財產利益是末[189]。惟這並不代表隱私權所乘載的資訊不具備經濟價值，不能被個人所控制、利用，或是不具備對世性，只是不特別以隱私財產權稱之而已。

[189] 馬俊駒，前揭註 173，頁 187。反對見解可參考溫世揚，前揭註 172，頁 109。其認為「人格商品化權」雖然成立於一定的人格要素（人格符號）之上，或者說「寄生」於姓名權、肖像權等具體人格權之上，但從其內容構造、制度功能等方面考察，其作為「商品化權」的一種具體形態，已非人格權範疇所能涵蓋，與其說是一種人格權，不如說是一種特殊的財產權。

doi:10.6342/NTU202301113

以下具體從隱私權的特性、權利主體、利用對象、可否轉讓、繼承，探討其經濟利益的保護。

第一款 隱私權的特性

首先由於隱私作為人格權之一並不若生命權、身體健康權等權利，高度涉及人身完整性，因此其實在隱私權下，存在為了賦予個人更多控制而去強調財產權的主張空間。再者隱私權作為人格特徵之一，隱私所涵蓋的資訊本身具備了「使用接近開放性（Zugriffoffenheit）[190]」，不同於名譽、行動自由、人身完整性、生命、勞動力、性自主等權利必須透過權利人本人的參與及協力始得加以利用，隱私權所乘載的抽象資訊得以在外於人格權人的掌控中被第三人利用，這也導致對於隱私的侵權變得普及且不易為權利人本人發現，但也正是因為這樣的一個獨自存在、第三人得以不受時間、空間及權利人生存與否限制而利用的特性，才提供了去探討個資本身可否交易以及如何進行交易的討論空間。

第二款 隱私的經濟利益

前述所提到關於人格權、財產權中一元論及二元論的文獻，多半在提到人格權的經濟利益時，僅以姓名權、肖像權為例，而並未提及隱私權的經濟利益保護。本文認為隱私權的經濟利益應同樣不可忽視，應肯認人格主體與相對人間可以基於平等地位締結契約，就個人資料的利用磋商一個雙方同意的「標的範圍」（像是利用的場合、方式及時間）及「效力範圍」（像是如讓與著作財產權般轉讓，還是以專屬授權或一般授權方式授權）。只要不違背善良風俗及強行規定，就應

[190] Büchler, AcP 301, 308 (2006) 轉引自黃松茂，前揭註 164，頁 11-12。使用接近開放性乃瑞士學者 Büchler 所提出之概念，其認為某些人格利益可以被第三人加以利用，而無需權利人之參與及協力，姓名跟肖像等人格特徵就是其一。相對的，名譽、行動自由、人身完整性、生命、勞動力、性自主，就必須透過權利本人。這樣的分類是因為科技發展才出現的，舉例來說，正是因為照相機的發明才讓肖像權侵害變得普及、容易、可能。這樣的接近開放性，以及得獨自存在而加以利用，不受時間、空間及權利人生存與否的限制，就會延伸出人格特徵之人格利益可否及如何進行交易的問題。

doi:10.6342/NTU202301113

尊重契約自由及私法自治，否則若一概否決人格主體對自己人格特徵的處分利用可能，反而才是對人格尊嚴與自主的限制。

然而就效力範圍部分，我國實務目前尚未肯認人格特徵在商業利用上的財產法益得為具有物權效力的讓與或專屬授權客體。（專屬授權指的是在被授權範圍內，以相當於原權利人的地位行使權利，可說是具有物權效力的授權，與「讓與」具有相似性質），僅肯認其得為債權效力的授權客體[191]。像是在 Janet 廣告代言案[192]跟袁惟仁肖像案[193]中，法院皆以人格權具有一身專屬不得終局轉讓為由，駁回了經紀公司基於人格主體同意，行使人格特徵在商業利用上的財產權主張。這與德國之司法實務相異，德國學者有提出限制性讓與概念，肯定人格權人得與相對人訂定物權性質的授權契約，以兼顧人格權人與被授權人的利益[194]。

就隱私權得否繼承方面，2018 年 7 月 12 日德國聯邦最高法院認定，Facebook 等社群網站的資料類似於私人信件或日記等物品，可以被視為係遺產而被繼承。最早 2015 年的一審法院基於繼承法認為社群媒體帳號可以如信件般被繼承人繼承。但上訴法院支持 Facebook 的主張，歿者和 Facebook 之間的契約已於自然人死亡時終止，且隱私權的主張應涵括於生前及死後，重啟其帳戶會侵害其隱私[195]。此即採取了否定繼承的觀點。

第四章　　資料性質理論的比較法觀察

從前章節兩項案例及隱私權的重新爬梳中得以發現，若要為隱私權於財產權或人格權之間定性，可能會流於法學概念上的爭執，而無助於實際上解決資料所

191 王瑋，前揭註 163，頁 3。
192 台灣台北地方法院 100 年度訴字第 1843 號判決。
193 台灣台北地方法院 108 年度訴字第 527 號判決。
194 謝銘洋，前揭註 169，頁 61。
195 翁清坤，（2018），〈賦予當事人個人資料財產權地位之優勢與局限：以美國法為中心〉，《臺大法學論叢》，47 卷 3 期，頁 969。

doi:10.6342/NTU202301113

有權、使用權間，載體與其乘載資訊間的權限爭議。重點在於特定的權利是否具備哪些功能：像是可否？及在甚麼條件下可轉讓、授權、交易、繼承？。此一觀點也可見於以下本文就比較法上的介紹，像是有文獻將所謂的「資料財產權」主張理解為係指資料應適用「財產交易規則」，易言之也就是聚焦於可否轉讓？有限制授權？的討論上。或許這正是英美法系與歐陸法系的差異，大多數文獻並不討論資料或是個資本身究竟屬「人格權」還是「財產權」，其關注的重心反而都在「資料利用關係」的具體設計以及相關立法建議上。

以下於第一節處理先決名詞定義問題，第二節介紹美國法上對於資料性質的立法倡議與實踐、學說各家見解、與歐盟 GDPR 的比較、以及中國學者的主張作為補充，讓所謂「資料是否具有財產權性質」的問題討論來龍去脈更加明瞭。於第三節則更細緻的討論資料財產權更具體來說是指有體財產權？無體財產權？公開權？還是其他像是海難救助或投資關係等天馬行空的資料利用關係。最後於第四節提出本文見解。

第一節　　先決定義問題

本文認為必須首先必須釐清當我們說「資料具有財產權性質」時到底所指為何？就前者「資料」而言，本處之所以使用迥異於第二章所使用的「隱私權的財產權面向」，原因有二，一是此處在討論文獻上並沒有區分「個人資料」、與「非個人資料」（如法人資料、去識別化、匿名化資料），二是本文也不認為個人資料跟非個人資料的區分在未來是一件容易區別的事，誠如於第二章第四節中所描述的去識別化裸照的案例般，常人對於自己的裸照會覺得縱使經過去識別化，仍然會覺得該幅照片及其從屬收益屬於自己，當然這樣的案例可能有人會認為遮蔽面部的裸照並不是一個去識別化、無法特定個人的照片，因此性質上還是個人資料，且還是受到傳統個資法制保障，不過這樣的質疑反而會恰好點出個人資料跟

doi:10.6342/NTU202301113

非個人資料的區分困難。因此，既然討論文獻上沒有切割個人資料、非個人資料出來談，且這樣的區分也著實不易時，本文在用語上就暫且迴避「隱私權」的用語，而改以「資料」稱呼。

另外就「財產權」的用語部分，所謂「財產權」在一般民法體系下有很多種可能，例如：土地的徵收補償金、租金、公司股份紅利、還是認股權等等族繁不及備載。財產權在憲法概念下並不以現金形式為限，其他足以表彰經濟價值的形式也可以被包含。而這樣的觀念套用在資料上，大體上指的就是資料作為一種財產，而得以使用、排除他人使用、移轉交易、佔有、或收益的權利。

不過有時候在討論資料的財產性質時，部分學者[196]看似僅指涉資料在主體間的「移轉規則」應參考有體財產的規則（下稱財產規則）[197]，而沒有仔細去討論到底資料的定性是否屬於財產權？屬於哪種財產權？這樣的論點終究還是跟主張「資料」是「財產權」有所區別，蓋資料有類似財產的性質，而應適用財產規則進行交易，僅是針對交易規則規範，並不涉及資料在法律上非屬財產的定義，然而若說資料是「財產權」，那麼這個主張將會更強烈，且不止於適用交易規則，還會適用全部財產權當前的保障體系。因此，為了方便後續的討論，本文在此將先就名詞上做出明確定義，後續本文提到「資料財產權」時，指涉的即是針對資料的定性，至於這裡所用的「財產權」究竟係指有體財產權、相當於智慧財產權的無體財產權、還是將資料主體比擬投資人的股份紅利權？這些屬於更細緻的分類，本文將在後續本節第三項逐一分論。於此先將「資料財產權」當作是較上位的概念。而若本文意在強調資料的移轉規則、可交易性、事前磋商價格可能性時，

196 Ignacio N. Cofone, *Beyond Data Ownership*, 43 CARDOZO L. REV. 11 (forthcoming 2021); Lawrence Lessig, *Privacy as Property,* 69(1) SOCIAL RESEARCH 247, 247-269 (2002). 前者的用語是"Property rule"，後者的用語是 "Property Regime"，兩者就內涵上應屬同一，不過後者並沒有強調自己對資料的性質主張僅限於移轉規則。

197 *Id.* 財產規則指的是雙方在事前進行就使用資料的價格達成協議。與之相對的乃責任規則，意指事後才對使用、或損害物品的損失、價值進行協商。兩個規則並非互斥，舉例來說，對於一個花瓶的使用，可以是事前議價，也可以是事後打破後才談賠償。財產規則跟責任規則的使用時機取決於事前交易成本的高低，如果事前進行協商的交易成本過大或是邏輯上不可能發生，則不會採用財產規則。

doi:10.6342/NTU202301113

則將會註明「財產規則」以便跟「財產權」做出區分，後續就其他學者的批評也會分成對「財產規則」及對「財產權」兩類，於此先行說明。

另外一點需要補充者是，美國法之財產權(Property Right)，乃泛指任何具有保護價值之經濟利益而言，與我國民法上財產權的概念不盡相同[198]。因此在本章的整理上，除非特別強調，否則若出現資料財產權的用語，係指美國法下的財產權概念，與我國物權法定下的財產權概念有所不同。蓋從法學的非本質主義立場，法律的概念並不指涉任何本質性的真實，法學概念只是人類社會生活裡的一種特定溝通形式，因此即使是法律中所提到的看起來有清楚經驗指涉對象的概念（例如本處的財產權），並不能想當然爾的就認定是在指涉那些經驗對象[199]。正如同美國法上的 Privacy 不能對應到我國民法及大法官會議解釋裡的「隱私」，以及德國法的「私領域」（Privatsphäre）一樣，美國法上的 Property Right 自然也不能完全對應到台灣的「財產權」，不過為了行文上的方便，在本章介紹美國法上學者對 Data Property Right, Data Ownership 等概念時，仍會使用財產權的用語，為免混餚，這個部分也先行說明。

第二節　近期對資料財產性格之主張

第一項　美國立法倡議

我們先回顧一下目前美國國內立法倡議家與立法實踐上，對資料跟財產權之間相關論述的主張為何[200]。美國非營利組織之立法倡議者 Jim Steyer 提出了你就是商品「You Are the Product」立法倡議[201]。這份倡議後來延伸成加州州長 Gavin

198 王澤鑑，前揭註 166，頁 311。
199 顏厥安，前揭註 147，頁 5。
200 Brittany Kaiser（著），楊理然等（譯）（2020）。《操弄【劍橋分析事件大揭祕】：幫川普當選、讓英國脫歐，看大數據、Facebook 如何洩露你的個資來操弄你的選擇？》，一版，新北市：遠足文化。頁 370。
201 Steyer 過去曾和加州消費者隱私協會(Californians for Consumer Privacy)參考歐盟的 GDPR 推動了《加州消費者隱私法案》（California Consumer Privacy Act）。具體的立法倡議仍未出現，

doi:10.6342/NTU202301113

Newsom 所提出的《數據分潤法》（*Data Dividend Law*），該法在規定蒐集個人數據使用必須提供補償。

Mark Warner 也認為數據分潤法可以使得加州成為美國聯邦立法的先驅，並提出幾項可能的內涵，一是無論消費者勾選了幾次「同意」，消費者都可以對科技巨頭至多收取 25%的分潤、二是除了讓消費者知道其資料的價值外，也該使得消費者有能力帶走他的資料，轉換服務提供者[202]。另外，Warner 本身也提出了《繞路法》（*DETOUR Act*）用以透明化消費者數據的價值，以便管制大型科技公司[203]。

參議員 John Kennedy 則提出（*Own Your Own Data Act*）[204]，理想上由 FTC 執法，規範個人應該擁有在網路上產出的個人資訊，但該法案僅短短三頁，雖然規範中包含消費者的資料複製、轉出、撤回權、網路服務商條約應簡化明瞭等規定，但其規範並不如 GDPR、CCPA 具有完善的資料可攜權。

前民主黨總統候選人 Andrew Yang 則在其提案中指出個人資料應該被當作財產權看待，也就是說人民應該對個人資料有所有權，Yang 認為如果個人沒有得到應有的補償、獲取同等的價值，則將形同對其自主跟數據尊嚴的否定[205]。

但其表態可見 Sam Sabin, *Nearly Half of Voters Support California Governor's 'Data Dividend' Plan,* MORNING CONSULT, (Feb. 20, 2019), https://morningconsult.com/2019/02/20/nearly-half-of-voters-support-california-governors-data-dividend-plan/.

[202] Andy Serwer, *Mark Warner: This will 'send a shiver down the spine' of Facebook, Twitter, and Google*, YAHOO FINANCE, (Nov. 15, 2018), https://finance.yahoo.com/news/mark-warner-will-send-shiver-spine-facebook-twitter-google-161313831.html?guccounter=1&guce_referrer=aHR0cHM6Ly9zdGF0ZXNjb29wLmNvbS8&guce_referrer_sig=AQAAAHAoiOeFyH_MFU8vy49mBtOCNTo3lhEFQZ8zUf-ez8GfTwHGr22dp6s8fmW48dRHqKwlj8JJ7s6UhZu1MmalyWgwURSQStgqiEps6KPV44HlOI_GGGnKm62cJQMJ8s2Am3-oSBpS7wXy9KNQJADQ4qyDOlfGO5jdMfenGUqZNrDu.

[203] 草案意在禁止大型線上服務商掠奪性、詐欺性資料利用，並促進此類行為研究下的消費者權利。H.R.8975, 116th Congress, https://www.congress.gov/bill/116th-congress/house-bill/8975/text?r=9&s=1.

[204] S.806, 116th Congress, https://www.kennedy.senate.gov/public/_cache/files/9/f/9ff92982-1a58-4cf5-9bda-8530e5078224/2D6F1D231B87F5B281A01893CEAA75DF.sil19328-own-your-own-data-.pdf.

[205] Marty Swant, *Andrew Yang Proposes Digital Data Should Be Treated Like A Property Right*, FORBES, (Oct. 1, 2019), https://www.forbes.com/sites/martyswant/2019/10/01/andrew-yang-proposes-digital-data-should-be-treated-like-a-property-right/?sh=1fcad6a83ab7.

doi:10.6342/NTU202301113

第二項　美國立法實踐

至於實際上的立法實踐，與此最接近的或許是懷俄明州，該州有明確的數據資產立法（*Digital Asset Legislation*）。除了規定數位資產是無形的個人財產外，也賦予了對數位資產應用的所有權和追索權[206]。在其 2021 年修正之《數位資產法》（Wyoming Digital Asset Statute）中將數位資產（Digital Asset）定義成「儲存於電腦可讀取格式、得以表彰經濟、財產、取用權的數位資產、證券、貨幣等」[207]。此州法將會讓數位資產在 Uniform Commercial Code (“UCC”) 第 9 條下受到相當於無形資產的保護。作為全美第一州，數位資產將在俄懷明州財產法架構下受到財產權保護、可買賣、租賃、授權、提存。

阿拉斯加[208]、佛羅里達[209]、科羅拉多[210]、喬治亞[211]、路易斯安納州[212]等州則明確將個資中與當事人生理連結較具特殊性的基因資訊，視為該資訊所指涉當事人的獨特、排他、專有財產，其中科羅拉多、喬治亞、及路易斯安納州明確將財產權範圍限縮於防止保險公司利用基因資訊而拒絕提供保險予當事人之目的利用[213]，而剩下的兩州雖然沒有明確的限制基因成為財產權後的用途，但也沒有明文將其融入現行的普通法訴因制度中(Cause of Action)。因此美國法上雖有部分

---

206 STATE OF WYOMING 66TH LEGISLATURE, http://www.wyoleg.gov.

207 WYO. STAT. ANN. §§ 34-29-101(a)(ii)(B) (2019). “"Digital asset" means a representation of economic, proprietary or access rights that is stored in a computer readable format, and includes digital consumer assets, digital securities and virtual currency”.

208 ALASKA STAT. § 18.13.010(a)(2) (2012). “a DNA sample and the results of a DNA analysis performed on the sample are the exclusive property of the person sampled or analyzed.”

209 FLA. STAT. ANN. § 760.40(2), (West 2010). “…The results of such DNA analysis, whether held by a public or private entity, are the exclusive property of the person tested, are confidential, and may not be disclosed without express consent…”

210 COLO. REV. STAT. § 10-3-1104.7(1)(a) (2012). “Genetic information is the unique property of the individual to whom the information pertains”

211 GA. CODE ANN. § 33-54-1(1) (2005). “Genetic information is the unique property of the individual tested”

212 LA. REV. STAT. ANN. § 22:1023(E) (Supp. 2013) “An insured's or enrollee's genetic information is the property of the insured or enrollee.”

