國立臺灣大學法律學院科際整合法律學研究所

碩士論文

Graduate Institute of Interdisciplinary Legal Studies
College of Law

National Taiwan University

Master's Thesis

機器學習時代下資訊隱私權的概念重構與保護機制：Julie Cohen的隱私間隙理論觀點

Information Privacy's Paradigm and Protection Strategies in Machine Learning Society: Julie Cohen's "Privacy as Room for Boundary Management" Theory

劉逸文

Yi-Wen Liu

指導教授：蘇慧婕博士

Advisor: Hui-Chieh Su, Dr.iur

中華民國 114 年 2 月

February 2025

doi:10.6342/NTU202500550

國立臺灣大學碩士學位論文
口試委員會審定書

機器學習時代下資訊隱私權的概念重構與保護機制：Julie Cohen 的隱私間隙理論觀點

Information Privacy's Paradigm and Protection Strategies in Machine Learning Society: Julie Cohen's "Privacy as Room for Boundary Management" Theory

本論文係劉逸文君（學號 R08A41025）在國立臺灣大學科際整合法律學研究所完成之碩士學位論文，於民國 114 年 1 月 23 日承下列考試委員審查通過及口試及格，特此證明

指導教授：

口試委員：

doi:10.6342/NTU202500550

誌謝

這本論文的研究初衷是源自於一個很直接的疑惑：「大法官說，資訊隱私權是個人對個人資料的自主控制，但是現在我們根本不知道自己的個人資料在什麼時候被蒐集、被蒐集了哪些、被做為什麼用途，那資訊隱私權到底有什麼用？」為了探索能夠解決這個疑惑的回答，從 2021 年 7 月第一次跟蘇老師討論研究議題，到 2025 年年初在兵荒馬亂中完成口試和論文定稿，歷時三年半。雖然這本論文並不具備費時三年半應有的品質，但它陪我上山下海、流連餐廳酒吧 KTV、打過很多場手球比賽，陪我成長、陪我度過黑暗和把腦袋與靈魂重新拼回來的過程。

在感謝之前，想略微說明這本論文是在什麼樣的環境條件下產生的，就會知道稍後提及的那些人們，對於我和這本論文是多麼重要。

約是碩二、碩三時、簽指導單後沒多久，我的身心腦解離了。腦袋陷入混亂的風暴中，無法記憶和思考，讀不懂文字、也無法組織和輸出一句完整的話，必須閉上眼睛、聚精會神才能費力地運轉腦袋。心情浮躁、恐慌、不安，睡不著覺也失去食慾，生活失去形狀。在如此惡劣的腦心環境下，因為有以下的這些溫暖人們的陪伴與幫助，這本論文才能順利（？）的產出，我也才能把自己拼湊回來、重新讓腦袋轉起來，完成論發與口試。

最感謝的人是我的指導教授——蘇慧婕老師。對於老師很抱歉的是，因為我沒有照顧好自己，而在破碎的狀態下接受指導和寫作論文；也因為我不願意求助和不懂自己不懂什麼的問題，讓老師在指導我時耗費許多心力（讓老師從協助者的角色變成牧羊人，對此很抱歉），我大概是老師最操心的指導學生吧><。因為論文寫作的時間長，同期的同門已經畢業、老師還沒收新的學生，有一大段時間，我是唯一在校的指導學生，因此有機會和老師單獨咪挺。那段單獨咪挺的時間，對我和論文都很重要，每次咪挺都像是一次治癒的療程，老師會耐心地等我組織我的想法、協助我整理思緒、給予我可行的研究建議。在這段時期，論文題目終

doi:10.6342/NTU202500550

於確定（花了一年）、論文的架構也出來了，我的心情和腦袋也逐漸安定。除了論文之外，老師總是溫暖地給予我鼓勵和稱讚，提醒我要對自己有信心，叮嚀我要記得休息，能夠成為老師的指導學生真的很幸運。雖然在預計畢業的期限前一個月出了大包、在老師很忙的時候還炸了老師一波，最後只能切掉第四章的最後一節、斷尾求生，對老師真的很抱歉。但來者可追，未來會繼續努力，希望可以成為擔起蘇門出身的身分的人。

感謝二位口試委員老師——林子儀老師和劉定基老師，感謝兩位老師同意延後口試時間，讓我能夠完成論文與畢業。就讀科法所的期間，修了林子儀老師的言論自由、隱私權，老師在課堂上總會以問答引導、刺激我們思考，感受到老師對於學術研究、教學的真誠，是散發著光輝的巨人。很幸運的是，托蘇老師的福，邀請到林老師擔任我的口試委員。在口試時，林老師得了流感，即便身體相當不舒服仍出席我的論文口試，對老師感到抱歉也非常地感謝老師。在整個口試的過程，林老師總是溫暖地鼓勵我、為我整理問題和提出修改的建議。在口試結束後，林老師把滿是筆記的口試本給我、讓我便於修改，從標點符號、文字用語、註腳格式到實質的論述架構與內容，老師都認真地看過再提出修正建議，非常感謝林老師。感謝劉定基老師在口試的時候，溫柔地指出論文論述不足的地方，在我沒能理解老師的問題時，引導我思考和回答、耐心地整理問題，即便我回答的文不對題、論文內容也有許多不足，老師也給予我鼓勵、提供加值論文內容的方向。感謝二位口試委員老師。

另外，在學習法律的路上，很幸運地得到許多師長的協助。感謝圖資系的楊東謀老師、鄭瑋老師。東東每次看到我，都會皺著眉頭問我說「啊妳在科法所還好嗎？論文還好嗎？」聽完之後繼續說「好啦！加油啦！」然後請我吃了好幾次便當。特別要感謝鄭瑋老師，提供我寫科法所讀書計畫的研究方向，而我的論文也確實與之相關，此外，也因為鄭瑋老師的建議（：去修目標指導教授的課），讓我能夠順利地簽到蘇老師當指導教授。感謝我的前導師，王皇玉老師，在院辦

doi:10.6342/NTU202500550

或導生宴和老師相遇時，都能得到老師溫暖的問候和關懷。感謝劉靜怡老師，在修老師資訊法專題過程中，練習了閱讀文本、思考議題、口頭呈現的能力，當時的文本內容也成為論文重要的研究素材。感謝楊岳平老師和詹森林老師，在趕論文的最後一段路，兩位老師給予了溫柔的鼓勵。特別是詹老師，老師在信件中給我在這階段調適心情的建議，以及持續堅持的動力。另外也要感謝手球隊的黃欽永老師和許君恆老師，兩位老師在我研究所的時期，給予許多體諒包容和照顧鼓勵。除了前面所提的老師之外，我對每一位曾經相遇的老師都很感謝，感謝老師們包容我的不成熟以及教導。

在師長之外，如果沒有蘇門互助會，這本論文、論發和口試無法完成，由衷地感謝蘇門的每一位溫柔的強者。首先要感謝詠綺，因為研究議題接近，詠綺不時會輸送給我有用的文獻素材，詠綺也是我最常討論論文的同門，因為我不常開口求助的性格，詠綺每次主動地問我論文還好嗎、要不要一起討論的時候，我都非常感謝，蘇老師與詠綺大概是比我更知道我的論文在幹嘛、會長什麼樣子的人了。感謝暖男睿恩，在咪挺和模擬口試時，我因為聽不懂問題、頭腦轉不動而卡住，睿恩總會鼓勵我、替我排除緊張，提醒我要對自己有信心，睿恩大概也知道我太客氣的性格，幫我在群組扣起蘇門模擬口試，超級感謝。再來要感謝國祐學長、劭楷學長、胤慶學長。國祐學長在咪挺的時候，分享經驗、指出我論述和思路不清楚的地方；模擬口試時協助我練習回答問題、教我回答問題的方法，跟我說我的寫作進步很多、讓我提升信心，非常感謝學長。劭楷學長參加了兩次的模擬口試，從口頭報告的重點、可能被問的問題，都給予真誠有用的建議。胤慶學長不僅閱讀完我的口試本、給予修正建議與鼓勵，在模擬口試時，替我預測問題、一句句帶著我練習回答問題，分享問答技巧和準備口試的方法，非常感謝學長。另外，在我 Instagram 上表示論文寫作的困境時，胤慶學長和睿恩分享了他們的經驗，讓我知道原來不是只有我有這個問題、還有處理問題的方法，非常感謝。也要感謝竟祐和碩謙，沒有你們的話論發和口試都無法順利完成，祝福你們在論文

doi:10.6342/NTU202500550

寫作的路上順利與收穫豐實！

再來要感謝我的科法所和 2416 朋們靜耘、安履、洵美學姐、Emma、莎莉、品聿、士呈學長，相互陪伴、餵食、找樂子來度過漫漫的研究所時期。特別感謝靜耘和安履，很想念我們一起修課、吃飯和玩樂的時光，我趕緊跟上你們的腳步。感謝一起擔任研究助理的夥伴們，前手培琪、詠綺、脩閔、紹孺、桂華，你們是最可靠的。

接下來是每一位在我寫論文的過程中，曾經給過我關懷與鼓勵的朋友們（真的很多，畢竟我寫了很久），為了避免漏掉先不一一列出，等到拿到畢業證書、開始感謝祭之後，再一一、實體地跟每一位致謝。也感謝每一位在我身陷黑暗時，和我吃飯、讓我心情安定、回想起自己是誰的人們。

最後要感謝我的家人、過去和現在的陪跑員們。謝謝我的父母，在物質和心理上給我最深厚堅實的支持，讓我在自由、安全與穩定的環境成長，接納並支持我每個決定，包含那些你們不能理解的，從不催促或是否定我，你們深厚的愛是讓我頂過挫折和恐懼的力量，我愛你們。再來感謝比我成熟與優秀的妹妹和弟弟，在寫論文的過程中，你們替我分擔了家務、給我心情上的支持、為我解憂，希望我們會一直如此互相理解與扶持下去。感謝我家的狗 nini，在家寫論文的時間都有妳陪伴，給我療癒。感謝曾經共享生活與靈魂的老張、冼、老江、世華、徐蕾，我們都放了一些什麼在彼此體內而長成了現在的樣貌，特別感謝老江，在準備研究所考試時幫我找考古題和準備方法；也謝謝徐蕾在我看不懂文獻時幫我分析，也給予我休息的時間。還有現在的陪跑員劉于霈，陪我度過最後衝刺的階段、給我衝刺的動能，接下來也會好好跑下去。最後要提醒自己，很幸運地在許多人的協助之下完成論文、學業，期許自己也成為有能力給予的溫柔強者。

劉逸文

2025 年 2 月 8 日

doi:10.6342/NTU202500550

中文摘要

本文旨在探索機器學習時代資訊隱私權之概念與應有的保障機制。機器學習模仿人類學習過程，其「學習」的方法係將資料視作現實的替代品，匯聚大量的資料、在資料中探索潛藏的規律。其中，以認識、剖析「人」為目標的機器學習技術，匯聚巨量的個人資料，以統計原理分析資料、製作人格模版，以人格模版作為認識與評價個人與人口群體的素材，進而對個人與人口群體之行為與偏好進行推論、預測。機器學習之個人資料蒐用活動，使既有的資訊隱私權典範理論——個人資料自主控制理論發生保障不足的問題。首先，個人實際上無從追蹤個人資料的流向與控制蒐用活動，亦無法拒絕資料的蒐用要求。此外，以群體為資料分析規模之機器學習技術之運作邏輯與結果已超出個人可理解與控制範圍。

因此在機器學習為重要的數位化資訊技術工具的時代，資訊隱私權應如何有效地給予個人保障？此為本文最原始的問題意識。而本文研究目的是提出適宜於機器學習時代的資訊隱私權理論。該理論所提出的資訊隱私權概念，必須能夠捕捉機器學習之個人資料蒐用活動的新興危害、風險，以及給予適當的回應機制。本文以美國學者提出之信任隱私理論與隱私間隙理論，進行理論之分析比較。

本文主張應採 Julie E. Cohen 的隱私間隙理論作為機器學習時代的資訊隱私權典範理論，以社會主體理論、實質自主觀點、基本權利符擔性理論重新建構資訊隱私權概念與保障機制。由於社會與主體是相互建構關係、自主性之發展受到外在環境影響，資訊隱私為個人能夠管理與他人資訊性邊界之動態間隙。基於主體性與人格之自由發展，資訊隱私權保障個人設定與他人資訊性邊界之決定與能力，使個人得以免於受社會結構過度認識、形塑而使主體性與人格僵化。機器學習利用巨量個人資料進行人格剖繪，係以非主體決定之人格模版附加於該主體之上、建構對其之認識與理解，構成資訊隱私權之干預。為適當保障個人資訊隱私權，機器學習技術之使用應受語義不連續原則與運作可課責原則之限制，限制個人資

doi:10.6342/NTU202500550

料之匯流，以及機器學習之運作應對受影響之個人與人口群體透明、開放以確保可課責性。

在論證上，本文在第二章檢視自主控制典範下的資訊隱私權在機器學習時代產生的問題。自主控制典範係為回應電腦與資料庫時代發生之國家監控問題，確保個人自主控制個人資料揭露對象與條件，以及決定自己如何被認識與認識之程度。然機器學習技術匯聚、分析巨量資料、製作人口模版而對個人與群體進行評價、推論與預測，透過資訊環境之支配力使個人與群體的行為、偏好逐漸貼合推論與預測結果，個人與群體因此凝著於預決之人口模版。然而，在機器學習時代，因被蒐用的個資多、蒐用者多，而現實上個人無法實現資料自主控制；此外，自主控制理論也無法給予推論個人資料保護，以及機器學習之預測被當成真實，而使人類未來被機器預言寫定的問題。

在第三章，本文比較信任隱私理論與隱私間隙理論之隱私、資訊隱私概念與保障機制。相較於信任隱私理論從個人資訊分享揭露關係對社會之意義，論證資訊隱私保障之正當性，以及以私人民事關係汲取出資訊受託人義務作為主要規範模型。隱私間隙理論提出隱私對主體性與人格發展之功能、隱私權之構成要件、隱私權保障體系與機制，建構融貫、具體系性的隱私權理論。隱私間隙理論主張隱私為個人控管邊界之動態間隙，以自主保障取徑、權能保障取徑、符擔性保障取徑建構隱私權保障體系。符擔性保障取徑下，隱私權保障領域擴張，包含限制個人被轉譯程度之語義不連續原則，以及個人與群體參與社會結構之形塑的運作可課責原則。

確認本文採取隱私間隙理論為新興資訊隱私權典範理論之後，第四章以隱私間隙理論建構機器學習時代的資訊隱私概念與保障機制。機器學習對個人資訊隱私造成的新興危害來自以下二途徑：推論與預測分析、機器學習邏輯的怪異與混亂。首先，機器技術對個人與人口群體之推論與預測分析，匯聚大量個人資料、

doi:10.6342/NTU202500550

進行人口剖析、製作人格模版，以該模版作為認識與評價個人與群體之依據，並藉由其對資訊環境之掌控能力，使人類之行為與人格發展貼合人格模版。再者，個人與裝配機器學習技術之數位服務與工具頻繁互動下，因機器邏輯之混亂與難以理解，影響個人自我認識的過程。在保障機制上，語義不連續原則限制個人被轉譯的細緻程度，原則上禁止個人資料跨脈絡之匯聚，且數位服務工具應設運作之中斷機制；運作可課責原則下，機器學習、數位服務與工具、資訊環境之運作的設計與佈局，應對受影響之個人與群體透明，開放其參與事前決策過程，並確保事後課責之實踐。

關鍵字：機器學習、隱私、資訊隱私、個人資料自主控制、個人資料保護、Julie Cohen

doi:10.6342/NTU202500550

ABSTRACT

This thesis aims to explore the information privacy's paradigm and the appropriate protection strategies in machine learning society. Machine learning is a technology imitating human learning process and "learning" from big data which is treated as a substitute for reality. In the vein of information privacy, it collects huge amounts of personal data, sorts and categorizes the data, and creates personality profiles to know a person or population groups and make judgements, inferences or predictions. The above-mentioned process challenges the probability of self-determination of personal information, the existing paradigm of the right to information privacy. Obviously, we cannot trace the situation that personal data processed and retained; therefore, self-determination of personal information cannot be realized. Moreover, machine learning is based on data collected and processed at population-scale, its logic and results are beyond the range individuals can imagine, understand, and manage.

As mentioned above, this thesis seeks to find the way to realize information privacy effectively in the era of machine learning. Hence, this thesis aims to find the information privacy theory suited in machine learning society. That theory needs to clarify the risk or harm caused by machine learning and the react mechanism to ensure the realization of the right to information privacy. This thesis' objectives are to illustrate and analyze privacy as trust theory and privacy as the room for boundary management and to make a comparison between two theories.

This thesis argues Julie E. Cohen's privacy as the room for boundary management theory as the paradigm of right to information privacy in machine learning society and argues that re-constructing the concept of information privacy and rebuild protection mechanism based on the concept of socially situated subjectivity, material liberal theory, and affordance-based approach to privacy. Subjectivity emerges from the society and environment that subjects are situated, and information privacy is the dynamic room for subjects to realize informational boundary management. To ensure subjectivity and personality to develop freely, the right to information privacy safeguards the aforementioned dynamic room, in order to guarantee people find ways to push back

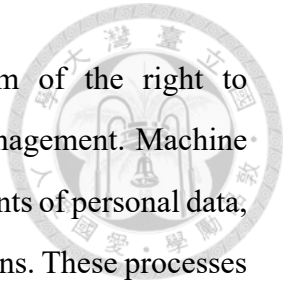
doi:10.6342/NTU202500550

against the social shaping from particular institutional, cultural, and material constrains that they encounter in their everyday lives. Evaluating people based on personality profiles made by machine learning constrains the right to information privacy. Machine learning should satisfy the requirement of the semantic discontinuity and the operational accountability principles. The semantic discontinuity principle aims to frustrate seamless personal data flow. The operational accountability principle requires the process of data collection and processing to be transparent at the appropriate level, and make sure that people affected by machine learning would have a say to co-determine the way they are read.

Chapter 2 examines the problems of self-determination of personal information paradigm. The self-determination of personal information paradigm occurs to confront government surveillance raised in computer and database era. It safeguards individuals to control over and determine the conditions of the use of their personal information in order to determine the way to be known. However, personal data self-management is hard to realize nowadays. Furthermore, machine learning evaluation, inference, and prediction raised problems that preemptive intervention and fossilization. These problems are beyond the coverage that safeguards by the right to information privacy based on self-determination theory.

Chapter 3 illustrates, analyzes, and compares privacy as trust theory and privacy as the room for boundary management. Privacy as trust theory builds on the function of personal information sharing relationships, it argues to establish information fiduciary duty as the regulation model. Comparatively, privacy as the room for boundary management theory constructs a coherent and systemic theory. It argues that privacy is a dynamic room for subjects to engage in processes of boundary management. It constructs the right to privacy protection system in three pillars: liberty-based, capability-based, and affordance-based approach, which provide the way to find the location of self-determination privacy and personal data protection. The coverage of the right to privacy discoursed from affordance-based approach is composed of two principles: the semantic discontinuity principle and the operational accountability principle.

doi:10.6342/NTU202500550



Chapter 4 constructs the concept and protection mechanism of the right to information privacy based on privacy as the room for boundary management. Machine learning inference and prediction is made through accumulating amounts of personal data, creating personality profiles, and human behavior or preference patterns. These processes constrain the right to information privacy. Moreover, machine learning inference and prediction are based on logic that humans cannot understand, thus interactions with machine logics disrupt processes of self-formation. The protection strategies are built on two principles. In order to ensure selves incomputable, the semantic discontinuity principle focuses on preventing seamless data collection and processing and requires to set gaps and breakdowns of translation. The operational accountability principle aims to guarantee people have a say in the operation and design of digital environments and technologies, machine learning included. To put it in detail, people should have an approach to access the relevant information, participate in the process of decision making, and build mechanisms to fulfill accountability.

Keywords: Machine Learning; Privacy; Information Privacy; Personal Data Self-determination; Personal Data Protection; Julie Cohen

doi:10.6342/NTU202500550

簡目

doi:10.6342/NTU202500550

詳目

doi:10.6342/NTU202500550

doi:10.6342/NTU202500550

doi:10.6342/NTU202500550

doi:10.6342/NTU202500550

第一章 緒論

第一節　問題意識與研究目的

資訊隱私權的內涵與保障範圍，是數位時代一項重要卻也棘手的議題。

在數位時代，電腦與網際網路是人們傳遞接收資訊的工具。影音、圖像、文字、語音等型態之資訊，被轉譯為數字 1 或 0，以無實際形體之光波或電波存錄於電腦、磁片光碟、硬碟等數位資訊工具中，透過光纖電纜和無線電波傳輸。資訊的儲存空間與傳播疆界等限制，逐漸解除。

數位化資訊技術與工具持續發展，其對人類與社會的意義不再只是傳遞接收資訊的功能，擷取、傳輸、儲存、運算分析數位資料的面向在現代被發掘、為經濟與社會所倚重。根據本文之歸納，數位化資訊技術之演進可分成三個方向：電腦之行動化、裝配於既有物件發展出智慧裝置；智慧裝置之間為溝通往來而使網際網絡的節點之密度與廣度擴大，形成物聯網；數位化資訊工具的運作邏輯、演算法從人類寫入專家規則模式，演變為機器自動化學習的機器學習模式。

其中，機器學習技術是使人類與自動化機器關係轉變的關鍵元素。人類使用電腦等機器來處理繁複的任務、問題，機器自動化運作的方式是依據設定的運作規則。過去，機器運作規則係由人類專家所寫下，以此將人類的智慧置入電腦，使之按照規則自動地為人類處理繁複的任務。此為基於規則運作（rule-based）專家系統模式（expert system）[1]。而至 20 世紀末之後，自動化機器發展出「學習」能力，如同人類學習過程，機器將蒐集得之資料、訓練資料作為認識現實之依據，在巨量資料中探索歸納出規則，發展機器學習（machine learning）之規則建構模式。上述機器學習技術的長處在於處理複雜、不存在人類已知規則的任務，並且

[1] *See* CHRIS WIGGINS & MATTHEW L. JONES, HOW DATA HAPPENED: A HISTORY FROM THE AGE OF REASON TO THE AGE OF ALGORITHMS 135-37 (2023).

doi:10.6342/NTU202500550

能夠順應情境學習、給予個別化回應，宛如擁有人類智力[2]。機器學習技術在資料社會被廣泛應用，例如商家對其商品之消費者購買關聯性分析、金融機構的個人信用評價系統、字元辨識系統、文字探勘技術、醫療診斷系統、語音與生物特徵辨識系統、中古車價格預測系統、電影推薦系統、搜尋結果排序、使用者網絡分析、自動化駕駛、圍棋對弈系統等[3]。

以巨量資料為基礎之機器學習技術，其資料處理與運算能力強化、精緻化智慧裝置與數位服務，並且因智慧裝置與服務之廣泛使用而擴增資料蒐集的範圍與精細度，二者互為表裡，驅動社會與經濟之發展。然而，在資料社會、資料經濟體下，個人資訊隱私權之保障受到挑戰。

今日，個人對其資料之自主控制是主要的資訊隱私權典範。在歐盟法秩序下，有歐盟基本權利憲章第 7 條與第 8 條、歐洲人權公約第 8 條，以及資料保護一般規則[4]等法規範，共同構成個人資訊隱私權概念與保障機制。而資料保護一般規則及其前身個人資料保護指令[5]為充實歐盟資訊隱私權內涵的具體規範，資料主體之知情同意、實踐自主控制之各項權利是規範的重點。歐盟肯認基本權利層次的資訊隱私權，並以個人自主控制為重要的權利內涵與保障機制[6]。在美國，是否存在憲法層次之資訊隱私權仍不明，今日個人資料所受到的保護規範主要是個人與資料蒐用者磋商成立的隱私條款，個人資料的保護機制是建立在市場機制、消費者保護的思維上。整體而言，個人在磋商階段的知情同意、磋商自主性之確保為關鍵，磋商成立的條件即為後續個人資料蒐用所依循的規則，包含個人對其資料的

[2] *See* ETHEM ALPAYDIN, INTRODUCTION TO MACHINE LEARNING 1-3 (Third edition ed. 2014).
[3] *Cf. id.* at 4-14.
[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [hereinafter GDPR], O.J. (L 119) 1-88.
[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. (L 281) 31-50.
[6] 參見劉定基（2017），〈大數據與物聯網時代的個人資料自主權〉，《憲政時代》，42 卷 3 期，頁 272；英文部分參見 Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEORGETOWN LAW J. 115, 123-131 (2017).

doi:10.6342/NTU202500550

後續控制方法[7]。

在我國，個人資料自主控制亦為資訊隱私權之典範。在司法院釋字第 585 號、第 603 號、第 689 號解釋與憲法法庭 111 年憲判字第 13 號判決（下稱 111 憲判 13 判決）的闡釋之下，我國憲法上資訊隱私權為個人資料自主控制，基於人性尊嚴、個人主體性之維護與人格自由發展而受憲法第 22 條保障[8]。所謂個人資料自主控制，包含個人在個人資料被蒐用之前與蒐用過程之事前控制與事後控制面向。個人資料之事前控制保障機制為保障人民有決定是否揭露、在何種範圍內、於何時、以何種方式、向何人揭露之權利；事後控制則為人民對其資料之蒐用知悉權、錯誤更正權、請求刪除權、停止與限制利用之權利[9]。受資訊隱私權保障之個人資料的範圍以資料之識別性為判斷標準，凡得直接或間接識別資料主體之個人資料，個人原則上對其有自主控制權，而不以資料私密性為斷[10]。而資料主體對其個人資料之自主控制非受絕對保障，國家基於公共利益，得在合於憲法第 23 條之規定下，強制蒐集使用個人資料[11]。個人資料中，具私密敏感性、與其他資料結合拼湊個人人格或生活圖像者，受資訊隱私權較嚴密之保障[12]。

然而，前述個人資料自主控制之資訊隱私權典範，在機器學習為關鍵數位化資訊工具技術基礎的數位時代，需要檢討。

首先，在當代的數位環境之下，我們對個人資料之自主控制幾乎無法實現。在事前控制的層次，個人資料在當代是我們與公私部門溝通往來與使用數位服務、開啟數位生活的必要素材，個人難以拒絕提供資料。公部門為了便利民眾而提供

[7] *See id.* at 132-137.
[8] 參見憲法法庭 111 年憲判字第 13 號解釋理由書第 31 段，以及司法院釋字第 689 號解釋理由書第 5 段、第 603 號解釋理由書第 8 段、第 585 號解釋理由書第 25 段。
[9] 參見憲法法庭 111 年憲判字第 13 號解釋理由書第 31 段、第 32 段。
[10] 參見憲法法庭 111 年憲判字第 13 號解釋理由書第 35 段、司法院釋字第 689 號解釋理由書第 7 段。
[11] 參見司法院釋字第 603 號解釋理由書第 9 段。
[12] 參見憲法法庭 111 年憲判字第 13 號解釋理由書第 45 段、司法院釋字第 603 號解釋理由書第 9、10 段。

doi:10.6342/NTU202500550

的線上服務，以及基於公共利益提供之社會福利或其他措施，頻繁地蒐集使用個人資料。例如我國外交部的線上申辦護照系統[13]、內政部的自然人憑證系統[14]、中央與地方政府的長照服務申請與審核系統，以及過去新冠肺炎期間我國政府的邊境管理、居家隔離與檢疫、電子圍籬、數位足跡、事後紓困措施等。就私部門蒐用個人資料之現況，由於數位裝置與服務已是現代個人的生活的重要工具。我們仰賴電腦與手機等智慧裝置中的通訊軟體與他人聯繫、透過社群平台得知親友與世界的近況、使用搜尋引擎服務查找資訊。此外，實體物件亦加入數位資訊網絡而形成物聯網，例如智慧手錶、智慧眼鏡、智慧家電、智慧車輛等。

其次，當個人資料蒐用的蒐用者、資料類型與數量、情境不斷擴增，個人對其資料在蒐集使用後的控制，現實上亦難實踐。個人資料被蒐用的範圍增廣、內容與種類更加細緻，且供個人資料流動的網絡也越加複雜與廣披。如釋字 603 號解釋與 111 憲判 13 判決原因案件事實所示，國家可能基於諸種行政目的強制蒐用個人資料，再為其他目的對資料進行二次、三次之利用，或者向外傳輸至其他組織機構。在數位化資訊技術持續發展之下，資料蒐用的價值上升、成本下降，公部門將既有的資料數位化儲存以增利用價值，或者增加蒐集之情境與資料種類[15]。除此之外，私部門更是推進數位化資訊技術之發展與應用的重要動力，並將資料之價值發揮至極致，甚而形成將資料當成產業發展關鍵動能的資料經濟[16]。個人資料因此可能在蒐用者之間、蒐用者本身內繼續、無盡地流動，甚至出現專營資料傳遞服務的資料仲介產業（data brokers）[17]。資料主體無法一一追蹤個人資料的流向與蒐用情況。

---

[13] 外交部領事事務局個人申辦護照網路填表及預約系統，https://ppass.boca.gov.tw/sp-ia-login-2.html（最後瀏覽日：02/05/2025）。

[14] 內政部自然人憑證管理中心，https://moica.nat.gov.tw/what.html（最後瀏覽日：02/05/2025）。

[15] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 13-16 (2006).