213 Kelli Rockandela, *A Myriad of Reasons to Celebrate: Why the Invalidation of Isolated DNA Patents is a Victory for Personal property rights*, 38 VT. L. REV. 225, 235-237 (2013).

doi:10.6342/NTU202301113

州將基因資訊界定為當事人之財產權，但結論上可能還沒辦法被法院接受做為訴訟之請求權基礎。

第三項　小結

上述雖然尚未介紹美國學者見解，不過我們可以先簡單稍微做個統整，除了最特別的俄懷明州立法外，其他政治人物或非營利組織的提議有幾個共同的特徵，一是雖然是廣泛性的強調資料數據財產權，但都項莊舞劍，實質上都在針對網路科技業巨頭 FAANG 如 Facebook、Apple、Amazon、Netflix、Google 等企業；二是美國民眾及其民意代表主要是對於企業（尤其是科技網路巨頭）無成本蒐集關於其個人資料的行為並據以獲利的行為感到反感，民眾本身原先可能沒有強烈到覺得該個人資料是相當於一項個人可資利用、轉讓的無形資產，然而直觀上，人們會認為縱使那些資料經濟價值不大或是因為資料累積的關係跟個人的連結已經薄弱，該類價值仍不該完全由企業所獨佔。反之，應該由跟那些資料最密切相關的個人取得控制、收益權，因此企業既然透過數據挖掘獲得鉅額商業利益，則作為其「原料」來源之個人就應該獲得合理補償、報償。

然而關於此點學者 Cofone 指出這樣的分潤主張並不必然涉及數據資料的權利定性，只需要承認其可透過市場於利用資料前磋商交易即可支撐這樣的主張[214]，因此其認為目前美國國內所提出的隱私財產權理論多半指的是資料的對價應適用財產規則，而不是指涉在對於資料的整個性質上應類同一般有體財產。因此他認為前面那些政治人物主張數據財產權的真正用意僅在於透過財產規則的事前協商、補償議價，提高資料主體對其資料的控制（Control）而已，而沒有具體對資料數據的性質定性。

[214] Cofone, *supra* note 196, at 11.

doi:10.6342/NTU202301113

至於俄懷明州的立法部分，或許會有人認為該法僅是針對虛擬貨幣、證券、或是「非同質化代幣」（Non-Fungible Token, NFTs）規範，然而若僅從法條定義看，法條用語為“includes”，顯見關於虛擬貨幣等僅是數位資產的例示。傳統上劃歸隱私權之個人資料在這樣的法條下，其實存在被劃歸為數位資產的解讀空間，只要該個人資料可被儲存成電腦得讀取的格式，且實質上得以表彰經濟上、財產上使用權限。就此部分，本文認為這項立法已經打破 Cofone 所作出「當前資料財產權的主張僅是針對移轉規則應適用事前磋商制度」的宣稱，俄懷明州的立法顯然是對資料的性質有全新的定性，而不是僅單就移轉規則作出宣稱，這部分應予注意。

第四項　美國學者主張

至於美國學者的主張，國內學者翁清坤已經在其對於我國是否應該賦予當事人個人資料財產權地位的文章中作出完整且詳細的介紹[215]，以下相關學說文獻蒐集部分源自該篇整理時所提及者，部分為本文蒐集，以下逐一重新蒐集統整：

第一款 主張資料是財產/適用財產規則者

（一）Alan Westin 是最早提出個資屬於財產權（property right）的人，其認為個人資訊是個人的人格自主決定，應該被定義為財產權，並適用美國法下財產權體制對公部門、私部門針對不當干預所施加的限制，且應受到正當程序的保障。具體而言，像是當個資被放入中央檔案時，必須通知個人，且個資主體要能夠審查關於他檔案的資訊，有權質疑其檔案是否遭到洩漏[216]。憲法第一修正案中關於財產有不被打擾的自由，也是支持的理由之一。

[215]翁清坤，前揭註 195，頁 941-1051。一些翁氏整理中未見的文獻可參照 Abraham Bell & Gideon Parchomovsky, *The Privacy Interest in property*, 167 U. PA. L. REV. 869(2019); Richard A. Posner, *The Right of Pricy*, 12 GA. L. REV. 393 (1977); Richard A. Epstein, *Privacy, Property Rights, and Misrepresentations*, 12 GA. L. REV. 455 (1978).

[216] ALAN WESTIN, PRIVACY AND FREEDOM 222 (1967).

doi:10.6342/NTU202301113

（二）其後以 Lawrence Lessig 為主最大宗的一群學者認為[217]，賦予當事人個資財產權地位，即相當於賦予個資控制權，使得當事人得決定是否及在何種條件下交易何種個資，並繼而取得其個資在市場上應有之價值，如此一般，不僅得避免資料蒐集者之濫用、掠奪，亦可藉由市場機制，排除政府過度介入，決定具有財產價值之個資之最有效率分配，並得達成個資、隱私之保護。另外，資訊使用有償的結果也將迫使資料蒐集者內部化蒐集、處理、利用或分享他人個資所衍生的外部成本，從而改變資料蒐集者行為模式而更加審慎蒐集及運用當事人個資之必要範圍，並減少客戶資料被蒐集的數量及遭濫用之機會，以提供隱私更大的保護[218]。

（三）Kenneth C. Laudon 認為，由於部分個資（基因資訊、信用歷史、醫療紀錄等）具有財產權的關鍵性特質，故應考慮以個資所有權的市場機制，使當事人能就個資運用獲得公平補償[219]。具體上國家應成立資訊市場（National Information Market, NIM），讓個人透過資訊帳戶（National Information Accounts, NIAs）、個資處理代理人（類似個資銀行的角色），以自由市場來促進社會效益最大化[220]。

---

[217] 其他還有認為賦予財產權可以強化資料主體控制權的還有 Jane B. Baron, *Property as Control: The Case of Information*, 18 MICH. TELECOMM. & TECH. L. REV. 367, 379-380 (2012); Andrew J. McClurg, *A Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 Nw. U. L. Rev. 63, 91 (2003).

[218] Lessig, *supre* note 196, at 247-269. 其認為對價性可以讓個資運用之外部成本內部化，市場能容許多元性，滿足不同人對隱私的看法，藉由適用財產體制，可經由協商為資料定價。Samuelson, *supra* note 142, at 1127, 1129, 1133.也認為成本的內部化有助於減少資料被蒐集。Dennis D. Hirsch, The Glass House Effect: Big Data, the New Oil, and the Power of Analogy, 66 ME. L. REV. 373, 385 (2014). 也採取相同立場認為應該使得資料蒐集成本被內部化，才能在長遠上讓資訊經濟永續。Carl Shapiro & Hal R. Varian, US Government Information Policy, (Presented at Highlands Forum, Department of Defense, June 8, 1997, Wash-ington, DC. Sponsored by the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence)), at 16, https://www.researchgate.net/publication/248244291_US_Government_Information_Policy.也同樣將此視為外部性問題，蓋隱私權人的資料被利用、負面影響，常無法向資料利用方有效反映其偏好。

[219] Kenneth C. Laudon, *Markets and Privacy*, COMMUNICATIONS OF THE ACM, Sept.1996, at 92-93.

[220] *Id.* at 100.同樣認為會有中介機構出現的有 John Hagel III & Jeffrey F. Rayport, *The Coming Battle for Customer Information*, HARV. BUS. REV., Jan.-Feb. 1997, at 53. 仲介產業的出現：Dennis J. McMahon, The Future of Privacy in a Unified National Health Information Infrastructure, 38 SETON HALL REV. 787, 816 (2008). 合作社性質：Information Commissioner's Office(ICO), *Big Data, Artificial Intelligence , Machine Learning and Data Protection*, Version: 2.2 (Sep. 4, 2017), 84-85, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

doi:10.6342/NTU202301113

Laudon 認為在財產權領域納入資料財產權，並不需要在美國財產法體系作出過多的調整，因為隱私的發展跟財產權有很深的淵源，且財產權體系也一向不吝於納入無體財產及肖像權，今天個人的數位人格圖像既然某程度相當於個人的物理肖像（肖像權），自然沒有不以同理納入財產權之理由[221]。

Laudon 並不認為這是出賣基本權利，因為隱私權在美國憲法地位不明，且就算承認它是基本權，也不代表基本權不能在一定限度內自由處分；另外 Laudon 也回應了自由市場可能造成市場力量失衡、資訊貧富不均的情形，其認為這可以透過現行主流銀行增加資訊管理的業務項目，藉此代理個體對大型機構抗衡。其認為總體上來說，隱私侵犯會在市場體系中漸漸減少，市場機制會使得資訊流動透明化，個人將對自我資訊擁有更大的控制[222]。

關於自由市場是否乃較佳的個資保護模式，Laudon 採取實證的角度認為，雖然像是汽車裡的安全氣囊，自由市場中廠商雖然沒有自主動機去安裝安全氣囊，而必須透過政府強制管制，然而如果套用在個資領域，如果告訴個人他的資訊在資訊市場中具有財產價值，個人就可能會傾向尋找值得信賴的機構為他確保該財產價值的收穫，因此長期來看，承認資料財產權有助於提升個人自主動機，而個人自主動機對個資保護的效果絕對好過於政府介入，政府僅需好好維持市場運行即可。

再者維護市場運行的成本可由市場參與者支出，並不會太高。至於面對個資所有權化後交易成本會太高的質疑，Laudon 認為交易成本只會上升到剛好足以嚇阻隱私侵犯的程度，個資交易市場將會打擊非法取得資訊的流通，企業也會透

[221] *Id.* at 102. 其他類似見解可見 McClurg, *supra* note 217, at 69-70. McClurg 認為消費者資料中的個人特徵累積起來也相當于一個個人的完整圖像。但其並沒有選擇 Laudon 的財產權途徑去保護該圖像，其認為賦予資訊財產權、創造市場機制雖然富有創意，然而制度上變動幅度較大，實踐上存在重大困難。於是 McClurg 先是批評傳統 Prosser 分類的四項隱私權侵害類型僅以 Commercial appropriation （商業上的擅自使用）保護名人的肖像、姓名等物理外在人格特徵有所不足，再轉而強調個資累積起來的人格圖像也應該受到侵權行為法下 appropriation 的保護，採取的是擴充現行侵權行為法保護範圍的途徑。

[222] *Id.* at 101.

doi:10.6342/NTU202301113

過競爭提供出更好的個資條款供消費者選擇[223]。相比目前企業浪費資金在侵犯隱私的行銷上（寄送型錄、垃圾郵件、行銷電話等），或是浪費在設計複雜的授權條款上，透過市場交易及管制讓資訊流透明化或許才是較佳的方式。

（四）Richard S. Murphy 主張，個資如同所有其他類型之資訊，乃屬財產[224]。Warren & Brandeis 採取非財產權的方式「發現」隱私權，是造成隱私侵權在民事法院發展不順利的主因[225]，另一個民事侵權保護隱私失敗的原因則是法院用統一客觀的社會標準、而非以主觀個人標準去衡量何謂隱私。

（五）Paul M. Schwartz 同樣認為當前個資規範體系缺乏客製化隱私協議的空間，進而導致隱私的價格歧視[226]（Privacy Price Discrimination），消費者僅能在接受或拒絕的雙元模型中選擇允許或禁止個資蒐集，其原因來自於市場上資訊不對稱，消費者甚至不知道自己的資訊正在被蒐集，或不知道自己其實有締約協商的可能，「知的成本」顯然過高[227]。市場上最後等於變相鼓勵企業著重於運用資金、技術開發侵犯隱私科技（Privacy-Invading Technologies, PITs）更甚於鼓勵研發隱私保護科技（Privacy-Enhancing Technologies, PETs）。不過財產化的提議可能不能解決問題，反而強化了既有市場主宰者的地位，重點還是應該擺在解決資訊不對稱上，譬如說透過政府介入隱私權同意條款的制定以破解企業條款所形成的框架效應[228]。

關於另一個財產化可能面臨的批評是他會忽略資訊隱私所重視的社會價值，像是作為民主社會的根基等。此一批評觀點傾向將資訊隱私認定為公共財[229]，

---

[223] *Id.* at 103. Samuelson, supra note 142, at 1135.也認同 Laudon 的觀點認為會產生可觀的交易成本。

[224] Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2383-84 (1996).

[225] *Id.* at 2389.

[226] Schwartz, *supra* note 178, at 2075-2076.

[227] *Id*. at 2081. 這樣的現象又稱有限理性（Bounded rationality）。

[228] Edward J. Janger & Paul M. Schwartz*, The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1242-44 (2002).

[229] See Schwartz, *supra* note 178, at 2084.

doi:10.6342/NTU202301113

其認為隱私不具競爭性與排他性，因此市場無法提供最佳的公共財供給[230]，再者公共財也不應被私有化[231]。Schwartz 對此認為即使是像國防、環境等高度公共財屬性的領域仍存在私有化如私人軍火公司、排放權等私有市場管制手段，因此公共財的公益性格未必與市場交易完全排斥[232]。

最後一個 Schwartz 所介紹關於個資財產權化的批評在於一旦財產化，個人就會變得容易將個資轉讓出去，並難以對此限制，Schwartz 認為這樣的批評誤解了傳統英美法上對財產的定義，財產權未必需要跟單獨排他、自由轉讓性掛鉤，例如智慧財產權中的著作權就是其一示例，著作權人享有一定年限後解除授權的權利。其甚至與本文在前述表達的立場相同，認為當前的個資其實已經高度被流通了，完全限制個資轉讓就認為能拒斥隱私侵害無疑是自欺欺人的；相對的，在有條件限制個資轉讓的財產權體系架構下，可能還會有其他修正市場的可能[233]。

Schwartz 提到當今市場上個資時常在主體不知情的情形下被交易，個資的商品化將有助於將資訊隱私的價值從零提昇到為正，這也許能提起我們對個資的重視[234]。而 Schwartz 的個資之財產權主張由五個要素構成，分別是：

(1)「不可轉讓性」（Inalienability，限制轉讓個資之權利，個資雖可轉讓但轉讓限制不因為第二次移轉而消失，當然這樣的轉讓必須透過一些可辨識措施如條碼等加以追蹤，並透過公權力機關監督）；

(2)「預設條款」（Defaults，以預設條款保障當事人，以選擇加入（Opt-in）條款的方式，讓資訊較充裕之業者必須主動揭露將如何運用個資，據以解決市場交易不對稱）；

[230] *Id.* at 2085.
[231] *Id.* at 2088.
[232] *Id.* at 2089.
[233] *Id.* at 2090-94.
[234] *Id*. at 2077. 所謂價格歧視是經濟學上的用語，指涉廠商不以對消費者生產的成本定價，而是以消費者對商品的需求彈性定價。

doi:10.6342/NTU202301113

(3)「退出權」（Right of Exit，個資交易的同意權行使，不僅最初得拒絕資料交易，也應嗣後有從交易退出的自由，隨時退出的自由據以保障自由決定與改變心意）；

(4)「損害賠償」（Damages)，隱私的損害通常難以估量，有些情形侵害者並沒有對被侵害者形成精神上損失，但卻獲利豐厚；在數據資料庫的情形，因為個資僅在聚集時始顯露價值，因此難以認定對個人隱私造成損害，反而會被認為是創造了價值。故 Schwartz 認為可採取定額、實際損害擇一的損害賠償機制據以嚇阻不法、維持市場秩序，該定額必須要與不法的發現率成反比，越難以發現的隱私侵害，定額賠償必須越高，藉此一方面解決個人缺乏救濟誘因的困境，以及同時防止市場濫用個資）；

(5)「機制」（Institutions，其認為市場應存在機制或機構據以 1)建立交易機制、造市，2)驗證交易雙方對其主張的個資是否合法，3)監督後續雙方是否遵守交易條件，以及監督市場是否有其他違反隱私保護之行為。其不認同前述 Laudon 提出的由個資銀行中心化代理個人進行此一功能，其認為此一造市或市場監督功能必須盡可能的去中心化，並鼓勵司法救濟，如透過個人私力救濟、團體訴訟、或由檢察長代表公益提起訴訟的方式。最後，Schwartz 也不支持使用檢舉獎金的模式，因為此一模式最後的審查負擔還是會落在 FTC 上，因而會形成過大負擔，當然 Schwartz 也認為為了不讓 FTC 承擔所有隱私適法性監督，最好還是應該效法德國成立個資單獨專責主管機關[235]。

（六）Vera Bergelson 指出 Prosser 教授[236]所提出的四項隱私侵權樣態，在法院實務運作下，不能有效解決當前個資被頻繁用於廣告等用途的情形，法院雖然認為該個資名單屬於企業財產，但並不認為該名單在被蒐集成冊前屬於財產。其

[235] *Id.* at 2056, 2060-69, 2095-127.
[236] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960). 也就是使人被誤解（false light），對私人生活侵擾（intrusion upon seclusion）,公開私人隱私（ public of disclosure of embarrassing facts）, 擅用姓名、肖像等（appropriation of name or likeness）。

doi:10.6342/NTU202301113

不認為在隱私侵權體系下擴張個資保護會是足夠的，而是應以財產權去正向建構，原因在於財產規則比責任規則有效率，且可以迴避損害小、認定困難的難題。當前侵權法制未能提供具有一致性與可行性的機制而保護個資。再者，美國法既已明示或默示認定個資是一種財產，因此將隱私納入財產體制也屬可行[237]。

具體上其認為個資作為財產並非絕對的由個人獨佔控制，還必須跟言論自調和，且必須要跟智慧財產權一樣有存續期間，不可繼承，以在資訊自由流通跟個資保障間取得平衡[238]； 再者第一次資料蒐集者在合法取得後應該得將資料用於研究及市場行銷用途；而政府得以基於課稅、教育、培訓目的蒐集並轉讓某些個人資訊;公共媒體得以發佈任何具有新聞價值的個人資料,無需徵得個人同意。

（七）Edward J. Janger 認為財產體系好過於責任體系，前者要求事前協商，使得所有人有權否決非自願性之揭露，避免資料利用者在責任體系下選擇「先上車，後補票」的「先違法，再賠償」的個資濫用情境。然而財產體系也不是沒有缺點，除了市場資訊不對稱外，在隱私的價值無法被輕易量化的前提下，消費者多半會為了價錢上的考量，選擇隱私保障不彰的服務[239]。Janger 的解決方案不是賦予個資完全可轉讓的財產權，而是賦予個資模糊受限制的財產權，其稱作 muddy property，讓所有人一方面有權否決非自願性之揭露，一方面透過司法手段懲罰後續利用、促進雙方就資料利用方式對話、最後透過法院解決爭議[240]。