[16] 美國學者 Shoshana Zuboff 教授對於資料經濟之形成與運作有鞭辟入裡之分析，參見：SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (1 ed. 2018).

[17] *See* EDITH RAMIREZ ET AL., *Data Brokers: A Call for Transparency and Accountability* (2014).

doi:10.6342/NTU202500550

再者，機器學習造成非個人可控與知悉的新興風險。在運作的邏輯上，如前所述，機器學習的長處在於協助人類處理蒐集到的巨量資料，在大量雜亂的資料中歸類出無法以人類邏輯解釋的規則或模式，資料主體與資料蒐用者皆無法確認資料處理之成果，難以切實控管個人資料的用途[18]。拼湊大量個人資料、進行分析比對之操作，可能會剖析出包含私密敏感、須特別保護以及原本不在資料集內的資料[19]。混合資料推論規則、建構模版，或是產出新的訓練資料、推論資料，單一資料主體撤回同意、要求刪除資料，也無法改變其資料對於既成模版、模型或是產生新資料過程的影響性[20]。機器學習時代的資料蒐集使用係取得大量資料作為分析現實情況的依據，以剖繪群體之人口圖像、建立人口模版之集體規模來運作，個人自主控制模式顯得無力[21]。

對於前述問題，各國的規範重點逐漸轉移。如我國憲法法庭在 111 憲判 13 判決中，對於衛生福利部中央健康保險署（下稱健保署）為辦理全民健康保險業務，強制蒐集使用人民病歷、處方箋、診療紀錄等資料（下稱健保資料），建立全民健康保險研究資料庫，並允許公務機關、學術研究機構，向健保署申請取用健保資料等事實，憲法法庭認為公務與學術研究機構得為統計與學術研究方式，累積科學知識公共財以提升醫療、公共衛生目的，取用健保署強制蒐集之含有人民敏感資料之健保資料[22]。然而資料主體因此對其個人資料失去控制，為避免逸脫個人控制範圍之個人資料遭濫用或不當洩漏，憲法法庭肯認個人對其資料之自主控制權有組織、程序保障面向。國家在強制蒐集使用個人資料的情境，應以法律明定蒐用目的與要件，並且依當代科技能力而採取組織與程序上必要防護措施，確保資料安全與正確，而此組織與程序之必要措施，國家應積極以法律或依法律明

[18] *See* Julie E. Cohen, *Turning Privacy inside Out*, 20 THEOR. INQ. LAW 1, 8 (2019).
[19] *See id.* at 8-9.
[20] See Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME LAW REV. 975, 991-92 (2023).
[21] *See* Daniel J. Solove & Woodrow Hartzog, *Kafka in the Age of AI and the Futility of Privacy as Control*, 104 B.U. L. REV. 1021, 1039 (2024).
[22] 參見憲法法庭 111 年憲判字第 13 號解釋理由書第 50、51 段。

doi:10.6342/NTU202500550

確授權之命令為之，包含為資料主體監督控管個人資料蒐用情況之獨立監督機制[23]。

此外，歐盟亦開始以《個人資料保護一般規則》等具體規範，以立法建構出個人資料蒐用活動應循規則與框架，例如對資料蒐集範圍與儲存期間的限制[24]、資料完整性與正確性確保之義務[25]、資料控管者在技術與組織面向之資料保護措施要求[26]、資料再利用之限制[27]等。在美國，雖然欠缺聯邦層級的個人資料保護規範，但各州開始設置相關規範，例如加州的《加州消費者隱私法》（the California Consumer Privacy Act）[28]與《2020 年加州隱私權法》（The California Privacy Rights Act of 2020）[29]對個人資料蒐用企業的義務規範[30]。

如前述，為回應數位技術對個人資料自主控制之挑戰，資訊隱私權的典範開始轉移。第一項轉移是從資料主體在資料蒐用之前的磋商與事後監督控制，轉移到資料蒐用階段的控管資料蒐用風險之個人資料保護機制[31]；第二項轉移是私人企業躍升為對個人資料自主控制之資訊隱私權的主要侵害來源，個人資料的流動，不限於公部門流至私部門此一流動方向，數位社會的私部門之間、私部門至公部門之個人資料流向更為活絡[32]，國家在資訊隱私權保障之角色從侵害來源，轉變為個人資料蒐用之管制者。

在數位時代以巨量資料為基礎之機器學習技術衝擊既有資訊隱私權典範，並發生新興的個人資料蒐用危害，因此，資訊隱私權之典範已有轉移趨勢。因此，

[23] 參見憲法法庭 111 年憲判字第 13 號解釋理由書第 61、64、65 段。
[24] GDPR, art. 5(c)(e), O.J. (L 119) 35-36.
[25] GDPR, art. 5(d)(f), O.J. (L 119) 35-36.
[26] GDPR, art. 24, 25, O.J. (L 119) 47-48.
[27] GDPR, art. 6(4), 28, O.J. (L 119) 37, 49-50.
[28] California Consumer Privacy Act, CAL. CIV. CODE §§ 1798.100-.192 (2018).
[29] California Privacy Rights Act, CAL. CIV. CODE §§ 1798.100-.199 (2023)
[30] 參件張陳弘（2022），〈美國加州消費者隱私保護法制之最新發展與比較法啟示〉，《當代法律》，6 期，頁 29-35。
[31] 參見劉定基，前揭註 6；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。
[32] 參見翁逸泓（2022），〈資料治理法制：歐盟模式之啟發〉，《東海大學法學研究》，64 期，頁 59-60。

doi:10.6342/NTU202500550

本文的研究問題是：在機器學習技術被廣泛應用的時代，資訊隱私權典範理論應如何變遷？

以下，本文援引我國學者之研究，進一步剖析前述問題。

劉定基在〈資訊的保鮮期限？──論被遺忘權幾個待解的習題〉討論被遺忘權之憲法基礎之段落，指出在現代個人資料為資訊技術、經濟、社會發展之重要資源而被頻繁蒐用的情況下，非所有因個人資料蒐用活動而起的傷害、風險都能納入個人資料自主控制典範的資訊隱私權處理。被遺忘權原本的紛爭背景是資料主體欲要求搜尋引擎業者，在以資料主體姓名為關鍵字的搜尋結果列表中，移除含有其姓名的特定搜尋結果。因在技術上涉及資料主體姓名之個人資料的蒐集處理，落入個人資料自主控制權討論範圍。劉定基採取德國聯邦憲法法院與美國學者 Robert Post 之見解，認為個人資料自主控制權處理的是「避免具有一定規模、系統性、將資料主體排除在外的黑箱式資料處理行為[33]」，然被遺忘權的紛爭在「特定個資單一、公開溝通傳播所生的影響[34]」，接近傳統人格權處理的公開揭露他人私人事務案件，應屬於傳統人格權之議題，只是傳播的場域發生在網路空間而產生特殊性[35]。劉定基進一步表示，並非所有與個人資料之蒐集使用有關之爭執，皆應劃歸資訊隱私權、個人資料自主控制權之範圍，現代個人資料被使用的情境越來越多，在涉及個人資料的事件，應細緻地區辨傳統民刑法與新興資訊隱私或個人資料保護規範的範圍[36]。

張陳弘即在〈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〉中，提到其中一項機器學習等數位化資訊技術之個人資料蒐用活動造成的新興危害、風險——資料主體同意個人資料蒐用的外溢效果。所為個

[33] 劉定基（2023），〈資訊的保鮮期限？──論被遺忘權幾個待解的習題〉，《政大法學評論》，174 期，頁 227。
[34] 劉定基，前揭註 33，頁 231。
[35] 劉定基，前揭註 33，頁 230。
[36] 劉定基，前揭註 33，頁 228。

doi:10.6342/NTU202500550

人資料之外溢效果，是指單一資料主體對個人資料之「同意」效果可能會影響相同群體之未同意個人料蒐用的他人。張陳弘以 2007 年馬偕醫院蒐集 29 名噶瑪蘭族人之唾液進行針對該族群之研究的計畫為例，整體噶瑪蘭族之生理、生物特徵資訊可能因少數族人之同意而被完整剖析[37]。

對於個人資料自主控制典範無法捕捉到個人資料蒐用活動的新興危害與風險的原因，邱文聰在〈從資訊自決與資訊隱私的概念區分──評「電腦處理個人資料保護法修正草案」的結構性問題〉文中給予可以進一步研究的方向。邱文聰指出，個人資訊對於人格自由之意義可分為外在行為與內在人格獨立性面向，對於二者之保護皆屬於一般人格權之範疇。外在行為自由面向是「免除對個人行動之外在限制的單純消極自由[38]」；人格獨立性的自由則涉及「特定之個人資訊與個人人格或主體性之形成間的緊密關連性[39]」。邱文聰指出，個人資訊與人格獨立性此一面向較欠缺發掘，而其認為對個人資訊此面向的保障，可連結到蒐集個人資訊用以產生具有人格形塑影響力之知識／權力此一活動[40]。

本文根據以上三位學者之研究，設定本文在探索新興的資訊隱私權典範時的三項研究目標。如張陳弘所指之個人資料外溢效果，本文設定的**第一項目標為找出以個人資料蒐用為基礎之數位化資訊技術對個人與社會造成的新興危害與風險，並以機器學習技術為焦點。第二項目標**則是根據學者邱文聰的研究，**新興資訊隱私權典範必須釐清個人資料與人格發展獨立性的關聯性。第三項研究目標是說明在新興的資訊隱私權典範下，回應個人資料蒐用造成的新興危害與風險的方法，即資訊隱私權之保障機制的問題。**

而如劉定基所述，個人資料蒐用活動造成的新興危害與風險皆歸由個人資料

[37] 劉定基，前揭註 33，頁 230-232。
[38] 邱文聰（2009），〈從資訊自決與資訊隱私的概念區分－評「電腦處理個人資料保護法修正草案」的結構性問題〉，《月旦法學雜誌》，頁 176。
[39] 邱文聰，前揭註 38，頁 176。
[40] 邱文聰，前揭註 38，頁 176-177。

doi:10.6342/NTU202500550

自主控制之資訊隱私權來處理，會發生保障不足的問題，應仔細釐清個人資料自主控制權與其他權利之間的關係，將個別危害歸由適當的權利處理、給予保障。然而，須先澄清的是，本文研究目的限在探索適當的新興資訊隱私權理論，新興理論在個別法秩序的實踐並非本文的研究目的。

第二節　研究範圍、研究方法與用語說明

必須先說明的是，本文不先對「資訊隱私（權）」、「個人資料自主（權）」、「個人資料保護（權）」等用語給予定義。理由是本文的研究對象——「資訊隱私（權）」並非穩定的概念，依時空、法秩序、學者見解等討論脈絡之不同，而有不同的意義。特別是「個人資料自主（權）」、「個人資料保護（權）」等用語皆與資訊隱私有關、但其關聯性並不清楚，用與、概念之間的關係也不易釐清，此亦為本文將資訊隱私（權）設為研究議題之緣由之一。

然而，本文之討論範圍仍須界定，從而本文廣泛地將「個人資訊以及其蒐用」對「主體性維護、人格發展」之意義設定為「資訊隱私」的討論範圍。除了本文的研究目的是釐清在基本權利層次之資訊隱私權概念，而切割將個人資料作為個人財產、從財產權保障去論述個人資料之保護與設計規範的討論。另一項理由是，我國憲法法庭在 111 憲判 13 判決的見解亦未詳予區分、釐清資訊隱私權、個人資料自主控制權與個人資料保護權之關係。

在研究方法上，本文採取文獻蒐集分析法，以美國學者提出之隱私權、資訊隱私權理論為主要的研究對象。

以美國學者提出之隱私權、資訊隱私權理論為研究對象之理由有三。首先，美國是第一個有體系地提出隱私權理論之國家，且對各國之隱私權、資訊隱私權、個人資料保護法發展有重要的影響力。1890 年，Samuel D. Warren 和 Louis D. Brandeis 的〈隱私權〉觀察到新聞媒體業者窺探公眾人物之私人生活並以手持相

doi:10.6342/NTU202500550

機記錄、製作八卦新聞，而在普通法體系找尋個人隱私保障之法源[41]；在 1970 年代，美國住宅、教育與福利部（Department of House, Education, and Welfare）之自動化個人資料系統諮詢委員會（Advisory Committee on Automated Personal Data Systems）在《紀錄、電腦 與公民權利》報告提出之五項公正資訊行為準則（Code of Fair Information Practices），對各國之資訊隱私法制影響深遠[42]。此外，在學說上，Alan F. Westin 的《隱私與自由》[43]為自主控制理論建構理論基礎。

第二個理由是我國隱私法制與美國的相近性。在憲法層次之隱私與資訊隱私保障，相較於歐盟有《基本權利憲章》第 7 條與第 8 條明定個人私生活權與個人資料保護權，我國與美國是透過實務逐步探索與充實內涵。我國憲法上隱私權保障範圍之判斷標準為隱私合理期待準則[44]，隱私合理期待準則為 1967 年美國聯邦最高法院 John Marshall Harlan 大法官在 Katz v. United States 案[45]的協同意見中，有關美國聯邦憲法增修條文第 4 條人民人身、住所、文件、財產不受不合理之搜索權利之保障範圍，所提出的判斷標準[46]。

如前所述，美國在憲法上的隱私保障是透過實務闡義充實，然而聯邦最高法院憲法實務遲遲未肯認憲法層次隱私權、資訊隱私權之存在[47]，因此，美國學者積極地論述隱私權與資訊隱私權對社會與個人的重要性，試圖在數位時代確立資訊隱私保障之正當性。此為選用美國之隱私權、資訊隱私權理論作為研究對象之第三個理由。

初步探索美國學者探索隱私權與資訊隱私權理論的文獻，本文選擇美國學者 Jack M. Balkin、Neil M. Richards、Woodrow Hartzog 與 Ari E. Waldman 等人主張的

---

[41] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. LAW REV. 193 (1890).
[42] 劉定基，前揭註 33，頁 270。
[43] ALAN F. WESTIN, PRIVACY AND FREEDOM (New edition 2015 ed. 1967).
[44] 參見司法院釋字第 689 號理由書第 7 段。
[45] Katz v. United States, 389 U.S. 347, 360 (1967).
[46] 參見司法院釋字 689 號解釋林大法官子儀及徐大法官璧湖部分協同部分不同意見書，頁 10。
[47] *See* Schwartz & Peifer, *supra* note 6, at 132-35. 中文文獻討論可參見陳起行（2000），〈資訊隱私權法理探討——以美國法為中心〉，《政大法學評論》，64 期，頁 306-307。

doi:10.6342/NTU202500550

信任隱私理論（privacy as trust）與資訊受託人（information fiduciary）義務規範模型，以及 Julie E. Cohen 的隱私間隙理論（privacy as room for boundary management）為主要研究理論。理由是此二理論重新建構在數位時代的隱私、資訊隱私之概念，提出個人資料之蒐用活動產生超出個人可控制風險的原因，以及建議之資訊隱私保障機制，能夠回應本文之研究目的。

應先說明的是，本文雖以美國學說理論為主要的研究對象，然本文的研究問題並不限於美國法之討論，數位化資訊技術與機器學習的發展、造成的傷害與管制方法為各個法秩序目前面臨之重要問題，因此亦可能涵蓋我國與歐盟法相關法制與學者之研究文獻。

本文蒐集的文獻以討論資訊隱私權理論的法學領域文獻為主。然因隱私權仍是發展中之權利，其體系與權利之間的分野並不明顯，再加上隱私權與資訊隱私權保障議題係因資訊技術之演進而逐漸興起，因此在文獻蒐集的主題上，在法學領域之文獻，擬納入有關隱私、個人資料保護、個人資料自主控制之有關主題之文獻；就非法學文獻部分，會涵蓋介紹數位化資訊技術工具之文獻。

如本節開頭所述，資訊隱私（權）、個人資料自主（權）、個人資料自主控制（權）、個人資料保護（權），用語上可能產生混淆，對此，本文將在各章節中，依該章節討論之典範理論與學說理論，說明個別章節下的隱私（權）或資訊隱私（權）的概念。

此外，在用語上本文不細緻區分「資訊」（information）與「資料」（data），雖然資訊學領域為深入研究資訊之角色、功用與特性，而可能對資訊與資料有所區分[48]，然而不區分亦不影響本文的研究，首先本文蒐集到的研究素材多未作此

[48] 例如資訊學領域下的知識管理學有關知識之研究發展出 DIKW 金字塔理論，該理論認為對知識生成，資料（data）、資訊（information）、知識（knowledge）、智慧（wisdom）具有前後階段的關係。詳細內容可參見：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 32-33；*See* Russell L. Ackoff, *From Data to Wisdom*, *in* ACKOFF'S BEST: HIS CLASSIC WRITINGS ON MANAGEMENT 2 (1999).

doi:10.6342/NTU202500550

區分，大都在資訊隱私框架下討論個人資料蒐集使用帶來的變化，至多為凸顯數位時代個人資料涉及的隱私問題時，專門使用資料隱私作為用語；其次，資訊學領域相關研究認為資訊是經處理、分析而具意義的資料，而在此所指之處理、分析者可能是人或是機器，而資訊隱私、個人資料保護所關注的便是蒐集處理後的資料或資訊、或者是資料或資訊對接收者的影響，不論從哪個層次，皆無區分之必要。

第三節　研究架構

如前所述，本文的研究目的是探索能夠回答機器學習時代的資訊隱私權概念相應的保障機制之資訊隱私權理論，且該理論應回答資訊隱私與人格發展、個人主體性維護之關聯性，以及捕捉機器學習技術產生的新興風險並給予相應的保障機制。研究方法與範圍是整理、分析與比較美國學者提出之信任隱私理論與隱私間隙理論。

第二章為現況之展開，即對既有典範之介紹與批評，以此論證資訊隱私權典範變遷的必要性。因此，本文在此先介紹個人資料自主控制典範，說明其理論緣起、理論基礎、規範原則與具體法規範。個人資料自主控制理論為私密典範面對電腦、資料庫、網際網路時代發生隱私權保障不足問題的解決方案。然而，在今日的資訊環境下，資訊隱私權典範自主控制理論再度受到挑戰。具體批評可分為三個層次：資料主體在現況下難以有效控制個人資料的問題、自主控制理論對人類理性的誤解、機器學習技術下推論個人資料與預測分析之新興傷害。

在第二章確認既有典範不足與變遷必要性之後，**第三章**為新興典範——信任隱私理論與隱私間隙理論的介紹、分析與比較。信任隱私理論是從實然的角度，觀察個人資料之分享揭露對於個人與社會的意義，個人因此在個別社會情境與關係中扮演適當的角色，而個人資料分享揭露的常規是人際互動依從的規則，而為建構社會必要的元素，應受法規範保障。信任隱私理論主張法規範應保障個人資

doi:10.6342/NTU202500550

料分享揭露關係中當事人之信任，而援用普通法之託管關係法理建構資訊受託人義務規範。隱私間隙理論則從隱私之經典定義——私領域之界分，說明為個人保留私領域對主體性之培育、人格自由發展的重要性，且除了個人設定私領域邊界的決定之外，隱私權保障之範圍應包含個人在社會環境下管理私領域邊界之實踐條件。因此隱私間隙理論採取擴張的基本權利理論，主張社會的環境與結構應具備足使基本權利實踐的要素，隱私權保障範圍不限於主觀的個人設定邊界決定之自主性與實踐條件，應包含客觀的環境條件。國家因此負有確保個人隱私權在社會環境實踐之積極義務，以此要求國家針對資訊環境之參與者訂定個人資料蒐集使用相關規範。經過本文的比較，本文支持隱私間隙理論作為數位時代的資訊隱私權典範理論。

第四章係根據隱私間隙理論，提出機器學習時代的資訊隱私權概念與保障機制。隱私間隙理論係在現有之資訊環境下討論隱私之概念，未區分隱私與資訊隱私。本文以美國社會學者 Irwin Altman 對個人邊界、隱私管理機制與策略的觀察，為隱私間隙理論填補隱私權與資訊隱私權之落差，進而提出本文主張的資訊隱私權概念。隱私間隙理論採取的資訊隱私權保障機制為論證應從物質環境之設計與佈局確保隱私權之實踐，即資訊隱私權之符擔性保障取徑。隱私間隙理論提出之符擔性隱私權保障取徑為語義不連續原則與運作可課責原則。在機器學習脈絡下，匯聚資料、製作人口模版、根據人口模版建構對個人與社群之認識，給予差別性的評鑑與回饋，個人與社群無法拒絕被以人口模版理解，此途徑已經構成資訊隱私權之干預。而在語義不連續原則與運作可課責要求下，機器學習之個人資料匯聚應受到限制，原則上禁止無縫隙的資料匯聚；此外，機器學習應用於個人與群體人口剖析，受機器學習之影響者應有參與決定之能力，包含機器學習運作之邏輯、資料來源的透明開放，以及設計過程的開放參與等要求。

doi:10.6342/NTU202500550

第二章 資訊隱私權之現有典範：個人資料自主控制之理論、制度與限制

個人資料自主控制理論成為資訊隱私權典範理論，是為了處理私密理論在電腦與資料庫時代對個人資料保護不足的問題。在本章，首先說明資訊隱私權在自主控制典範之前的發展，本文介紹開創隱私權討論之 Samuel Warren 和 Louis Brandeis 的獨處權（The Right to Be Let Alone）[49]，以及資訊隱私權的核心概念——私密理論，以此鋪陳自主控制理論的發展背景。

第二節進入個人資料自主控制理論之討論，包含自主控制理論發展的資訊技術背景以及理論建構的基礎。第三節是自主控制理論下的資訊隱私保護規範體系，包含個人對其資料之事前控制權、事後控制權與個人資料蒐集使用原則。

本章第四節則是整理學者對於個人資料自主控制理論的批評，分為三個面向：實踐上的困難、對人類理性的誤解，以及因機器學習技術而顯現的問題。

第一節　資訊隱私早期的發展：“The Right to Be Let Alone”、私密典範

在個人資料自主控制理論之前，主要引導規範的資訊隱私理論是保護個人秘密與親密關係之私密理論。而私密理論成為早期的規範典範，是因為其抓準隱私權這項模糊的權利之核心、不可化約或取代的意義。因而在私密理論之前，本文將先說明隱私權的緣起——Samuel Warren 和 Louis Brandeis 提出之獨處權（The Right to Be Let Alone）概念。

第一項 新興大眾傳播資訊技術與“The Right to Privacy”

隱私權出現在法律領域的討論，始自 1890 年美國法律學家 Samuel Warren 和

[49] Warren and Brandeis, *supra* note 41.

doi:10.6342/NTU202500550

Louis Brandeis 發表的〈隱私權〉一文。Warren 和 Brandeis 著作此文之起因是新興的大眾傳播資訊操作與技術——八卦新聞、手持相機的興盛，干預公眾人物的私生活安寧。Warren 和 Brandeis 以隱私權為題，透過普通法中不被打擾的權利之解釋，建立一項普通法上的權利。

19 世紀末，報紙媒體興盛、數量繁多，報紙媒體業者為了競逐大眾的注意力使用新興的手持相機之即時攝影工具（instantaneous photography）擷取、記錄公眾人物的私人生活，製作聳動的八卦新聞（yellow journalism），例如從屋頂、窗外偷拍名人在家宅內的生活，或者潛入家宴蒐集新聞素材。嚴重地侵害公眾人物的私人生活領域[50]。譁眾取寵的新聞媒體挖掘原只存在於個人家宅、私人關係中的家庭關係、私人對話、性生活細節等資訊，加油添醋、寫成新聞，再端進大眾的視野，供人翻閱、品咂、評論。對於私生活被揭露的人而言，私密事務為人所知、成為大眾話柄，將產生莫大的精神痛苦[51]。此外，隱然存在的私生活被侵入、擷取風險，讓人們的生活無法安適、如坐針氈、瞻前顧後。

為了處理前述由新聞媒體與新興資訊工具對個人造成的侵擾，Warren 和 Brandeis 試圖在普通法體系中建立隱私權的概念。由於社會的變遷，普通法系統逐漸開拓其保障的個人權利，從實際損害、實體財產之侵害，向精神損害、無體財產權擴展。對個人生活面向的保護，不只是能夠生存的程度，個人自由開展其生活的能力亦受普通法保護[52]。

因此 Warren 和 Brandeis 以普通法保護個人獨處、私生活不受打擾的權利（the right to be let alone）之概念為基礎，進而主張普通法保護個人有決定其思想、感受、情緒與他人溝通的程度，個人的思想、感受、情緒在未得其同意之下不被強迫揭露，個人亦得決定揭露的範圍[53]。是為 Warren 和 Brandeis 主張之隱私權的內

[50] *See id.* at 195; *See also* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 10-12 (8 ed. 2024).
[51] *See* Warren and Brandeis, *supra* note 41, at 196.
[52] *See id.* at 193-95.
[53] *See id.* at 198.