其認為在隱私所有權化之後，會使得辨別權利人及其權利範圍成本提高、且分散的資訊所有權可能會造成跟未分配所有權前（屬於公共財的情形）一樣的混亂，舉例來說，讓郵寄名單上的每個人都有權行使否決權的時候，同時也會讓名

---

237 Vera Bergelson, I*t's Personal But Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 414 (2003).
238 *Id*. at 438-439.
239 Neil Weinstock Netanel, *Cyberspace Self-governance: A Skeptical View from Liberal Democratic Theory*, 88 CAL. L. REV. 395, 476 (2000).
240 Edward J. Janger, *Privacy Property, Information Costs, and the Anticommons*, 54 HASTINGS L.J. 899, 916 (2003).

doi:10.6342/NTU202301113

單喪失價值[241]。不過結論上，其認為成本高不代表不可行，在有更大的社會目的存在時就可以正當化[242]。為了解決上述資料庫資料的揭露及資料價值不高，但個別協商成本過高的困境，Janger 認為可以透過標準化隱私協商條款或是透過團體協商代表的指定，來解決資料庫中資料主體分散行使權利的困難，舉例來說，可以參考美國破產法關於債權人遴選代表協商的規定[243]。

（八）Patricia Mell 主張，個人特質(persona)通常藉由可識別特定當事人之個資而加以綜合描繪、剖析，因此，其應由當事人「擁有」之，其對於個資這項財產的觀點，相較於前述 Bergelson 的觀點來得絕對，其認為其他所有相關利害團體如盈利事業、公眾、或政府對個資財產的權利都應該在個人之下[244]；由於個人特質具有高度可識別性、且電腦科技使得個人特質（電磁紀錄）可以獨立於個人而被轉讓，因此 Persona 也跟財產越趨接近，因此，當事人對於其電子個人特質運用上，應擁有法律上之控制力[245]，不過 Mell 的觀點比較像是透過財產權的模式賦予個人資料自主權，使得個人得以控制資料不向第三人在目的外利用、以及使得個人得以對其個人圖像的正確性與否近用與更正，關於使用這些資料是否應該要補償或收費，他是採取否定立場的，原因在於不是所有個人資料的使用都可以直接連接到收益，例如政府、保險公司、醫院、學校在使用時就不是[246]。

（九）Kevin Miller 主張，當前環境著重於以市場取向謀求解決之道，賦予個資財產權地位之主張，是在政治上、文化上更有吸引力的選擇，因為兼具經濟誘因的政策主張將比單純以憲法上隱私基本權主張而更能有效減緩個資被大量

---

241 相同觀點可見 NIVA ELKIN-KOREN & ELI M. SALZBERGER, LAW, ECONOMICS AND CYBERSPACE: THE EFFECTS OF CYBERSPACE ON THE ECONOMIC ANALYSIS OF LAW 50 (2004).其認為由於個資複製再利用成本相較於有體物來得低，排除他人使用（控制）的邊際成本通常會高過於提供予他人使用的邊際成本。

242 *Id.* at 922.

243 *Id.* at 924.

244 Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 69, 76 (1996)

245 *Id.* at 81.

246 *Id.* at 78.

doi:10.6342/NTU202301113

蒐集與監控[247]，這個主張有兩個面向，一是提高資料蒐集利用成本，讓資料更難取得[248]，二是其相當於認為就資料預測模型的利用乃資料原所有人的特權，而非蒐集者的權利，原權利人可以進而限制、排除他人使用、收益。雖然一般情形下，個人人格特徵、姓名等不被認為是著作權的一類，而科技公司運用所演算法則有被認為有被認定具有著作權的可能，然而 Miller 提出的質疑在於如果今天該演算法高度模擬特定個人決策時，是否也同時代表該演算法具有高度人格內涵？此時該演算法的利用是否就不該被承認屬於科技公司的著作權，而反而應該由原人格權人取得控制[249]？Miller 認為雖然相關論述仍需補充，然而此一方向確實值得思考。

（十）其他還有 Catherine M. Valerio Barrad 主張，基因資訊具有值得保護之財產利益[250]。以及前述曾經在病歷資訊利用問題介紹過的 Mark A. Hall 也分析，有存在於醫療資訊上之財產權，並建議允許病人擁有得將其醫療資訊授權使用之權利，以促進電子病歷之商業化運用[251]。以及 Jamie Lund 提議，應賦予個資財產權地位，透過當事人管制、監督其個人在外流通之個資之正確性，從而減少不正確個資流竄之資訊汙染（information pollution）之現象[252]。礙於篇幅且其文章內容大致上主軸差異不大，故不逐一介紹。

第二款 資料財產權的理論依據

主張資料財產權的理論大致可分成三類，分別是勞動理論、效益理論以及人格理論，以下分別簡述之：

（一）勞動理論

---

247 Kevin Miller, *Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm*, 19 J. TECH. L. & POL'Y 105, 141 (2014).
248 *Id.* at 142.
249 *Id.* at 144.
250 Barrad, *supra* note 154, at 1062-63.
251 Mark A. Hall, *Property, Privacy, and the Pursuit of Interconnected Electronic Medical Records*, 95 IOWA L. REV. 631, 653 (2010).
252 Jamie Lund, *Property Rights to Information*, 10 NW. J. TECH. & INTELL. PROP. 1, 11 (2011).

doi:10.6342/NTU202301113

勞動理論認為任何人對於其以勞力所取得或創造之物應擁有所有權[253]。約翰洛克主張，每個人對於其自身應擁有財產權（Every Man has a Property in his own Person.），任何事物只要與其勞力相混合，自應屬其財產。此又稱作獎賞勤勉理論（Lockean labor-desert theory），從洛克提倡的自然法出發，本於自然正義原則，投入心血從事創作，即可享受勤勉勞動的成果，有權控制、自由處分其著作。

有學者就基於此採取資料蒐集者（業者）歸屬說[254]，只要業者正當蒐集符合個資法，根據洛克的勞動正當論，即將數據賦予給業者[255]。但同樣的理論也有認為個人對於其個資應優先擁有財產權，原因在於「付出勞力者取得所有權」必須建立在該標的原先不屬於任何其他人時才成立[256]，該個資既然非屬於存在於自然狀態下的無主物[257]，資料蒐集者自不應擁有優於當事人之財產權。

（二）功利理論

功利理論指的是財產權應該分配到人類福祉最大化的狀態，這個理論面臨最大的挑戰在於什麼是福祉？又該福祉應該如何衡量[258]？何謂最大人類福祉，有以經濟效率為解釋者[259]。像是 Posner 就主張因為個體雜誌訂戶就其訂閱紀錄此項個資利益小、雜誌社若要逐一徵求其同意成本會大過於該訂閱名單本身的價值，因此不必徵求當事人同意，直接就有處分權[260]。不過像是前述的 Bergelson 跟 Laudon 都認為這項推論有瑕疵，當前資料法制對於資料主體造成的成本其實不會因為蒐集方可以不經同意而直接處分而變小，反而資料主體必須承受大量的垃圾信件、電話，並付出相當成本反制之。換言之，資料蒐集的成本沒有合理轉嫁

253 Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1380-1 (2000).
254 朱宸佐（2020），〈人工智慧時代數據財產權的保護路徑〉，《月旦民商法雜誌》，67 期，頁 142。
255 Cohen, *supra* note 253, at 1381.
256 *See* Bergelson, *supra* note 237, at 379, 400-01, 420.
257 *Id.*
258 Cohen, *supra* note 253, at 1381.
259 ROBERT D. COOTER & THOMAS ULEN, LAW AND ECONOMICS 44-46 (4th ed. 2004).
260 RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 36-39, 271-89(4th ed. 1988).

doi:10.6342/NTU202301113

予資料蒐集者，此一外部性導致市場失靈[261]。有認為解決之道在於將個資的財產權分配與個資所指涉的當事人，讓交易成本大到剛好可以嚇阻非法使用個資的程度[262]，並藉由協商減少濫用個資的外部性問題。

至於從個體功利角度看，對個資的法律上所有權會使得個人能對其個資有高度的控制，個體可以決定他願意為了多少金錢上、非金錢上的利益去分享個資。這可以滿足不同人對個資的不同偏好，對於個體也是效益最大[263]。

（三）人格理論

人格理論源自於黑格爾哲學，其主張為了增進個人自我發展，每個人對外部環境資源應有控制權，而控制權可藉由財產權形式達成[264]。Margaret Jane Radin 將財產分成個人財產（Personal Property）與可替代財產（Fungible Property），前者的損失無法透過金錢或可替代物補償，然而後者可以，其認為個人財產應該比可替代財產接受更多法律保障[265]。個資是個人自我認同與人格建構所不可或缺，不得與當事人分離，然而個資對資料蒐集者而言，只是一個可替代、分離的財產，因此個資之財產權應該分配給與個資最緊密連結的當事人，因為維護個人自我認同價值大過於對於資料蒐集、利用者的市場交易價值。

或許有認為這樣的論點看似跟個資可交易性、財產權化的觀點相悖，其實 Radin 也對此回應，提到理想上確實這些個資不該具備可交易性，然而在非理想的、不對等的世界裡，部分的可交易性應該還是可以被容許的[266]。另外也有認為這是對人格的物化，然而 Bergelson 則以一個例子反駁，指出讓個人得以決定是否出售婚戒並不會貶低婚戒本身的情感價值，當前美國法已經在破產法規定容許個人保留信件、相片、日記、老家等與人格緊密關聯的財產，顯見人格的財產並

[261] Laudon, *supra* note 219, at 102-3; Bergelson, *supra* note 256, at 422.
[262] Bergelson, *supra* note 237, at 426.
[263] Bergelson, *supra* note 237, at 428.
[264] Baron, supra note 217, at 367, 380, 395 (2012).
[265] Margaret Jane Radin, *Market-Inalienability*, 100 HARV. L. REV. 1849, 1880-81(1987).
[266] *Id.* at 1903.

doi:10.6342/NTU202301113

不是陌生概念，故應該於隱私個資中援引，賦予個人對蒐集者相當程度的財產上控制權[267]。

第三款 小結

綜合上述可見美國就隱私財產權的論述多半集中於西元 2000 年前後，而其立論動機主要是為了提升個人資料的自主控制、以及為了回應個資被廣泛交易買賣、利用的趨勢才有此一發想。由於隱私權跟財產權歷史發展早期於美國高度重疊，因此並不存在特別高的論述上、立法上阻力。其等提出了透過讓第三方蒐集成本提高的方式、令蒐集者賠補償權利人的方式、高額罰金嚇阻隱私侵害的方式、資訊市場建立的方式、政府草擬隱私權利用的定型化條款並提供一定的市場監管等方式，建立一套「財產規則」以取代當前的「責任規則」。

其等認為財產規則是透過事前協商的方式取得資料利用的共識，而有助於避免未經同意的資料利用，而責任規則某種程度上則是縱容資料蒐集利用者得以「先上車、後補票」，事後賠償的方式不妥的原因在於隱私侵犯行為以及損害都不容易被發現及量化，且有時權利人可能也僅有財產上損失，而沒有人格侵害，因此無法在傳統人格權體系下得到賠償，因此責任規則下容易造成人格權名存實亡的情形。

最後，其等都發現美國法院實務其實傾向於否認多數的資料隱私侵害主張，主要原因在於 Prosser 提出的四項隱私權侵害不夠全面，且傳統對隱私的想像上也過度著重避免秘密洩漏，而非著重個人自主收益、交易、利用的部分。另外，其等也多少提到美國法院實務運作上多半拒絕承認資料具有財產權，而僅在企業

[267] Bergelson, *supra* note 237, at 432.

doi:10.6342/NTU202301113

蒐集的資料集中才承認其財產權地位，對於尚未被收集的個人資料，法院並不認為屬於財產權，這樣的結論無異加劇了個資商品化、被無償利用的困境[268]。

至於其他採用財產權、或財產規則的優點還有因為財產權的利用主觀上允許差異，所以也較符合個人與個人間的不同，注重隱私者得以花費成本與資料蒐集者協商，以拒斥其個資的商品化[269]。除此之外，本文認為在上述學者見解外，關於認定為財產權的優點，除了第二章提所到資料財產權理論可作為賦予個人對去識別化資料控制同意權的理論基礎。還有一點，那就是資料財產權可以作為隱私權的備位填補規範，以前述於本章第一節、第一項學者楊岳平所提到的個人對其病歷是否具備資料可攜權為例，我國目前尚未引入資料可攜權，惟如果透過承認資料具有財產權、適用財產規則時，個人就得以自由掌控個資的轉讓，雖然資料可攜權還要求要通用格式轉出，與財產權的自由轉讓並不完全一樣，但某種程度上資料財產權所能賦予個人的權利仍與資料可攜權類似，只是又再更全面，甚至不如說是資料可攜權有點像是財產權眾多權能（尤其是自由轉讓權能）的一束變形[270]。

最後關於承認資料是財產或應適用財產規則的缺點，於上述文獻整理中也可略知一二，首先，有認為（一）隱私相當於人格，而承認作為人格權的資料得以買賣將貶損人格權，再者（二）自由市場無法解決資料蒐集者與被蒐集者間的高度資訊不對稱[271]，（三）個人都有一控制否決的權利將造成資料利用效率下降，

[268] 有認為既然企業對於其蒐集之顧客資料、聯絡方式等擁有財產權，個人相對的也應該對於其自身的姓名等個資擁有相同的財產權。也就是說既然該企業對所蒐集、持有的消費者姓名、個資可以被法院認為是營業秘密，該消費者個人也亦應該擁有對等之財產權。Ann Bartow, *Our Data, Ourselves: Privacy, Propertization, and Gender*, 34 U. S. F. L. REV. 633, 634 (2000).

[269] Samuelson, *supra* note 142, at 1134-1135.

[270] See Jacob M. Victor, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 YALE L.J. 513 (2013). 該文認為歐洲的 GDPR 草案與 Schwartz 建議提出的財產規則體系類似，包含被遺忘權等規定，本文此處也是認為資料可攜權或是被遺忘權等規定其實某種程度也跟此處美國學者所倡導的「資料財產權」相似。

[271] 關於此除前述介紹外也可參照 Daniel D. Barnhizer, *Propertization Metaphors for Bargaining Power and Control of the Self in the Information Age*, 54 CLEV. ST. L. REV. 69, 70-73 (2006).其提到個資的財產交易化以及隱私契約條款的產品化，已經使得個人對於交易條件不再存在議價空間。

doi:10.6342/NTU202301113

效益減低，（四）由於單一筆個資的經濟價值低，因此個人缺乏救濟誘因，導致隱私權保障體系難以仰賴個人。

上述文章其實都有針對各點回應，如第一點就有認為不該讓高大上的道德綁架實然面的思考，第二點及第四點則有回應必須透過公權力有限度的介入，透過個資代理人、機構等角色的介入去改善協商、救濟成本的問題，或是透過科技方式減輕代理成本過高的問題。至於第三點則是所有隱私保護規範於立法論上都必須面臨的挑戰，本文認為必須回到資料利用的效率與個資保護對於民主制度的權衡論證評估上，由於相關文獻也多，故亦非本文所欲聚焦者。以下本文將針對美國學說上對於隱私財產權的批評略作介紹，雖然上述於介紹支持的相關論點時已經多少提及（如前段提到的四點），然為免掛一漏萬，以下以完整的一目介紹。

第四款 主張資料不是財產/不適用財產規則者

（一）關於是否應該賦予資料財產權屬性，Cofone 對此的批評整理非常全面，故先以其見解展開。首先，Cofone 認為美國法上談的資料財產權屬性並非真的為資料的法律性質定性為財產權，而僅是在交易規則上認為資料應該適用「財產規則」。其對於資料適用「財產規則」有所批評，其主張有四項缺點[272]：

一是不對等的市場地位將會使得資料主體更陷不利[273]。蓋資料市場中，資料主體與科技巨頭將會存在不對等的談判地位，此不僅止於資源上的落差，更是因為消費者面對科技巨頭時常常只能選擇委屈接受不佳的隱私權條款，或是全面拒絕使用服務[274]。再者，由於資料主體無法準確知道資料將如何被使用、風險高低、

[272] Cofone, *supra* note 196.

[273] Edward J. Janger & Paul M. Schwartz, *supra* note 228, at 1242-44. 其等也指出消費者難以表達隱私偏好，市場就無法提供競爭、提出更好、更符合個人的隱私權條款。現行企金融企業採行的選擇退出告知事項也會形成框架效應，很容易將選擇退出描述成個人會面臨損失，藉著心理學上個人對損失的敏感大過於對取得的企求，企業會利用此一資訊不對稱，操縱個體去盡量選擇不退出，簡言之，只要資訊不對稱存在，市場機制、告知說明、跟選擇退出機制皆不能帶來更多談判。

[274] 即使是前述支持隱私財產權的 Schwartz 也同意此一觀點，其也認為當前個資市場存在的價格歧視，就是源自於資料處理公司沒辦法依據個人的偏好對消費者個資做出定價，因而僅能做出雙元的、全有全無的、收集或退出的個資處理。消費者在資訊市場上存在結構性脆弱，資訊嚴重不對稱的情形。*See* Schwartz, *supra* note 178, at 2077-2078.

doi:10.6342/NTU202301113

因此也不會對資料使用價值做出妥善定價，此部分就正如同傳統個人所適用的資料告知後同意，也會因為難以預見將來資料會如何被使用，而難以使資料主體在事前做成有效同意[275]。

二是資料累積所表彰的價值無法被賣斷制的市場交易模式評估。蓋在大數據盛行的今日，最有價值的可能不是特定個別的資料，而是眾多公開、非公開、個人、非個人資料綜合交互參照、累積分析所得出的結果，因此假如要針對個別資料定價不但會是困難的，而且可能會忽略資料累積綜效而低估價值[276]。再者，如果此處的資料指涉的是個人得以控制之個人資料，則去識別化或匿名化之非個人資料即不受到財產規則所保護，但是現行實務上該資料下仍會被科技巨頭拿來做群體分析，此時這部分的收益究竟誰可以分潤就會成為這個理論所漏未處理的。又，市場賣斷制其實有很嚴重的問題 因為資料對於個體造成個資風險是持續的，並無法隨著賣出而永遠與個人切割，因此此時資料處理（購買）者將會有濫用資料或疏於維護資料安全的道德風險存在，而此著實對貫徹個資保護不利[277]。最後，就算只談個人資料，個資在移轉的同時也可能會對其他群體產生外部性，舉例來說，我的資料被我賣出時，可能將會有助於他人的個資被再識別，或被統整而再次被榨取出其他經濟利益。也就是說個人資料如本章第二節、第一項、第二款所

---

[275] 相同批評可見 James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1, 20 (2005); Tanith L. Balaban, *Comprehensive Data Privacy Legislation: Why Now is the Time?,* 1 CASE W. RES. J.L. TECH. & INTERNET 1, 21 (2009). 後者指出在個資下創設財產權無助於解決個人無法做出自主有效決定的問題，且一但一家公司掌握個人可識別個資，最後在該個資的流通下，也會難以確定最初是誰違反合意轉讓的，因此個人若欲提起訴訟，也會在損害主體的確定上存有對誰提起訴訟的困難。附帶一提，Balaban 認為傳統美國法上的侵權、契約以及財產權保護體系都無法解決美國當代隱私權難題；反之，其認為美國必須採納如歐盟般的全域單一標準立法，包含賦予個人更多訴權、採取選擇加入制、確保企業蒐集透明、個人更高控制等制度。

[276] Jerome 跟 Steel 等人也指出單一的個人數據並不值錢。*See* Joseph W. Jerome, *Buying and Selling Privacy: Big Data's Different Burdens and Benefits*, 66 STAN. L. REV. 47, 52; Emily Steel et al., *How Much Is Your Personal Data Worth?*, FIN. TIMES (June 13, 2013), http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html. "Those bits of information are often sold for a fraction of a penny apiece."

[277] 個資的一個特性即是其不具競爭性(Non-Rivalrousness)，一個人的使用並不會影響另一人的同時使用，正是這樣的特質才是導致個資過度被濫用的主因。相同批評可見本節第三項第一款以及 Balaban, *supra* note 275, at 22; Jerry Kang & Benedikt Buchner, *Privacy in Atlantis*, 18 HARV. J.L. &TECH. 229, 241(2004).

doi:10.6342/NTU202301113

述，有時候個資所牽涉者不只是單一個人的事，因此很難將權利劃歸於單一主體進行市場交易。

三是如果僅是把可交易性、適用財產規則跟具有財產權利性質畫上等號，無疑是忽略了資料同時屬於資訊隱私權所具有的其他言論自由保障、人格自由保障等面向[278]。

四則是適用財產規則將會跟傳統資訊隱私權所強調的目的限制原則衝突，蓋賣斷制將會使得目的限制這樣個人原先所掌握的「控制」不復。

（二）其他批評者還有如 Baron，其雖然認為使個人擁有個資可以使其得以自由決定其運用[279]，然而這個控制未必是，也未必需要是源自於傳統財產體系所賦予的架構，事實上，一個完善的隱私控制架構多半只是看起來像財產體系架構而已。這涉及到現行體制對財產的定義，舉例來說，如果對於財產的定義是單一、可識別主體、對特定物的絕對控制時，資訊隱私很明顯的不會符合這個定義；而如果對財產的定義是具備對世效者，則資訊隱私也不見得在所有情形都該具備此一效力，再者，資訊隱私與財產權最相斥的地方在於財產具備可自由轉讓性，然而如果要賦予資訊權人控制，勢必沒辦法完全地承認自由轉讓性，而這樣的妥協，就會使得整個「資訊財產權」變得不像「財產權」[280]，因此結論上 Baron 認為賦予個資財產權的主張無法解決大多數問題，相反的，針對該資訊特定領域的政策、公私利益團體角力才會定義出該資訊的控制程度。簡言之，援用財產概念跟提升控制的強度間沒有太大的關聯[281]。

（三）Peter K. Yu 就關於大數據時代下是否該接受資料庫數據以「資料創造者權」（Data Producer's Right）的方式賦予財產權保障，其認為若賦予個人或企

[278] 關於此類認為將人格權財產權化是一種對人格權的窄化、矮化的見解可以參照 MARGARET JANE RADIN, CONTESTED COMMODITIES (1996)其同樣認為將隱私賦予財產權相當於是將投票權變成可買賣的客體，其結果就算有助於投票率提升，但仍是對於自由民主社會的侵害。
[279] Baron, *supra* note 217, at 367, 380.
[280] *Id.* at 383, 384.
[281] *Id.* at 415.

doi:10.6342/NTU202301113

業此一權利將會造成市場障礙，而這項主張應只是歐盟欲對抗美國科技巨頭濫用資料利用的一項工具性主張而已，再者，從企業界沒有人在做相關的立法推動，也可見企業偏好資料的自由流動，並認為這樣才能鼓勵創新。故結論上不贊同「資料創造者應享有資料財產權」。

不過應注意者係，這邊討論的資料創造者權是針對非個人（nonpersonal）、匿名化（anonymized）、機械產生的（machine-generated）數據[282]，與本文所欲關注的個人資料財產權化稍有不同，不過由於 Yu 也在文章中表示[283]匿名化資料跟個人資料之間的界線越來越模糊，因此相關的討論還是有參考價值。

（四）其他還有 Mark Lemley 從隱私權的角度出發，認為一個可授權出去的智慧財產權模式，可能會賦予個人相較於現在更少的保護[284]。且其認為就資訊隱私財產權而言，沒有一個好的市場解決方案，仍必須透過其他「告知後同意」等機制落實真正的選擇自由[285]。

由前述可見 Cofone 所提出的四項反對理由，基本上與其他美國反對派學者意見大同小異。Cofone 在結論上認為由於財產規則跟責任規則並不衝突，故應該混合使用，責任規則不能捨棄的原因在於僅有它才能內部化個資移轉所生之外部風險，蓋在個資不法使用或損害發生時，責任規則才能讓損害被精準的估價，此時補償才會有效率。至於責任規則下所應適用的注意義務部分，因為個資不法使用的風險發生取決於資料蒐集者單方，因此課予其嚴格責任比較能內化此外部風險。最後，Cofone 也表達了對現行隱私法制大半採取行政法管制路線的不滿，蓋其認為行政上是否開罰、進行訴訟都取決於政府，過於被動，無利於權利行使；再者，縱使行政調查啟動，如果該受利用之個資已取得個人同意，縱使個人受有

[282] Peter K. Yu, *Data Producer's Right and the Protection of Machine-Generated Data*, 93 TUL. L. REV. 859 (2019).
[283] *Id.* at 920-921.
[284] Mark A. Lemley, *Private Property: A Comment on Professor Samuelson's Contribution*, 52 STAN. L. REV. 1545, 1551(2000).
[285] *Id.* at 1554.

doi:10.6342/NTU202301113

經濟上損失，在現行個資法制下依然無法開罰。因此其認為應該從參考 GDPR 第79、82 條，推導出個人針對損害的訴訟途徑，或是透過進行團體訴訟的方式解決權利難以歸屬於個人的問題。簡言之，其認為財產規則跟責任規則要並用、行政管制跟民事救濟要雙雙健全、而資料蒐集者跟資料主體間的關係可參考忠實義務。

相較之下，翁氏的結論也有點類同，都是試圖在「全面認同將資料劃歸現行財產權體制內」以及「維持傳統個人資料保護的人格權立場」間求取平衡。翁氏認為隱私權財產權化時，重要的財產權權能（如「自由轉讓原則」）既然將會被嚴重限縮，則賦予個資財產權地位的取向即不大具說服力。再者，臺灣既已有個資法全面賦予當事人對於各行各業蒐集其各種類型個資之一定控制權，而不像美國只有個別領域的分散立法，故縱未另賦予個資財產權地位，仍可落實個資之保護。不過其仍指出就個資保護層面而言，我國仍可適度善用財產權之理論與市場機制，避免蒐集者未支付完整對價的搭便車行為，並迫使其內部化蒐集的成本，以減緩個資之濫用，或是積極參與業者（如醫療、金融、網路、行銷）在當前大數據時代日益興盛以個資為基礎所進行之運用開發，進而更平等參與個資供需交易市場之運作，進而避免業者單方剝削式掠奪、濫用。以第二章、第一節、第二項的健保資料庫案為例，翁氏即認為與其訴諸稍嫌空泛的公共利益概念以尋求正當化之基礎，不如嘗試透過減收健保費之方式，而吸引欲少繳健保費之當事人經告知後選擇而評估是否授權其病歷資料而供第三人研究之用，減緩當前該資料庫供研究所衍生之正當性爭議。

第五款 小結

統整來說，美國國內對於隱私財產權此一議題，不論是實務或是學界仍有不少反對意見，有認為當前資訊個資市場欠缺完整數據交易機制、無法妥善定價、且個資蒐集過程並不透明，議價困難，此些客觀情狀將導致數據交易的成本大於

doi:10.6342/NTU202301113

收益[286]，因此結論上其等認為賦予被蒐集者資訊財產權會延伸過高的交易成本，甚至阻礙資訊流通；也有認為個人資料財產權化可能會形成個資價值不易評估、資訊不對稱、人格商品化、進而損害當事人人性尊嚴與人格發展，甚者造成虛偽資訊的過份保障、資訊利用的不效率、公益研究窒礙難行、新聞言論自由受高度限制等負面結果。

不過追根究底可以發現，學者間對於何謂「隱私財產權」的定義其實是存在歧異的，而且這最主要體現在此一財產權的「可轉讓性」之上，批評者大多會聚焦於此一點上，但無獨有偶的是，支持財產權者幾乎都會對「可轉讓性」做出妥協，也就是僅承認部分的可轉讓性。此時就會面臨兩個核心問題，一是少了可轉讓性的「隱私財產權」還是不是「財產權」？二是如果它還是「財產權」，那麼它跟現行隱私體系的保護手段的差異又在哪裡？這些文獻是否過於強調資料為「隱私權」或「財產權」這樣的一個概念法學上的區分？本文認為從前章隱私權與人格權的爬梳中可見，自實然保障隱私的角度而言，強調一定程度的不可轉讓性、無論是以何種方法賦予個人對個資的持續性控制、並輔以其他代理、機構監管、個人團體救濟管道等方式，據以解決市場失靈、資訊不對稱等困境，才是一個比起糾結於定性問題，更能切中議題核心的思考途徑。

第五項　與歐盟 GDPR 的比較

以上大致介紹完關於個資財產權於美國國內的正反意見，也大致對於資料財產權跟資料隱私權的論證有所了解，從中約略可見有些主張途徑是主張效法歐洲的單一個資專責機構，可見美國學者對歐洲法律的想像是正面的，由於有美國學者認為歐盟 GDPR 的立法實際上用語跟內涵都跟早期美國國內「資料財產權」的

[286] Schwartz, *supra* note 178, at 2059.

doi:10.6342/NTU202301113

論述有異曲同工之妙，故以下將簡單介紹相關論點，並把「資訊財產權」概念與歐盟現行隱私保障的法律比較，釐清其異同。

有認為歐盟 GDPR 的目的在於保護個人自主、隱私權，但並沒有觸及個人資料的財產特性[287]，同樣的，也有學者比對歐盟現行的個資保護法律，發現歐盟沒有採取財產規則的個資保護架構[288]。但本文發現有學者如 Victor 就提出反對意見認為歐盟 GDPR 於 2012 年提出的 GDPR 草案，雖然不完全採取財產權的用語，但藉由賦予權利主體知情權、訪問權、刪除權、可攜權等方式，認為 GDPR 在一定程度上也發現、並接受了個資被當作財產、正在被交易的事實[289]，蓋該草案跟前述 Schwartz 於 2004 年所提出的財產權體系模型有相當程度的類似[290]，皆對於數據隱私施加財產規則的保護[291]。Victor 對 Schwartz 提出的資料應適用的財產規則，整理出三項特色，分別是一、資料主體的權利原則上僅得部分分離於主體外，二、資料本身存在有移轉後仍拘束第三人的物上負擔，三、救濟上適用財產規則下的救濟。

而第一項可以對應到刪除權（被遺忘權），蓋無論資料經幾次轉手，原權利主體永遠有刪除的權利，這也意味著個人資訊永遠不能「賣斷」，而第二項的部分則對應到 GDPR 草案第 17 條(2)，其規定資料使用者必須採取所有合理措施以通知正在處理個資的第三方刪除有關該個資的一切連結與複製品，這相當於是財產規則超越契約規則的「對世效」。最後第三點關於財產規則救濟的部分，Victor 認為 GDPR 草案中關於禁制令（Injunction）、企業未落實被遺忘權可能面臨的罰鍰（50 萬歐元或該企業一年中、全球 1%的營收）、資料主體的近用、修正、

[287] Colin Tankard, *What the GDPR Means for Businesses*, 6 NETWORK SECURITY, 5–8. (2016).
[288] Purtova, *supra* note 179; NADEZHDA PURTOVA, PROPERTY RIGHTS IN PERSONAL DATA: A EUROPEAN PERSPECTIVE (2011).
[289] Victor, *supra* note 270, at 513.
[290] Schwartz, *supra* note 178.
[291] Victor, *supra* note 289, at. 515-516.

doi:10.6342/NTU202301113

刪除權等，都跟財產規則下的財產回復請求權（Injunction）以及懲罰性賠償金（Punitive Damages）相類似[292]。

從上述討論或許可總結說這個「資料財產權」的主張，在其「可轉讓性」也受到相當程度的限制時，其實也跟一般有體物的「財產權」想像不同，而現行歐盟個資保護規則的發展，像是可攜權、刪除權等，某種程度確實也很像個人對於傳統財產的控制[293]，因此也不難理解為何會出現上述認為兩個進路（無論是稱之為財產權、或不以財產權稱之）殊途同歸的看法，此時似乎是否認為其係「財產權」僅是一種概念法學之爭，而喪失實質上的意義。

第六項　中國學者主張

前述介紹完美國的學說見解，並與歐盟的個資法制做了簡單的比較，由於在蒐集文獻時發現中國學者對此議題也有評論，故以下簡單介紹之，使討論更加充實。

美國及歐洲的立法上大多聚焦於個人資料的保護，大多將資料蒐集者理解為隱私的潛在侵犯者，雖然 Lawrence Lessig 提出資料財產的概念，然而並未受到學界太多重視，不過近年在中國這項議題引起了許多討論，尤其是針對大數據屬於國家發展基礎資源的角度上，討論了許多關於非個人資料權利歸屬的議題。

其文獻主要討論範疇是針對非個人資料，像是企業生產數據、網路爬蟲數據等資料應如何建立起法制。雖然不特別指涉關於隱私財產權的部分，不過部分關於數據的性質描述仍具有相當參考價值，另外中國方面在用語上多採用「數據」而非「資料」，為免混淆不再進行轉換，統一使用原文文獻的用語「數據」，兩者內涵相同僅用語有異，先行敘明。

---

[292] *Id*, at 523-526.

[293] 周林彬、馬恩斯（2018），〈大數據確權的法律經濟學分析〉，《東北師大學報》，292 期，頁 35。其等也認為所謂被遺忘權本質上是默認個人對個資享有佔有權的前提下所產生的一種返還佔有請求權，是典型的物上請求權。

doi:10.6342/NTU202301113

第一款 具體主張

其中也有認為不該糾結於權利定性、歸屬者，認為數據的所有權遠沒有使用權重要。與其追問數據權利歸屬，毋寧辨明數據行為的邊界[294]。但也有像是劉小紅等認為數據財產權是權利主體參與分配的關鍵，也是權利人對其所有或控制的數據享有占有、支配、流通和分配關係的法律表現。數據的非獨立性或依附性並不能掩蓋其財產屬性。數據是一種特殊的財產，既不同於有形財產，也不同於智慧財產權等無形財產，兼具人格屬性和財產屬性，依據洛克的勞動財產權理論，數據加工過程的各參與者皆能主張分配的權利。

不過劉小紅也提到基於自由市場跟數據本身的特性，數據的受益分配可能會有不公平的可能，像是一般人對數據加工、使用等技術陌生，導致數據利用的透明度低，效益的生成及其收入分配就會容易形成「黑箱效應」;又或者是當數據與其他生產要素的交錯導致數據作為生產要素的獨立性受到挑戰，特別是當數據和演算法作為人工智慧發展的共同要素時，人工智慧的比重與其所利用的數據間分配缺少合理的分潤機制；最後則是在大數據時代下，數據價值在各領域壟斷的大公司將更容易發揮規模優勢、技術優勢，造成在收入分配中參與主體力量的對比失衡，阻止公平價值的實現。因此即使加工過程的各參與者皆能主張分配，分配結果可能會有未盡公平的情形[295]。

另外就數據的法律定性上，程嘯也持類似見解，認為數據應當作為民事權利的客體[296]。一方面這會使得自然人有權控制個人資料，從而能防止個人資料被洩漏和非法利用所引發的一系列問題。另一方面，數據處理者也可以藉由將數據當

[294] 許可（2021），《數據要素市場的大哉問》，載於：https://ppfocus.com/sg/0/te71a8d59.html（最後瀏覽日 06/16/2022）。
[295] 劉小紅（2020），〈數據按貢獻參與分配實現的法律意蘊〉，《月旦民商法雜誌》，70 期，頁 77。
[296] 程嘯（2018），〈論大數據時代的個人數據權利〉，《中國社會科學》，3 期，頁 106-107。

doi:10.6342/NTU202301113

作民事權利客體的手段，將自己蒐集、儲存的數據加以壟斷控制，以進行投資挖掘其中所蘊含的巨大價值。

不過程嘯認為個人數據權跟企業數據權必須做差異規範，就個人數據權而言，並非如物權般的絕對權，只有防禦的功能，像是知悉個人數據被收集、被基於何種目的而加以收集，以及使用的目的、方式、範圍；知悉個人數據被轉讓並在未經同意拒絕轉讓的利益；查詢個人數據並在個人數據出現錯誤或遺漏、缺失時有權要求刪除、更正或補充的利益。不承認個人擁有積極的財產上權利的原因在於在絕大多數的情形，人們根本沒有意識到自己產生了怎麼樣的以及多少數量的個人數據，遑論對其加以收集並與以變價。且大數據時代與以往的很大不同在於，個人數據正在以前所未有的數量跟種類被產生、收集、儲存、利用，是網路科技的產生跟大幅發展，才使得很多個人數據（網路交易資料、網路瀏覽資料、網路社交資料等）得以被收集並加以儲存[297]。