doi:10.6342/NTU202500550

涵，而個人的思想、情感一旦揭露，即掉出隱私權的保障範圍[54]。

另外，Warren 和 Brandeis 透過隱私權與普通法的名譽權、智慧財產權法的著作權之比較，分析隱私權之特徵。隱私權與名譽權的相近之處，在於二者皆在對抗因揭露、傳播關於權利主體之事務而造成的精神、情感上傷害。而二者不同的是，名譽權在意的是個人與外部社會、他人之間的連結被破壞，即名譽、社會形象的貶損；隱私權則保護個人內心世界的平穩，即揭露行為對個人的自我評價、情感造成的波動與扭曲。隱私權雖與著作權都是保護個人無形的精神產物不被公開，而有相似處，然而，著作權保護的是公開行為帶來的財產利益，而隱私權則是保護個人因免於強制揭露而產生的心靈平靜與安適[55]。因此，隱私權保護的是個人的內在自由，其性質是來自人格不受侵犯的法理，非財產權[56]。

Warren 和 Brandeis 之主張的重要性，在於他們辨識出當時人們之私人生活被侵擾的朦朧感受，賦予規範性意義，並找到在訴訟上可資主張的法律依據與救濟途徑。Warren 和 Brandeis 的隱私權是因新興的媒體操作和資訊工具之社會變遷而起，保護無形的私人思想、感受、情緒不被揭露，以個人自願公開為權利範圍的極限。因其保護的是個人免於私生活內容被揭露而有的內在平靜感受、生活發展自由，屬於人格權性質。

而 Warren 和 Brandeis 也僅是點出人們隱私權保障的需求，並未建立完整、穩固的隱私權理論及規範框架，或許他們亦無意為之。無形的個人思想與情感、內在心靈平靜、私生活範圍等，皆是抽象、模糊而難以操作的概念。美國普通法系統的隱私權輪廓係由後續侵權行為實務案件所累積，侵權行為法學者 William Prosser 在 Warren 和 Brandeis 之後，整理了 19 世紀末至 20 世紀中之美國有關隱私侵權行為的案件，歸納出四種類型：侵害他人幽居獨處或私人事務、公開揭露使

[54] *See id.* at 199.
[55] *See id.* at 200.
[56] *See id.* at 205.

doi:10.6342/NTU202500550

人困擾的私人事實、公開揭露致使他人遭受公眾誤解、為自己利益而使用他人姓名或肖像[57]。除了民事關係中的隱私權，美國在憲法層次，聯邦最高法院在涉及不同的憲法增修條文案件，含糊地表示存在受憲法保障的隱私利益，係由個別憲法增修條文保障範圍的暈影疊合之下映照出的。聯邦最高法院所承認的隱私利益，有基於憲法增修條文第 4 條、第 5 條以及其他條文而保護到的身體與財產之空間隱私[58]、自主做成重大決定的隱私、私人事務不被揭露的隱私[59]。

第二項 資訊隱私權的私密典範與其侷限

早期學說與實務探索隱私權內涵的過程中，縱因各說論述路徑與關注利益不一，而無得以服眾的單一隱私概念，然隱私仍有其核心意義，使得隱私權有不可被其他權利取代之受保障必要。隱私的核心概念為個人未公開、未曾揭露之秘密，以及涉及個人親密關係之事務，因此發展出秘密理論與親密理論。根據 Daniel Solove 的整理，其將保障個人未公開領域、資訊之隱私權理論稱為「秘密典範」[60]，而本文將另一主流理論——親密理論[61]，與秘密理論併而稱為「私密理論／典範」。

第一款 資訊隱私權的秘密與親密理論

隱私、資訊隱私雖然是一含糊的概念，其仍有不可化約的意義：個人的私密空間與私人事務。私密典範下的隱私權便是保護個人的私密空間不被他人侵擾、私密事務不被揭露的狀態。而獨處、事務私密性也是 Warren 和 Brandeis 辨識出的隱私利益[62]。

私密典範認為隱私權所保障個人的資訊隱私是秘密、涉及私密生活之資訊。

---

[57] *See* William L. Prosser, *Privacy*, 48 CALIF. LAW REV. 383 (1960). 中文翻譯與介紹參見王澤鑑（2012），《人格權法：法釋義學、比較法、案例研究》，頁 215，臺北，自版。
[58] *See* SOLOVE, *supra* note 15, at 63-64.
[59] *See id.* at 64-67.
[60] *See id.* at 111.
[61] *See id.* at 34.
[62] *See* Prosser, *supra* note 57.at 392.

doi:10.6342/NTU202500550

秘密是指原本被掩蓋、隱藏而不為人知的資訊[63]。私密資訊則根據資訊內容所涉主題係依社會通念判斷，屬於私人、不被公知之事務，而為判斷，例如身體私密特徵、性生活、生理健康狀況、財務資訊等[64]。

秘密理論認為隱私權保護原本不為人所知之資訊不被強迫揭露，能維護個人的人性尊嚴、確保其行為與人格發展自由，為建構隱私權的正當基礎。想像一個全然透明的社會，社會中的個人毫無遮蔽他人目光、聽聞、知悉的私人空間，所有個人資訊皆可任意散布。首先，不顧個人的意願而恣意觀看、取用、傳播、任意曝光所有個人資訊，係貶抑個人的尊嚴[65]。另外，就行為與人格發展自由之影響，完全敞開個人生活於社會、他人的視野中，使社會規範與他人期待流入、滲透個人生活所有層理，一則個人因欠缺不被外界眼光檢視的私密領域，而不願做出未成熟或荒誕的行為，而這些行為卻是磨練新技能、進行思想實驗所必要的[66]；其次，個人必須時刻要求己身行為符合社會期待，難以獲得片刻輕鬆，而此自我檢視、緊繃壓抑、懼怕社會制裁或負面評價的心緒，除了拘束個人行為之外，可能導致過度的心理壓力，甚至是心理崩潰[67]；最後，道德上自主的人，必須能夠反思、批判社會規範並獨立地做出遵循與否的決定，而對社會規範的反思與批判須有探索、試驗不合常規的思想與行為之空間，完全透明的社會壓縮此空間至幾不存在的程度，探索、試驗、表達、討論、挑戰常規正當性可能對個人帶來不利影響、成本過高，個人失去道德自主的可能性[68]。

從上述論點可知，一不被揭露而得以放鬆、自在抒展的生活範圍，是人們在摩肩接踵的現代社會生存所必須，私密理論即認為此範圍是不為人所知之秘密以及親密關係。

---

[63] *See* DANIEL J. SOLOVE, *supra* note 15. at 21.
[64] *See* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 19-20 (1 ed. 2018).
[65] *See* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE LAW J. 421, 447 (1980).
[66] *See id.* at 449.
[67] *See id.* at 449.
[68] *See id.* at 449-50.

doi:10.6342/NTU202500550

另一項保護個人資訊不被任意揭露的原因是，個人能夠透過資訊保留與揭露之安排，構築與維持人際與社會關係、經營社會形象[69]。個人資訊是他人、社會認識個人的基礎，個人在不同社會情境中，依其扮演的社會角色常規、與他人的關係，自主決定個人資訊揭露的內容、程度、範圍，形塑他人對己之認識、外在形象，建構多層次的社會關係。而個人亦可選擇隱藏互動對象不喜歡的意見與行為，維持人際關係[70]。除此之外，有關個人親密生活、涉及不符合社會常規行為之資訊之揭露，將造成個人脆弱化、或顯露在緊密連結關係產生的情感，個人透過這些資訊的分享，表示信任並加強、維繫親密關係[71]。

第二款 私密典範下的資訊隱私規範

私密理論因直指資訊隱私權之核心，而被立法者與司法實務接受。在我國，刑法第 315-1 條第 2 款規定，無故竊錄他人非公開活動、言論、談話或身體隱私部位者，處罰之。旨在保護個人隱私而限制國家監察人民通訊內容之行為之通訊保障及監察法，在第 3 條規定該法適用之通訊內容以有隱私或秘密之合理期待者為限。電信法第 6 條規定不得盜錄電信事業及專用電信處理之通信而侵害他人秘密，電信事業更有保護通信秘密之義務。而隱私權在民事關係上，自 1999 年民法第 195 條第 1 項有關人格權侵害的非財產損害賠償規定增列隱私，到大法官在釋字第 585 號及 603 號解釋明白說明隱私權的內涵之前，法院對民法第 195 條第 1 項的隱私權之解釋雖仍不穩固[72]，但從上述階段有關資訊隱私侵權行為的判決中，

---

[69] *See id.* at 450.

[70] *See id.* at 450; *See* WALDMAN, *supra* note 64. at 19-20. 有關社會角色、互動與隱私的關係，另可參考 Erving Goffman 的劇場理論。Goffman 將個人與社會互動場境比擬為社會角色與戲臺。個別的社會關係通常會產生適宜於該關係之參與者行為常規，參與者依循該常規而行動、他人亦期待該常規被遵守，而維持穩定的社會互動關係。如劇場的運作，角色扮演者（個人）根據角色的劇本（行為常規）演出。而資訊隱私如同演出時觀眾看不到的後臺，個人得以在此放置、施展不符常規的行為，釋放不符常規的情緒，練習尚未成熟的行為，以及切換劇本，準備上戲。*See* ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE 106-14(1959).

[71] 詳言之，不合常規的行為會對個人帶來負面評價或不利後果；而就涉及性的層面，連結到人類的生物本質，動物在性行為的過程防備性、警戒心較低，而需要於具安全性、可信任的環境進行；而涉及親子照護養育、情愛關係之資訊，因屬於人際之間緊密連結關係的資訊，通常也會被看作是親密資訊。

[72] 有未說明隱私權內容，而直接以某資訊是個人隱私、某行為係侵害隱私權的模式來論理之判決

doi:10.6342/NTU202500550

可以看出法院認定的資訊隱私範圍確是較貼近個人私生活層面的，如身體健康與疾病資訊[73]、性行為[74]、洗澡如廁等私密生活[75]、電話通訊內容[76]、住址及電話號碼[77]、住宅內非公開活動[78]、財務狀況[79]等。而孫森焱認為民法第 195 條第 1 項的隱私權是「以保護個人的私生活為內容」，而「揭露他人個人生活或家庭生活」構成隱私權侵害[80]。

而德國民法透過第 823 條第 1 項的概括條款連結基本法第 1 條與第 2 條的一般人格權，涵蓋到隱私權保護。法院實務在人口普查案之前主要是採取領域理論為主流見解，領域理論將個人生活分成隱密領域、私密領域、個人領域三個層次，隱密領域為極度私密之個人事務，涉及人性尊嚴的核心而受絕對保護；而因個人與他人、社會的交疊，私密、個人領域的事務受隱私權保障的程度降低[81]。

在美國，資訊隱私之私密典範可在憲法層次對隱私利益的保護及民事隱私侵權行為法中見得。聯邦最高法院目前雖未賦予隱私權憲法上權利地位，然在 Griswold v. Connecticut[82]案中提出了暈影（penumbra）理論，Douglas 大法官主筆的多數意見表示，個人的隱私領域可能受到憲法個別條款之保障範圍所涵蓋。而

（參臺灣高等法院 89 年度上易字第 400 號民事判決、臺灣高等法院 89 年度上易字第 611 號民事判決、臺灣高等法院 臺中分院 93 年度上易字第 445 號民事判決、臺灣高等法院 臺南分院 90 年度訴易字第 9 號民事判決、臺灣高等法院 高雄分院 92 年度訴字第 9 號民事判決）。而有較詳盡地說明隱私權內涵者，認為隱私權是「不讓他人無端干預其個人私的領域之權利」（參最高法院 93 年度台上字第 1979 號民事判決、臺灣高等法院 90 年度訴字第 139 號民事判決、臺灣高等法院 94 年度重上字第 106 號民事判決），為人格權性質（參最高法院 93 年度台上字第 1979 號民事判決、臺灣高等法院 90 年度訴字第 139 號民事判決），保護私人生活不被知悉、揭露個人生活或家庭生活構成隱私權侵害（參臺灣高等法院 94 年度重上字第 106 號民事判決、臺灣高等法院 高雄分院 91 年度上易字第 37 號民事判決）。

[73] 臺灣高等法院 臺中分院 93 年度上易字第 445 號民事判決。

[74] 臺灣高等法院 90 年度訴字第 139 號民事判決。

[75] 臺灣高等法院 高雄分院 92 年度訴字第 9 號民事判決。

[76] 臺灣高等法院 89 年度上易字第 400 號民事判決、臺灣高等法院 89 年度上易字第 611 號民事判決。

[77] 最高法院 93 年度台上字第 1979 號民事判決。

[78] 臺灣高等法院 臺南分院 90 年度訴易字第 9 號民事判決。

[79] 臺灣高等法院 94 年度重上字第 106 號民事判決。

[80] 孫森焱（2020），《民法債編總論上冊》，頁 221，自版。

[81] 王澤鑑，前揭註 57，頁 231-234。

[82] Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

doi:10.6342/NTU202500550

私密典範在美國憲法增修條文第 4 條的憲法實務案件甚為明顯，該條保護人民身體、住所、文件與財物不受政府不合理拘捕、搜索、扣押，其重要目的之一為保護個人隱私[83]，聯邦最高法院在判斷政府行為是否構成隱私權干預係賴於 Harlan 大法官在 Katz v. United States[84]案的協同意見書提出的隱私合理期待判準[85]，要件有二：個人有主觀隱私期待、該隱私期待係客觀上合理，隱私合理期待判準衍生出公開原則、第三人原則等次原則，在資訊隱私脈絡下，個人資訊一旦公開或揭露給第三人，即不受隱私權所保障[86]。

而美國的隱私侵權行為法中，涉及資訊隱私者為 Prosser 整理的第二種案型：公開揭露使人困擾的私人事實[87]。典型案例如將他人過去不堪的事蹟製作為節目在電視或廣播播送。本案型有三項要件：公開揭露行為、私密事實、揭露具冒犯性。其中，事實之私密性要求該事實非已公知，Prosser 認為個人在公開場所的私人行動以及非機密之公共檔案不具有私密性，而若資訊之揭露係因個人非自願公開，該資訊因揭露自願性有瑕疵而仍受隱私權保護[88]。

第三款 秘密典範的問題

私密理論對於資訊隱私權保障的關鍵是資訊所涉事務的性質、公開與否的問題，因而發展出第三人原則、公開原則作為輔助判準。越接近個人私生活領域核心事務之資訊，受隱私權保障程度越高，而如個人外表、職業、公共場所之活動等非私密資訊，可能不受保障。縱使為私密資訊，經合法揭露、公開即脫離資訊

[83] SOLOVE, *supra* note 15, at 13.
[84] Katz v. United States, 389 U.S. 347, 360 (1967).
[85] *Id*. at 360-61; 林子儀（2015），〈公共隱私權〉，《第五屆馬漢寶講座論文彙編》，馬氏思上文教基金會，頁 41。
[86] 張陳弘（2018），〈隱私之合理期待標準於我國司法實務的操作—我的期待？你的合理？誰的隱私？〉，《法令月刊》，69 卷 2 期，頁 84-85；林子儀，前揭註 23，頁 44-46。
[87] 第一種案型「侵害他人幽居獨處或私人事務」聚焦在獨處、隔絕他人的利益；第三種案型「公開揭露致使他人遭受公眾誤解」著重個人形象不受扭曲之保護；第四種案型「為自己利益而使用他人姓名或肖像」主要是關注個人姓名或肖像的財產利益。相關文獻中文部分參：王澤鑑，前揭註 57，頁 215-217；英文部分 *See* Prosser, *supra* note 57.
[88] *See id.* at 392-97.

doi:10.6342/NTU202500550

隱私保護範圍。

私密典範的特性也是其最顯著問題，以資訊性質和公開與否來判斷保障範圍過度限縮資訊隱私權。如前述，資訊私密性是私密理論下的資訊隱私權界限，因此開展出第三人原則，即已公開或已揭露給第三人之私密資訊，或者公開場所的私人行動等非私密資訊，不受資訊隱私權保障[89]。上述問題在類比資訊的時代並不明顯，然而在電腦、資料庫、網際網路等數位資訊技術流行之後，改變資訊的記錄、儲存、傳遞與接收的主要型態與模式。過去人際溝通往來係當面交流、書信、電話，而數位時代下的人們仰賴數位資訊技術與他人、公私部門交往聯絡，與數位資訊技術互動之行為轉置成資料，留存、傳輸於電腦或網路上的資料庫；公共空間中的私人行為或個人資訊，可能被監視器或其他資訊技術長期記錄、大量擷取，拼湊出個人的私生活圖像。上述情況在私密典範下，因揭露給第三人、已公開等理由而不受資訊隱私權的保障，如此結論使得個人資訊隱私幾不存在，網頁瀏覽紀錄、通聯紀錄、聊天訊息、電子郵件內容等資料，以及聚合大量公開或非私密資料所形成的私生活態樣，俱屬公共領域的資訊，任人取用，個人的私領域危如累卵。

前述問題彰顯了出自報紙、相機為首要資訊媒介與工具的私密理論，面對電腦、資料庫、網路等新的技術工具已有不足，人們重新辯證資訊隱私權的應有典範。在此背景下，個人資料自主控制理論成為新興的資訊隱私典範，將資訊隱私權的保護力推展至所有個人資訊、資訊公開揭露後的階段。

第二節　資訊隱私現有典範——個人資料自主控制之理論介紹

自主控制理論主張資訊隱私權保障個人有自主地決定資訊揭露與否、揭露對象、揭露程度、揭露範圍之權利。理論目的是在處理電腦、資料庫、網際網路出現、流行後所產生國家以及後來加入的私部門以掌握個人資料方式執行的監控問

[89] 參見林子儀，前揭註 85，頁 44-46。

doi:10.6342/NTU202500550

題，自主控制理論認為以個人知情同意為條件的個人資料蒐集使用，能夠阻絕秘密情蒐與監控行為。而理論的基礎係對個人自主性的尊重，因個人資訊是人際交往、相互認識的媒介、素材，應由個人自己管領私密領域的邊界、發展多元的社會關係。因此本節將介紹自主控制理論的發展與基礎。

第一項 技術背景：電腦、資料庫與網際網路

自主控制理論的出現，主要是為了回應資訊數位化與電腦、資料庫與網際網路等相關技術工具所帶來的個人資料化與監控的資訊隱私威脅。

先略為說明自主控制理論提出時的技術背景。資訊數位化是指將資訊以可被運算的數字型態表示，並由無形的光波或電波作為介質而便於儲存與傳輸。1960年代，數位資訊科技在戰爭結束後從軍事用途解放而逐漸普及、純熟。電腦是負責運算、儲存數位資料的自動化工具，硬體內配有儲存空間與運算處理單元，數位資料儲存於硬體內的儲存空間或外部硬碟，以供內部程式與外部裝置存取[90]。資料庫是指有相關聯的資料為了服務一個或多個用途而儲存在一起的資料集合[91]，存在於電腦系統中。網際網路是連結個別電腦主機網域組成的網絡[92]，在自主控制理論出現的年代，電腦相當昂貴，一臺主機可能同時連結數臺終端裝置，透過分時處理（time sharing）和遠距存取（remote access）技術分配、共享資源，可見網絡的雛型[93]，商用網際網路到 1990 年代才普及[94]。而自主控制理論的發展有兩波，第一波是回應電腦與資料庫的問題；第二波則是因網際網路普及而發展出強化的自主控制理論。

在電腦、資料庫與其他資訊技術工具輔助下，個人的特徵、性格、行為等資

[90] *See* ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 11-15 (1971).
[91] *See* SATINDER BAL GUPTA & ADITYA MITTAL, INTRODUCTION TO DATABASE MANAGEMENT SYSTEM 3 (Second editon ed. 2017).
[92] *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VANDERBILT LAW REV. 1609, 1618 (1999).
[93] *See* MILLER, *supra* note 90, at 15-20.
[94] 參見 Douglas E. Comer（著），鄭王駿等（譯）（2019），《電腦與網際網路國際版》，頁 18，全華。

doi:10.6342/NTU202500550

訊被轉換為資料，流入公、私部門掌握的資料庫當中，資料庫之間彼此串聯而累積出詳實的個人資料檔案。以公部門而言，除了已行之有年的人口普查[95]，隨著國家任務的擴張，政府部門為了行政、社會福利、犯罪偵查等目的蒐集、儲存人民資料。私部門亦然，工業化之後社會分工日趨細緻，人們與私部門建立繁複的關係，個人資料在交涉的過程進入由私部門掌握的資料庫。

公、私部門蒐集、儲存大量的個人資料與建立個人檔案產生個人資料化與監控的問題。個人資料化為個人的生理或心理特徵、經驗、行為等資訊被轉換為數位資料。因科技持續發展、升級，個人資料化被取得的範圍更廣且深、個人資料檔案的內容更細緻。在主動揭露的部分，數位資訊科技持續升級，資料儲存成本下降，資料主體與公、私部門交涉時，被要求提供的資訊項目增多，例如向曾經近用司法資源的人民進行司法滿意度調查；雇主要求求職者做人格測驗並將測驗結果納入評估[96]。而因監視器、竊聽器、電子腳鐐等電子裝置，個人的活動在不自覺之下被長時間、自動地蒐集[97]。此外，資訊被擷取的範圍除了外在行動，包含生理條件，如基因、抽血檢查的項目、心跳、腦波等，以及從生理資訊推測出的心理狀態，如測謊等。

個人資料化造成個人無法控制其資料與受錯誤評價的問題。個人資料失控是指個人資料的蒐集與使用的情境、資料的正確性逸脫資料主體和資料控制者的控制。主要的原因是資訊溝通型態與參與者的改變，過去資訊溝通的方式是人際互動和以實體載體來傳遞資訊；在數位時代，數位資料係由人類無法直接控制的光波、電波等無體物質傳遞，因此，電腦等數位工具系統加入資訊溝通過程，代替人類記憶、處理、傳輸資訊，人類操作電腦與資訊互動。個人資訊進入數位系統之後可能經歷：數位化輸入、硬體儲存、軟體程式近用、網路傳輸、進入其他系

[95] *See* SOLOVE, *supra* note 15, at 13-14.
[96] *See* WESTIN, supra note 43.
[97] *See* Charles Fried, *Privacy*, 77 YALE LAW J. 475, 475-76 (1968); *see also* WESTIN, *supra* note 43, at 69-90.

doi:10.6342/NTU202500550

統等環節，而硬體、軟體、系統、網路由不同的服務提供者維護。一則資料主體難以確實、即時地掌握資訊的處理流程、近用者[98]；二則各個環節可能因硬體毀損、軟體故障、內部人員故意或過失、外部人員侵入，發生資料不正確、過時、外洩[99]。在各環節多以自動化系統彼此相連、傳遞無體資訊的資訊溝通環境下，個人資料傳播的範圍與模式，資料主體難以想像與確認，資料的正確性、安全性也隨著其在資訊系統中流轉的時間和歷程而下降。

公、私部門與個人交涉、作成決定時，為求客觀、效率，以評估個人資料檔案的方式取代實際的溝通互動，例如信用評分報告、求職履歷檔案。如前述，個人資料檔案的資料在資訊系統中幾經流轉，有過時、不正確的可能性，根據有錯誤的資料檔案做出的評估決定即有瑕疵。縱使資料正確，無節制地拼湊其他情境下蒐集的個人資料，將資料移出原始蒐集情境，置於其他目的下使用，可能發生不當詮釋的問題。舉例而言，在信用評分報告不當列入學歷，給予高中肄業者較低的信用分數；某公司評估求職者的資格時，篩掉因參與民權運動而被判以毀損公物罪的某 A[100]。

數位資訊技術工具能夠蒐集個人在實體空間與數位空間的行為活動，產生監控的疑慮。監控是指以影響、管束、保護或指引為目的，而集中、持續、系統性地關注個人[101]。公部門為國家安全、犯罪偵查等公益目的，私部門為評估是否與個人建立關係，而利用監聽器、監視器、定位系統長時間、不間斷地擷錄特定空間內或特定個人在實體空間的行為活動，以及持續、廣泛蒐集特定個人在數位空間留存的資料、行為軌跡，聚集成資料檔案，細緻地描摹、模擬、推論出資料主體的性格、生活態樣，已屬於監控的行為。

監控是一種社會控制的手段，適度的監督與控制機制能夠維持秩序，例如設

[98] *See* MILLER, *supra* note 90, at 26-32.
[99] *See id.* at 25-32.
[100] *See id.* at 32-38.
[101] *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. LAW REV. 1934, 1937 (2013).

doi:10.6342/NTU202500550

置在公共場所的監視器、國會議事直播等。然而，不當、過度的監控，將造成個人心理不適、改變行為順從常規，以及監控者與被監控者之間權力失衡、能動性遭到抑制的影響。當人們感受到來自他人的眼光、持續的關注，會有不自在、不安、焦躁的心理狀態。此外，受到監控的人為避免被負面評價、受到不利待遇，順從監控者的眼光而自我審查、自我約束，做出符合監控者意志的行為[102]。監控者與被監控者之間存在權力不對等的現象：監控者透過持續觀察知悉被監控者曾做過的行為，被監控者懼怕揭露其行為之後帶來的負面影響[103]；監控者累積資料熟識被監控者，針對其性格、習慣、偏好等投放資訊、說服被監控者作出特定行為[104]；監控者蒐集多數被監控者資訊後，將被監控者分群，根據群體的特性為差別對待[105]。

第二項 資訊隱私的個人資料自主控制理論

個人資料自主控制理論認為面對資訊數位化及相關資訊技術工具帶來的個人資料化、監控的現實，以資訊私密性之保護為核心的秘密理論，既以私密性之要件過度限縮資訊隱私權的保障範圍，資訊隱私權又只有排除他人侵害資訊私密性的消極權能，對個人之保護顯有不周。

首先，在資訊數位化的時代，數位資料是個人與政府和私人之間主要的資訊溝通素材，但對於分享、揭露給第三人的個人資訊，未必被認為已非屬隱私，例如行政院內政部為減少租屋者經濟負擔，推出 300 億元中央擴大租金補貼之租金補助專案，申請人須提供身分證字號等身分驗證資訊、戶籍及通訊地址、撥款帳戶、租屋地址及契約，以及申請人的配偶與子女身分證字號等身分驗證資訊申請租金補助，以上資訊縱使已供予內政部作為租金補助資格審核之用，我們也不認為這些資訊因此不屬於個人隱私[106]。再舉一例，我們使用聊天軟體與親友聯繫，

[102] *See* SOLOVE, *supra* note 15, at 106-109.
[103] *See* Richards, *supra* note 101, at 1953-55.
[104] *See id.* at 1955-56.
[105] *See id.* at 1956-58.
[106] 300億元中央擴大租金補貼專區，https://has.cpami.gov.tw/house300e/（最後瀏覽日：12/26/2024）。

doi:10.6342/NTU202500550

傳送文字、語音、圖片與影片資訊，分享心事與生活，聊天軟體的訊息傳遞使用者與接收者、軟體開發者俱有聊天的內容資訊，然而我們仍認為這些訊息是個人隱私。再者，在資料庫集中儲存大量個人資訊以及電腦資訊處理的技術背景之下，被秘密典範認定非屬隱私之非私密資訊與前述已揭露資訊，仍可能透過個人資訊的聚合而拼湊出個人私生活的風貌，例如購物網站上的購物紀錄是消費者與購物網站業者為了完成交易所產生的資訊，然而，業者能夠透過購物紀錄資訊，推論出該消費者是否養寵物、喜愛的動畫或明星、閱讀偏好，甚至是性傾向或生理需求等私密資訊，基於行銷目的，寄送符合消費者偏好與需求的廣告。

從前述內容可知，資訊數位化改變資訊溝通模式以及開發出資訊的潛能，在以數位資料為主要媒介的資訊溝通模式下，發生個人資料化的現象，縱使我們仍認該資訊為個人隱私，也因溝通模式之改變而向他人揭露；數位資料被聚集經處理分析後有產出更多資訊的能力，個人資料被挪為其他目的使用，不具私密性的資訊成為分析推論私生活資訊的素材，而透過持續蒐集處理與分析大量的個人資料來認識資料主體的行為，產生潛在的監控威脅。

為了回應前述問題，自主控制理論主張資訊隱私是個人自己決定個人資訊與他人溝通與交流的時點、條件與程度[107]。自主控制理論將資訊隱私權的保障推展至所有個人資訊，資訊隱私權的保障利益隨之擴張，包含資訊的私密性與個人的自主性，權利功能從消極排他權擴及積極地要求實現個人資料的自主控制。

對於從私密資訊擴張到所有個人資訊的理由，除了回應資訊數位化這項現實改變所致之個人資料化與資料累積而生的監控危險之外，Alan Westin 對隱私社會功能的討論可資為據。為了穩固隱私權的基礎，Westin 主張隱私不是依附於現代社會現實所產生的，而是根植於人類的生物本能。為了生存，動物需要有足量水、食物維生且不被掠奪、掠食者入侵的個體與群體地域；在群體中，個體以距離設

[107] *See* WESTIN, *supra* note 43, at 7.

doi:10.6342/NTU202500550

定的機制來維持親密關係；然而，對某些動物而言，群居也是禦敵和維持群體多樣性的必要機制[108]。如上，隱私是個人私領域與社會、公領域之間的界線，Westin 進而主張隱私因社會文化、人際關係、個體而有殊異。Westin 舉了數個國家或地區的社會常規論證隱私界線因社會文化而異的主張，有些地區重視家族、社群之間的互助與分享，家族成員不分親疏或男女而共居一屋、比身而寢；有些地區則裸身生活；亦有地區的家宅不設門戶，可隨意走入他人屋內[109]。隱私的界線與管領是個人建立與維繫不同人際、社會關係的必要條件：個人身處於社會當中，勢必因人際互動或其他因素而備感壓力，隱私使個人能夠隱藏自我、釋放情緒；個人藉由控管涉己之資訊的流動，設定與他人的關係、互動規則，與控制他人對己之認識[110]。

隱私是個人設定自我、他人、社會之間的距離與生活領域的界線，在資訊隱私的脈絡下，隱私的界線係由個人資訊的往來設定的，因資訊隱私主體、所涉關係、社會文化而有不同，資訊隱私的範圍不應以秘密性界分，而是由資訊隱私主體及所處情境、社會決定。

自主控制理論擴張資訊隱私權保護的第二個取徑是將理論基礎建立於個人的自主性：自主性的展顯、自主性的維護。在自主性的展顯，個人是個人資訊之使用的決策者[111]。一方面是基於資訊與個人之間的連結、歸屬關係，個人資訊應屬個人的管領支配範圍；另方面則是個人資訊的社會功能、工具價值，即個人透過個人資訊流的分享與節制，控管他人對己的認識、與他人建立與維繫關係。此涉個人對其形象、人際關係的自主性。而就自主性的維護，個人是獨立、自我負責、有道德能動性的存在，能夠審慎思考、安排人生並予以實踐。然而，人不是遺世獨立，而是生活與社會中、與其他行動者共存，審慎思考與實踐決定的自主能力

[108] *See id.*
[109] *See id.*
[110] *See id.*
[111] *See* Schwartz, *supra* note 92, at 1558-60.

doi:10.6342/NTU202500550

必然受其他行動者影響。當個人審慎思考作成決定、實踐決定的過程受到外力干預，個人的自主能力與自我決定便受到抑制。例如以個人無法拒絕的方式說服該個人作成有利於說服者目的而非個人設定之目的之強制行為[112]。利用數位資訊技術工具實際觀看或暗中蒐集資料的監控行為，形塑監控者與被監控者的權力不對等關係，強迫被監控者服從或幽然地操弄被監控者的行為，限制個人的自主性。

因此，不論是從個人對其資訊的管領關係、對形象與社會關係的安排與維護、對抗權力不對等下自主性的喪失，自主控制理論認為應是個人自己決定個人資料是否、如何被使用。而回復並保護個人資訊隱私的自主性的方法是讓個人在資料蒐集與使用的過程有控制、參與決策的能力。由自主、理性的個人根據當下的情境，評估個人資料揭露與保留對己的利益與可能產生的風險，決定哪些個人資料應保留、哪些得揭露，以及揭露的條件[113]。且因個人資料是否為隱私這項問題，亦須依所涉文化脈絡、個人偏好判斷；又因非傳統所認之隱私資訊經數位技術加工後，產生讓個人感到隱私被侵害的結果，資訊隱私的範圍擴及所有的個人資料。

第三節　個人資料自主控制典範：知情同意原則、事後控制權、個人資料處理原則

面對電腦自動化機器、資料庫系統、網際網路等資訊數位化技術工具造成的諸項資訊隱私問題，個人資料自主控制理論被廣為接受，成為資訊隱私、個人資料保護規範的典範。自主控制典範引導三項立法方針：資料主體知情同意、個人資料蒐集使用原則、資料主體行使權利之事後控制模式，以下逐一介紹。

第一項 事前同意：知情同意原則

知情同意原則，是自主控制典範實現個人自主最重要的立法原則。其意義為

[112] *See id.* at 1653-58.
[113] *See* ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, *Records, Computers, and the Rights of Citizens*, 38-40 (1973).

doi:10.6342/NTU202500550

向資料主體取得個人資料之前，告知其有關資料蒐集、處理之情事、目的、方式、資料的蒐集或處理者身分等資訊，並取得資料主體的同意，作為個人資料蒐集、處理的條件[114]。

知情同意在道德上效力是個人欲與他人建立關係時，根據雙方的溝通與協商，考慮自己與他人的條件、審慎評估利弊，以授予權利、負擔義務的意思，並作出具同意與他人成立關係之意思的行為[115]。對現代社會，上述機制以個人自由、理性的決定，安排人際關係、訂立規則、構築社會，取代王權、親族家長等上位權威頒布的命令[116]。在法規範領域，知情同意原則亦不陌生，如契約關係的建立、所有權的讓與、侵權行為以當事人同意為阻卻違法事由等[117]。

知情同意對資訊隱私權之保護舉足輕重。在侵權行為法層次，法院實務認為當事人自願提供個人資料不構成隱私權之侵害[118]。而在個人資料保護規範，自主控制理論認為所有個人資料皆為資訊隱私權的保障客體，法規範原則上不代替資料主體決定何為隱私而應保留、何種情況則可揭露的問題，以此實現資料主體的自主決定權。知情同意被認為是當事人的授權機制，是資料蒐集、處理合法要件之一。

知情同意是個人資料蒐集使用相關規範之核心原則。在美國法，雖然目前在聯邦法層級僅有限定在個別資料屬性或法律關係之隱私規範[119]，一般性資訊隱私

---

[114] *See* Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 MD. LAW REV. 439, 450 (2020); *see also* Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 BOSTON UNIV. LAW REV. 593, 599-600 (2024). 中文文獻參見劉定基（2013），〈析論個人資料保護法上「當事人同意」的概念〉，《月旦法學雜誌》，218 期，頁 146。

[115] *See* Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. UNIV. LAW REV. 1461, 1468 (2019).

[116] *See id.* at 1467-68.

[117] *See id.* at 1468-71.

[118] 王澤鑑，前揭註 57，頁 285。

[119] 例如健康資訊轉移與責任法（Health Information Portability and Accountability Act of 1996）、家庭教育權與隱私法（Family Educational Rights and Privacy Act of 1974）、公正信用報告法（Fair Credit Reporting Act）、金融服務法（Gramm–Leach–Bliley Act）、錄影帶隱私保護法（Video Privacy Protection Act）等。

doi:10.6342/NTU202500550

或個人資料保護規範僅在州法層級可見[120]，然而，根據取用個人資料者的身分，在公部門取用的情形，進入憲法增修條文第 1、4、5 條等相關條文或涉及隱私利益的案例法規範框架，而就私人取用個人資料，美國實務上將個人與取用個人資料之私部門之間的法律關係以消費關係視之，落入聯邦交易委員會（Federal Trade Commission）的管轄範圍[121]。聯邦交易委員會以聯邦交易委員會法第 5 條對業者欺罔（deceptive）或不公正（unfair）交易行為之管制，作為保護消費者隱私的手段，在操作上，未適當告知消費者資訊行為可能構成不公平交易行為[122]。

而在歐盟的資訊隱私、個人資料保護規範架構，知情同意原則的色彩更清晰。與美國顯然不同的是，隱私權與個人資料保護權具有基本權地位，分別訂在歐盟基本權利憲章之第 7 條與第 8 條，第 8 條第 2 項便規定個人資料之處理必須是基於當事人同意或法律有規定，方能取得正當性。而資料保護一般規則是歐盟目前重要的資訊隱私規範之一，確保個人對其資料的控制是重要的立法目的[123]。知情同意原則化作一般、特種、兒童個人資料的合法處理依據之一，訂有寬嚴不同的要件[124]；此外，在資料主體權利的章節，一開始便規定資料主體與資料控管者之間的透明溝通程式要求[125]，以及資料控管者對資料主體的告知義務[126]，是為知情的體現。

---

[120] 例如加州隱私權法（California Privacy Rights Act）、維吉尼亞州消費者資料保護法（Virginia's Consumer Data Protection Act）、科羅拉多州隱私權法（Colorado's Privacy Rights Act）等。*See* Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME LAW REV. 975, 983-84 (2023). 有關加州隱私權法的中文介紹，可參：張陳弘，前揭註 30，頁 24。

[121] 相關中文文獻可參見劉定基（2009），〈欺罔與不公平資訊行為之規範—以美國聯邦交易委員會的管制案例為中心〉，《公平交易季刊》，17 卷 4 期，頁 57-91。英文文獻部分：Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEORGE WASH. LAW REV. 2230 (2015).

[122] 同前註，頁 66-67。*See* Richards and Hartzog, *supra* note 110, at 1471.

[123] 歐盟資料保護一般規則前言第 7 段。

[124] 歐盟資料保護一般規則第 4 條第 11 項規定一般同意的定義、第 7 條對一般同意訂有更詳盡的條件；第 6 條第 1 項為一般個人資料的處理要件，資料主體同意規定在 a 款；第 8 條針對兒童制定特別的規定，原則上 16 歲以下的兒童資料之處理應得監護人的同意；第 9 條第 2 項 b 款則規定，若要以資料主體同意為合法處理特種個人資料的依據，必須取得資料主體「明確」的同意，比一般同意的情形更嚴格。

[125] 歐盟資料保護一般規則第 12 條。

[126] 歐盟資料保護一般規則第 13 與 14 條。

doi:10.6342/NTU202500550

而我國的個人資料保護法，對於一般個人資料，在第 15 條與第 19 條分別就公務與非公務機關，規定當事人同意為合法蒐集、處理、利用的事由之一；在第 16 條與第 20 條則是資料原始蒐集目的外處理、利用之合法要件，當事人同意亦為其中一款。就特種個人資料，則是在第 6 條規定以當事人同意作為合法要件僅得限於取得書面同意之情形。而知情同意的定義與條件，第 7 條與第 8 條規定，公務與非公務機關應告知法定事項所取得之同意，才是我國個人資料保護法下適格的同意；第 9 條規定公務與非公務機關取得個人資料的來源非來自當事人提供時，仍應告知法定應告知事項[127]。

第二項 事後控制權

在資料蒐集處理關係當中，個人資料給出之後，通常將逸脫資料主體可控範圍，為了彌補個人作為資料主體在此關係當中的弱勢地位，自主控制典範以制定個人對其資料的具體控制權利，作為回復資料主體地位的手段[128]。在美國，第一個公平資訊行為準則是由 1973 年美國住宅、教育與福利部（Department of House, Education, and Welfare）組成自動化個人資料系統諮詢委員會（Advisory Committee on Automated Personal Data Systems）在〈紀錄、電腦與公民權利〉（Records, Computers, and the Rights of Citizens）報告中提出的[129]，這份報告不僅提出五項準則，同時說明個人資料保護規範必須使資料主體在資料蒐集處理的過程中，有參與的權能[130]。美國的各部隱私法通常設有資料主體的知情權、近用權、更正權等權利[131]。以加州的隱私保護法制為例，2020 年通過、2023 年施行的加州隱私權法（California Privacy Rights Act）取代 2018 年通過、2020 年施行的加州消費者隱私法（California Consumer Privacy Act），現行的加州隱私權法除了延續前法，設有知情、近用、刪除、退出等權利，再加入對敏感個人資料使用與揭露的

[127] 更詳細的說明，可參劉定基，前揭註 121。
[128] *See* Solove, *supra* note 20, at 979.
[129] 劉定基，前揭註 33，頁 270。*See id.* at 979-80.
[130] *See* ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, *supra* note 108, at 40-41.
[131] *See* Solove, *supra* note 20, at 979-81.

doi:10.6342/NTU202500550

權利、錯誤個人資料的更正權[132]。

於歐盟法，個人資料保護相關規範實現個人控制的方式亦為設計更細緻的資料主體權利[133]。資料保護一般規則在第三章訂有資料主體的權利，第 13 與 14 條為個人資料被蒐集處理時資料主體的受通知權、第 15 條為近用個人資料蒐集處理相關資訊之權利、第 16 條為錯誤資料的更正權、第 17 條是資料的刪除權、第 18 條是限制處理資料的權利、第 20 條為資料可攜權、第 21 條為拒絕特定處理行為的權利、第 22 條則是不受自動化決策權[134]。

我國的個人資料保護法，第 10 條規定當事人有查詢或請求閱覽資料的權利，在第 11 條第 1 項規定當事人的更正權、第 2 項是停止處理請求權、第 3 項為資料蒐集目的消失或期限屆滿時的刪除或停止處理請求權、第 4 項為違法蒐集、處理、利用個人資料之刪除或停止蒐集、處理、利用之請求權，第 12 條為資料被侵害時之受通知權。有關知情同意權之相關規定，已如前述，於茲不贅。

第三項 個人資料蒐集使用原則

在事前與事後之控制權之外，以實踐自主控制之個人資料蒐集使用原則逐漸形成，建構起個人資料蒐集使用的規範框架。如前所述，第一個個人資料蒐集使用原則是 1973 年由美國的住宅、教育及福利部之自動化個人資料系統諮詢委員會提出之〈紀錄、電腦與公民權利〉報告所建議的「公正資訊行為準則」(Code of Fair Information Practices)，該準則內含五項個人資料蒐集使用原則[135]。根據學者劉定基之翻譯，此五項原則為：「(一) 禁止秘密的個人資料檔案系統；(二) 人民有權得知其何種個人資料被蒐集及如何被使用；(三) 除非經過同意，個人有

[132] 加州隱私權法之介紹參見張陳弘，前揭註 30；加州消費者隱私法之介紹參見：王德瀛（2020），〈簡評加州消費者隱私保護法－規範重點與其對美國隱私保護的影響〉，《科技法律透析》，32 卷 3 期，頁 19-27。

[133] *See* Christophe Lazaro & Daniel Le Métayer, *Control over Personal Data: True Remedy or Fairytale?*, 12 SCRIPTED 3, 21-27 (2015).

[134] 有關各項權利詳盡的介紹可參考：PETER CAREY, DATA PROTECTION: A PRACTICAL GUIDE TO UK AND EU LAW 122-54 (5th edition ed. 2018).

[135] 參見劉定基，前揭註 33，頁 270。

doi:10.6342/NTU202500550

權防止為了特定目的蒐集的個人資料，被用於其他目的；（四）人民有權更正或修改關於其個人的資料；（五）任何建立、保存、使用或傳遞個人資料的機構，必須確保相關資料具有可信度，以符合其欲使用的目的，並採取合理的預防措施，以避免資料遭不當使用。」。

另一個重要的個人資料蒐集使用原則為 1980 年經濟合作與發展組織（Organization of Economic Cooperation and Development）提出的八項個人資料保護原則。根據劉定基之整理，此八項原則為：「蒐集限制、資料關聯性與正確性、目的特定、使用限制、安全維護、公開透明、個人參與、課責原則」。[136]。而我國之個人資料保護法係以九項原則作為立法原則，分別為：限制蒐集原則、內容正確性原則、目的明確化原則、限制利用原則、安全保護原則、公開原則、個人參與原則、責任原則、比例關聯原則[137]。

而歐盟的資料保護一般規則第 5 條第 1 項訂有六款立法原則，(a)款為合法、公正與透明原則，要求個人資料之處理必須符合第 6 條第 1 項所訂之合法蒐用事由之一，且處理行為應公正、透明；(b)款為目的拘束原則，規定資料之蒐集必須基於特定、明確與合法之目的，蒐集之後的處理行為亦受該目的之拘束；(c)款是資料最小原則，該原則係指個人資料之處理行為，依合法蒐集目的判斷，必須是適當、有關聯性且必要；(d)款是資料正確性原則，要求個人資料必須保持正確且在可能情況下更新；(e)款是儲存限制原則，原則上個人資料在蒐集目的消逝後，便應刪除或去識別化；(f)款是完整、秘密與安全原則，意指個人資料必須是在具備適當的資料安全保護機制之下處理[138]。

第四節　個人資料自主控制理論的問題

自主控制典範以知情同意原則、事後控制權、個人資料處理原則，有效地將

[136] 劉定基，前揭註 33，頁 270。
[137] 參見王澤鑑，前揭註 57，頁 248-249。
[138] *See* CAREY, *supra* note 134, at 32-40.

doi:10.6342/NTU202500550

資訊隱私權的保障範圍推進到所有個人資料、充實資訊隱私權之權能、規制個人資料的流動，試圖解決電腦、資料庫系統、網際網路技術下，個人資料悄然無息地被持續蒐集、使用、傳輸、儲存，而產生的個人資料失控現象以及資料檔案之監控疑慮、私密資訊再製問題。

然而，自主控制典範並未如期預期地切實保護個人資訊隱私，而仍飽受檢討與批評。在實際操作時，個人資料蒐集與處理關係中的雙方當事人磋商能力不對等、被蒐集的個人資料超過個人控制能力範圍，事前知情同意機制與設置個人事後控制權的成效不彰；自主控制理論認為個人有能力理性計算個人資料揭露的利弊與做成自主決定，這項理論預設受到反駁，一則因個人資料的蒐集處理的風險與利益實非個人在決策當下能夠想像的，二則因個人是座落在社會中的，其自主性受外在條件影響；此外，資訊技術持續發展，當巨量資料與演算法技術出現之後，資料的蒐集與處理又再對人類造成新的威脅，資訊隱私理論面對新的問題、挑戰：從他人資料推論出的個人資料、預言並實現預言的預測分析技術。

第一項 自主控制的弱化：當事人磋商能力不對等、瑣碎個人資料

第一款 當事人磋商能力不對等

在自主控制理論下，當事人同意是開啟個人資料蒐集處理關係的合法條件，是為實踐事前控制的首要機制。然而，實際上資料主體的選擇與同意被限制在資料蒐集者提供的框架下，加上數位服務使用者的網絡效應，個人資料蒐集處理關係的當事人欠缺對等的協商能力，知情同意之事前控制手段無法反映資料主體的真實隱私偏好。

第一個在事前階段削弱個人自主性的理由是資料主體對於同意權行使的想像侷限在資料蒐集者給予的格式、條件[139]。當我們近用公、私部門的數位服務，該服務詢求個人資料最常見的方式是跳出含有數位服務的隱私條款、同意與不同意

[139] *See* Ari E. Waldman, *Privacy, Practice, and Performance*, 110 CALIF. LAW REV. 1221, 1249-51 (2022).

doi:10.6342/NTU202500550

的按鈕的視窗，我們行使同意權的方式只有瀏覽隱私條款、點選同意或不同意，通常不存在隱私調整的選項，或者是即時溝通調整隱私條款的管道，若我們不同意隱私條款的內容，便無法近用該服務。此外，在我們瀏覽網站時，若該網站將取用瀏覽紀錄、cookies 等資料，會在頁面上覆蓋一部分的告知與請求同意的畫面，凸顯同意按鈕，以尋求資料主體的同意。

而數位服務使用者的網絡效應是指特定網絡的使用者數量越多、該網絡的價值越高[140]，以傳真機網絡為例，若世界上只有一臺傳真機，該機器毫無用途；傳真機的數量越多，越能實現快速便捷傳遞資訊的功能[141]。數位資訊技術亦然，對資料累積、推論規則為基礎操作的數位資訊技術而言，取得更大量、有品質的資料，推論的結果會被認為更貼近現實；而對連結使用者的社群平台，使用者的數量是吸引潛在客群的關鍵因素，我們會為了取得他人的資訊、與他人聯繫、在線上空間宣告自己的存在，而去使用吸引到大量使用者的社群平台。使用者無法抗拒這些社群平台提出的服務隱私條件，亦難退出平台，產生使用者切換平台成本過高而選擇留下的鎖入效應[142]。因此當特定數位服務業者擁有大量使用者、佔據市場重要地位時，使用者只能接受業者的條件，或者放棄享受該數位服務。

第二款 瑣碎個人資料

另一個對自主控制典範的有力批評是針對事後控制權規範模式的，如美國隱私法學者 Daniel Solove 的主張，現有的科技運作下，資料主體沒辦法透過事後行使更正、停止處理、刪除等權利，一一掌握、管理每個被蒐集的個人資料，本意在於回復個人弱勢地位，讓資料主體保有掌控個人資料可能性的諸項事後控制權，資料主體反而因此需承擔管理責任與管理失敗的風險[143]。

---

[140] *See* Kenneth A. Bamberger & Orly Lobel, *Platform Market Power*, 32 BERKELEY TECHNOL. LAW J. 1051, 1067-68 (2017).
[141] *See id.* at 1068.
[142] *See id.* at 1068-69.
[143] *See* Solove, *supra* note 20, at 985.

doi:10.6342/NTU202500550

詳言之，造成前述問題的原因是被蒐集處理的個人資料、蒐集處理個人資料的組織皆難以計數，遑論個人資料之流動並不會停留於個別組織，而是在組織內不同部門、在不同的控管或處理組織之間流轉，個人資料流在我們渾然不覺之下形成複雜而難以追蹤的網絡，更有無數的個人資料流動其間。

例如我們欲透過甜點店的官方網頁訂購一條蛋糕，通常會揭露個人資料的階段是註冊會員（可能設有連結其他社群帳號的快速註冊、登入選項）、填選寄送地點、線上結帳，若選擇連結個人 LINE 帳號的快速登入方式，選擇公司為寄送地點、線上刷卡結帳方式，必須揭露的個人資料可能有 LINE 帳號、姓名、手機號碼、地址、信用卡資訊等，除了甜點店之外，官方網站軟體系統、甜點店顧客管理後台系統、實體資料庫系統、線上支付金流等業者皆可能取得前述資訊。這項問題在物聯網技術出現、穩定發展之後更顯嚴重，個人被蒐集的資料與加入蒐集處理的組織更多。

假設某 A 完成性別錯置手術、戶政事務所之性別變更程序，而欲知悉有哪些組織有其舊的性別資訊，以便行使更正權，依目前的個人資料蒐集處理運作實況，某 A 無從知曉哪些組織有其性別資訊；縱使知悉，要與每一組織溝通、提出更正要求、確認更正完畢，相當曠日費時。

第二項 人類理性決策之限制

由個人理性衡量利弊，決定資料揭露與否、揭露目的、揭露條件之知情同意，是自主控制理論保護個人對資訊隱私權自主性實踐的首要機制。然而，人類的理性能力存在著界限，資訊不充分之認知限制、理性計算的上限、系統性心理偏誤之限制等因素，會影響決策時的理性[144]

理性衡量利弊的前提是掌握足量的資料蒐集處理資訊，而資料蒐集處理關係

[144] *See* Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality: A Survey*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION 17 (2005).

doi:10.6342/NTU202500550

當事人之間存在相當大的資訊落差。首先，個人資料蒐集處理的過程與方式、參與資料蒐集處理過程的第三人、蒐集處理行為所生的風險等資訊，掌握在資料蒐集處理方手上[145]；再者，資料蒐集處理者提供的隱私條款對欠缺專業知識與經驗的資料主體而言，複雜、抽象而難以理解。個人無法切實知情，決策的理性殊值可疑。

而理性計算有其上限是人類天生內建的機制，指當個人面對超出理解能力範圍外的複雜狀況，我們無法察覺、記憶、理解其間的複雜、陌生資訊，審慎評估的理性能力被抑制，轉而以簡單的心智模式、粗糙的策略、探索學習，做出有勇無謀的決定。這項機制之目的是避免在此情形出動理性，勉強作成最佳決策，將使個人不堪負荷[146]。而個人資料的蒐集處理對於個人而言，屬於上述超出理性能力範圍外的複雜狀況，理性的決定並不存在。

決策也可能受系統性的心理偏誤影響，而不純然理性。詳言之，理想的理性決策過程是審慎估算後做出利大於弊的決定，然而決策者的心理可能因某些因素而受到動搖，這些因素會使個人當下的感受壓過理性，影響決策，例如表現利益與弊害的手法、對未來偏好的錯誤想像、過去經驗的渲染、看重眼前的快樂而非未來等，這些因素可能都會影響個人做出的決定[147]。而現在個人須面對是否給予個人資料之決定，通常是想要近用某些數位服務或是取得優惠、利益，個人資料蒐集者也不會清楚地告知資料主體個人資料蒐集處理的風險與危害，且個別的個人資料、資料處理行為，對個人而言，傷害的感受不明顯。因此，個人可能為了取得服務或優惠而低估個人資料的風險，做出過度樂觀而不理性之決策。

第三項 巨量資料與機器學習的新挑戰：推論個人資料、預測分析

今日，自主控制理論之所以受到強烈檢討，最關鍵的理由依然是技術發生革

[145] *See id.* at 17.
[146] *See id.* at 17-18.
[147] *See id.* at 18.

doi:10.6342/NTU202500550

新性的變化：巨量資料為基礎之機器學習之出現。上述技術之發展，改變資料的可利用性，與數位產業互為表裡，一齊帶動數位社會運行。巨量資料技術使被蒐集、儲存的個人資料數量更多、範圍更大且更加精緻；其中，機器學習演算法技術則逐步提升自動化機器處理資料的能力。在技術的加成之下，公、私部門蒐集大量的資料、建立資料庫、分析資料建立模板與規則，以模板與規則來理解現實世界，進而推論未知之事實、預測未來。

然而，數位社會的這類操作，一則係以含有個人資料之數位資料為素材；二則推論與預測的結果可能影響個人甚深，而再度引發個人的資訊隱私侵害之疑慮，作為資訊隱私權典範之自主控制理論，無從支應新技術的帶來的資訊隱私權干預問題，受到深刻地檢討，並帶起探索新興資訊隱私權典範的討論。

第一款 巨量資料與機器學習

在以資料為發展核心的數位時代，環繞於數位資料之蒐集處理的新興技術工具不斷演進，發展出諸如巨量資料、人工智慧、機器學習、物聯網、資料探勘、雲端運算、機器人等技術，在用語上，這些概念常指涉不只一種技術，有時指某種操作、有時是數種技術或操作的結合，不易清楚地界分、定義。本文無意一一介紹新興的數位技術之定義、釐清關係，而認為在電腦與資料庫系統之後，最顯要的資訊技術變革在於資料的數量更多更細緻、資料處理能力更好。因此，本文首先選擇強調資料蒐集處理之規模變化的巨量資料，再揀選以資料進行推論與預測分析之關鍵技術——機器學習，作為數位時代重要的技術背景介紹。

巨量資料之用語指涉的概念不一，有指一項操作[148]、一種產業[149]、或是產業

[148] *See* A. Michael Froomkin, *Big Data: Destroyer of Informed Consent*, 21 YALE J. LAW TECHNOL. 27, 31 (2019); *see also* GLORIA GONZÁLEZ FUSTER & AMANDINE SCHERRER, *Big Data and Smart Devices and Their Impact on Privacy*, (2015); see also Kate Crawford & Jason Schultz, *Big Data and Due Process：Toward a Framework to Redress Predictive Privacy Harms*, 55 BOSTON COLL. LAW REV. 93, 96 (2013).
[149] *See* Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NORTHWEST. J. TECHNOL. INTELLECT. PROP. xxvii, 243 (2013).

doi:10.6342/NTU202500550

運作之教示[150]。較廣泛的來說，巨量資料是指蒐集大量的資料，處理、分析大量的資料，探索現實運作的模板與規則、發掘未知之知識、產生洞見，進而解決現有問題甚至是根據數位現實脈動預測未來。其特色有二：一為需要有取用、清理、分析大量資料之技術與工具；二則資料蒐集處理目的為辨識未知規則或模板、預測未來[151]。具體的技術工具包含：數位通訊網絡、集合式伺服器、高強的電腦系統、機器學習、物聯網[152]等。

演算法最基本的意義是「藉由輸入特定的要求，而能夠得出一定的結果，以解決所設定任務的數學公式，而不限定任務為何[153]」，是人類使用電腦解決問題的方法[154]。早期的演算法係以人類輸入的規則為基礎解決問題；爾後隨著被擷取、儲存的資料數量與類型增生，人類不再只使用已知的規則進行演算、處理資料，而是開發出由機器在巨量資料中探索、學習資料之間呈現的關聯性與規則之以資料為基礎的機器學習，機器學習為第二波的人工智慧技術，其重要性為發掘出人類未知的知識與規則之能力[155]。

巨量資料與機器學習的運作是以大量資料建構、梳理出現實，探索事物未知的規律或模板，以現有的資料作為已知事實，推論、猜測已存在之其他事實，或者推測未來，能夠處理人力未能企及的資訊數量、取得人類已知範圍以外的知識。

---

[150] *See* Mark Burdon & Mark Andrejevic, *Big Data in the Sensor Society*, *in* BIG DATA IS NOT A MONOLITH 61 (Cassidy R. Sugimoto, Hamid R. Ekbia, & Michael Mattioli eds., 2016).