至於企業數據的部分，其認為企業對其合法收集的個人數據的權利不應該建立在自然人對個人數據權利的基礎上，或認為是派生於政府的授權許可，而應當立足於大數據時代數據活動的實際情況，肯定這種權利是原始取得的權利，並將之作為絕對權，賦予跟物權同等程度的保護，唯有如此，才能在個人數據上建構一個既能有效的保護個人權益，又能充分維護數據活動自由的民事權力格局[298]。

而李愛君則近一步比較了數據跟無體財產權的差異認為[299]，實體物透過占有，無體權利則是透過授權表彰控制，數據非智慧財產權，蓋數據不需有獨創性，不具有期限性、沒有法定性（權利範圍不用經過申請、審查、公告、批准等法定程序）。但數據也非有體物，蓋數據不具有物理壟斷性，可以輕易地被複製。相較於有體物所有權通常具有完整的所有權使用、收益、交換、完全排他等面向，數

[297] 程嘯，前揭註 296，頁 115。
[298] 程嘯，前揭註 296，頁 122。
[299] 李愛君（2018），〈數據權利屬性與法律特徵〉，《東方法學》，3 期，頁 67。

doi:10.6342/NTU202301113

據權利卻時常是分散而不完全的。又，雖然數據跟營業秘密多少有些相像，但並非所有數據都是營業秘密（營業秘密必須有價值、屬於該領域秘密、且受到保密手段保護）。

李愛君認為數據屬於民事權利客體。有財產權（有價、可轉移）、人格權、以及國家主權的性質共同存在。制度建構上他討論了公平法途徑跟數據財產權建構途徑，其認為透過公平法或數據財產權建構制度雖然最終都是為了增進社會效益，但具體上，透過公平法調整的法律關係是經營者與其他經營者的關係，直接保護的是市場競爭秩序等公益；而數據財產權所調整的法律關係則不限於經營者之間，重點是權利人的私益。也就是說公平法只能對抗市場中的商業主體，但數據財產權可以對抗其他一切主體。但在認定標準上，公平法是概括條款，內容較空泛，且認定違反的主觀性較強，執法也比較不可預測，因此透過公平法中保護營業秘密的條款來保護數據財產是不妥的。

趙雲等人將主體分為資料使用者(Data Users)、資料處理者(Data Processors)、資料購買者(Data Purchasers)，後二者屬於資料控制者。在資料尚未去識別化、一般化之前，資料使用者應對該資料有所有權、控制權，但當資料處理者為該資料經上述手段附加商業價值之後，則會由資料處理者取得所有權。如果該附加價值的資料再經轉手，則又會屬於資料購買者所有。因為去識別化及其他資料處理讓資料產生附加價值，才使得資料有財產權的性質，這個財產權並不同於傳統財產權，而有必要以資料財產權稱之[300]。此一財產權可以獨佔使用、收益及拋棄，配套措施是交易安全跟交易者必須可歸責，而劃定哪些資料是屬於可交易的將有助於防止資料洩漏。結論上其等認為應以人格權、財產權雙元保護模式針對資料立法，必須有基於契約的精神及懲罰性賠償，另一方面應該採取過失推定的侵權責任，讓資料控制者負證明無過失的責任[301]。

[300] Xiaolan Yua & Yun Zhao, *Dualism in data protection: Balancing the right to personal data and the data property right*, 35 COMPUTER LAW & SECURITY REVIEW 5, 6 (2019).
[301] *Id.* at 10-11.

doi:10.6342/NTU202301113

第二款　　小結

從上述中國學者的文章中可見，中國學者聚焦的乃大數據權利，也就是不限於個人資料，包含其他已去識別化的個資、工廠生產資料等非個資資料。其等會區分個人資料與非個人資料並對其法律定性做不同規範，並著重於權利歸屬與分潤的機制。其等指出了資料財產權與傳統物權、智慧財產權的不同，卻又認為必須賦予資料權一個獨立的民事上權利地位以保障不論是個人或是企業在數據經濟下的利益，不過在論述中似乎可見其等對於企業的數據權更加重視，並著重非個人資料的挖掘、利用。

第七項　本節總結

本項介紹了美國國內與資料財產權相關的立法、實踐、以及學說上正反的學說見解，並與歐盟 GDPR 對照發現此一理論與 GDPR 的某種相近性，最後介紹了一點中國學者的見解，凸顯同一資料財產權問題，但著重於非個人的不同面向。由於本文的焦點在於如何為個人對其個資、或去識別化個資賦予更多控制，因此焦點仍會聚在美國法上關於資料財產權的正反意見。

綜上所述，可簡單總結多半學者其實並不認為隱私權跟財產權（責任規則與財產規則）是一個二擇一的定性問題，縱然定性成財產權，仍有財產權可轉讓性要在多大程度上受限制、隱私侵害本身不容易被發現、交易成本過高、機構代理問題、個人欠缺救濟上誘因、公權力的角色及應盡之市場管制義務等問題。個人對個資、零碎去識別化「個資」的掌控不足或是希冀藉由財產權理論向企業尋求賠補償的動機雖然在直觀上合理，但實踐上無疑仍有許多困難必須克服。至此大約可有一個粗略的想法，就是具體制度的設計可能重於權利本身的定性，就算說個資具有「財產權」，此一「財產權」的理解也與傳統的財產權理解不同，此時是否要重新為此一權利命名？還是擴張財產權底下分肢概念如智慧財產權、物權去將個人資料納入此一體系？以下於本節第三項細究之。

doi:10.6342/NTU202301113

第三節　資料財產權更細部的區分

由於前述介紹的美國法對資料財產性格的討論大抵都是針對資料移轉規則是否應採取事前磋商議價的財產規則、或是泛論是否應肯認「資料財產權」並納入現行財產權體系中保障，並沒有仔細的去區分資料在「財產權保障體系」下的其他可能，也就是前述大多僅針對資料在人與人之間的動態關係，而並未針對資料本身更細緻的法律性質討論（例如：究竟係哪種財產權？）。而這個問題之所以在我國的討論脈絡重要，是因為我國對財產權的保護其實不是司法實務者說一句「資料具有財產權屬性」即足，例如過往研究即認為，財產權在我國民事私法體系並非具有特定內涵之法律概念，法律所保護者是特定的權利，如所有權、債權、著作權等，因此最終途徑上還是必須仰賴立法的明文承認[302]。

另外，前述對財產權的想像雖未明說，但美國法上以其等以完全轉讓、賣斷的論述假設前提下，似乎背後的假設都是以買賣為交易關係的所有權形式，這樣的討論似乎稍嫌狹隘，蓋資料本身的法律性質定性在「財產權」的概念下其實存在許多可能，以下將簡要探討：

第一項　資料為有體財產權？

典型對資料的想像源自於「數據挖掘」的概念，很多人認為數據相當於這個世紀的新石油，然而資料並不像石油或是一般有體物有著典型財產的稀缺性（Scarcity）、競爭性（Rivalrousness，指A在使用時，B就無法使用），這樣的觀點已經被一些學者所點出（整理如表二）[303]。這樣的特質產生最主要的問題就是資料權利的歸屬難以分配，也就是說當一筆資料同時涉及複數人時，究竟資料

[302] 黃松茂，前揭註 164，頁 252。

[303] Lauren Henry Scholz, *Big Data is Not Big Oil: The Role of Analogy in the Law of New Technologies*, 85 TENN. LAW REV. 863 (2021). 其認為不該將資料的性質在邏輯上、法律上都跟石油天差地遠。另外其他指出資料的非獨享、非互斥、非競爭性者還有 ROBERT D. COOTER & THOMAS ULEN, *supra* note 259, at 44-46.

doi:10.6342/NTU202301113

的控制權利是分別共有（得以各自處分應有部分）？公同共有（處分需經過多數同意）？還是任一主體沒有釋出權，僅有拒絕資料釋出被處理、利用之否決權[304]？問題的核心就是在資料涉及多主體時，各主體間得否及如何共同編輯、共同享有權限的問題。

表二、相異處[305]

	資料	一般有體物（以石油為例）
稀缺性	持續產生	天然生成、有限
使用之邊際效益[306]	與其他資料交互運用，邊際利益會增加	遞減
競爭性	同一筆資料可「同時」被不同人利用[307]。	無法「複製」、「同時被多人所利用」、使用後燃燒不可逆
可替代性	不可替代、資料有獨特性	可替代、各地的石油功能上相同
與主體之關係	沒辦法專屬於個人，或僅與個人相關，可能會與單、複數人在未來相關。	不與人相關，至多僅單純所有關係。
利用方向	企業、政府追蹤、交易、分析。	自然資源的開發

[304] MacCarthy, *supra* note 134. 文章中提到這是 Larry Downes 的觀點。
[305] Partially summarized from Scholz, *supra* note 303.
[306] MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA AND COMPETITION POLICY 200-201 (2016); OECD, *surpa* note 138, at 34.
[307] Mell, *supra* note 244, at 69.

doi:10.6342/NTU202301113

型態	甚至不是無形資產？	有形資產
誰擁有	難以界定、資料本身沒有地域性，有體物的產權分配無法提供資料權利歸屬分配參考。	通常是國家，擁有規則是屬地原則。

第二項　資料為無體財產權？

第一款 學說介紹

Julie E. Cohen 提到主張應該「承認可識別個資具有財產權」的有兩種人，一是為了蒐集取得資料所有權的數據處理商，二是一些認為這能賦予個人更多控制、取得金錢對價補償的學者，但其認為這樣的主張並無法涵蓋個資的所有面向[308]，且會讓我們對於個資的想像窄化成異於身外之「物」[309]。

僅管可交易性可以被限制，或是讓個人存有一些不可交易的優先控制權，如同智慧財產權人有對其著作的一些不可轉讓的控制權利般，然而個資的保護目的跟智慧財產權的保護目的並不相同，賦予前者財產權地位的理由在於，經濟理論上是基於個人就個資的談判交易成本較大，因此才將初始資料權利指定給個人所有，而賦予後者財產權的理由是在於智慧創作具有公共財性質，必須透過公權力立法保障才能促進創作與社會最大效益。個資在此一方面與智慧財產權相比，顯然並沒有同等重大的公共財特質，相對的，其價值是可以由私人蒐集取得的[310]。

不過 Cohen 指出當前智慧財產權的發展隨者科技進步，越來越容易對於無形資產的使用附加限制，與目前難以對個資後續利用施加限制的法制現況對比，

[308] Cohen, *supra* note 253, at 1378.
[309] Cohen, *supra* note 253, at 1379. 但 Cohen 確實提到窄化成物的優點在於權利邊界相較於「人性尊嚴」來的清楚。
[310] Cohen, *supra* note 253, at 1387.

doi:10.6342/NTU202301113

可以發見我們社會對個人主張個資的重視、或是對於個資保護價值的重視，都大大少於對於出版商及資料處理者所主張智慧財產權的重視[311]。資料蒐集者持續從個人身上奪走了一些屬於個人的經濟利益，這份價值轉移不但沒有被凸顯出來，更沒有合理的正當理由足以正當化。很多時候我們所聽到關於「賦予個資財產權」將會延伸過高的「交易成本」並「有損效率」的抗辯，事實上是過於簡單的化約，交易成本是制度設計的一個工具，何謂有效率應該要以社會的角度思考之[312]。

雖然將個資財產權化可能會促進更多的個資交易，而非更多的隱私，然而若參考智慧財產權的轉讓限制架構，不採取「賣斷制」的隱私交易架構，就有可能提供個人更好、更持續的對個資的控制，財產權架構可以同時是緊密、帶有連續控制、且有效率的[313]。

由上可見 Cohen 應該可以被歸類為認同將個資類同智慧財產權保護途徑的學者，無獨有偶的，其他像 Bergelson 也認為定性成無體財產權似乎比定性成有體財產權更接近一點[314]，蓋兩者都是無體、非稀缺性、非可替代、不具競爭性、且有經濟上價值者。

然而定性成無體財產權最大的困難在於，「創新性」的欠缺，蓋個人資料有時候僅係事實爾，而從權利創設目的論，也可見智慧財產權的目的是外部的，也就是著重公開，但數據分析則是著重內部利用、不公開的；再者，著作要有原創

311 Cohen, *supra* note 253, at 1389.
312 Cohen, *supra* note 253, at 1390.
313 Cohen, *supra* note 253, at 1391. 周林彬、馬恩斯，前揭註 293，頁 32。「將大數據界定為財產權和人身權意味著截然相反的資源稀缺度，將大數據界定為知識產權或物權也意味著截然不同的制度成本，前者限制交易而後者鼓勵交易」。雖然周跟馬氏同樣認為財產權化會促進更多交易，不過其等認為在債權、智慧財產權、物權等制度選擇上，應以物權賦予數據權，效率會最高，主因在於債權容易形成壟斷與不正競爭，交易成本高，而智財是以限制利用鼓勵創新，與數據強調共享、交互利用不同。詳參同註，頁 33 以下。
314 認為個資跟智慧財產權中的著作權很像者有 Bergelson, *supra* note 237, at 436.但美國著作權法所保障的是具表現性的工作產出，而非其背後單純的點子或事實。

doi:10.6342/NTU202301113

性、專利要有新穎性與進步性，數據則不然。最後，數據財產也不像智慧財產具有期限性[315]。

再者，有認為承認個人資料是財產權，相當於是承認個資為一種新型態的智慧財產權，但這項新型態的智慧財產權將會比傳統的更廣且定義更模糊[316]。甚者，具體來說，就有認為承認個資中的財產權利將會使得現行智慧財產權領域中不具有著作權性質的事實被重新拿出來爭論是否具備著作權性質，並對既有著作權體系造成混亂[317]。有認為目前著作權保障的是資料蒐集者聚集成資料庫的排序、整理價值，與隱私所欲保障的個人人格圖像控制、避免不當取得、利用，並不相同，個人隱私及特徵並不是個人的創作產出，並不受到著作權保障[318]。

另外，也有認為基於資料累積的效果，資料的價值有時難以顯現，或是一直呈現非常浮動的狀態。像美國聯邦法院就因資料跟不同東西結合，或用不同演算法運算的結果即會產生不同價值[319]，在數據不可被特定及準確評估價值的情形下，認為數據並非無體財產，僅可能構成營業秘密而已[320]。

然而單一個人所擁有的個資很可能難以滿足營業秘密應具備的「有價性」要件[321]，蓋單一數據可能難以被認為有商業價值，僅組合起來的資料庫才有足夠商業上價值，進而有成為營業秘密的權利客體的可能。

---

315 朱宸佐，前揭註 254，頁 143-145。

316 McClurg, *supra* note 217, at 92; Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1065-73 (2000).

317 *See* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1294-95 (2000); Samuelson, *supra* note 324, at 769-72; Samuelson, *supra* note 142, at 1140-42.

318 Mell, *supra* note 244, at 66-67.

319 Andy Patrizio, ***Why*** *Your Big Data Needs Good Algorithms,* DATAMATION (Nov. **25, 2015),** https://www.datamation.com/data-center/why-your-big-data-needs-good-algorithms/.

320 Scholz, *supra* note 304, at 879; Feist Publ'ns, Inc., v. Rural Tel. Serv. Co., 499 U.S. 340, 361 (1991) 該案中電話簿中的姓名跟電話號碼被認為僅是事實不是值得保護的智慧財產權； *re* TXCO Res., Inc., 475 B.R. 781, 804-05 (Bankr. W.D. Tex. 2012) 在該案中資料庫僅可能在州法下被當作營業秘密保護。認為資料庫屬於營業秘密者可參考：Walter W. Miller, Jr. & Maureen A. O' Rourke, *Bankruptcy Law v. Privacy Rights: Which Holds the Trump Card?*, 38 HOUS. L. REV. 777, 782 (2001).

321 European Commission, *Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, SWD(2017) 2 final (Oct. 1, 2017), 20, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0002&from=EN. 一般認為營業秘

doi:10.6342/NTU202301113

不過也有認為比起如其他智慧財產權體系般，透過財產權賦予資料在使用方面排他性的絕對控制，歐盟營業秘密法從侵權角度禁止特定取得、散布、使用等不正行為反而較能平衡資料保護與資訊自由流通間的關係[322]。基本上認定成營業秘密與僅認定為財產權是完全不一樣的保護模式，前者要求資料創造者採取合理措施以確保資料秘密性，後者則是禁止所有產生的數據在未獲得同意限制或例外的情形利用[323]，究竟是否有必要引介營業秘密模式以保護個資，仍有所爭議。

最後，其他也有認為若將隱私納入智慧財產權體系保障將會有損於智慧財產權體系的完整性，蓋隱私並不要求要能促進科學與實用技藝的進步[324]。再者，傳統美國法上在憲法第一修正案的前提底下，非常重視資訊的自由流通，像最高法院就曾於 1991 年否定電話黃頁排序的著作權主張。甚者，市場派的經濟理論學家也認為資訊的自由流通才能使得市場完全競爭。以上種種主張都使得在美國主張資訊財產權去類同智慧財產權途徑將會面臨巨大困難[325]。

第二款 「發現」與「創造」，誰取得財產權？

營業秘密法及著作權法之所以賦予所有權人此一關於抽象資訊的財產權，有一說即是因為該抽象資訊具有某種程度的「創新性」，是憑空而生，是為了獎勵其創造。對比個人資料（包含基因資訊），此時可以發現個人資料的財產價值在這一觀點上並不是源自於個人的「創造」、「努力」、「思考」，反之是企業所投入的蒐集成本、分析成本，才真正現實化了這份財產價值。

密有三構成要件：秘密性（相同社群間通常是否知悉標準）、因秘密性而生的商業價值、以及是否採取保護措施。

322 Josef Drexl, *Designing Competitive Markets for Industrial Data-Between Propertisation and Access*, 8 J. INTELL. PROP. INFO. TECH. & ELECTRONIC COM. L. 257, 291 (2017).

323 Yu, *supra* note 282, at 899.

324 Pamela Samuelson, *A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy,* 87 CAL. L. REV. 751, 776 (1999); U.S. Const. art. I, § 8, cl. 8; see also Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1246-58 (1998).