[151] *See* Crawford & Schultz, *supra* note 148, at 96; *see also* Froomkin, *supra* note 148, at 31. 就「大量資料」的定義，原始的定義是以 3V 判斷：容量、速度、多元性（volume, velocity and variety）；爾後出現 7V 判準，除原本的三項以外，另加上：資料的黏著性、易變性、真實性、不穩定性（viscosity, variability, veracity, and volatility）。上述內容參見：*See* FUSTER AND SCHERRER, *supra* note 148, at 10; *See* Kevin C. Desouza & Kendra L. Smith, *Big Data for Social Innovation*, 12 STANF. SOC. INNOV. REV. 39 (2014).

[152] *See* Burdon & Andrejevic, *supra* note 150, at 61; *see* FUSTER AND SCHERRER, *supra* note 148, at 61.

[153] 參見呂胤慶（2021），《公部門中的人工智慧—人為介入作為正當使用人工智慧的必要條件》，國立臺灣大學法律學研究所碩士論文，頁 14，註 9。*See* Hideyuki Matsumi & Daniel J. Solove, *The Prediction Society: Algorithms and the Problems of Forecasting the Future*, UNIV. ILL. LAW REV. 10 (forthcoming).

[154] *See* ALPAYDIN, *supra* note 2, at 2.

[155] 更詳細的介紹，請參見呂胤慶，前揭註 153，頁 13-17；邱文聰（2020），〈第二波人工智慧知識學習與生產對法學的挑戰——資訊、科技與社會研究及法學的對話〉，李建良編，《法律思維與制度的智慧轉型》，頁 135-166，元照。

doi:10.6342/NTU202500550

對私部門而言，能夠了解消費者、市場的脈動，做出較佳的經營策略、精準行銷，甚至影響消費者的決策，形成數位經濟體；而公部門，能夠擬定更好的政策、提升行政效能、有效偵查或預防犯罪[156]。

在前述操作中，個人有雙重角色：資料的生產者、資訊的消費者或作用對象[157]。我們除了主動提供資料以外，個人資料亦經常在我們與數位資訊裝置互動間被動地流出，如瀏覽網頁之瀏覽紀錄、使用智慧手機導航服務的定位資訊、智慧居家助理擷錄的聲紋資訊、與聊天機器人溝通時的用語習慣資訊、悠遊卡記錄的搭乘大眾運輸工具通勤資訊、為快速通關的臉部特徵資訊等。而我們提供個人資料的目的常是為了使用數位資訊服務，例如個人化的音樂、商品、新聞之推薦服務，因此同時為資訊的消費者；此外，在我們未使用數位資訊服務的情境，也可能受到巨量資料與機器學習推論與預測的結果影響，例如信用評分機構根據其他個人與被評分者的資料，估算與被評分者交易之風險與打分數[158]；企業徵才時，以過去員工的資料建置自動化篩選系統，初步淘去被系統判定為不適任之應徵者[159]。

因此，個人既為巨量資料與機器學習之素材——個人資料之提供者，又為資料蒐集處理之結果的作用對象，資訊隱私權干預的疑慮再起。而自主控制典範面對這些新的數位技術工具，除了自主與理性預設的理論根本問題尚未解決、資料主體自主控制力弱化的現象再加劇之外，亦無法處理巨量資料與機器學習下使用個人資料做成推論與預測分析之資訊隱私權的議題，詳述如下。

第二款 推論個人資料

[156] *See* FUSTER AND SCHERRER, *supra* note 148, at 8; *see also* Tene & Polonetsky, *supra* note 149, at 243-51.
[157] *See* ALPAYDIN, *supra* note 2, at 2.
[158] *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION, 22-25 (First Harvard University Press paperback edition ed. 2016).
[159] *See id.* at 36-38.

doi:10.6342/NTU202500550

推論，簡言之，是使用已知之事實猜測其他事實[160]。在涉及個人資料的情境，公、私部門蒐集來自於自然人之資料，再生產關於被蒐集之資料主體或其他自然人的其他資訊[161]。可知，推論的方向有二：推論同一自然人之資料、推論其他自然人之資料。前者涉及個人資料的去識別與再識別之個人匿名性問題；後者則關於被推論出的資料主體應如何保護議題。

首先說明從含有特定自然人資料之資料集，推論同一自然人的其他資訊的情況。在巨量資料與機器學習等數位技術工具的輔助之下，原為點狀、缺漏的個人資料，透過資料的串聯與比對拼湊出資料集內人們更詳盡的資訊，有可能產生新的個人資料。例如購物網站不斷蒐集、累積個人的購物紀錄資訊，推論出資料主體的月經週期、懷孕等資訊[162]。

除了產生新的個人資料以外，推論出資料集內自然人資訊的情況也會發生在去識別化資料集之再識別。去識別化要求係為處理電腦資料庫技術產生的個人被監控疑慮，為了保護個人的匿名性並同時兼顧資料的可利用性，將資料經一定方式處理後削弱其可識別性是權衡之下的措施。資料的去識別程度與可利用性為此消彼長關係，去識別化程度越高、資料連結至特定個人的難度越高、須更多額外資料輔助連結，通常越難識別個人的資料、可利用性越低。依去識別化程度低至高可分：直接識別資料（如姓名、住址、身分證號碼）、間接識別資料（如生日、住址、IP 位址、定位資訊）、可連結至特定群體的資料（如電影或購物偏好）、無法連結至特定個人的資料（如民調結果、人口調查統計結果）、與人無關的資料（如天氣）[163]。具體的去識別化措施有：刪除或改寫、假名化、加入雜訊、聚合資料等[164]。

---

[160] *See* Matsumi & Solove, *supra* note 153, at 9.
[161] *See* Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NORTHWEST. UNIV. LAW REV. 357, 361 (2022).
[162] *See id.* at 378-79.
[163] *See* Boris Lubarsky, *Re-Identification of "Anonymized" Data*, 1 GEORGET. LAW TECHNOL. REV. 202, 203-04 (2017). 有關去識別化資料的分類與舉例，係整理自該文的頁 203 至 204 之文字與圖表內容。
[164] *See id.* at 205-08.

doi:10.6342/NTU202500550

而會發生再識別風險的情況有：去識別化程度不足、假名化資料逆向處理、連結不同的資料集。詳言之，去識別化程度不足是指資料集中仍殘留可識別的資訊，例如在多數情況下，性別、生日、郵遞區號資料之結合可識別出特定自然人；或者搜尋引擎使用者之搜尋紀錄資料集縱使已除去個人姓名、IP 位址等直接識別資料，藉由搜尋紀錄的分析仍可能推論出使用者的年齡、性別、學歷、工作等資訊。而假名化處理係將某些與資料集連結會發生可識別性的額外資訊與該資料集分離保管，以保有可利用性，然而，若額外資訊被發掘、外洩或者額外資料可從已公開資料取得，假名化資料可能被逆向處理而解鎖識別性。另外，資料集之間的連結是常見的再識別方法，例如取得公眾人物的性別、生日、郵遞區號號碼，結合匿名的醫院病歷資料集，可比對出該公眾人物的健康資料[165]。而值得注意的是，去識別化資料的再識別風險會隨著數位資訊技術的發展而有變化，因此原先已充分去識別性的資料可能在未來因技術進步而可再識別。未來，完全去識別化資料或是數位空間中個人之匿名性或許不存在。

在推論同一自然人資訊的情況，自主控制典範面臨的問題有二。首先，資料主體在做個人資料揭露與否的決定時，根本無從評估揭露的風險，不知資料揭露後，能否在現在或未來透過資料串聯而推論出其他個人資訊，縱使是資料蒐集、處理者，也無法確知該項資料未來會被如何使用，遑論無專業知識能力之資料主體。再者，非個人資料或去識別化資料之處理、連結，也可能析出個人資料，此時，因資料主體不知悉而無從實現自主控制[166]。

推論是分析已知事實推導出未知的事實，誠如前述。而第一種情況是**以某甲**的已知事實、**推論某甲**的未知事實；以下要說明的是第二種情況：**以某甲**的已知事實、**推論某乙**（自始不在資料集的自然人）的未知事實。

此涉及「剖繪」（profiling）這項技術。剖繪是指「為資料控制者判斷、評估

[165] *See id.* at 208-12.
[166] *See* Solow-Niederman, *supra* note 161, at 361; *see also* Froomkin, *supra* note 148, at 32-33.

doi:10.6342/NTU202500550

之目的所為，發現資料庫中資料關聯性，及關聯性分析之結果適用於主體，藉以區辨（individuate）、描述主體或識別主體所屬群體、類別的程序[167]」。剖繪係對人做出的推論[168]，可分為二階段理解，第一階段是根據蒐集到的已知資料集，以機器學習處理、分析，讓自動化機器在大量的資料中，學習資料點（data points，例如自然人）與變項（variables，例如人的特徵）之間的關聯性（correlation），建立執行分群、排序等功能的演算法模型，將資料集內的人分類成不同的群體資料夾（profile），同一群體資料夾內的人們有共享的特徵，例如偏好、社交模式、行為等，此一階段可理解為形成群體資料夾的階段。第二階段是將不在已知資料集的其他自然人，投入依資料集形成的演算法模型中，根據該自然人與群體資料夾內人們共享的特徵予以歸類，並推論該自然人擁有被分到的群體資料夾人口的其他特徵[169]，因而可從已知自然人資料推論未知自然人資料。舉例而言，某 K 旅遊網站依照過去所有使用者的訂購紀錄資料，推算出購買日本冬季滑雪套裝行程的消費者有年齡 25 至 35 歲之間、沒有小孩、喜愛戶外運動等特徵，當一位新註冊的使用者也訂購了日本冬季滑雪套裝行程，K 旅遊網站的演算法模型便將其歸類、認定具有上述幾項特徵，進而依這些特徵推薦符合使用者預算與偏好的行程、機票等旅遊資訊。

前述情形會發生少數人同意牽連多數人之少數暴力[170]、資料主體之間橫向串聯關係的現象[171]，而自主控制典範力有未逮。在此所指之少數暴力現象是指在資料集內少數人的同意會影響到資料集外共享相同特徵之其他人的權利與自由之行使，資料蒐集處理者只要取得足夠數量、具代表性的使用者資料作為樣本，便可

[167] 鄭詠綺（2023），《論歐盟社群媒體平台精準投放之管制架構：以私生活權之保障為中心》，國立臺灣大學法律學研究所碩士論文，頁 2。
[168] *See* Matsumi & Solove, *supra* note 153, at 9-10.
[169] *See* Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE LAW J. 573, 607 (2021); *see also* Solow-Niederman, *supra* note 161, at 361-62, 384-85. 中文文獻參見：鄭詠綺，前揭註 167，頁 2-3。
[170] *See* Solon Barocas & Helen Nissenbaum, *Big Data's End Run around Anonymity and Consent*, *in* PRIVACY, BIG DATA, AND THE PUBLIC GOOD 44, 61-63 (Julia Lane et al. eds., 1 ed. 2014).
[171] *See* Viljoen, *supra* note 169.

doi:10.6342/NTU202500550

推測樣本外其他人口的樣貌[172]，縱使樣本外的其他個人並未同意被如此推論、未與資料蒐集處理者建立關係。同樣地，被剖繪與分類至群體資料夾、將自己部分特性推論與套用至同群體的他人身上，如此後果並不在資料主體做資料揭露與否決定時可想像風險範圍內[173]。此外，被推論的資料主體之自主控制權應如何確保，亦是棘手問題，假使被推論之資料主體知悉後反對此推論、要求刪除被推論的資料，而有效、根本性地刪除該資訊的方法為斬斷資料蒐集處理者做此推論的路徑，亦即消除資料集內能夠做出此推論的資料，然若原本在資料集內的資料主體已同意該資料之使用或是不願刪除資料時，將發生資料主體之間自主控制權的衝突[174]。

學者 Salomé Viljoen 提出資料橫向關係理論，指出數位時代公、私部門蒐集大量數位資料以機器學習進行剖繪、推論、預測的操作手法，以分析資料主體之間的相似度、人口與特徵之關聯性、歸類出一個個共享特徵的人口群體資料夾之方式，建立起資料主體與同群體之他人的橫向關係。而自主控制典範下現有的資訊隱私保護、個人資料保護法制卻只規範資料主體與資料蒐集處理者之間的直向關係，規範方向與數位經濟、數位社會的運作脫鉤[175]。

在推論他人資料的情形，可以看出現在資料主體對其資料之自主控制權的行使，會影響、牽連他人的自由與權利。以 Viljoen 所舉的例子或能更深刻地說明：設 T 平台係專為刺青愛好者打造的社群平台，使用者能在 T 平台上與同好交流、分享刺青的資訊，上傳刺青圖樣並說明刺青圖樣的涵義，而根據 T 平台使用者上傳的刺青相關資訊，某些刺青圖樣是黑道或犯罪組織的標記，警察機關掌握此類資訊之後，能夠透過監視系統、盤查等方式鎖定特定人，將其歸類為潛在犯罪份子，或者對於刺有犯罪組織標記的犯罪嫌疑人存有偏頗的負面印象。自主控制典範下的資訊隱私權無法觸及這些潛在的傷害、風險。

[172] *See* Barocas & Nissenbaum, *supra* note 170, at 62-63.
[173] *See* Froomkin, *supra* note 148, at 33.
[174] *See* Solove, *supra* note 20, at 991-92.
[175] *See* Viljoen, *supra* note 169; Solow-Niederman, *supra* note 161, at 385.

doi:10.6342/NTU202500550

第三款 預測分析

巨量資料與機器學習帶來一項嶄新的操作個人資料行為：預測分析。預測分析是加入時間尺度——針對「未來」的推論、剖繪[176]。而這項新的資料處理行為對個人、人類產生了新的風險、危害，學者重新思索資訊隱私權在數位時代的定位、應如何回應新技術與新操作的新問題。需先說明的是，機器學習預測分析的操作與問題正在發展中，本文在此以學者 Hideyuki Matsumi 與 Daniel Solove 針對數位技術預測分析全面性的研究為主要素材，探索這項技術可能存在的問題。

自古，人類自然地會根據經驗以某些徵兆預測他人未來行為或活動，例如某補習班推論出現於臺大霖澤館與萬才館周圍、目測年紀約 20-25 歲的人是法律系的學生，並預測他們近年會參加司法官、律師高考，而對他們發宣傳單。然而，機器學習所執行的預測分析與人類預測不同，機器學習預測是以數學、統計精算為原理，根據大於人類可理解範圍之資料量、標準化處理的數位資料，執行人類無法處理的複雜運算，以大量的資料分析事物運作的規則，並以此推論相似情境會依同一規則發展。依過去「事實」資料、先進的演算法「自動化運算」所得出的預測結果，會被認為是科學、客觀、不偏頗、不會失誤的正確結果，且時常是人類想像不到的知識，從而被廣泛使用，以美國為例，目前在信用評分、犯罪預測、職場員工評量、學生學習能力、保險風險評估等領域皆有機器學習參與[177]，甚至已發展出推論經濟產業[178]。

Matsumi 與 Solove 指出機器學習預測有二項錯誤預設，一為將過去當成未來，二則忽視未來的變動性而對預測結果深信不疑[179]。在錯誤的預設前提之下，機器學習預測應用時發生四種漸進式的現象，第一種是個人固著與社會凝固，演算法為過去資料顯示的人類行為與活動製作模板，並將該模板套用於未來，社會因此

[176] *See* Matsumi & Solove, *supra* note 161, at 11-12.
[177] *See id.* at 14-20.
[178] *See id.* at 14-20.
[179] *See id.* at 14-20.

doi:10.6342/NTU202500550

按照模板的形狀凝固、個人則固著於演算法據過去資料形成的刻板印象，失去能動性。第二種是預測結果不可驗真，我們能夠驗真已知、已發生之事實所做的推論，然而未來仍未發生，我們無法確認預測是否為真，該不知真偽之預測結果卻已體現於某具體決定，自此影響事物的流動、走向，所謂具體決定小如數位服務的客製化資訊推播、大則如雇主使用演算法對求職者所做的不適任判斷。第三種是預先介入，延續不可驗真性的討論，預測結果被認定是真實的事實後，影響人們後續的安排、處置，事物流動朝向預測的方向發展，加深預測影響力及不可驗真性，例如學習成效演算法模型根據某國中學生過去課業表現，判斷其數學能力不佳，預測這位學生的會考分數不會達到均標而需接受數學輔導，這位學生被安排輔導之後會考的數學成績確實達標，然而在未來（即會考）到來之前已有干預介入（即安排數學輔導），預測結果成為後續事物發展的劇本設定之一且無法驗明真實性。第四種是自我實現的預言，意指演算法的預測結果成為人類的認知，進而促進預測結果的實現，Matsumi 與 Solove 係以學業能力演算法模型預測舉例，該演算法模型根據國小學童的學業表現，將其分類為學習能力強、學習能力待加強二種，被評測為學習能力待加強的學童，可能認為這項結果係經科學精算認證而選擇放棄學習或學習動力下降[180]。

說明機器學習預測會發生的現象之後，Matsumi 與 Solove 從三個面向討論人類的自由與權利所受到的限制：機器打造未來、被預測者無能為力、抑制人類做出不同行為之可能性。首先，如同前述四種現象所示，機器學習預測的結果，具有製造未來的效果而不再只是推測，人類應是「自己人生的作者[181]」，能夠想像、計畫自己的未來並逐步實踐，然而機器學習預測的實踐，替代人類決定未來的劇本，翦除不同結果發生的可能性。再者，作為被預測者的人類僅能接受演算法的預測與決定而無能為力，機器學習預測被認為比人類預測更為科學、客觀、公正、

[180] *See id.* at 22-31.
[181] Matsumi 與 Solove 在此引用 Julie Cohen 的主張，Cohen 認為個人應能決定自己如何與社會、他人互動並建立關係，是自己人生的作者，而個人如此能力應受隱私權保護，*see id.* at 32.

doi:10.6342/NTU202500550

精確，縱有不精準結果發生之可能性，也為了追求效率而容許有此犧牲，被犧牲、因預測結果而受不利對待的個人，難以舉證尚未發生的預測不當、有誤，僅能接受結果。最後一個侵害人類自由與權利的面向是翦除人類做不同行為的可能性，人們因自我實現預言現象、害怕受到不利對待，傾向避免去做可能產生不利影響的行為，更加強個人與社會凝固於演算法預測結果的問題，而此種讓人類害怕受懲罰來達成規訓、控制行為的操作，監控的疑慮再起[182]。

而現有的資訊隱私法、個人資料保護法制無法辨識出機器學習預測分析的專有侵害，從而無從回應。首先，機器學習預測分析干預的是人類「未來」決定、行為的可能性，而資訊隱私法、個人資料保護法制的規範設計模式，如同我們熟悉之司法權的事後性質，主要處理的是權利侵害發生後的問題，對於尚未發生的未來，我們無從論述侵害何在，而現有規範也未針對此問題有專屬的安排。其次，機器學習所據的是過去、已知的事實資料，預測無從驗真的未來，現有個人資料保護法下的更正權僅能處理演算法依據的事實資料真實性的問題，對於不知真否、甚至被逐步實現的未來，並非更正權或個人資料保護法任一權利的打擊範圍。最後，如前所述，在此所指之預測分析是針對未來的剖繪，因而承繼其技術基礎——剖繪的問題，即個人資料保護規範未注意到數位時代下資料主體橫向串聯的關係。

[182] *See id.* at 31-38.

doi:10.6342/NTU202500550

第三章 資訊隱私典範之重省：信任理論、隱私間隙理論

本章旨在整理本文認為有力成為機器學習時代下的資訊隱私權典範理論之學說，並在本章最後進行比較，提出本文支持的理論。根據本文所蒐集的文獻，選擇信任理論與隱私間隙理論作為整理、比較的學說，理由為此二學說除了是重要的資訊法、隱私法學者所提出與支持，此外，這二個學說較為完整，涵蓋隱私的社會意義、法規範層次的隱私概念，至隱私法應從的規範模型[183]。

本文所選擇的信任理論與隱私間隙理論皆關注到資訊隱私、隱私與社會的關聯性，由此展開有別於強調個人自主、個人行使權利之隱私權既有典範的論述。惟此二理論所觀察的隱私的社會關聯性並不相同，信任理論觀察到的是個人資料分享揭露的社會功能；隱私間隙理論則是從人格發展、主體性與社會環境的依存關係面向，開啟隱私與社會的互動關係。將在以下章節詳述。

第一節為信任理論以及根據該理論發展出的規範模型，有 Jack Balkin 提出的資訊託管關係／資訊受託人義務、公共受託人、公共信任理論。第二節則為 Julie Cohen 提出的隱私間隙理論之理論整理，包含建構隱私間隙理論的基礎、隱私間隙理論本身，以及間隙理論主張的隱私保障之二項原則。第三節為理論的比較分析。

第一節　信任理論與資訊託管關係模型、公共受託人模型、公共信任理論

信任理論是美國有力的新興資訊隱私理論，主張、支持該理論的資訊法學者

[183] 在此二理論之外，還有Helen Nissenbaum提出的脈絡完整性理論（Contextual Integrity）、Fred H. Cate等學者提出的使用管制規範取徑、Kate Crawford等學者提出的巨量資料正當程序規範模型，以及原有的個人資料自主控制與人格權模式等。參見 Hirsch, *supra* note 114; Bert-Jaap Koops & Masa Gahic, *Unite in Privacy Diversity: A Kaleidoscopic View of Privacy Definitions*, 73 S. C. LAW REV. 465 (2021); Julie E. Cohen, *How (Not) to Write a Privacy Law | Knight First Amendment Institute*, https://knightcolumbia.org/content/how-not-to-write-a-privacy-law, (last visited May 12, 2024).

doi:10.6342/NTU202500550

眾多。信任理論是從實然的角度觀察個人資訊在現代的流動方式、個人資訊的揭露分享對個人與社會的功能，論證信任是驅動個人資料流動的要素，形塑個人資料分享關係當事人對個人資料流動的期待。信任理論最有力的一項主張是在法規範層次，根據美國普通法既有的託管法之法理，主張個人資料分享為一種資訊託管關係，取得個人資料者應負如律師、醫師、會計師之專業受託人義務，建構個人資料的蒐集使用規則以及對蒐集使用者之規範。

在理論的建構層次，本文選擇 Jack Balkin、Neil Richards、Woodrow Hartzog，以及 Ari Waldman 等學者的學說為主要整理分析對象。其中，Ari Waldman 將信任理論的基礎紮根於社會學理論，以此論證個人資訊有超出個人利益之社會功能。因而在此部分，本文採取 Waldman 的見解說明信任理論的基礎。而根基於信任理論所開展的個人資料分享揭露法規範，就前述規範蒐集使用個人資料之私人關係的資訊受託人模型，本文選擇最具代表性的學者 Jack Balkin，以及提出較為完整模型的學者 Neil Richards 和 Woodrow Hartzog 作為說明。除此之外，本文也會介紹 Priscilla Regan 主張的公共受託人理論，公共受託人理論的貢獻在於建立獨立的個人資料監管機關之必要性。另外，Dennis Hirsch 的公共信任理論將社會對於蒐集使用個人資料的公、私部門的信任類比為公共財，並援用經濟學的理論證成規定個人資料蒐集使用規則的必要性。

本節在第一項說明信任理論的理論基礎，再於第二項分就資訊受託人模型、公共受託人理論、公共信任理論提出不同層次的個人資料蒐集使用法規範模型。

第一項 資訊隱私權的信任理論

信任理論主張資訊隱私是一種社會結構，建立在資訊分享者對彼此的信任。所謂信任是指一種由於我們對他人行為模式的正向期待而產生的人際互動禮儀（interactional propriety），且該互動禮儀已經成為社會常規[184]。信任理論建構上述

[184] *See* WALDMAN, *supra* note 64, at 50.

doi:10.6342/NTU202500550

主張的方法，是從實然的觀察，去批評既有的資訊隱私概念，再提出信任作為替代的隱私概念。

根據 Ari Waldman 的信任理論，原本的資訊隱私典範有二點問題：第一點是以單一概念理解、第二點是以個人權利理解隱私。Waldman 主張，資訊隱私是依附於個別脈絡的，在不同脈絡下，資訊隱私的內涵不同，無法以一概之[185]。且，以個人權利理解資訊隱私並不足夠，資訊隱私有超出個人權益的社會功能，因有個人無法支配與控制的部分，政府有介入的餘地，制定資訊隱私規範[186]。Waldman 拆解單一隱私概念的方法是根據美國重要的隱私法學者 Daniel Solove 主張的傘狀隱私概念；而對個人權利的抨擊，則是採用近年新興的隱私社會價值理論。以下分別說明。

首先，針對第一項問題，Waldman 反對單一概念理解隱私，而支持 Solove 主張的傘狀隱私概念。所謂傘狀隱私說明在隱私此一語彙之下，其實指涉了許多事物，這些被指稱為隱私的事物，在概念上有相近性卻又不完全重合，彼此共享部分特徵而可被劃在同一類別之下。依 Solove 對隱私理論之整理，不被打擾的權利、限制接近、控制個人資訊、人格、親密，皆可被劃屬隱私此一語彙。

信任理論認為資訊隱私權保護的是數位社會中人們對於個人資料分享與使用規則的信任，資訊隱私法的功能不再是點狀式地保護少數被承認的資訊隱私權傷害，而應積極地根據個別情境建構能夠維護並增強人們信任的個人資料分享與使用規範，規範的內容應帶有實質的價值，而不只是形式的程序規定。

信任理論有二個重要的理論基礎：一為資訊隱私權具有無法被個人權利觀點涵蓋的社會價值；二是「信任」為維繫個人資料分享揭露關係的要素而應受保護。

第一個理論基礎——資訊隱私權具有社會價值這項論點，旨在破解資訊隱私

[185] *See id.* 5.
[186] See *id.* 7.

doi:10.6342/NTU202500550

權被純粹以個人權利看待的傳統觀點。傳統觀點下的資訊隱私權是個人事務，私密理論認為保護隱私係為了保護個人不為人知的私密領域；自主控制理論保護資料主體判斷資料的主觀價值再做出揭露與否決定的自主性。以上的隱私觀所保護的都是個人尺度的，然而，近年有許多學者開始主張隱私含有超出個人以外的社會價值，泛稱隱私社會價值理論。本文以下採學者 Ari Waldman 整理的社會價值理論以為介紹[187]。

Waldman 推展隱私社會價值理論的方式是先以 Daniel Solove 強調多元隱私概念的傘狀隱私（privacy umbrella）為始，展現出在不同情境下隱私保護之目的皆不同，說明以單一概念理解隱私之不可行[188]；在 Solove 之後，Waldman 援引社會學者 Robert Merton 和 Erving Goffman 的理論，說明隱私——在此為個人資料的分享揭露——的社會功能是社會互動參與者具有共識的個人資訊流動規則，使社會互動所必要的個人資訊流動持續運作；最後一項問題是決定上述個人資料流動規則的方式，對此 Waldman 介紹學者們過去嘗試根據實際的資料流動所整理的資訊流模型與脈絡完整性理論，再提出更具有規範性、以信任為個人資料流動規則應保護判準的信任隱私理論。以下詳述之。

首先說明 Daniel Solove 的多元隱私概念。Solove 認為隱私無法也不應以單一的概念來定義。Solove 先整理出六種主流的隱私權理論[189]，這些理論各自有關注的面向與存在的意義，卻也各有缺漏之處，難以取得可服眾的單一隱私概念[190]。Solove 認為隱私實際上是以多種相近的概念組合而成的語義網，各個概念有獨立的意義，彼此之間又有交疊之處。以個人資訊的蒐集使用流程而言，不同的階段各有需保護的隱私利益。資料蒐集階段在意的是監控與訊問的疑慮；資料處理階段則關注聚合、識別、資安、再利用、隔絕等；而資料的傳播聚焦於秘密性、揭

[187] *See id.* at 34-45.
[188] *See id.* at 35-37.
[189] 六種主流理論為：獨處權、物理上限制他人接近、秘密、控制個人資訊、人格保護、親密。
[190] *See* SOLOVE, *supra* note 15, at 13-38, 39-40.

doi:10.6342/NTU202500550

露、可近性、挪用、勒索、扭曲等問題；另外，侵入私密領域與決策的干預可能構成隱私侵害。以此說明，隱私之概念在不同的情境下，指涉的概念與保護的利益亦有差異[191]，以單一概念定義隱私權並不可能。

拆解單一概念隱私觀點、確認隱私在個別情境各有指涉的利益之後，Waldman引用社會學者 Robert Merton 和 Erving Goffman 的理論，進一步說明隱私的社會功能。Merton 觀察到個人資訊的選擇性分享與流動，使人們能夠在生活中扮演數個角色，例如某甲同時是小孩的家長、公司的職員、社團的社長。不同的社會角色有其依從的行為常規、需要不同的個人資訊量來運作。而 Goffman 的社會角色理論更立體地呈現出個人資訊流的社會功能。個人資訊的選擇性揭露與流動讓人們在不同的社會關係、情境中展顯不同的形象，以此建構不同的生活領域，人們因此願意參與、開展多樣的社會生活與關係，社會互動因此可能、因此豐富充沛。進一步而言，決定個人資訊分享揭露的常規是參與者共同建立與遵循的，舉例來說，當雇主在面試員工時，除特定職業以外，應徵者不需也不會揭露生理狀況與感情狀態等資訊，雇主亦不詢問。由此可知，個人資訊流動的常規是人們在參與社會互動情境時必要的行為準則，亦為進入社會關係或情境之前評估的事項，成為參與者的期待之一[192]。因此，在隱私社會理論之下，單純個人資訊流常規的破壞行為亦可能構成隱私侵害，不須有實際損害出現。

接下來的問題即為是什麼樣的社會常規？就這個問題，Waldman 給出的答案是「在個別情境中被信任的資訊常規」。首先，Waldman說明，在其之前已有法律與社會學者就此問題提出見解：James Rachels、Edward Tverdek、法律學者 Lior Strahilevitz 的資訊流模型，以及法律學者 Helen Nissenbaum 有名的脈絡完整性理論。上述學者的理論亦是以社會理論為基礎，從實然的角度，分別提出在情境中決定資訊隱私的可參因素。例如資訊流模型的參與者身分、資訊類型與性質、資

[191] *See id.* at 101-70.
[192] *See* WALDMAN, *supra* note 64, at 37-39.

doi:10.6342/NTU202500550

訊流動網絡之特性等；和脈絡完整性理論從既存的社會常規所析出的社會情境性質、資訊性質、接收者身分、接收者與資訊主體關係、分享揭露與後續傳輸的條件等要素[193]。

然而，Waldman 認為，要為資訊隱私規範打下穩固的基礎，必須有具規範性的要素，即社會情境中的「信任」。這項主張也就是信任理論第二個重要的基礎。在這裡必須回答二個層次的問題，一為信任的重要性；二是情境中的信任何在。

關於信任的重要性問題，根據 Richards 和 Hartzog 的定義，以個人的角度觀察，信任是一種心理狀態，指即使他人可能做出傷害行為，擁有信任者仍願意承擔風險、展現出脆弱而與他人交流互動[194]；而從社會互動的觀點，Waldman 表示信任是一種存在於人際互動參與者間，期待他人將依循已被接受的社會常規行為的社會資本[195]。在買賣交易、親密與友誼、發表網路言論等關係中，一方當事人因資訊落差的存在、個人資訊的揭露、言論的發表，而在交易或交往關係中承擔受到傷害的風險，處於相對脆弱的境地。為了維持關係的運作，這些關係通常存在保護脆弱的一方當事人、使之信任風險不會發生的機制，例如交易關係中的契約、社交平台的隱私設定、匿名言論[196]。因此可知，對於一方特別脆弱的關係，信任是使這些關係運行不輟的關鍵要素，如 Richards 和 Hartzog 所述，信任是使關係建構與維繫的「黏著劑」[197]，因而必須有保護脆弱方之信任的機制存在。

在數位社會，個人資料主體在個人資料揭露之後也發生脆弱性[198]，而其間的信任展現於人們願意揭露個人資料並承受因此而生的脆弱。首先，最顯而易見的是對個人資料自主性的喪失，一旦個人資料分享揭露之後，資料主體難以追蹤個人資料使用情況，縱使行使限制利用、停止利用、刪除等個人控制權利，資料主

[193] *See id.* at 40-45.
[194] *See* Neil M. Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STANF. TECHNOL. LAW REV. 431, 448 (2016).
[195] *See* WALDMAN, *supra* note 20, at 51.
[196] *See* Richards & Hartzog, *supra* note 194. at 452-56.
[197] *See id.* at 451.
[198] *See id.* at 449.

doi:10.6342/NTU202500550

體也難確認該權利是否切實落實。再者，數位空間是由難以計數的軟體、硬體系統架構而成，不同的系統各有其營運者，數位資料在許多系統之間流轉，可能因為系統營運者的內部管理不當或防止外部駭客的機制保護力不足，而發生個人資料外洩的事件。最後是個人資料蒐集使用帶來的監控、操弄、未來可能性被凍結的問題，透過個人資料的持續蒐集而監視、控制被監控者的行為與思想是隱私權經典的議題，至今是重要的問題；而操弄是指幽微地引導個人的行為決策，個人以為的自主決策其實是在不自覺中被引導的，並非真正地自主，操弄方式有二，一為介面系統設計者以引導使用者做出符合系統設計者利益的決定，二則透過個人資料彙整出的個人資料檔案被用來分析、剖繪資料主體的人格圖像、習慣偏好、生活樣貌，根據人格剖析的結果，精準地投放足以刺激個人做成特定行為的資訊；而未來可能性被凍結則是指在前一章提到的預測分析技術帶來的問題，簡言之，今日的演算法預測分析技術將過去的經驗製成預測未來的模型，對未來做成預斷之後，以做出具體決定、預先介入導引事務發展方向、被預言者自我實現預言的方式實踐預斷結果，凍結未來發展的可能性。除了對個人資料自主控制的能力喪失之外，個人資料外洩、監控、操弄、未來可能性被凍結等問題，可能會導致個人的財產損失、行為自主性被抑制、人格發展自由受到侷限，甚而將社會發展凝固於基於過往經驗製成的模板，可變動性不復存。

個人資料之揭露所造成的脆弱化問題，除了發生在資料主體身上以外，也有可能影響第三人的權益，即前一章所述之推論他人資料之技術，應用後製造或再製不公正的社會關係的問題。詳言之，個人資料控管者蒐集、分析握有的個人資料檔案，描摹整體或特定群體的圖像或特徵，而對特定人口群體為差別待遇[199]。例如銀行透過過往行員與客戶交涉的經驗、客戶提供的資料，製作還款能力預測模型，該模型摹臨出在社會上屬經濟弱勢的某少數族裔的特徵圖像，包含消費的習慣、居住地區等特徵，一日某 A 欲向該銀行申請貸款，並未提供族裔資料，仍

[199] *See* Viljoen, *supra* note 169, at 630-32.

doi:10.6342/NTU202500550

因還款能力模型根據某 A 提供的其他資料，推論其為還款能力不佳的少數族裔，銀行因此拒絕某 A 的申請。

另外，除了原始的個人資料蒐集使用者，第三人也有可能是造成個人陷於上述脆弱境地的行為者。可能發生於原始資料蒐集者將個人資料再以買賣或其他原因傳輸予第三人，例如資料仲介（data broker）；亦有可能是第三人以非法方式取得個人資料，如駭入系統、內部員工外洩等[200]。

而信任，作為一項社會資本，是對於他人將依循某種可接受的常規而行為的期待，使人們願意涉險、接受脆弱處境而從事社會活動。所謂社會資本，Waldman 援引社會學者的研究，是人們相互為了利益而合作協調的社會生活面向，例如網絡、常規、信任等面向，是基於社會關係與網絡而來的資本。微者如個人因其社會地位而得到的優勢；宏者如國家或群體從合作、文化交換等互動中得到的集體利益。在社會中，人們行動的依據可能是基於經驗或獲取的資訊與知識。然而，有時人們對於未來的發展欠缺資訊，在此等具有不確定性的情形下，單純希望、信心、信任是處理不確定的機制，希望是被動、消極、無根據的想望；信心是獲取某些資訊之後知情的希望；而信任則是更積極地處理不確定性的策略，能夠解決資訊量不足的問題。人們因具備信任，即使在資訊缺乏之下，仍然能夠並願意行動。信任是社會互動順暢運作的必要基礎[201]。

那麼連結到第二個問題：在個人資料蒐集使用有關之情境中，信任是如何形成的。如 Waldman 的解析，信任可分為三種：個別性、制度性以及一般性的信任。個別性指對於特定個人或組織機構的信任，如我們在註冊使用數位服務時，以數位服務提供者的使用者條款內容與磋商結果，決定是否與該數位服務提供者建立關係；制度性的信任指人們以政府、企業、特定制度的形象，寬泛地認為其是否

[200] *See* Richards & Hartzog, *supra* note 194, at 451.
[201] *See* WALDMAN, *supra* note 64, at 51-52.

doi:10.6342/NTU202500550

值得信任；一般性信任則是指社會中廣泛存在的信任氛圍[202]。

反覆互動、明示或暗示、互惠（reciprocity）、移情（transference）是四種信任產生的原因。反覆互動是指在每次的人際互動中，因對方展現值得信任的反應、正向的回饋，而逐漸累積的信任感，例如我們願與守信、守密的朋友分享秘密。明示或暗示行為是因對方以明示或暗示方式，展現值得信任的外觀，引導他人授予信任，如保密條款、醫師問診。互惠與移情涉及對陌生人產生信任的情境。互惠是指在某些社會情境中，信任是一種遊戲規則，必須釋出信任、揭露來換取好處或玩遊戲，參與者願意承受風險、揭露的前提是知道能夠因此得到回饋，根據 Waldman 的研究，有些同志社群的交友平台便是依循互惠機制運作。而移情則是指我們把對某些人、某些機制的信任，轉移給其他陌生人，像是需要某些專業協助或者跨入陌生領域時，時常會尋求師長親友引介的專業或領域內人士；或者我們傾向對口碑好的醫院有更高的信任度[203]。

數位社會中，蒐集使用個人資料的企業、組織為了取得人們的信任，經營在意使用者隱私、致力於保護隱私的形象，並且在使用者的介面加入引誘使用者信任的元素，例如張貼其不會將個人資料移作他用或是不會外洩信用卡資訊等標語。而政府的政策亦朝向鼓勵企業向大眾、使用者公開隱私政策的透明化方向推進，以透明加強使用者評估風險的依據，增強使用者信任[204]。

在個人資料蒐集使用情境，Waldman 提出二項讓人們對網路服務產生一般性與制度性信任的因素。第一項是「大規模（bigness）」，人們會對有大量使用者的網路服務抱有高度的信任感，例如 Meta 公司的社群平台服務以告知個人目前正在使用該服務的一般或交友圈中的使用者數量，讓潛在使用者認為大眾或是信任的朋友都在使用服務，信任該服務而加入。另一項因素是「社群感（community）」，

[202] *See id.* at 51.
[203] *See id.* at 52-54.
[204] *See id.* at 49-50.

doi:10.6342/NTU202500550

例如在與朋友聊天時，見到朋友的頭貼而產生熟悉、親近的感受而自在地吐露；將現實生活具有親疏遠近之朋友在社群平台上同質化，容易讓使用者認為這些「朋友」都是一樣值得信任的，因而鬆懈在社群平台揭露分享個人資訊[205]。

另外，人們會對在網路空間遇到的人（包含陌生人）投以信任，重疊的社會網絡、共享小群體的社會認同是重要因素。使用者收到一名陌生人的交友邀請或訊息時，若發現自己與這名陌生人的共同好友越多，越容易對該陌生人產生信任感；此外，若使用者發現該陌生人與自己同屬於特定緊密小群體，例如同志社群、客家人、某原住民族群等，使用者可能展現出更高的信任感[206]。

更微觀地檢視數位服務的設計中會帶給使用者信任感的因素，以 Facebook 為例，在動態消息區塊，演算法根據其所預測的使用者偏好，投其所好地推播廣告或貼文，為了讓使用者更輕易地接受這些非由朋友發布的貼文，Facebook 會貼文上醒目的地方標示出使用者朋友當中按該貼文讚的朋友，提升使用者對此貼文的親切感，並且以淺色、縮小的字體標上「贊助」，減少使用者的排拒感。如此設計的好處，讓使用者放下戒心關注該貼文，博取使用者的注意力來賺取廣告費，且以此窺探使用者的喜好[207]。

綜上，信任隱私理論觀察到個人資料之揭露分享可能對資料主體、社會帶來傷害風險，使之處於脆弱境地，而為了使具有社會互動重要性的個人資料分享活動得以持續進行，應保護能夠推進人們願意參與有風險、充滿不確定性的活動的元素——信任。而人們在個別情境所信任並作為行為依據的個人資訊蒐集使用常規，便是資訊隱私。資訊隱私除了具有保護個人權益的功能以外，亦為各社會互動關係、場域的背景條件，資訊隱私對整體社會的價值在於，確保社會互動所必要的個人資料分享活動運行不輟。

[205] *See id.* at 56-57.
[206] *See id.* at 59.
[207] *See id.* at 85-92.

doi:10.6342/NTU202500550

第二項 信任隱私理論下的規範模型

保護資訊隱私之規範是讓數位社會能夠健全發展的背景條件。信任隱私理論認為唯有建立可信任的個人資料蒐集使用規則，人們才願意真誠地使用數位服務與商品、參與數位社會活動，持續分享供應有品質的個人資料，數位社會方能穩健地演進。而如 Waldman 的分析，要整體性地建立數位社會對個人資料蒐集使用活動的信任感，必須從個別性、制度性、一般性三個層次的信任著手。對應上述三個層次，以下分別介紹以信任隱私為理論基礎而進一步提出規範模型的 Jack Balkin、Neil Richards 和 Woodrow Hartzog 的資訊託管關係、模型； Priscilla Regan 的公共受託人模型；Dennis Hirsch 的公共信任理論。

第一款 資訊託管關係模型

自主控制典範下，個人資料流動原則上是由具體情境中的雙方當事人自主協商、達成合意來開啟以及決定流動的條件，成立資訊關係。所謂資訊關係，是指任何需要個人資訊來推進或達成特定目的之關係[208]。而數位社會的整體環境即是由無數資訊關係累積形成的。欲建立健全、可信任的數位環境，須先調整個別資訊關係的條件，資訊託管關係模型便是以此為目標。

資訊託管關係模型論者認為個人資料蒐集使用關係具有普通法的專業託管關係中的權力不對等、信任以及因信任而生的單方脆弱與剝削可能性之特性，二者可類比，因而主張將託管關係的諸項受託人義務導入個人資料蒐集使用關係作為主要的規範架構，以酌情揭露（discretion）、誠實告知（honesty）、保護安全（protection）義務修正原以自主控制理論為典範的公正資訊行為準則，並加入忠實（loyalty）義務處理資訊託管關係中的受託人自利和機會主義問題[209][210]。

---

[208] *See* Richards & Hartzog, *supra* note 194, at 451-52.
[209] 支持資訊託管關係模型之不同學者所主張之義務的名稱與內涵略有不同，本文以 Neil Richards 和 Woodrow Hartzog 的見解為主、Jack Balkin 為輔。
[210] *See* Richards & Hartzog, *supra* note 194, at 457.

doi:10.6342/NTU202500550

主張資訊託管關係模型的學者中，最著名的是 Jack Balkin。Balkin 提到美國普通法對當事人間特殊的信任關係設有保護機制——託管關係中的受託人義務，由於託管關係之特性以及當事人間的授信行為，國家介入私人關係進而要求一方當事人不背棄他方當事人之信任是合理的。典型託管關係中的受託人如醫師、律師、會計師，這些專門職業的從業人員因業務性質及職業專業性，會取得並管理患者或客戶的某些資產（asset），如身體健康、財產等重要事務以及敏感的個人資訊，患者或客戶因交予資產而承擔風險，且雙方存在知識與能力的落差而弱勢方在事前無從判斷交易風險，事後無法監督、控制，僅能單純信任受託人的專業。託管法設定了專業受託人的義務作為保護弱勢一方當事人信任的機制，要求受託人不背棄託管人之信任，使託管交易關係得以存續[211]。

Balkin說明，一般的專業受託人義務有二類：照顧義務（duty of care）和忠實義務（duty of loyalty），前者要求受託人依其職責行為而不損害客戶或患者的利益；後者要求受託人更積極地為客戶或患者的利益。通常，專業受託人因業務之性質，常取得客戶或患者的私密敏感資訊，受託人亦就個人資訊部分，負有保密、不以損害患者或客戶方式利用之義務[212]。以受託人義務作為保護弱勢託管人的機制，避免損害之發生，維持雙方的信任。

如本文在前所述，資訊關係中，個人資料的蒐集使用者擁有專業資料科學的知識、技術與設備，資料主體行為自主性之行使受制於個人資料蒐集使用者提供的環境，無從有效地判斷風險與進行事後的監督。而個人資料被蒐集之後，資料主體喪失對資料的自主控制能力，資料亦可能外洩或向外傳輸，並且在演算法的協力下，握有大量個人資料的組織或機構對於數位社會的人們，具有監控、操弄、凍結未來發展可能性的能力。然而，為了取得個人資料，數位產業經營隱私保護者的形象，推出隱私保護政策，以獲取資料主體的信任，資料主體亦因此授予信

[211] *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 UC DAVIS LAW REV. 1083, 1205-08, 1215-16 (2016).
[212] See *id.* at 1208.

doi:10.6342/NTU202500550

任、交予個人資料。資訊關係中存在著託管關係之當事人間知識與權力落差、弱勢當事人受到損害的風險、雙方之間的信任等特性。此時雙方建立「資訊託管關係」，揭露個人資料者為資訊託管人、接收個人資料者為資訊受託人、個人資料之揭露為託管人之授信行為[213]。

資訊關係之受託人因此應負有類似於專業受託人之義務，保護資訊關係的信任、平衡權力關係、維繫數位社會的運轉。資訊受託人義務之成立，根據 Balkin 的見解有三個要件：（一）當個人、組織或機構為取得信任而經營重視隱私的外在形象；（二）當個人、組織或機構使資料主體合理地信任其個人資料不會被揭露或濫用；（三）當資料主體上述信任依社會通念客觀判斷認屬合理[214]。

而義務的內容，除了一般託管關係中受託人對個人資料之保護與保密的義務之外，還有針對資訊託管關係之特殊問題而設之其他義務內容，具體來說，有酌情揭露（discretion）、誠實告知（honesty）、保護安全（protection）與忠實（loyalty）義務。在功能上，前三項義務是修正並充實原有的公正資訊行為準則，最後一項是專為數位企業的自利與機會主義問題所設。

第一目 資訊受託人的酌情揭露、誠實告知、保護安全義務

資訊受託人的酌情揭露義務是對秘密原則的修正。限制個人資料流動是個人資料保護的基本原則，資料主體基本上對於個人資料揭露對象都會保有某程度的保密期待，期待個人資料不被恣意揭露，或是在雙方議定的蒐集使用目的範圍內有限度的流動。然而，一般情境下，人們不會期待所有個人資訊的分享對象對其所接收到的所有資訊完全保密，而是希望資料被妥善使用；且在資料經濟下，幾難期待個人資料在揭露後僅作一次性地使用，然若以雙方合意之目的作為流動條件之限制，又落回自主控制典範的資料主體自主性實際上被控制的問題。酌情揭露義務要求資訊受託人應注意其所接收到的個人資料之揭露僅能限於有節度的範

[213] Richards & Hartzog, *supra* note 194, at 450.
[214] *See* Balkin, *supra* note 211, at 1223-24.

doi:10.6342/NTU202500550

圍內。所謂「有節度之揭露」係要求資訊受託人依個案情境，選擇揭露的資料內容與對象，並且避免明顯傷害資料主體而不合社會常規的揭露，例如造成其受到不當的負面社會評價之揭露。另一種有節度的揭露是模糊化的揭露，即使個人資料非秘密，資訊受託人揭露時仍應保留一定的模糊性，例如社群平台限制未經授權之第三人對平台上的個人資料之近用，在社群平台發布公開或半公開貼文，即等於公開資料、全網公開[215]。

誠實告知義務則是修正公開透明原則。公開透明原則是自主控制典範的重要原則，要求蒐集使用個人資料的組織或機構對個人揭露個人資料蒐集、使用之實踐，以及事後告知資料濫用或外洩的問題事件，另外亦須對大眾公開隱私政策與實踐。然而原有的公開透明原則並沒有發揮作用，資料主體仍無法理解個人資料蒐集使用行為的具體狀況與風險。誠實義務除了調整告知的強度以外，亦加入警示之規範建議，並提出幾項產業內部政策建議。對於告知的調整，主要是資訊受託人需積極主動地告知且以資料主體能理解之方式，告知的內容則至少是讓資料主體知悉其與資訊受託人之權利義務關係。而立基於信任理論的誠實義務，為了減少資料主體理解繁多資料蒐集使用者隱私政策與實踐之負擔，在告知事項新增可信度，要求資訊受託人誠實地告知資料主體能否寄予信任，若向資料主體表示可寄予與實際不符的信任程度，可能構成美國聯邦交易委員會法第 5 條之欺瞞行為而受處罰，在此的重點是要讓資料主體瞭解仍須對資料蒐集使用者、數位商品服務抱有懷疑，不能全然信任。最後，誠實義務鼓勵數位產業自願加強隱私保護之自律意識，包含內部政策與組織架構皆以隱私保護、增強信任為調整方向，例如對特種資料設有特殊資安保護機制、加強人員訓練、自主刪除已無使用必要的資料、設置適當的隱私侵害事件回應機制等[216]。

保護安全義務來自於安全原則。安全原則要求資料控管者保護資料的安全、

[215] *See* Richards & Hartzog, *supra* note 194, at 459-62.
[216] See *id.* at 462-65.