325 Samuelson, *supra* note 324, at 770.

doi:10.6342/NTU202301113

因此如果很簡化的說，智慧財產權之所是財產權是在於其「創造」，而個人資料之所以在某些觀點下不是財產權，就是在於其是「被發現」價值而非主動「創造」價值。這點關於「發現」與「創造」間的幽微差異，才是造成一則被認為係屬財產權，一則被認為非屬財產權的原因，本文認為其他學者所提出的「不可耗盡性」、「無體」、「難以表彰佔有」、都不是真正區別兩者應該為差別待遇的合理理由[326]。

	資料	無體財產權
相同處	無體、非稀缺性、非可替代、不具競爭性、有經濟上價值。	
與人格權近似度	高，倘屬個人資料則無法拋棄，僅得授權範圍內使用。	像是著作權下有保障公開權、改作權，人格權屬性高
關於第三方利用的態度[327]	資料發展較強調資料的快速移轉、蒐集、分享	賦予財產權會形成獨佔、阻礙合作與進步[328]。
創新性	資料利用、處理者對於所處理的資料只是經手欠缺與無體財產權最重要的要素「創新性」	必須具備創新性才可被承認受財產權保障。

[326] 程嘯，前揭註 296，頁 106。「知識產權的權利人具有較高程度的易受侵害性。但這並不妨礙法律上為鼓勵更多的發明創造而確立知識產權制度，如賦予著作權人以發表權、複製權、發行權、出租權、展覽權、表演權、放映權、廣播權、信息網絡傳播權等人身權利和財產權利，從而確保權利人對作品的控制。因此，就數據能否作為民事權利客體的問題，關鍵不在於數據的自身的特性，而在於法律是否有必要將其作為某種民事權利的客體。換言之，即便數據具有非獨占性的公共物品的屬性，但基於某種需要與價值判斷，立法者依然可以通過法律規定賦予民事主體對數據某種壟斷的專屬權利而人為地製造稀缺性。」

[327] Michael Mattioli, *The Data-Pooling Problem,* **32** BERKELEY TECH. L.J. 179, 179 (2017).

[328] Nathan Newman, *Search, Antitrust, and the Economics of the Controlof User Data,* 31 YALE J. ON REG. 401, 435, 450-54 (2014).

doi:10.6342/NTU202301113

第三項　資料為公開權？

公開權乃個人得用以控制其姓名、肖像、聲音、簽名或足以識別其身份之其他特徵之商業運用的權利[329]，與資料的性質比較異同如下：

	資料	公開權
性質異同處	資料的非法利用未必需要公開。	請求基礎必須公開使用。
立基	個人資料：個人尊嚴	財產權，類似商業利用權（著作權、商標權）
保護範圍	傳統隱私行動軌跡、書信內容等低價值資料也會在保護範圍內。	實踐上易受限於高商業利益的名人姓名、肖像、聲音等。
救濟	資料的損害賠償不容易顯現在單次違法利用上（資料累積的效果）	易對每次侵害請求損害賠償

第四項　其他可能？

[329] 王澤鑑，前揭註 166，頁 311。

doi:10.6342/NTU202301113

至於其他關於資料本身性質的看法還有認為醫療資料應該屬於基礎建設者[330]、蓋基礎建設的特色在於其非競爭性、本身無價值但對下游需求有幫助、以及得以用其完成私人、公益產品。這樣的主張於本文來看大約是將資料當作公共財，不過關於這項的理論的其中一個挑戰在於基礎建設的定義則存在歧異[331]。

另外在資料與人的互動關係上，有認為資料蒐集者與資料主體間是類似海難救助者的關係[332]，其認為資料蒐集、處理者就像是在大海上去救援船難的搜救者，在茫茫數據海中挖掘殘餘價值，對於其因為數據挖掘所創造的價值，資料主體或其他關係人雖然才是主體，但救難者應該可以分一杯羹，其認為從社會效益的觀點觀察，這或許是一個讓參與者都能分配到利益(雖然可能很複雜，且未必公平)，又能促進資料流通的方式。本文認為這是描述資料利用關係的理論，其雖然沒有明確肯定資料作為財產權利，但隱約同意資料的有價性於受利用時須受補償。

最後也有認為資料主體與資料蒐集者間屬於投資關係者[333]，其主要論點大約是投資者與消費者不同之處在於，投資是持續性關係，投資人可享有資訊請求權，監督公司運作的權利，這部分就會類同現行個資法資料主體對於資料後來如何被利用的監督權，因此與其說資料主體是消費者用自己的資料向公司購買服務，不如說資料主體本身就入股，文章也針對個人資料跟非個人資料作出區分，其認為個人資料對公司來說應屬於債務，有嚴格的保護規範，且得經要求後刪除；至於非個人資料則被認為是股東權益，公司應發行有價證券以換取此類資料，不過最重要者在於文章認為，即使在資料主體同意提供資料予公司後，仍會保有些許財產上利益（這邊對財產權採取容許限制轉讓性的寬鬆見解，認為同意提供予公司並沒有等於移轉全部財產上利益）。

---

330 W. Nicholson Price II, *Risk and Resilience in Health DataInfrastructure,*16 COLO. TECH. L.J. 65, 67 (2017).

331 *What Is Infrastructure? Definition and Examples,* MARKET BUSINESS NEWS (MBN), https://marketbusinessnews.com/fmancial-glossary/infrastructure-defition- means/.

332 Scholz, *supra* note 303, at 890.

333 Kim, Tae Wan et al, *Data and Manure: Are Data Subjects Investors?*, 18 BERKELEY BUS. LAW J. 65 (2021).

doi:10.6342/NTU202301113

第四節　本文見解

第一項　回應對資料財產權理論之批評

本文認為翁氏的介紹著實鉅細靡遺，惟其既一方面贊同不應賦予資訊隱私財產權地位，卻又說該概念有值得借鏡之處，究竟所指為何，似仍有釐清之必要。本文認同倘若引進財產權的概念於隱私權中，無疑是很難用傳統「所有權得自由移轉」的角度去移植套用於資訊隱私權，然而財產權的理解未必要僅限於自由移轉的角度去理解，仍有「僅租不得賣斷的」類似地上權、役權的面向可資援用[334]，像是前述 Kim 等用投資關係、Suter 用信任授權關係分別看待資料利用關係的理論，就皆是從資料利用關係乃「繼續性、持續性」的角度觀察。從此一角度出發有兩項考量點，一是得以確保人格、個人歷程(Profile)不成為失去掌控的客體，二是只要未來當事人發現不對勁，永遠享有中止同意的權利，這正好符合資料利用關係是一個繼續性關係的本質。

本文幾經搜尋發現其實美國法上也有類似的主張，像是 Basho 就認為應該依據《統一計算機信息交易法》（Uniform Computer Information Transactions Act, UCITA）建立一套個資授權體系，此一授權係可撤銷、非賣斷、授權內容包含提供資訊的內容、使用資訊的限制、應得的補償，以及第三人利用的規則，一但被

[334] *Id,* at 84. 該篇認為如果資料移轉後的控制權不屬於財產權的一部分，那麼就只能解釋成資料主體自始都沒有移轉資料所有權予該企業，此時資料主體就會是類似資料出租人、或貸方的角色，作者認為這樣所賦予的控制並不會輸給認定資料移轉是財產權移轉，而且反而更強。

doi:10.6342/NTU202301113

授權方違反規則，授權方就可以撤回授權[335]。這樣的授權體系正是建立在個人（消費者）對於其個資具有財產權的基礎之上[336]。

且正如同著作權被承認為財產權的歷史，以及其後續所發展出的「本人享有一定拒絕改作權」一般，財產權化反而是更強化個人自主權。況且群體中有些人可以選擇出賣個資，有些人則可以選擇過拒絕出賣的生活，這相比將隱私權政策交由政府或機構在多方折衝下訂立一個低標準但全體適用的隱私權規範，或許是一個讓個人「更自由」、「更客製化」去決定自己的隱私利用的方法。因此縱使不包含自由移轉的特色，其實並不會減損引入財產權概念所帶來的益處。

至於關於財產權的賦予可能帶來的資訊不對稱、市場失靈、交易成本過大、言論自由受到限制等等批評，除了前述提及的 Cofone 對財產權化後市場地位不均的質疑外，美國隱私法學者 Julie E. Cohen 也認為[337]凸顯財產權性格無助於加強個人的自主與社會參與，因為在個人渺小的基礎下，就算有財產權作為靠山，仍會在市場上受到談判力量、資訊懸殊的影響而無法發揮自主，再加上如果在蒐集初的目的無法精確特定的情形，更容易將被蒐集個資的個人打入談判弱勢的一方。

本文對此的回應如下：首先，這牽涉到我們對於市場要介入多少的政策選擇，如果認為市場會有所不公，應該是要去管制市場而非自始自終否定市場的存在。再來關於資訊不對稱，其論理乃資料的利用沒辦法在授權之初就確定，而蒐集方的利用利益則是一開始就特定，因此雙方會有資訊不對稱以致賣方受到不公平對

---

[335] Kalinda Basho, *The Licensing of Our Personal Information: Is It a Solution to Internet Privacy?*, 88 CAL. L. REV. 1507, 1525 (2000). 只不過應注意者係授權體系並非萬能，財產權下的授權體系並無法解決市場力量不對等、資料蒐集者與個資主體資訊、談判力量不對稱的問題。舉例而言企業有可能會利用拒絕提供服務、或提供價格優惠等方式驅使消費者選擇低度隱私保護的授權約款，Basho 就此提出的解決方案並沒有別出新意，與大多數學界相同，採取個資代理人、情報仲介(Infomediary)的方式，替個人評估個資價值、談判磋商授權條款、監督企業、網站合規履行個資授權約款。See *Id,* at 1527-30.

[336] *Id,* at 1526-7. 不過 Basho 確實點出幾點關於隱私財產權可能必須面臨的挑戰，像是財產權的範圍究竟應該多大？資訊能在多大程度上被控制（個人能完全掌握每一份關於自身的個資流動）？還有延伸出的交易成本問題（現存既已流通於資訊市場的姓名、地址、聯絡電話如何處理？）。

[337] Cohen, *supra* note 253, at 1381, 1391.

doi:10.6342/NTU202301113

待的情形發生。本文認為這樣的狀況並不僅是出現在資訊被賦予財產權之後，在現行的體制下，蒐集資訊時的告知後同意一部分被大力批評的原因也與此雷同，這乃隱私蒐集內在必定存在的難題，因此光憑資訊不對稱其實並不足以拒卻財產權概念的引入。

接者，關於假如讓個人都擁有資訊財產權將會使得企業蒐集、或公益研究的交易成本過大而有損社會最大利益的說法。本文認為第一，這些關於交易成本的論述目前仍屬理論階段，而未有實證研究支持[338]；第二，難道目前的告知後同意模式、專責機構、事後撤回權等就不存在交易成本嗎？所謂的交易成本難道僅限於得以金錢去具像的成本嗎？正因為目前的制度也必須尋求當事人同意或以抽象公益去正當化去平衡人格權與公益，因此若要說當前制度的交易成本相較於賦予財產權的隱私資訊來的低，或許還是不夠嚴謹。第三，財產權仍有社會義務的面向，因此縱使引入財產權的概念，並不當然會導致以後任何公益目的研究都必須付出更高的協商、取得同意授權的買入資訊成本，甚至說如果該類資料具有重大公益（例如：欲運用健保資料庫建立之健康大數據平台[339]、目前由公股銀行主導的開放銀行 API 平台嫁接[340]等等。）參照前述所介紹的 Price 教授的見解，將該類資料當作如公共財般的基礎設施（infrastucture）也未嘗不是解決之道。因此關於交易成本的批評，本文認為並不足以拒卻本項概念的引入。

最後關於新聞言論自由將因此受限的論述，本文認為同樣問題也是一樣存在於當前的隱私制度中，當前隱私權的概念相當程度也跟言論自由產生衝突。典型認為的衝突是新聞自由遭受限制以致監督公益功能不彰，或是政府、企業資訊不

338 同樣也未有實證研究發現，如果賦予個人對去識別化（匿名化）健康資訊一定程度的自主控制權，就會無可避免地導致生醫研究被阻擋。*See* Rothstein, *supra* note 51, at 10.

339 科技部生科司（2021），科技部生科司 110 年度健康大數據永續平台之「建置轉譯導向生醫巨量資料」詳細計畫書申請須知，載於：https://www.most.gov.tw/most/attachments/cd750957-fc6f-4fe5-8052-ff6615a0ba37（最後瀏覽日期：2021/06/26）。旨在建立臨床資料數據資料庫，包含「病理資料」、「基因體資料」、「影像資料」，並結合家族史、生活形態如飲食運動等「結構化電子病歷資料」，追蹤治療副作用、存活率等治療史，以利後續臨床資料庫的結構化應用。

340 工商時報（12/31/2020），〈開放銀行第二階段 2 團隊入榜〉，https://www.chinatimes.com/newspapers/20210101000237-260202?chdtv.

doi:10.6342/NTU202301113

夠公開，甚至有虛偽隱匿的權限，以致社會效益減低。上述當然有其質疑的道理，然而隱私權跟言論自由的衝突並不僅止於此，對於個人而言，倘若沒有隱私權作為維護其內在人格獨立發展的最後一道界線，其所為的言論也難保是自由的。因此隱私權跟言論自由的關係絕對不是單純點出衝突如此簡單而已，其比例權衡調適衝突的面向實需要更多討論，而本文並不認為財產權化後會帶來多少的不同。

第二項　強化資訊隱私財產權性格的益處

回應至此，或有認為本文的回應僅說明了資訊隱私的財產權化並不比當前制度來得差，而未有甚麼非選擇此一概念的必要，因此本文以下將正面建構強化資訊隱私財產權性格的益處。

關於財產權可能帶來的益處，除了前述翁氏整理美國學者所提出的「直觀上最符合人民對控制權的想像[341]、具有經濟上的誘因足以促進權利行使[342]、將蒐集方的利用成本內部化[343]，具現化了隱私的價值、減少政府官僚體系的干預[344]」等多項優點外，本文認為還有一個——增加人民救濟管道的優點，此一優點其實有點類似於 Cofone 所講的個人就資料利用請求民事損害賠償相關訴訟的促進，不同處僅在於，Cofone 認為這不需要透過強調資料具有財產權就可以達到，而本文認為若強調資料的財產權將更有助於去強化此類訴訟之發展。

舉例而言，在健保資料庫案中，在去識別化已經走入困境，而國家又不將資料蒐集利用的公益目的說明清楚時，除了目前學者所強調地嚴格要求完整的目的說明、以及確實的蒐集利用前通知外，其實存在另一種權利主張方法，亦即透過財產權面向的強化，讓權利主體得以主動藉由其他救濟管道切入。也就是說，如

341 Baron, *supra* note 217, at 367, 380; Janger, *supra* note 240, at 916; Victor, *supra* note 270, at 518.
342 Miller, *supra* note 247, at 141.
343 Samuelson, *supra* note 142, at 1127.
344 Balaban, *surpa* note 275, at 21.

doi:10.6342/NTU202301113

果不能從行政法院中得到禁止健保資料庫資訊轉出的判決，或許可以從健保資料庫的蒐集利用已逾越醫療契約的約定，轉而請求違約金或是損害賠償的角度出發。藉由強調隱私權的財產權性格，作為凸顯隱私權受侵害的救濟方法之一。

從此一角度出發的優點在於，縱使在公法上認為蒐集利用方的行為合法，從而不構成隱私權侵害時，亦得使權利所有人藉由主張隱私財產權因公益犧牲而應受補償的方式，使得蒐集方利用資訊隱私的成本內部化。此一方式或許對該個案無顯著幫助（因為損害已經造成，且隱私損害通常是不可回復），但本文認為此類以金錢補償作為負面誘因的方式，對於未來的案件肯定會發揮促使相關機關進一步注意隱私權保護的功用，如同 Lawrence Lessig 所指出的[345]，財產體制（property regime）優於「責任體制」（liability regime）之處在於，前者要求取得標的物前，應先經協商，而後者則容許先取得標的物，嗣後再以損害賠償方式而支付價金，前者無疑更著重於預防與面向未來性。這類從民事救濟的管道去主張不當得利或是違反醫療契約的損害賠償，無疑是仰賴隱私專責機構把關、或是仰賴行政法院做出判決禁止健保資料轉出外的另外一種賦權於個人的救濟可能。

以上關於這些優點，正適合作為現今人們漸漸不若以往重視隱私權的一記警鐘，因為當隱私不再是抽象的人格、情感利益時，它將變得更具備普遍可理解性，或許就可以讓隱私的概念更深植於人心，因此本文並不認為這是一種人格商品化的展現，縱使真的是商品化的展現，本文也認為如果商品化可以讓人們具體感受到它的無價，或許從結果論上來看並不會貶抑人格，當然，關於這種藉由引入財產權概念，使其具體符合權利主體對資訊隱私的想像，進而讓主體權利意識崛起的過程，或許需要更多心理學上的研究始得以支持。

然而姑且不論引入財產權是否會激發人民對隱私的注重，當代社會中，其實資訊早已是有價，而只是沒有被凸顯而已，無論是科技巨頭的客戶資訊蒐集還是

[345] Lawrence Lessig, *The Architecture of Privacy,* 1 VAND. J. ENT. L. & PRAC. 56, 63-64 (1999).

doi:10.6342/NTU202301113

健保資料庫案裡的研究目的利用，資訊的利用絕非不存在財產權性格，正如同翁氏或多或少地認為市場概念得以借鏡並引入台灣當前隱私權架構一樣，凸顯對價性這頭早已存在於我們所處房間裡的大象，或許正是比健保資料庫案中以抽象公益概念帶過細緻討論的正當化個資蒐集過程，更來得容易說服人。

第五章　　結論

本文從歷史脈絡出發，從我國近年幾個重大的政府資料庫建立案例中，重新盤點資訊隱私權於近年來所面臨的挑戰為機關常以「資料已經去識別化故無涉隱私」的邏輯不獲得同意就進行目的外利用。這一邏輯非但忽視去識別化資料的研究利用仍可能對群體描繪、對個體比對，造成隱私上的傷害，甚者在大數據技術的發展下，即使再高程度的去識別化資料，都可能使個人被再識別，此一科技上的發展造成了去識別化的定義、技術、定位上困境。