doi:10.6342/NTU202500550

避免外洩。而保護安全義務要求資料受託人將自己視為資料管理者，確保資料蒐集使用整個過程中的安全性，包含再利用、向第三人傳輸。保護義務的內涵可分為四個面向：一般性措施、資料外洩、資料匿名性之維持與敏感資料的特別保護、後續使用與傳輸。所謂一般性的措施包含定期稽核管理的資料狀態、定期評估資料蒐集使用的風險、最小化的資料蒐集與處理、更新資料保護技術等，確保資料外洩、識別風險升高、敏感資料喪失保護、後續使用與傳輸之資料安全性與保護力鬆動等情事不會發生。在資料外洩部分，除了防火牆、使用者驗證、加密機制以外，應設回應資料外洩事件的機制，且不只是外洩事件的發生，提升外洩風險的行為也構成違反保護義務之行為。資料之匿名性與敏感性的保護是對於特別敏感的個人資料設特別保護，且適當地去識別化處理一般與敏感個人資料，此時應搭配時下的技術措施，例如 K 匿名性或差異化隱私技術。而後續使用與傳輸之保護是指受託人將資料做原始目的外之使用，或是向外傳輸給第三人時，必須確保再利用或傳輸是在符合原始蒐集使用情境下的資料保護要求，例如自我要求或者要求第三人具有相同或更高的防止外洩機制與資料保護能力，或是資料匿名性與敏感性不因此喪失等，要求第三人的具體方法有以契約拘束。整體而言，形成複雜而多層次的資料保護機制[217]。

第二目 資訊受託人的忠實義務

相較於前述程序性義務，資訊受託人的忠實義務是對於個人資料蒐集使用之具有道德性的實質要求。典型託管法忠實義務的核心宗旨是受託人應將客戶的利益置於優先於受託人自己利益的位置。在資訊受託人的情境，忠實義務被用來處理數位產業利用資料主體脆弱性的機會主義問題。因資料主體在今日的數位環境揭露個人資料後，承受喪失自主性、能動性之脆弱風險，忠實義務即要求數位企業不應以趁人之危的方式不當獲取商業利益。

[217] *See id.* at 465-68.

doi:10.6342/NTU202500550

所謂機會主義指數位產業為了追求企業利益而剝削人類資訊的行為。詳言之，第一個為企業已利而剝削人類資訊的行為是人格剖繪與分類篩選，從監控技術與實踐、精準行銷的歷史發展可知，蒐集大量的人類資料進行特徵剖繪與人口分類之活動，使掌握此能力的個人、組織或機構能依其需要，以特定特徵標定人口進行有效的治理活動，而產生單方的政治、經濟、社會力量落差。與實體世界一樣，網路空間亦出現了監控與精準投放資訊的操作，數位產業蒐集使用個人資料的初衷是為消費者利益改善服務品質，而在今日，目的已變成為了企業利益而影響使用者的行為[218]。第二個層次是輕推，輕推指政府、企業、個人利用認知和行為科學之技術確保自己或他人作出特定決策。根據認知和行為科學研究，人類時常在某些情境下作不理性的決策，而能夠控制決策做成的環境者，也能控制決策的結果，因此有論者提出二項對決策環境控制者的道德性要求：以被輕推者之利益來設計輕推機制、人類能自由地做出非預設值的選擇。而數位企業作為設計人們作出隱私決策與使用環境的控制者，能輕推人們作符合企業利益而非個人利益的決定與使用行為[219]。最後一個層次是操弄，根據 Shoshana Zuboff 對監控資本主義的研究，監控資本主義的數位產業不只是蒐集個人資料預測使用者的偏好及未來的行為趨向，目前已發展至操弄使用者作出符合企業或廣告主需求的行為，例如劍橋分析事件中 Facebook 對使用者政治行為的操弄[220]。

資訊受託人的忠實義務之設計目的是要受託人在資料主體揭露的範圍內，為資料主體的最佳利益而行動。其實質內涵可分成三部分：強制或禁止規定、例外規定、指引規範的作用。

自主控制理論決定個人資料蒐集使用條件的方式是由當事人磋商，磋商結果指引資料蒐集使用者的行動。而信任理論資訊託管關係之忠實義務指引資訊受託

[218] *See* Neil M. Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. UNIV. LAW REV. 961, 969-73 (2021).
[219] *See id.* at 973-75.
[220] *See id.* at 975-76.

doi:10.6342/NTU202500550

人行動的準則是個人資料主體的「最佳利益」，意指資訊受託人決策、處理資料、設計介面時應以資料主體之福祉優先為預設值，在追求獲利的同時，亦須以賦權於資料主體的方式進行。所謂福祉係指一切資料主體交予資訊受託人管理的事務，除了個人資料以外，可能還有時間、注意力、經驗、人際關係、財務狀況等。何謂資料主體的最佳利益並非由當事人協商判斷，而是由掌握完整資訊與條件控制能力的專業資訊受託人與立法者決定，資料主體因此不會做出喪失能動性的個人資料蒐集使用決策。然而，為資料主體判斷何為最佳利益難免招致家父長主義的批評，對此，支持最佳利益論者回應，託管法之受託人義務有家父長主義色彩之規範是常態，如醫師並非所有取得患者同意的事項都可以執行、公司法亦設有董事對利益衝突事項應迴避之受託人忠實義務要求；此外，資訊環境基本上由資料蒐集使用者控制，資料主體的自主可能性幾不存在，加上理性決策的難題，為保護資料主體，某程度限制其自主性是必要的[221]。

資訊受託人的忠實義務可分為三個層次。第一層次為強制與禁止規定，包含禁止利益衝突之介面設計與資料處理、禁止免責。禁止利益衝突可分成二個面向：避免利益衝突和避免義務衝突，前者指受託人應避免追求自己利益之行為與託管人之利益有所衝突，後者為避免資訊託管關係之義務與受託人的其他義務衝突。詳言之，資料蒐集使用者具有為資料主體福祉的行為義務，其在蒐集處理資料、設計產品或調控資訊環境的時候，不能與上述行為義務衝突。具體來說，禁止利益衝突之要求至少能改良目的拘束原則及資料最小原則。蒐集與使用資料之目的並非當事人同意即可，應限於正當利益、排除純粹行銷與詐欺目的之資料蒐集使用。另外，當資料蒐集使用的原始目的已達成，資訊受託人應刪除資料，不得為自己利益而保留資料。而上述強制禁止規定不可透過免責機制而規避，忠實義務是對託管人最基本的保護[222]。

[221] *See id.* at 986-95.
[222] *See id.* at 996-99.

doi:10.6342/NTU202500550

第二個資訊受託人忠實義務的層次是例外規定。受託人義務之規範體系對前述禁止利益衝突、禁止免責等規定設有容許例外情形的機制，有個案調整的空間，資訊託管關係亦然。應設第三方組織、機構或法院，根據個案中資料主體的損益、受託人的利益、可預期風險、外部性、權力結構等因素，綜合判斷表面上利益衝突的行為，是否實際上不會造成資料主體損害[223]。第三個忠實義務的層次是對其他義務的指引及補充作用。例如當受託人不知告知的內容是否符合誠實義務要求，或者不確定資安系統是否足夠嚴實時，可用資料主體的最佳利益當成指引來判斷[224]。

第二款 公共受託人模型

要打造保護資訊隱私的可信任數位環境，除了以資訊託管關係穩固個人資料主體對個人資料蒐集使用者的信任感之外，建立制度性的信任也是重要的一環。Priscilla Regan 在信任理論的脈絡下，挪用通訊傳播法領域的「公共受託人（public trustee）」模式及「公共利益、便利及必要（public interest, convenience and necessity）」法理，主張網路行動者，即個人資料蒐集使用者，為公共受託人，並倡議設置上位的獨立監管組織，統合性地處理與巨量資料、網路有關的新興問題，如個人資料保護、反競爭、假訊息等。

在通訊傳播法領域，20 世紀初期美國政府欲對於時興的廣電媒體進行管制，採取公用事業的規範模式，視廣電媒體為有使用無線電波此類具稀缺性公共資源優先權的公共受託人，以大眾為受益人，由美國聯邦通訊傳播委員會（Federal Communications Commission，簡稱 FCC）分配無線電頻譜、發給執照，為授信的行為[225]。而在管制上，FCC 以「公共利益、便利及必要」作為分配頻譜與發給、

[223] *See id.* at 1001-02.
[224] *See id.* at 1002-03.
[225] *See* Erwin G. Krasnow & Jack N. Goodman, *The "Public Interest" Standard: The Search for the Holy Grail*, 50 FED. COMMUN. LAW J. 605, 610, 628 (1998).

doi:10.6342/NTU202500550

廢止執照之指導原則[226]。

Regan 認為，今日使用巨量資料、演算法技術的網路行動者掌控數位社會人們傳遞與獲取資訊的重要管道、開展日常活動與人際往來的工具，與巨量資料、演算法技術有關之組織與傳輸機制是支持數位社會運作的基礎設施，而此類基礎設施之順暢運作有賴於個人資料的供給，個人資料之供給則來自於人們對基礎設施的信任，信任這些基礎設施相關組織不會損害人們的自由與權利。人們的信任是網路行動者取用的稀缺公共資源，就此而言，網路行動者為公共受託人，基於公共利益、必要性與便利性原理，對公共受託人應有適度的治理[227]。

而治理的制度上，如同 FCC 之於廣電媒體，對於網路行動者亦應設有具獨立性的上位監管組織。Regan 進一步說明，因數位網路所涉議題廣泛，包含個人資料保護、反競爭、假訊息等，同時觸及不同單位的職掌事務，然而，數位網路及個人資料蒐集使用的議題的行動者與技術同一、亦具有高度技術性，相較於分散於個別現存的組織管領，新設整合型組織會是更好的選項[228]。

就監管組織之設計方式，「獨立性」是最核心的概念。首先，因過去網路自律政策的失敗以及網路自由的確保，在組織架構上應採取公私協力、相互協助並制衡，公部門的參與可貫徹公益保護、加強國家協助的可能性；私部門則懷有技術與專家資源、敏於技術與商業模式的發展、具實際影響數位環境的能力，並且避免數位技術落入國家控制[229]。

其次，關於組織之人事，首長之選任可考慮複數首長搭配交錯任期設計，避免政黨影響力過大而喪失獨立性；而組織成員部分，必須有跨科際的專家存在，

[226] 參見黃銘輝（2009），〈法治行政、正當程序與媒體所有權管制－借鏡美國管制經驗析論NCC對「旺旺入主三中」案處分之合法性與正當性〉，《法學新論》，17 期，頁 108；劉靜怡（2006），〈言論自由：第六講：言論自由、媒體類型規範與民主政治〉，《月旦法學教室》，42 期，頁 36-37。
[227] *See* Priscilla M. Regan, *A Design for Public Trustee and Privacy Protection Regulation*, 44 SETON HALL LEGIS. J. 487, 502-05 (2020).
[228] *See id.* at 502-05.
[229] *See id.* at 506-07.

doi:10.6342/NTU202500550

例如資訊通訊、資料、社會學、法律等領域，因此可設計有資格限制之提名制，緩和政治性[230]。資金來源可考慮二種方式，一為該組織自編預算後交國會審；二是由受治理的網路行動者繳交費用作為獨立的經費來源[231]。最後是透明性要求，由於該監管組織之獨立性與高度技術性，監督該組織之運作的方式亦為重要課題，有關執掌事務的執行，可建立內部的研究機構或委由外部機構研究，而研究所得作為組織運作的依據應可供外界檢視或第三方驗證，此外，組織之運作成果，亦可設有第三方驗證的機制[232]。

第三款 公共信任理論

信任隱私理論是從個人資料揭露對整體社會之影響此視角來推導隱私之內涵並建構理論。從正面論述，妥適的隱私保護、個人資料蒐集使用規則是架構健全的數位社會的骨幹；而在不具備妥適的規則的情況下，個人資料分享揭露會產生危害，破壞大眾對數位社會之參與的信任感，數位社會因此難以健康地發展。公共信任理論即以經濟學關於公共財相關理論與模型，從反面討論欠缺隱私保護對整體社會的傷害性，來證立完全由當事人自主協商、市場運作形成隱私保護規則之不可行，以及政府介入訂定具有強制力的規範之必要性。

公共信任理論攻擊自主控制理論、市場機制的主要論點是個人資料揭露的外溢效應：個人資料揭露的成本不只反映在資料主體身上，而會外溢由社會他人共同承擔，此為當事人自主交易之市場機制無法消化的成本。因巨量資料與機器學習發展，個人資料之揭露產生二種外溢效應，第一種是直接性的，資料主體揭露的是共享個人資料，即該資訊本身是複數自然人的個人資料，如在社群平台張貼與他人的合照；第二種是間接的，因巨量資料與機器學習的出現而使個人資料在聚合、特徵剖繪技術的加值下，被推論成為共享相同特徵的他人之個人資訊，例

[230] *See id.* at 508-10.
[231] *See id.* at 508-09.
[232] *See id.* at 511-12.

doi:10.6342/NTU202500550

如懷有身孕之使用者的數位服務使用行為被製成行為模板，有相似行為模板與特性之使用者被推論亦懷有身孕，即便從未揭露懷孕資訊[233]。

基於對個人資料揭露外溢效應的觀察，公共信任理論提出隱私是一項公共財的主張，若完全依賴市場機制來建立個人資料蒐集使用規則，會發生真正公共財的悲劇問題。

先略說明公共財與公共財的悲劇的概念。真正的公共財具有非排他性、非競爭性之特性，非排他性指所有人都可同時近用該資源，互不相斥；非競爭性指特定近用者對資源之享受，不會減損他人享受該資源的能力，例如空氣、漁場。而此二特性是市場不會消化使用該資源的外部成本的原因，因為不需處理通常也不會減損該資源的可用性，且該資源亦不專屬於任何人，沒有人有必要處理公共財的外部成本，產生大家都想享受資源而不願付出的搭便車問題[234]。然而外部成本仍存在，若資源使用者毫無節度地剝取資源，超過某個臨界點，會發生資源耗盡之公共財的悲劇。

而公共財的悲劇又可分為真正與不真正，二者差異在於非競爭性的程度，以及悲劇發生後是由誰承擔的問題。不真正的公共財悲劇發生在具有完全非競爭性的資源，也就是所有人享受該資源的能力都是一樣的，且每個人承擔的外部成本也相同，例如空氣。而真正的公共財悲劇則發生在半競爭性的資源，半競爭性指該資源被利用的程度若超越某個臨界值，該資源將發生競爭性，因此該資源的真正使用者以及大眾所承擔的外部成本是有差異的，例如漁場，當漁場的使用程度在臨界值以下，魚資源的更新與收取並未失衡，該漁場可永續；然若使用漁場的程度超出臨界值，則每一單位的使用會產生無法被消化的使用成本，且該使用成

[233] *See* Dennis D. Hirsch, *Privacy, Public Goods and the Tragedy of the Trust Commons: A Response to Professors Fairfield and Engel*, 65 DUKE LAW J. ONLINE 67, 70-71 (2016). Dennis Hirsch 之研究主要是建立在與其有相同問題意識的學者 Joshua Fairfield 和 Christoph Engel 文獻：Joshua Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE LAW J. 385, 389 (2015).

[234] *See* Hirsch, *supra* note 233, at 71-72.

doi:10.6342/NTU202500550

本對於漁場使用者及大眾是有不同的，漁場的枯竭是漁場使用者本身造成的，並由其承擔，故為真正的悲劇[235]。二者的差異在於管制的力道與方式[236]。

將隱私定性為公共財的主張有二個層次：第一個層次是學者 Joshua Fairfield 和 Christoph Engel 的理論，他們從資料主體（個人）以及與資料主體共享特徵的人口群體（群體）的角度看待個人資料揭露外部效應問題，認為問題在於個人利益與群體利益相反，也就是個人在做成個人資料揭露決定時，只關注自己的利益，這項揭露行為卻對於與之共享特徵群體中的他人之利益有所減損，這是個人無法顧及的。因此 Fairfield 和 Engel 提出的解方是資料主體群體之合作協商方案[237]。

而本文所稱之公共信任理論是由採取信任隱私理論之學者 Dennis Hirsch 所提出另一個層次的觀察。以信任作為隱私之內涵下，所有資料主體的信任是公共財，而公共財悲劇出現於數位企業恣意取用資料主體的信任來蒐集使用個人資料，若無節制地取用資料主體的信任，卻未採取保護個人及社會的適當措施，資料主體的信任終將崩盤，而拒絕透露或隱藏真實資訊。詳言之，資料主體對個人資料不會被濫用的信任是支撐數位經濟運轉的動力，而這項資源是所有參與數位經濟的企業都可以取用的，在信任未崩盤時，特定數位企業對信任的取用亦不會影響其他企業，是具有非排他性、非競爭性的公共財。然而，此信任如同漁場一般，在適當的取用之下，該資源有回復與更新而源源不絕的能力，但當個人資料的濫用行為過度氾濫，耗盡資料主體的信任，大眾將不再願意真誠地參與數位經濟的運作，數位企業難以取得充分且有品質的個人資料，發生真正的公共財悲劇[238]。

Hirsch 以此論證政府有介入維護資料主體的信任的空間與必要性，並援引學者 Carol Rose 所主張之公共財治理策略。Rose 提出的公共財治理策略有四項：什麼都不做（Do-nothing）、禁止新成員加入（Keepout）、建立使用規則（Rightway）、

[235] See *id.* at 77-80.
[236] *See id.* at 81-82.
[237] *See id.* at 82-83.
[238] *See id.* at 83-85.

doi:10.6342/NTU202500550

設定財產權（Property）。而決定採取哪項策略的方式是從管理公共財之成本、使用者使用資源應付成本、資源消耗所產生的成本，三個面向來計算。當取用的程度低、外部成本未對資源與社會產生壓力時，可採什麼都不做策略；當取用程度與外部成本所致之壓力升高，可採取管理成本較高之禁止新成員加入或建立使用規則策略；最後若資源被取用的程度已接近耗盡的臨界值，則應採成本最低、保護效率最高的設定財產權方式[239]。

Hirsch 認為今日整體社會對個人資料蒐集使用之可信度已產生疑慮、信任感下降，但大眾仍願意揭露、未臨近耗盡的臨界值，應在禁止新成員加入或建立使用規則之間選擇。而顯而易見地，禁止新成員加入這項策略將會抑制數位創新與資訊之多元性，並不適合作為數位經濟治理的策略。因此，為了保護整體數位社會的信任感，維持高品質個人資料之供給與流動，應以建立個人資料蒐集使用規則的公共財治理策略來保護信任隱私[240]。

第二節　隱私間隙理論（Privacy as Breathing Room for Boundary Management）

美國法律學者 Julie Cohen 提出隱私間隙理論，認為隱私是人們喘息的空間（breathing room），此空間使置身於特定社會、文化下的人們能夠管理、調節邊界（boundary management），發展自我並且定義、重新定義自己，因此是動態的過程。而此喘息空間，即隱私，是物質性（physical）、空間性（spatial）、資訊性（informational）、認識性（epistemological）的[241]。

隱私，最根本的意義涉及個人／私領域與社會／公領域之分界的討論[242]。

---

[239] *See id.* at 87-88.
[240] *See id.* at 88-91.
[241] *See* Cohen, *supra* note 18, at 12-13; *see also* Julie E. Cohen, *What Privacy Is For?*, 126 HARV. LAW REV. 1904, 1906, 1908 (2013).; *see also* JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE, 148 (2012).
[242] *See* SOLOVE & SCHWARTZ, *supra* note 59, at 39-41.

doi:10.6342/NTU202500550

Cohen 的隱私間隙理論便從二個面向建構：個人與社會的關係、個人與實體環境的關係。個人與社會的關係較鉅觀、廣泛，係在討論個人與制度、文化、實體環境等外於個人之條件的綜合；個人與實體環境則較微觀，特定在個人與實體環境的限制與預設條件之互動[243]。

整體而言，隱私間隙理論是建立在 Cohen 採取的實質自主觀點，係對傳統隱私理論建立在古典自由主義之形式自主觀點的反動。Cohen 的實質自主觀對形式自主觀的批判可分為三個層次：主體與社會的關係、主體性的建立、基本權理論。Cohen 的實質自主觀認為主體生來置身於社會，二者關係密不可分，並非如形式自主觀將主體、主體性獨立於社會與環境來想像；從而主體性的建立，對實質自主觀論者而言，與社會、主體置身的環境密切相關，社會、文化等外在環境會形塑置身其中之主體的主體性；在主體具體實踐其自主性、實現自由與平等基本權利保障部分，除了消極不受外在條件侵害、積極賦能予主體實踐自主、自由和平等面向以外，應將實體環境的符擔性（affordance）加入考量，實體環境的安排亦應使主體實現其自主、自由、平等。

對應前述三個層次之批判，Cohen 在第一層次——個人與社會關係部分，提出「社會主體理論」，主張主體與社會相互依存、關係切不可分。關於主體性建立之第二層次，在以社會主體理論理解主體與社會的關係之上，Cohen 提出「玩」（play）作為主體與社會互動關係模式之理解方式。而第三層次的基本權理論，Cohen 則推出比現有基本權理論更為廣泛——包含至實體環境配置亦應有利於主體性培育、實踐主體之自主性與基本權利保障——的基本權利理論。

以上為建構隱私間隙理論的理論基礎，因此本文在隱私間隙理論之前，在本節第一項先說明前述三個層次的基礎理論：第一款為社會主體理論，第二款為玩之主體與社會互動行為、關係模型，第三款是論及實質環境符擔性的基本權利理

[243] *See* Cohen, *supra* note 18, at 12, 15.

doi:10.6342/NTU202500550

論。爾後，再進入隱私間隙理論之說明。

第一項 隱私間隙理論之理論基礎：實質自主理論、基本權利的符擔性

進入隱私間隙理論之建構之前，須先說明 Cohen 的隱私間隙理論的立論基礎在二個層次上與傳統理論不同：自主理論與基本權利理論。

第一個是自主理論。傳統自由主義採取形式自主理論，主體的主體性是與生俱來的，只要未受外在環境之壓抑，主體之自主性便能完整地行使；而 Cohen 採取的實質自主理論批評傳統隱私權理論錯解主體性建構的過程，提出主張主體性是在社會與主體互動中形塑的「社會主體理論」。

延續社會主體理論的主體與社會為相互牽連關係之主張，Cohen 在隱私權保障的層次，提出基本權利的符擔性概念，意指在建構基本權利之內涵時，應把基本權利保障實踐的場域——物質環境——之條件納入考量。

第一款 實質自主理論：社會主體理論（socially situated subjectivity）

承上，本項說明隱私間隙理論的重要立論基礎：社會主體理論[244]。社會主體理論的核心概念是社會——主體所置身的環境——與主體之間是緊密、相互影響的關係。詳言之，主體是在其所處的社會與文化背景下產生與形塑；而主體所處之社會的物質、空間等外在環境之存在，亦係由主體解讀、理解。主體與其置身的外在環境形成緊密、無法分割的關係。

Cohen 認為古典自由主義有二項錯誤預設：心智與肉體分離、主體與空間各自獨立。Cohen 主張主體是心智與肉體的結合，而主體是置身在空間與環境之中的，主體並非抽離於社會、環境、空間。而其說明主體與外在環境為緊密關聯關

[244] 本文之所以將 Cohen 之“socially situated subjectivity”取名為社會主體，是因為該理論的核心主張是主體是置身於社會中的、二者關係緊密不可分離，因此本文以「社會主體」說明主體與社會為相互形塑、相互依存之關係。與社會主體理論相對的是形式自主理論，形式自主理論認為主體、主體性是外於社會而存在的。

doi:10.6342/NTU202500550

係的是從哲學、社會學、認知學等領域的研究，整理分析出「體現」（embodiment）這項概念。

體現在說明主體性與外在環境是緊密依存、相互映照與影響而產生。因此可分從二個方向理解：一為體化感知（embodied perception and cognition），此為從主體性的形塑與重構出發，論述主體性之形塑受到物質、社會秩序、文化等外在環境因素影響；第二個方向是外在環境、空間的存在與產生並非絕對、客觀的，而是由置身其間的主體賦義、由主體主觀的感受而具備意義，此為體現空間（embodied spatiality）之意涵。本款分於第一目與第二目介紹體化感知、體化空間此二概念。

第一目 體化感知（embodied perception and cognition）

體現的第一個面向是說明主體形塑方式之體化感知。體化感知指「自我（self）與肉體（body）是合一的，而肉體置身於社會與物質環境，媒介（mediate）著經驗與感知[245]」。在此要說的是，自我並不是遺世獨立的，而是與肉體合一，生長於存在社會秩序、蘊含文化的物質世界，因而自我的養成、形塑與發展受到社會、文化、物質的影響。

前述論點是 Cohen 從社會學、哲學、認知理論等學科對自我與外在世界之關係的觀察與研究析得。首先，社會學的「展演」（performance）與「區別」（distinction）之概念，說明人的社會化過程是在其置身的社會脈絡中，透過感知、觀察而進行的。詳言之，人在日常活動與行止之間「展演」出其內化社會秩序與風俗的成果，此內化的過程可能是接受、協商調整、拒絕；人們透過展演的行為之異同——差異來自於置身的領域或階級不同以及所接收到的風俗或秩序之別——區別人我[246]。其次，批判理論援引傅柯的凝視之規訓作用的研究，進而主張人類對於性別、種族、階級等社會秩序之順從與實踐，實際上是被他人之凝視規訓

[245] *See* COHEN, *supra* note 241. at 37.
[246] *See id.*

doi:10.6342/NTU202500550

的[247]。第三，現象學認為，知識之產生與體現認知緊密相連、無法切割，肉體調控著我們對於外在世界與現實之感知與理解。而我們所用的「隱喻」（metaphor）可資佐證，隱喻是人們將其所感知之外在世界事物，轉化、指涉為抽象的概念，例如比喻某人的「論點如同岩石一般堅硬」、「立論基礎宛如流沙般不穩固」[248]。

第二目 體化空間（embodied spatiality）

體現的第二個面向是體化空間。西方古典的自由主義認為，自主的主體是獨立於外在空間、世界而存在的，空間對於主體而言，只是一個存在的絕對客觀條件，宛如裝著一個個獨立主體的容器。然而，Cohen 批判古典自由主義的方式是引據認知理論對空間的理解——空間是主觀的，「空間是依照主體置身以及生活觸及的環境而被經驗，而人們理解空間的方式是體化感知」，此過程是「自我本位」（egocentric），因此，「空間是以體化感知而理解，同時亦以人類的活動而產生、而存在」[249]。

第三目 「玩」作為主體與社會的互動模式

主體不只是消極地接受外在環境的形塑，也會形構主體性形塑的外在環境、社會結構。Cohen 認為人類影響置身的外在環境的方式是透過「日常活動」（everyday practice）的「玩」（play）。

根據社會主體理論，人類每天在其所置身的物質、文化空間中生活、活動，以體化感知建立對外在事物的理解、辯證與建構主體性。而此形塑關係並非單向的、人類並非被動地單純接受外在世界的形塑，同時，人們也透過每一天的活動去影響、形構其所在的環境，決定主體性生長的條件[250]。在此前提下，Cohen 認為理論化人們形塑外在世界過程之最佳模型是「玩」。此模型並沒有具體的定義

[247] *See id.*
[248] *See id.* at 38-39.
[249] *See id.* at 39.
[250] *See id.* at 50-51.