定義上去識別化於各國基於歷史脈絡等因素，用語、內涵皆有所不同，有時甚難比較援用而僅得在該國法脈絡下理解；技術上不同去識別化模型存有不同去識別化程度定義，再識別風險的衡量標準與參數也多少存在差異，最重要者係技術上並無「不可能再識別」的定義，而只有風險量值的高低區分。本文在理解到去識別化於定義、技術上難以整合的情形後，認為仍不該放棄整合出單一標準。具體上應區分不同利用目的、不同資料類型、不同個資主體、適用不同授權模式，而具體授權模式下個體也應該要能選擇不同去識別化模型，在最大可允許限度上設計其同意，另外個人也應該要能對不同模型下所生的再識別風險，得於具體量化、統一標準、平易近人的告知後理解，並保有隨時廢止同意、退出、刪除等權利。最後就去識別化的定位，本文認為，應於概念上將歐盟 GDPR 所謂依當時科技、常人努力不可再識別的「匿名化」概念限縮，將該概念跟其他 GDPR 下的個資同意、組織、程序保障脫鉤會較妥適。理由除了當代再識別技術愈趨發達外，

doi:10.6342/NTU202301113

另一理由在於如果不如此限縮解釋，就勢必將永遠忍受資料蒐集方可能會以資料已匿名化為由，據以規避取得同意。本文認為應該在法體系定位上將去識別化手段理解為資安風險管控手段，而非影響個資定義、或影響個資保護規定適用範圍需要討論的前提。再者，也應該將去識別化處理此一資安風控手段本身就視為係個資的「處理」，因此原則上需經個資主體同意，始能較縝密的保障個資。

除此之外，本文雖贊同學者所提出以「動態同意」、「後設同意」等靈活設計使得個資主體得以於個資利用歷程中永保控制，惟本文認為於理論上，何以個人得以對「去識別化（匿名化）個資」存有此一控制，舊有理論欠缺充足說明，故試圖以比較法上資料財產權的觀點挪用補充，該理論較符合個人直觀，可能可以擴張個資定義，增強個人對個資的持續控制，以更完善地解決去識別化困境。

為了徹底分析資料財產權可否「補充」去識別化困境解方，本文先從備具爭議的病歷資訊、基因資訊利用爭議說明起。從中理解到，無論是何種資訊，因為其勢必要附著於某物理實體或電磁紀錄上，因此導致利用時無法擺脫「財產權」與「隱私權」之間的衝突，蓋隱私權於許多情形只能限制財產權的行使，使用受益、交易授權轉出等面向並不受重視。基於此本文從最上位的人格權、財產權區分，重新爬梳了隱私權的定位，結論上本文認為隱私權不像生命、身體等人格權具有高度的人格屬性，反而像姓名、肖像、著作權存在更多財產權用益的面向，且在資料挖掘、利用盛行其道的今日，更有愈趨朝此方向靠攏的趨勢。基於此，討論隱私權用益面向不但可能，且也屬必要。但具體上究竟該從一元論觀點於人格權下討論用益面向，還是從二元論觀點於財產權下討論？本文不採取歐陸法系的概念法學區分，參考學者觀點直接跳過區分討論，進入功能上的可否、優劣討論，像是可否轉讓、授權、交易、繼承等。

最後本文於比較法上梳理了美國法資料財產權主張的由來，發現晚近的主張主要意在對抗來自「私人」的隱私蒐集處理濫用，藉由強調財產權的素樸直觀想像，強化個人權利意識，並有意透過市場機制賦權於個人，讓個人得以在交易前

doi:10.6342/NTU202301113

談判、跳過交易受損害時得以請求賠補償，並輔以政府管制、機構代理等制度設計據以解決無論任何理論都必須面對的侵害不易察覺、資訊不對稱難題。然而對資料財產權理論而言，也有「難以處理市場失靈」、「交易成本過大」等劣勢，尚待科技及立法管制面的解決。

在同時比較歐盟的 GDPR 規範後，本文發現美國的資料財產權主張與歐盟資料可攜權、刪除退出權等規定在某些程度也異曲同工地相似，此或許係因美國欠缺聯邦層級隱私權單獨統一立法之故，不過最重要者係此應證了前述認為隱私權討論須採功能性分類討論，而非概念名詞分類的觀點。在認識到此後，本文認為雖然我國法及我國隱私權去識別化困境與美國法的脈絡稍有不同，然而資料財產權理論以所有權觀點出發，基於人對財產具有控制的素樸想像，應仍有助於建立個人在資料關係中持續性的控制，進而有機會解決前述之去識別化資料如何賦予個人控制的難題。只不過若欲賦予個人對資料的持續性控制，此一理論可能並非唯一解答，其他投資關係理論、信任授權理論、或是如第二章所述，透過擴大個資定義，擴大隱私體系保護範圍，應仍得以對此問題提供解套。

至於其他資料財產權理論中，關於個資利用金錢上補償、允許市場交易、擴大救濟可能等理論特色，本文基於功能性觀點，認為未必需要直接引進理論，即可以逕就可否交易等具體隱私保護措施進行攻防。至於若為強調個資的用益面向，而欲引入該理論，本文認為具體立法上或許得以營業秘密法的模式來規範會較妥適。蓋營業秘密作為無體財產權，性質上與個資作為無體物來說最為接近。其目的皆在避免外洩，在資料經濟的發展下其等也都具有一定經濟價值，僅在創新性的面向上，因個資缺乏「勞動力」、「智慧」的投入，故難以類比智慧財產權模式。不過就此本文認為只是不重要的差異爾，蓋依照洛克的觀點，無論是自有的財產、還是經勞力而得的財產，都應該受到法律同等保障，故只要個資有價，且得以建立歸屬控制，其用益面向就應該受到保障，至於其權利名稱是否要稱作營業秘密並不那麼重要。

doi:10.6342/NTU202301113

參考文獻

一、中文文獻

（一）專書

Brittany Kaiser（著），楊理然等（譯）（2020）。《操弄【劍橋分析事件大揭祕】：幫川普當選、讓英國脫歐，看大數據、Facebook 如何洩露你的個資來操弄你的選擇？》，初版，新北市：遠足文化。

Viktor Mayer-Schönberger（著），林俊宏（譯）（2015）。《大數據:隱私篇：數位時代，「刪去」是必要的美德》，初版，台北市：天下遠見。

王澤鑑（1998），《侵權行為法第一冊，基本理論：一般侵權行為》，初版，臺北：自刊。

王澤鑑（2012），《人格權法》，初版：臺北：自刊。

向淑君（2011）。《敞開與遮蔽:新媒介時代的隱私問題研究》，初版。中國：知識產權。

何建志（2016），《醫療法律與醫學倫理》，三版，台北：元照。

肖莎娜．祖博夫（著），溫澤元、林怡婷、陳思穎（譯）（2020）。《監控資本主義時代（上卷）：基礎與演進》，初版。台北：時報文化。

洪遜欣（1976），《中國民法總則》，初版，台北：自刊。

張陳弘、莊植寧（2019），《新時代之個人資料保護法制：歐盟 GDPR 與台灣個人資料保護法的比較說明》，初版，台北：新學林。

陳聰富（2014），《醫療責任的形成與展開》，初版，台北：台大出版中心。

doi:10.6342/NTU202301113

黃立（1995），《民法債編總論》，二版，台北：元照。

（二）專書篇章

林子儀（2002），〈基因資訊與基因隱私權—從保障隱私的觀點論基因資訊的利用與法的規制〉，收於：Robert Heuser（等著），《當代公法新論（中）－翁岳生教授七秩誕辰祝壽論文集》，頁 693-726，初版，元照。

陳文吟（1997），〈探討美國 Moore vs. Regents of the University of California 對生化科技的影響〉，收於：曾陳明汝教授祝壽論文集編輯委員會，《智慧財產權與國際私法—曾陳明汝教授六秩誕辰祝壽論文集》，頁 221 以下，初版，蔡明誠發行。

邱文聰（2018），〈初探人工智慧中的個資保護發展趨勢與潛在的反歧視難題〉，收於：劉靜怡編，《人工智慧相關法律議題芻議》，頁 153-175，元照。

謝銘洋（1999），〈論人格權之經濟利益〉，氏著，《智慧財產權基本問題研究》，頁 37-62，初版，翰蘆。

（三）期刊論文

王紹睿（2018），〈淺談人工智慧系統的隱私資訊安全保護機制〉，《科儀新知》，215 期，頁 74-84。

朱宸佐（2020），〈人工智慧時代數據財產權的保護路徑〉，《月旦民商法雜誌》，67 期，頁 129-149。

何明諠（2016），〈數位時代的隱私邊界：以健保資料庫與 ETC 交通資料庫為例〉，《台灣人權學刊》，3 卷 4 期，頁 139-153。

何建志（2020），〈COVID-19 疫情期間防疫與隱私之平衡：相關法律議題分析與社會正義觀點〉，《台灣法學雜誌》，387 期，頁 23-32。

doi:10.6342/NTU202301113

吳全峰、許慧瑩（2018），〈健保資料目的外利用之法律爭議：從去識別化作業工具談起〉，《月旦法學雜誌》，272 期，頁 45-62。

吳侑霖、張育瑋、呂佩玲（2019），〈科技執法於易肇事路段之應用－以台 2 線萬里隧道為例〉，《臺灣公路工程》， 45 卷 2 期，頁 14-25。

宋皇志（2018），〈巨量資料交易之法律風險與管理意涵—以個人資料再識別化為中心〉，《管理評論》，37 卷 4 期，頁 37-51。

李崇僖（2020），〈在瘟疫蔓延中檢視個資保護法制〉，《台灣法學雜誌》，387 期，頁 39-43。

李斯壯、黃彥男（2019），〈數位時代之數位隱私保護〉，《國土與公共治理》，7 卷 4 期，頁 30-39。

李愛君（2018），〈數據權利屬性與法律特徵〉，《東方法學》，3 期，頁 64-68

周林彬、馬恩斯（2018），〈大數據確權的法律經濟學分析〉，《東北師大學報》，292 期，頁 30-37。

林志六（2003），〈病歷之所有權、閱覽權與謄寫請求權〉，《醫望雜誌》，21 期，頁 93-95。

林昕璇（2020），〈論大規模政府監控之資訊隱私保障—評析美國聯邦法院相關裁判〉，《台灣民主季刊》，17 卷 2 期，頁 43-93。

邱文聰（2018），〈被淘空的法律保留與變質的資訊隱私憲法保障──評最高行政法院一○六年度判字第五四號判決與相關個資法條文〉，《月旦法學教室》，272 期，頁 32-44。

祝亞琪、魏銪志（2016），〈行動支付之個人資料去識別化方法〉，《電腦稽核》，34 期，頁 18-27。

doi:10.6342/NTU202301113

翁清坤（2020），〈大數據對於個人資料保護之挑戰與因應之道〉，《東吳法律學報》，31 卷 3 期，頁 79-159。

翁清坤，（2018），〈賦予當事人個人資料財產權地位之優勢與局限：以美國法為中心〉，《臺大法學論叢》，47 卷 3 期，頁 941-1051。

馬俊駒（2016），〈人格與人格權立法模式探討〉，《重慶大學學報(社會科學版)》，22 卷 1 期，頁 184-196。

張兆恬（2016），〈人體生物資料庫之隱私權爭議：美國法的啟示〉，《法律與生命科學》，5 卷 1 期，頁 29-46。

張陳弘（2018），〈國家建置全民健康保險資料庫之資訊隱私保護爭議－評最高行政法院 106 年度判字第 54 號判決〉，《中原財經法學》，40 期，頁 185-257。

張陳弘（2018），〈新興科技下的資訊隱私保護：「告知後同意原則」的侷限性與修正方法之提出〉，《臺大法學論叢》，47 卷 1 期，頁 201-297。

程法彰（2020），〈我國資通訊產業的個資去識別化運用爭議〉，《萬國法律》，230 期，頁 73-81。

程嘯（2018），〈論大數據時代的個人數據權利〉，《中國社會科學》，3 期，頁 102-208。

楊立新，林旭霞（2006）·〈論人格標識商品化權及其民法保護〉，《福建師範大學學報（哲學社會科學版）》，136 期，頁 184-196。

楊岳平（2021），〈重省我國法下資料的基本法律議題—以資料的法律定性為中心〉，《歐亞研究》，17 期，頁 31-39。

doi:10.6342/NTU202301113

溫世揚（2013），〈析「人格權商品化」與「人格商品化權」〉，《法學論壇》，149 期，頁 107-111。

葉志良（2016），〈大數據應用下個人資料定義的檢討：以我國法院判決為例〉，《資訊社會研究》， 31 期，頁 1-36。

劉小紅（2020），〈數據按貢獻參與分配實現的法律意蘊〉，《月旦民商法雜誌》，70 期，頁 65-82。

蔡甫昌、莊宇真、陳俞璇、葉曉宜（2020），〈病歷與健康資料研究應用之倫理與法律〉，《台灣醫學》，24 卷 5 期，頁 471-489。

蔡昀臻、樊國楨（2016），〈大數據之資料去識別的標準化實作初探：根基於 ISO/IEC 2nd WD 20889：2016-05-30〉，《資訊安全通訊》，22 卷 4 期，頁 1-26。

簡宏偉等著（2020），〈大數據運用與隱私保護－手機定位資訊於防疫應用之法律問題研析〉，《國土及公共治理季刊》，8 卷 3 期，頁 64-75。

顏厥安（2002），〈財產、人格，還是資訊？論人類基因的法律地位〉，《台大法學論叢》，31 卷 1 期，頁 1-44。

（四）學位論文

王瑋（2020），《人格特徵商業利用之研究》，國立台灣大學法律學研究所碩士論文。

陳泓歷（2017），《基於差分隱私之資料去識別化保護與隱私洩漏風險評估系統》，逢甲大學通訊工程學系碩士論文。

黃松茂（2008），《人格權之財產性質以人格特徵之商業利用為中心》，國立台灣大學法律學研究所碩士論文。

doi:10.6342/NTU202301113

（五）政府出版品

經濟部標準檢驗局（2019），《CNS 29100-2:2019 資訊技術-安全技術-個人資訊去識別化過程管理系統-要求事項》。

（六）網路資料

Google，《GOOGLE 如何匿名處理資料》，載於：https://policies.google.com/technologies/anonymization?hl=zh-HK。

台權會網站，《健保資料庫訴訟案》，載於：https://www.tahr.org.tw/cases/NHID。

司法院網站（2022）《健保資料庫案言詞辯論新聞稿》，載於：https://www.judicial.gov.tw/tw/cp-1887-629970-b76ca-1.html。

交通部公路總局網站（2020），《公總與中市警合作台 61 線區間測速 109 年 1 月 15 日上路》，載於：https://www.thb.gov.tw/sites/ch/modules/news/news_details?node=eeb33aa6-58a1-4d5d-b6aa-28dd4d5270b0&id=0393a5b4-649f-45d6-9549-3927b7b35fe7。

何琳潔（2019），《你的個資真的已經匿名化了嗎？》。載於：https://infolaw.iias.sinica.edu.tw/?p=1831。

吳全峰（2018），《個資保護再思考》，載於：https://tw.appledaily.com/forum/20180625/D43MRQWXCC7AX5KKKDBGTFKKF4/。

吳全峰（2019），《不用你同意，政府做莊賣個資？》，載於：https://infolaw.iias.sinica.edu.tw/?p=984。

doi:10.6342/NTU202301113

林其樺（2015），〈一般常見把姓名、身分證字號隱碼的做法，其實並不等於將個人資料「去識別化」〉，《關鍵評論》，載於：https://www.thenewslens.com/article/33049。

科技部生科司（2021），《科技部生科司 110 年度健康大數據永續平台之「建置轉譯導向生醫巨量資料」詳細計畫書申請須知》，載於：https://www.most.gov.tw/most/attachments/cd750957-fc6f-4fe5-8052-ff6615a0ba37。

高速公路局網站（2022），《111 年國道智慧交通管理創意競賽》，載於：https://www.freeway.gov.tw/Publish.aspx?cnid=2863。

許可（2021），《數據要素市場的大哉問》，載於：https://ppfocus.com/sg/0/te71a8d59.html。

新北市政府警察局（2019），《平均速率科技執法》，載於：https://www.traffic.police.ntpc.gov.tw/cp-2772-44747-27.html。

衛生福利部中央健康保健署網站（2020），《防疫再升級 健保雲端系統提供高風險地區旅遊史》。載於：https://www.nhi.gov.tw/News_Content.aspx?n=FC05EB85BD57C709&s=012016EE70C9A226。

衛生福利部疾病管制署網站（2020），《「COVID-19(武漢肺炎)」防疫新生活運動：實聯制措施指引》。載於：https://www.cdc.gov.tw/File/Get/t-_Xs5DDee2qzBFC1fRXJA。

二、英文文獻

（一）專書

doi:10.6342/NTU202301113

Becker, L. C. (1970). Property Right: Philosophic Foundations. Routledge and K. Paul.

Bentham, J. (1690). The Theory of Legislation. Oceana Publ'ns, Inc.

Blackstone, W. (1766). Commentaries on the Law of England (facsimile ed.) (1766). The University of Chicago Press.

Cooter, R. D., Ulen, T. (2004). Law And Economics (4th ed.). Addison Wesley.

Elkin-Koren, N., Salzberger, E. M. (2004). Law, Economics and Cyberspace: The Effects of Cyberspace on the Economic Analysis of Law. Edward Elgar Publishing.

Mayer-Schönberger, V., Cukier, K. (2013). Big Data: A Revolution That Will Transform How We Live, Work, and Think. Harper Business.

Posner, R. A. (1998). Economic Analysis of Law (4th ed.). Aspen.

Purtova, N. N. (2011). *Property rights in personal data: A European perspective*. BOXPress BV.

Radin, M. J. (1996). Contested Commodities. Harvard University Press.

Schroeder, W. J., Martin, K. M. (2005). Visualization Handbook. Academic Press.

Sprankling J. G., Coletta, R. R., Mirow, M. C. (2006). Global. Issues in Property Law. West Academic Publishing.

Stucke, M. E., Grunes, A. P. (2016). Big Data and Competition Policy. Oxford University Press

Underkuffler, L. S. (2003). The Idea of Property: Its Meaning and Power. Oxford University Press.

doi:10.6342/NTU202301113

Waldman, A. E. (2018). Privacy as Trust: Information Privacy for an Information Age. New York Law School.

Westin, A. F. (1967). Privacy and Freedom. Athenum.

（二）專書篇章

Allen, A. L. (1997). Genetic Privacy: Emerging Concepts and Values. In Rothstein, M. A. (Ed.), *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era* (pp. 31-59). Yale University Press.

Bittner, P. (2018). Intellectual Property Management Challenges Arising from Persuasive Digitalisation: The effect of the Digital Transformation on Daily Life. In Seuba, X. et al. (Ed.), *Intellectual Property and Digital Trade in the Age of Artificial Intelligence and Big Data*. (pp. 67-74). CEIPI-ICTSD.

Gray, K. & Gray, S. F. (1998). The Idea of Property in Land. In Bright, S. & Dewar, J. K. (Ed.), *Land Law: Themes and Perspectives* (pp. 15-51). Oxford University Press.

Hugenholtz, P. B. (2017). Data Property in the System of Intellectual Property Law: Welcome Guest or Misfit?. In S. Lohsse, R. Schulze & D. Staudenmayer (Eds.). *Trading Data in the Digital Economy: Legal Concepts and Tools: Münster Colloquia on EU Law and the Digital Economy III* (pp. 75–100). Portland: Hart/Nomos.

Wen-Tsong, C. (2021). Digital development and privacy: Is there a way to alleviate the uneasy tension? In Chien-Liang, L. (Ed.), *The Way to Law: IIAS's 10th Anniversary* (pp. 461-474). Institutum Iurisprudentiae Academia Sinica.

doi:10.6342/NTU202301113

（三）期刊論文

Ad Hoc Committee on DNA Technology, American Society of Human Genetics (1988). DNA banking and DNA analysis: points to consider. *American journal of human genetics*, 42(5), 781–783.

Annas, G. J. (1999). Genetic privacy: There ought to be a law. *Tex. Rev. L. & Pol.*, 4, 9.

Balaban, T. L. (2009). Comprehensive Data Privacy Legislation: Why Now Is the Time. *Case W. Res. JL Tech. & Internet*, 1, 1.

Barnhizer, D. D. (2006). Propertizataion Metaphors for Bargaining Power and Control of the Self in the Information Age. *Clev. St. L. Rev*., 54, 69.

Baron, J. B. (2011). Property as control: the case of information. Mich. *Telecomm. & Tech. L. Rev.,* 18, 367.

Barrad, C. M. V. (1992). Genetic information and property theory. *Nw. UL Rev*., 87, 1037.

Bartow, A. (1999). Our date, ourselves: Privacy, propertization, and gender. *USFL Rev.*, 34, 633.

Basho, K. (2000). The licensing of our personal information: Is it a solution to Internet privacy. *Calif. L. Rev.*, 88, 1507.

Bell, A., & Parchomovsky, G. (2018). The privacy interest in property. *U. Pa. L. Rev.*, 167, 869.

Bergelson, V. (2003). It's personal but is it mine-toward property rights in personal information. *UC Davis L. Rev.*, 37, 379.

Bloustein, E. J. (1964). Privacy as an aspect of human dignity: An answer to Dean Prosser. *NYUL rev.,* 39, 962.

doi:10.6342/NTU202301113

Bovbjerg, R. R., Sloan, F. A., & Blumstein, J. F. (1988). Valuing life and limb in tort: Scheduling pain and suffering. *Nw. UL Rev.*, 83, 908.

Chen, C. M., Jyan, H. W., Chien, S. C., Jen, H. H., Hsu, C. Y., Lee, P. C., Lee, C. F., Yang, Y. T., Chen, M. Y., Chen, L. S., Chen, H. H., & Chan, C. C. (2020). Containing COVID-19 Among 627,386 Persons in Contact With the Diamond Princess Cruise Ship Passengers Who Disembarked in Taiwan: Big Data Analytics. *Journal of medical Internet research*, *22*(5), e19540.

Cofone, I. (2021). Beyond data ownership. *Cardozo L. Rev.*, 43, 501.

Cohen, J. (2000). Examined Lives: Informational Privacy and the Subject as Object. *Stan. L. Rev.*, 52, 1373-1438.

Colonna, T. E. (1998). Protection of Privacy in Personal Genetic Information. West Virginia Journal of Law and Technology, 2(2), 1.

Demsetz, H. (1967). Toward a Theory of Property Rights. *The American Economic Review*, 57(2), 347-359.

Drexl, J. (2017). Designing competitive markets for industrial data. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, 8, 257.

El Emam, K., & Alvarez, C. (2015). A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques. *International Data Privacy Law*, 5(1), 73-87.

Epstein, R. A. (1977). Privacy, Property Rights, and Misrepresentations. *Ga. L. Rev.*, 12, 455.

Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, 10(1), 11-36.

doi:10.6342/NTU202301113

Haddock, D. D., & Kiesling, L. (2002). The Black Death and property rights. *The Journal of Legal Studies*, 31(S2), S545-S587.

Hagel III, J., & Rayport, J. F. (1997). The coming battle for customer information. *The McKinsey Quarterly*, (3), 64.

Hall, M. A. (2009). Property, privacy, and the pursuit of interconnected electronic medical records. *Iowa L. Rev.*, 95, 631.

Hall, M. A., & Schulman, K. A. (2009). Ownership of medical information. *JAMA*, *301*(12), 1282–1284.

Hirsch, D. D. (2013). The glass house effect: Big Data, the new oil, and the power of analogy. *Me. L. Rev*., 66, 373.

Hull, S. C., Sharp, R. R., Botkin, J. R., Brown, M., Hughes, M., Sugarman, J., Schwinn, D., Sankar, P., Bolcic-Jankovic, D., Clarridge, B. R., & Wilfond, B. S. (2008). Patients' views on identifiability of samples and informed consent for genetic research. *The American journal of bioethics: AJOB*, *8*(10), 62–70.

Janger, E. J. (2002). Privacy Property, Information Costs, and the Anticommons. *Hastings LJ,* 54, 899.

Janger, E. J., & Schwartz, P. M. (2001). The gramm-leach-bliley act, information privacy, and the limits of default rules. *Minn. L. Rev.*, 86, 1219.

Jerome, J. W. (2013). Buying and selling privacy: Big data's difference burdens and benefits. *Stan. L. Rev.*, 66, 47.

Kang, J. (1997). Information privacy in cyberspace transactions. *Stan. L. Rev.*, 50, 1193.

Kang, J., & Buchner, B. (2004). Privacy in Atlantis. *Harv. JL & Tech.*, 18, 229.

Kim, T. W., Lee, J., Routledge, B., & Xu, J. (2021). Data and Manure: Are Data Subjects Investors?. *Berkeley Bus. LJ*, 18, 65.

doi:10.6342/NTU202301113

Koskinen, J. S. S., Kainu, V. M. A., & Kimppa, K. K. (2016). The concept of Datenherrschaft of patient information from a Lockean perspective. Journal of Information, *Communication and Ethics in Society*, 14(1), 70-86.

Laudon, K. C. (1996). Markets and privacy. *Communications of the ACM*, 39(9), 92-104.

Lemley, M. A. (1997). Romantic Authorship and the Rhetoric of Property. *Texas Law Review*, 75, 873.

Lemley, M. A. (1998). The modern Lanham Act and the death of common sense. *Yale LJ,* 108, 1687.

Lemley, M. A. (2000). Private Property: A Comment on Professor Samuelson's Contribution. *Stanford Law Review*, 52(5), 1545-1557.

Lessig, L. (1999). The architecture of privacy. *Vand. J. Ent. L. & Prac.*, 1, 56.

Lessig, L. (2002). Privacy as property. *Social Research: An International Quarterly*, 69(1), 247-269.

Lin, M. M. (1996). Conferring a federal property right in genetic material: Stepping into the future with the Genetic Privacy Act. *American Journal of Law & Medicine*, 22(1), 109-134.

Litman, J. (1999). Information privacy/information property. *Stan. L. Rev.*, 52, 1283.

Lund, J. (2011). Property Rights to Information. *Nw. J. Tech. & Intell. Prop.*, 10, 1.

Mattioli, M. (2017). The data-pooling problem. *Berkeley Technology Law Journal*, 32(1), 179-236.

McClurg, A. J. (2003). A thousand words are worth a picture: A privacy tort response to consumer data profiling. *Nw. UL Rev.*, 98, 63.

McMahon, D. J. (2008). The future of privacy in a unified national health information infrastructure. *Seton Hall L. Rev.*, 38, 787.

doi:10.6342/NTU202301113

Mell, P. (1996). Seeking shade in a land of perpetual sunlight: privacy as proeprty in the electronic wilderness. *Berkely Tech. LJ*, 11, 1.

Miller Jr, W. W., & O'Rourke, M. A. (2001). Bankruptcy Law v. Privacy Rights: Which Holds the Trump Card. *Hous. L. Rev.*, 38, 777.

Miller, K. (2014). Total surveillance, big data, and predictive crime technology: Privacy's perfect storm. *J. Tech. L. & Pol'y*, 19, 105.

Mossoff, A. (2003). What is property-putting the pieces back together. *Ariz. L. Rev.*, 45, 371.

Murphy, R. S. (1995). Property Rights in Personal Information: An Economic Defense of Privacy. *Geo. LJ*, 84, 2381.

Narayanan, A., & Shmatikov, V. (2010). Myths and fallacies of" personally identifiable information". *Communications of the ACM*, 53(6), 24-26.

Nehf, J. P. (2005). Incomparability and the passive virtues of ad hoc privacy policy. *U. Colo. L. Rev.*, 76, 1.

Netanel, N. W. (2000). Cyberspace self-governance: A skeptical view from liberal democratic theory. *Calif. L. Rev.*, 88, 395.

Newman, N. (2014). Search, antitrust, and the economics of the control of user data. *Yale J. on Reg.*, 31, 401.

Ohm, P. (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA l. Rev.*, 57, 1701.

Org. for Econ. Co-Operation & Dev. (OECD) (2013), Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value. *OECD Digital Economy Papers,* 220, 4.

Posner, R. A. (1977). The right of privacy. *Ga. L. Rev.*, 12, 393.

doi:10.6342/NTU202301113

Price, W., & Nicholson, I. I. (2017). Risk and resilience in health data infrastructure. *Colo. Tech. LJ*, 16, 65.

Prosser, W. L. (1960). Privacy, *Cal. L. Rev*., 48(3), 383-423.

Purtova, N. (2008). Property in personal data: A European perspective on the instrumentalist theory of propertisation. *Eur. J. Legal Stud*., 2, 193.

Radin, M. J. (1987). Market-inalienability. *Harvard law review*, 100, 1849-1937.

Radin, M. J. (2006). A comment on information propertization and its legal milieu. *Clev. St. L. Rev.*, 54, 23.

Rocher, L., Hendrickx, J. M., & De Montjoye, Y. A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. *Nature communications*, 10(1), 1-9.

Rockandel, K. (2013). A Myriad of Reasons to Celebrate: Why the Invalidation of Isolated DNA Patents Is a Victory for Personal Property Rights. *Vt. L. Rev*., 38, 225.

Rothstein, M. A. (2010). Is deidentification sufficient to protect health privacy in research?. *The American Journal of Bioethics*, 10(9), 3-11.

Samuelson, P. (1999). A New Kind of Privacy-Regulating Uses of Personal Data in the Global Information Economy. *Cal. L. Rev.,* 87, 751.

Samuelson, P. (1999). Privacy as intellectual property. *Stan. L. Rev.*, 52, 1125.

Scholz, L. H. (2018). Big data is not big oil: the role of analogy in the law of new technologies. *Tenn. L. Rev.*, 86, 863.

Schwartz, P. M. (2003). Property, privacy, and personal data. *Harv. L. Rev.*, 117, 2056.

Suter, S. M. (2003). Disentangling privacy from property: toward a deeper understanding of genetic privacy. *Geo. Wash. L. Rev.*, 72, 737.

doi:10.6342/NTU202301113

Sweeney, L. (2002). Achieving k-anonymity privacy protection using generalization and suppression. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5), 571-588.

Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, 2016(6), 5-8.

Veale, M., Binns, R., & Ausloos, J. (2018). When data protection by design and data subject rights clash. *International Data Privacy Law*, 8(2), 105-123.

Victor, J. M. (2013). The EU general data protection regulation: Toward a property regime for protecting data privacy. *Yale LJ*, 123, 513.

Volokh, E. (1999). Freedom of speech and information privacy: The troubling implications of a right to stop people from speaking about you. *Stan. L. Rev.*, 52, 1049.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4, 193.

Weeden, J. L. (2006). Genetic liberty, genetic property: protecting genetic information. *Ave Maria L. Rev.*, 4, 611.

Yu, P. K. (2018). Data producer's right and the protection of machine-generated data. *Tul. L. Rev.*, 93, 859.

Yu, X., & Zhao, Y. (2019). Dualism in data protection: Balancing the right to personal data and the data property right. *Computer Law & Security Review*, 35(5), 105318.

（四）研討會論文

Bauer, C., Korunovska, J., Spiekermann, S. (2012, May 15) *On the Value of Information: What Facebook Users are Willing to Pay* [Conference Presentation] Proceedings of the 20th European Conference on Information Systems, Barcelona,

doi:10.6342/NTU202301113

Spain. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1196&context=ecis2012.

Shapiro, C. & Varian, H. R. (1997, June 8). *US Government Information Policy*. [Conference presentation] Highlands Forum, Department of Defense, Washington, DC. https://www.researchgate.net/publication/248244291_US_Government_Information_Policy.

Westin, A. F. (2007, Oct. 1) *How the Public Views Privacy and Health Research, Results of a National Survey Commissioned by the Institute of Medicine Committee on "Health Research and the Privacy of Health Information: The HIPAA Privacy Rule"* [Conference presentation]. Institute of Medicine Committee Meeting, https://www.ftc.gov/sites/default/files/documents/public_comments/health-care-delivery-534908-00001/534908-00001.pdf.

（五）網路資料

(N.d.). Experian Official Website. https://www.experian.com/consumer-products/identity-theft-and-credit-protection.html

Australian Medical Association (2005, July 20). *AMA Poll Shows Patients Are Concerned About the Privacy and Security of Their Medical Records*. AMA. https://www.ama.com.au/media/ama-poll-shows-patients-are-concerned-about-privacy-and-security-their-medical-records

Brewster, T. (2017, Dec. 19). *120 Million American Households Exposed In 'Massive' ConsumerView Database Leak.* Forbes.

doi:10.6342/NTU202301113

https://www.forbes.com/sites/thomasbrewster/2017/12/19/120m-american-households-exposed-in-massive-consumerview-database-leak/?sh=72dbdffb7961

European Commission (2017, Oct. 1). *Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, SWD(2017) 2 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0002&from=EN

Gregorio, G. D. (2022). Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society. Cambridge University Press. https://www.cambridge.org/core/services/aop-cambridge-core/content/view/A3F61C6368D17D953457234B8A59C502/9781316512777AR.pdf/Digital_Constitutionalism_in_Europe.pdf?event-type=FTLA

Hern, A. (2017, Aug. 2). *Anonymous' Browsing Data Can Be Easily Exposed, Researchers Reveal*. The Guardian. https://www.theguardian.com/technology/2017/aug/01/data-browsing-habits-brokers

Information Commissioner's Office (ICO) (2017, Sep. 4). *Big Data, Artificial Intelligence, Machine Learning and Data Protection*. Version: 2.2. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

MacCarthy, M. (2018, Nov. 2). *Privacy Is Not A Property Right In Personal Information*. Forbes. https://www.forbes.com/sites/washingtonbytes/2018/11/02/privacy-is-not-a-property-right-in-personal-information/?sh=24ea407a280f

doi:10.6342/NTU202301113

Oberhaus, D. (2017, Aug. 3) *Your 'Anonymous' Browsing Data Isn't Actually Anonymous.* VICE. https://www.vice.com/en/article/gygx7y/your-anonymous-browsing-data-isnt-actually-anonymous

Patrizio, A. (2015, Nov. 25) *Why Your Big Data Needs Good Algorithms.* Datamation. https://www.datamation.com/data-center/why-your-big-data-needs-good-algorithms/

Sabin, S. (2019, Feb. 20). *Nearly Half of Voters Support California Governor's 'Data Dividend' Plan.* Morning Consult. https://morningconsult.com/2019/02/20/nearly-half-of-voters-support-california-governors-data-dividend-plan/

Serwer, A. (2018, Nov. 15) *Mark Warner: This will 'send a shiver down the spine' of Facebook, Twitter, and Google*. Yahoo Finance. https://finance.yahoo.com/news/mark-warner-will-send-shiver-spine-facebook-twitter-google-161313831.html?guccounter=1&guce_referrer=aHR0cHM6Ly9zdGF0ZXNjb29wLmNvbS8&guce_referrer_sig=AQAAAHAoiOeFyH_MFU8vy49mBtOCNTo3lhEFQZ8zUf-ez8GfTwHGr22dp6s8fmW48dRHqKwlj8JJ7s6UhZu1MmalyWgwURSQStgqiEps6KPV44HlOI_GGGnKm62cJQMJ8s2Am3-oSBpS7wXy9KNQJADQ4qyDOlfGO5jdMfenGUqZNrDu

Steel, E., Locke, C., Cadman, E., Freese, B. (2013, June 13) *How Much Is Your Personal Data Worth?*. Fin. Times. http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html

Swant, M. (2019, Oct. 1). *Andrew Yang Proposes Digital Data Should Be Treated Like A Property Right*. Forbes. https://www.forbes.com/sites/martyswant/2019/10/01/andrew-yang-proposes-digital-data-should-be-treated-like-a-property-right/?sh=1fcad6a83ab7

doi:10.6342/NTU202301113

What is Attribute and Record Suppression. (n.d.). IGI Global. https://www.igi-global.com/dictionary/attribute-and-record-suppression/72012

What Is Infrastructure? Definition and Examples. (n.d.). Market Business News (MBN). https://marketbusinessnews.com/financial-glossary/infrastructure-definition-means/

Working Party Article 29. (2007, June 20). *Opinion 4/2007 on the Concept of Personal Data*. 01248/07/EN WP 136. https://www.Clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf.

Working Party Article 29. (2014, Apr. 10). Opinion 05/2014 on Anonymisation Techniques. 0829/14/EN WP216. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

doi:10.6342/NTU202301113