doi:10.6342/NTU202500550

人類形塑環境的行為或過程，而是著重於特徵的描述。

根據社會學的觀察，相較於市場、政府的行為與活動具有計畫性，人類在日常生活裡的行動是根據個別情境的具體狀況與當下需求，所做出的回應，難以預測且有機動性，亦因此具有創造力[251]。例如人們在公共空間的行為會根據其需求與目的、空間的特性、主體的性格與特色等因素而異，公民團體的成員可利用公共空間的可視性倡議、提出訴求；少數文化群體的成員也透過公共空間的廣泛、難以標定特定個人的特性，而隱身、發展群體的特殊文化[252]。

人類的前述日常活動可用「玩」此一行為理解。「玩」是人類自幼即有的基本行為，即使到了成年時期，依然是人們認識、發掘、連結世界的重要方式。如我們所知，「玩」通常是在特定的物質環境或遊戲規則之下，但即使是相同的規則、場域、參與者，根據每位參與者在每個瞬間依當下環境與想法的變化而做出的判斷、策略、行動，每一場遊戲的過程與結果都不一樣。而遊戲雖有預設之目的，但該目的能否達成、每位參與者之目的是具有開放性的，而遊戲規則或實踐的場域也可能因參與者的回饋、行動而調整。

回到人們與社會結構的互動。社會是由實體場域、個別制度、角色常規、其他社會規則架構而起的，人們的日常活動就像不斷流動於社會結構之間的液體，液體的流動方向受到框架限制，但亦可透過液體對框架的來回撞擊而改變、重塑社會框架的形狀。「玩」即類似此概念，人們透過展演（performance）、遵守（conformity）與建構社會結構的常規、制度、物體互動，根據社會框架進行機動性的行動，人們以日常活動影響與重塑社會結構、挑戰主流。而「玩」與社會結構的互動有二個面向，第一個是政治性的，塑造（reproduction）與對抗（resistance）社會結構；第二個是貼近日常活動的，以置身的外在環境條件，進

[251] *See id.* at 51.
[252] *See id.* at 52.

doi:10.6342/NTU202500550

行可預測（predictability）與隨機（contingency）活動[253]。

個人、人們經由「玩」去形塑、改變其生存與生活的外在環境，又，該外在環境會影響主體性的生成，可知「玩」是達成個人自主、集體民主不可或缺的活動。

第四目 小結：隱私間隙理論的自主觀點

綜上，對於傳統自主理論想像主體、自我是獨立於社會、孤島式的存在，主體性、自主性是與生俱來的，並非在社會中養育而成之觀點。Cohen 反駁此模型過度理想化，自我是由社會形塑的，是體化經驗的產物。事實上，人們生活在社會網絡中，而此網絡內存在無數相互交織的關係、行動、信念，吾人置身其中而表述自我、形成自我。

再者，自我之發展具有偶然性（serendipity）。日常生活存在著制度、文化、物質環境等事物，這些事物形構成生活上的限制，約束著人們的人際關係、活動、思想，使其之發展具有可預測性。而人們面對上述事物所樹立的規矩，透過玩，來回地挑戰規則的容許性、在規則內發展新的操作、對抗或突破規則，主動地改變、形塑置身的環境。微觀而言，人們當下的每一個舉動、決策，受到過往經驗的無數個關係、行動、想法牽引、影響，因此生活中每一個場景內存在的人事物、人事物的活動有一定程度的偶然、不可預測性，並非必然。自我的表述與發展是主體與偶然存在的人事物互動下偶然形成的。

第二款 基本權利的符擔性（affordance）

除了自主理論，Cohen 亦採取實質化的基本權利理論。社會主體理論認為主體性的形塑、培育深受外在環境的影響，外在環境包含其他主體和物質環境，基於此理解，實質基本權利理論將基本權利之功能擴大至對於物質環境，亦要求其

[253] *See id.* at 53-56.

doi:10.6342/NTU202500550

在設計與配置上應有助於基本權利之實踐，而為基本權利的符擔性（affordance）。

所謂基本權利的符擔性係指為了使基本權利之實踐可能，基本權利之保障擴及要求物質環境之設計與配置使該功能有實現的空間，亦即物質環境應具有某些使基本權利可能實現的賦能要素（enabling properties）[254]。

符擔性所討論的是有機體（organism）與環境的關係，也就是外在環境能夠被有機體使用而發生的功能，不論該功能是否被強調或知悉。因此，特定環境物質可能有數項甚至無數的符擔性，例如湖水的符擔性包含飲用、划船，但不包含行走、食用[255]。而基本權利的符擔性要求對於人造物之設計上更加彰顯，人造物的設計能夠積極地促成、限制，或是完全排除特定功能之實現。例如菜刀之刀柄係為了便於切割；公園長椅的設計者為了不讓人們躺著睡覺而在長椅中央加上把手[256]。另外，物質環境之賦能要素存在集體（collective）的面向，數位網路是顯而易見的例子，網際網路是由無數的電腦、手機、資料庫等節點相連，因此數位化資訊得以傳遞與被取用[257]。

而在基本權利保障的層次，Cohen 指出符擔性係從物質環境（materiality）為出發點展開論述，與從自由為出發點（liberty-based）和從權能為出發點（capabilities-based）去論述基本權利之保障，會導引出不同的基本權利內涵。從權能為出發點之論述，會找出基本權利保障之實踐的最低門檻條件，例如擁有某些物質資源或具備特定智識能力等；而從物質環境為出發點論述的符擔性取徑，則是關注基本權利是如何透過物質環境之限制或容許性來實踐[258]。

Cohen 以更具體的例子說明：資訊設施等資源的接近使用能力或是該資源的分配是否不足，是從權能為出發點去論述基本權利保障會關注的層面；符擔性取

[254] Cohen, *supra* note 18, at 17.
[255] *See id.* at 18.
[256] *See id.* at 18.
[257] *See id.* at 18.
[258] *See id.* at 18.

doi:10.6342/NTU202500550

徑會考慮的是資訊設備與通訊協定運作的結果對於基本權利保障的影響。另一個例子是設計不當的信用評等或雇用系統對特定種族或社會弱勢群體造成歧視結果之問題，從自由為出發點的論述會將焦點放在該個人或群體受到的不利益或歧視結果；從權能為出發點的論述，則會在意弱勢群體能否接近使用必要資源或近用時遭遇的阻礙；符擔性取徑則是檢視物質環境之實體建設或市場環境是如何促成或容忍歧視[259]。

基本權利的符擔性所討論的是以物質環境的佈局與設計去影響整體社會結構運作的結果、甚至改變社會結構，因此關懷的範圍包含構成社會的各個因素，以及各因素之間的互動。Cohen 例示三項影響社會結構的因素：社會技術系統（sociotechnical system）、拼裝體（assemblage）、制度（institution）。社會技術系統是技術性因素與社會性因素互動之下所呈現出的佈局（arrangement）；拼裝體則是指異質性實體（heterogeneous entities）排列組合（ordering）的模式，使這些實體在特定時點運作[260]；社會技術系統與拼裝體反映並且再製、強化背後隱藏的政治與經濟權力。這些因素會影響實體設施的設計、商業模型、組織運作政策、行動者的實踐等各個面向，以及面向之間的互動關係。Cohen 認為，透過重新建構物質環境的符擔性——促進、容許、限制特定用途，能夠去牽動社會技術系統、拼裝體、制度等要素的系統性運作[261]。

第二項 隱私間隙理論

首先，主體之主體性是在社會諸多環境條件與主體的自我表述之間形成的[262]。而制度、文化、物質等社會環境條件在本質上具有形塑主體之傾向與能力，因此

[259] *See id.* at 18.
[260] 國立臺灣大學建築與城鄉研究所教授王志弘在其文章中對於拼裝體之說明為「異質元素的集合，彼此間有所關連，還能有所作用，並創造出不斷塑造、解離、拆散和重塑的領域，即『去領域化』（de-territorialization）和『再領域化』（re-territorialization）的動態過程」。參見王志弘（2015），〈拼裝都市論與都市政治經濟學之辯〉，《地理研究》，62 期，頁 110。
[261] *See* Cohen, *supra* note 18, at 19-20.
[262] *Cf. id.* at 20-21.

doi:10.6342/NTU202500550

壓迫主體做出超出預期、隨機、偶遇性的決策與行動的彈性空間，然而，上述彈性空間是主體展現獨特性之展現與實踐自主性之必要條件。主體在此空間進行自我表述、定義與重新定義自我與他人，主體性因而浮現。此彈性空間便是隱私間隙理論所主張之「隱私」。

說明何謂隱私之後，接續著辨識現代主體所生活之數位社會環境存在的隱私侵害，包含數位技術發展下，逐步改變的原有監控環境和主體對隱私之期待、產生新興的監控模式、機器學習引致的新興隱私侵害途徑。

辨識出數位時代的隱私侵害之後，為保障主體阻擋、對抗外在形塑力之彈性空間——即隱私——之存在，在基本權利的層次，除了基於個人資料自主權、保障個人對其資料之自主性而設有之諸多衍生權利之外，在基本權利的符擔性要求下，主體生活的社會環境條件亦應以保障隱私之趨向設計與配置。在 Cohen 的研究下，保障隱私之條件有語義不連續原則、運作可課責原則。

第一款 隱私是主體進行邊界管控的間隙（room for boundary management）

Cohen 定義隱私是「為了使主體能夠管理與他人之邊界來定義與重新定義自我與他人的呼吸間隙」。Cohen 對於隱私的想像仍是源自於隱私最古典的意涵——個人與社會之間的阻隔而其特殊處在於將隱私設定為「產生足夠私人性（private）與珍視隱私（privacy-valuing）之主體的必要條件」[263]，而隱私的條件蘊含著「一動態的間隙，該間隙存在係為了使社會主體能夠經由定義與重新定義自己為主體，來從事邊界管理的活動[264]」。

根據 Cohen 採取實質的自主觀——社會主體理論，主體不可避免地生活於充滿其他人事物的社會中，主體的生成、主體性的養育、個人的自我發展與自我表述，皆受到外在社會環境中諸項因素的牽引。其他人事物可能基於種種理由，例

[263] *Id.* at 12.
[264] Cohen, *supra* note 18, at 20.

doi:10.6342/NTU202500550

如獲取政治或經濟利益，而壓迫、穿透、侵蝕、破壞私人領域。主體未必有能力阻抗來自外在環境的影響、侵擾、壓迫，若主體之私人領域不復存，社會主體的自主性、多元性、自決與思辨能力、創造力大幅減損，民主社會的活水泉源被閉塞而停滯。

因此，隱私是保護社會主體的私人領域之必要條件，也就是界於主體與外在社會環境之間、阻隔出私人與公共領域的「間隙」（room）。而此空隙的功能是提供生存於社會的主體，在面對種種來自外在環境之活動、拘束、壓迫，能夠自主管理自我與外界的邊界（room for boundary management）。主體因此能夠遁回空隙呼吸、喘息（breathing room），並且能夠進行對自己與他人的定義、重新定義。而因外在環境對私人領域的侵害根據社會、時空、脈絡而有不同，從而此一隱私間隙具有變動性[265]。隱私之內涵必須進入個別社會與時空環境具體分析。

因此，Cohen 在說明現代的隱私——作為保護社會主體之私人領域、確保足夠私人性與珍視隱私之主體生成的條件——應有的內涵時，實際地分析生活於數位社會的主體正面臨的私人領域侵害：數位監控。再提出隱私間隙理論下，數位時代隱私保障應有的內涵：語義不連續原則、運作可課責原則。

第二款 數位社會的隱私侵害：數位監控

要瞭解主體在數位社會遭遇的隱私侵害，應整體性地掌握主體身處的社會環境，包含地理空間以及隱私干預活動。因此本款第一目介紹數位社會的地理空間，第二、三目則是 Cohen 指出現代數位社會主體受到主體性發展干預——數位監控。

第一目 數位地理空間

數位資訊技術的發展與應用造就數位社會的出現，使人類文明進入數位時代。

[265] Cohen 之原文為“Privacy is a dynamic condition that is best described as breathing room for socially situated subjects to engage in processes of boundary management through which they define and redefine themselves as subjects.”. *See id.* at 28.

doi:10.6342/NTU202500550

依社會主體理論，主體所置身的空間、外在環境培育了主體性。欲瞭解主體性在數位社會是如何培育、面對的威脅與傷害等問題，須先掌握主體生存與生活的外在環境——數位社會之「空間」（space）。Cohen 認為，不應將數位空間看作一獨立、嶄新的事物來賦予定義，而應仔細檢視數位資訊技術如何改變我們所經驗的空間[266]。

Cohen 理解數位社會空間的核心概念是：數位網路不是一獨立於實體空間的存在，而是疊加關係，共同構築了數位社會主體的生存與生活環境。

延續跨學科的研究方法，本部分 Cohen 取用地理學、社會學、網絡學等學科研究來論證前述主張。論證方式是先以社會學的研究提出空間構築的基本模型——千層酥（mille-feuille）模型；再使用地理學描繪地圖（mapping）之研究方法，具體地描繪當代數位社會空間的輪廓。描繪地圖方法能夠對於觀測的空間進行一定程度的抽象化、表徵化，瞭解數位空間受當代地理、政治與社會權力之力量形塑後的整體風貌[267]。

所謂千層酥空間模型，是由社會學與哲學領域研究空間的學者 Henri Lefebvre 提出的。Lefebvre 認為地理空間宛如千層酥（mille-feuille），是由貨品流、資訊流、人流等複數的網絡層層疊加而成的。新的網絡出現之後會繼續疊加在既有的地理空間上，使既有的物理空間產生質變，當代人類生活的空間場域因此逐漸演變。例如城鎮內的市場、國內市場、國際市場，與實體商品市場、資本市場、勞動市場，以及資訊溝通網絡、公路運輸等，各為網絡。而每疊加一層網絡，便會改變空間原有的樣貌。Cohen 以實體運輸為例，空運網絡出現之後，改變原先由公路、鐵路、水運等網絡構築的空間之城市間的關係，美國紐約飛到法國巴黎的航行時間，甚可能短於從紐約開車到美國某鄉鎮的時間[268]。

---

[266] COHEN, *supra* note 241, at 41.
[267] *See id.* at 42. 在此之「空間」非指有形、實體空間，而是社會主體身處的外在環境。
[268] *See id.* at 41-42.

doi:10.6342/NTU202500550

現代社會主體所生活的地理空間是疊加數位資訊網絡層之後形成的，具體而言，加入了建設數位資訊網絡的硬體設施、數位服務與工具，以及控制硬體設施、數位服務與工具的行動者。首先，數位資訊網絡是建立在實體空間的硬體設施之上，例如光纖管線、路由器、資料庫、電腦、智慧裝置等；再者，數位網絡技術的發展使實體空間產生變化，例如資訊技術專業人才與資金進駐高科技產業園區，帶動周邊地區的發展；此外，能夠實際掌控資訊與通訊設備與技術的行動者，能藉由對設施之控制與組織運作邏輯的安排，來支配數位資訊網絡空間的資料流動，因而影響著社會與經濟的活動[269]。

而疊加數位資訊網絡之後的現代地理空間發生一些量變與質變。Cohen 提到，在資訊傳播的廣度與密度面向，資訊可透過資訊網絡而傳得更遠，資訊傳播者與受眾之間的資訊流動更為緊密、密合。在經濟、商業的面向，資訊汰舊換新的速度益發快速，影響流行文化的新陳代謝，使得商品的供應鏈更加敏感與脆弱，個人化服務與精準資訊投放技術，改變行銷手法與商業模式。另外，數位資訊技術帶來許多新穎的人類活動與行為，例如智慧裝置與定位技術連通實體與數位資訊空間，人類在實體空間活動影響其接收到的數位資訊、其所接收的數位資訊亦影響實體空間行動。在社會權力結構面向，數位網絡資訊技術資源的分配具有政治與經濟的影響力，掌握數位資源者能夠支配言論市場與商品市場，而佔據政治、經濟決策的關鍵地位[270]。

第二目 數位監控：標準化監控、空間性暴露監控、主體協助監控與自我監控、調節式監控

認識現代社會主體所置身的生活場域之後，Cohen 指出四種數位社會的監控活動，分別是因個人資料蒐集活動所致之個人資訊性透明的標準化監控、主體在實體與數位空間暴露之監控、主體協助與自我監控而成為監控活動一環、調節式

[269] *See id.* at 42-43.
[270] *See id.* at 44-45.

doi:10.6342/NTU202500550

監控。

1. 標準化監控

標準化監控是指 Foucault 所提出的以統計方法將使規則常態化，達成規訓效果的監控手法。標準化監控的運作方法是規訓者根據特定常規，廣泛地將個人特徵化、分類、特定，再將這些個人編列階級，給予包含不合格或失格的評鑑，是一種以廣泛適用的常規去定義受評鑑者（judicial subject）的評鑑系統（judicial system）。Cohen 也提到，Foucault 的標準化監控模式不需存在中心化的監視系統，而是透過公部門與私部門的統計與精算治理方法，分散在市民生活的各項習俗慣例、規範制度、組織機構運作[271]。

Cohen 指出，標準化監控雖以個人資料之蒐集為基礎，但在此模式之下，個人的資訊性透明不只來自資料蒐集活動，還包含透過共享的特徵、屬性將個人連結至依常規製作的特定群體類別，並以對該群體的評價、印象去定性被歸入類別的個人。因此標準化監控伴隨著二種不對等的權力結構，第一種存在於階級化治理、評價系統中的階級、類別之間；第二種則是監控者／評鑑者與被監控者／受評鑑者之間[272]。而此標準化監控系統適用的時機涵蓋對未來政策之制定，以及對過去歷史的描述、定性[273]。

對於數位社會標準化監控的結構與運作手法，Cohen 採用社會學者 Kevin Haggerty 和 Richard Ericson 的「監控者拼裝體／集團」（surveillant assemblage）概念理解之。監控者拼裝體是由不同但彼此相連的公私部門活動構成的，這些公私部門活動試圖掌握存在於空間中與人們認知上的資訊流，來控制資訊帶來的權力。Haggerty 和 Ericson 的監控者拼裝體的監控手法除了 Foucault 提出的常規規訓之外，

[271] *See* COHEN, *supra* note 241, at 136.
[272] *See id.* at 136-37.
[273] *See id.* at 137.

doi:10.6342/NTU202500550

還有透過利誘，使主體願意受監控[274]。

Cohen 結合 Foucault、Haggerty 和 Ericson 理論而描述的數位社會標準化監控，將主體寫定於特定脈絡，限制了主體掙脫給定之框架而在不同脈絡之間展顯自我而逐步發展出主體性的可能，也限制了主體拒絕被常態化、主張多元性的能力。甚至以利誘手法逐漸奴化主體，使之失去反思、質疑與抗爭的意志。根據以上的描述，Cohen 分析出數位社會的監控有一源係來自資訊處理活動，特別是分析個人資訊建立公私部門分類與排序的邏輯[275]。

2. 空間性暴露監控

在現代社會結構下，主體隱私間隙受到減損的第二個途徑是空間性暴露的問題，此一問題是指監控者集團在實體與數位空間設置監控系統與建立空間規則，並以讓被監控者在實體與數位空間中感到暴露的方式，使其自動地依循監控者設計的規則活動。此類監控的特色在於，監控者不需持續實際地觀看，只要被監控者瞭解存在被監視的可能性，便將自我規訓，是透過被監控者的不安全感進行監控。Cohen 說明，使主體在空間中暴露之操作，帶來幾項影響主體性發展的變化：對主體而言，除了上述的因不安全感而自我規訓之外，當主體無法避開監控活動、無法確認監控者之評價，將逐漸消極、服膺於監控系統；對空間來說，該空間因為被設定規則、設置監控系統、以符合監控利益方式設計，而具有場域性（placeness），意即該空間被定性，被限定於特定使用規則、方式或群體；而就主體性發展，空間的動態性與關係性被抑制，主體性發展的脈絡與敘事背景被寫定。整體來說，監控者因此可以預測被監控者行為、被監控者則無法預期監控之存否與行為的後果，改變空間的權力結構[276]。

空間性的暴露也存在於數位空間，實體空間中的監視系統更加廣佈於數位空

[274] *See id.* at 137.
[275] *See id.* at 137-38.
[276] *See id.* at 138-42.

doi:10.6342/NTU202500550

間，使用者操作數位資訊網絡服務之軌跡、傳輸的資料可能被該服務提供者、網絡服務的硬體與軟體設備商、資料庫系統商取得或取用。此外，相較於實體空間，數位資訊網絡空間對一般使用者而言，不存在「家宅」此一使主體完全放鬆自在的場域，然如家宅等隱身泡泡（invisible bubble）允許個人進行完全不受拘束的心智與身體活動，係主體性發展之要件，在數位資訊網絡空間並不存在。因此在數位空間，亦發生了上述實體空間中的主體消極、服從監控系統，以及空間之使用規則被限定而影響主體性發展的問題。此外，Cohen 提到，透過使主體在數位空間中暴露的手法，主體的線上行為將消極地服從於數位空間規則，加強主體之行為偏好被轉譯為資料的進程[277]。

3. 主體協助與自我監控

第三種的數位網絡社會環境危害主體性發展之方式更為危險，係將開放與透明常規化使主體服從該規則，並馴化主體進行協助監控與自我監控。為使個人、使用者接納、習慣資料蒐集使用之要求，監控者集團以「資料越多越貼近使用者偏好與需求而越好用」、「資料越多越貼近現實」、「提供個人資料有益於社群」、「資料是社會進步的動能」、「資料是數位經濟的石油」等說法進行說服個人交予資料，或施以小惠誘使使用者加入個人資料提供活動，逐漸使個人與社會習慣個人資料蒐集使用成為常態。除了打造有利資料蒐用的資訊環境、卸除個人與社會的戒心之外，監控者集團進而馴化主體使之成為監控集團的成員，進行協助監控與自我監控，包含上繳資料與參與強加模板之活動[278]。

在協同監控部分，Cohen 指出，如鄉民上傳不符合社會道德倫理之照片或事件來引起網路公審、個人上傳包含他人個人資料之文字或照片等行為，讓監控者集團能夠更加洞悉個人、他人、社群、社會之圖像；另外，Cohen 亦表示，個人可能會以人工方式處理分析資料以進行人口剖繪與評價，例如雇主在網路上肉搜

[277] *See id.* at 142-43.
[278] *See id.* at 142-43.

doi:10.6342/NTU202500550

求職者之資訊，根據人格圖像做成評價，如此加深主體做出符合好的評價的人格模板之行動。Cohen 認為主體之自我監控不只是指接受資料蒐集使用指令而已，亦有追求好的資訊社群形象而自行跳入監控者集團推出的優良行為模板[279]。

4. 調節式監控

數位社會的監控有另一種型態：調節式監控。調節式監控是一過程，指監控的品質、內容是根據主體行為而調整，根據某些主體不理解的邏輯決定對其行為之回饋。在數位社會，政府追求行政效率、國家安全等公益，以及資訊資本主義的私人企業為獲取經濟利益，打造不利於民主自決的個人舒適圈，皆採用調節式監控，使人民、公民、消費者有高度可預測性，置於政府、企業掌控範圍內。然而，人民對於政府與企業調節式監控操作之存在或具體實踐卻不知情。

公民性（citizenship）受政治、經濟等制度，以及物質環境——包含資訊通訊技術——的影響。公民性是一連串的實踐，投票、公共辯論、搜尋與接收資訊等皆屬之。上述實踐行動的方式、內容、範圍、地點等受到政治與經濟力的配置。舉例而言，若某民主政府決定建造供公共辯論的民主實體與線上大論壇，匿名性、字數限制、是否有自動審查機制、檢舉制等決策，將影響公民辯論的場域、方式等。企業的政策涉及公民討論的議題、建築物等財產影響公民集會遊行時的路線[280]。而公民能夠觸及的資訊以及社群與公民性之培養、實踐有關。數位社會的資訊通訊技術發展下，搜尋引擎、社群網絡平台、資訊內容格式變革等技術的出現以及其設計方式，改變人類的資訊近用與人際、社群聯繫[281]。

而監控本質上為進行社會控制之方法，有效地使人們自動遵循特定社會規範[282]。對政府而言，為追求為行政效能、國家安全等理由，會採行適當的監控手段，

[279] *See id.* at 143-45.
[280] *See* Cohen, *supra* note 14, at 1912-13.
[281] *See* Cohen, *supra* note 14, at 1913.
[282] *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 UNIV. PA. LAW REV. 477, 493-94 (2006).

doi:10.6342/NTU202500550

例如公共場所監視器之設置[283]。而對企業，相較於洞察、配合消費者需求，創造符合自己利益之需求毋寧是更有效賺取利潤、避免風險與無效消耗的手段。

調節式監控的特性在於，除了監控行為原有的具特定目的、常態性、系統性、聚焦等性質以外，能夠廣泛地針對每一被監控者持續修正回饋。建立在二個技術背景上：一為數位工具與其介面之設計上，努力於讓使用者感受不到持續性的資料蒐集與調節回饋之存在，回饋所依循的邏輯被黑箱演算法掩蓋，以便取得使用者以自然互動而生的資料；二是數位工具強勢地進入人類日常生活，廣泛地存在，人類被監控的活動範圍劇增[284]。

因此，在數位資訊通訊技術輔助下，政府與企業可能基於追求公共利益與商業利益目的而進行調節式監控。然而 Cohen 指出，整體來說，調節式監控是採用資訊資本主義[285]之私人企業主要的獲利手法，其大量蒐集資料、反覆鍛煉資料、亟力剝削資料價值，追求最大化的經濟利益[286]。例如為商業利益而激發消費者做出特定經濟行為之輕推（nudge）；以及為建立人民特定政治取向而打造客製化資訊空間——即言論濾泡（speech filter）。輕推和言論濾泡的核心操作便是調節式監控，分析個別的消費者、公民之特性與行為輸入（input）給出不同的回應[287]。

Cohen 指出，數位社會的公民性格係由偏好行政效能、國家安全等公益之政府、資訊資本主義的私人企業，協同操作調節式監控而培育。培育出的公民性格並非自由民主社會所喜，活絡的自由民主社會需要知情、具批判性思考能力、積極參與公共討論的人民，而調節式監控下的人民被個別化、量身打造式的說服，其決策受到政府、私人企業牽引，自主性減損。此外，自由民主的公民性格需要能夠觸及多元言論的「不舒適感」，人民因此存有積極對抗反對言論、實現政治

[283] *See id.* 493-94; *see also* Cohen, *supra* note 241, at 1914-15.
[284] *See* Cohen, *supra* note 241. at 1913-14.
[285] *See id.* at 1915-16.
[286] 根據 Cohen 的說明，資本主義指以控制生產與累積的方法，開發能夠在資本上取得之剩餘的最大值，追求獲益最大化。資訊主義指以累積知識、追求資訊處理的高度複雜性為行動的取向、方針。*See* Cohen, *supra* note 241, at 1915-16.
[287] *See id.* at 1916-17.

doi:10.6342/NTU202500550

理想的渴望，公民社會因而活絡；若人民浸淫於根據其偏好而量身製作資訊空間，個別化資訊環境之舒適感使之怠惰，為政治理想而掙扎、奮鬥的性格逐漸被馴化[288]。

第三項 隱私間隙理論隱私權之保障領域：語義不連續原則、運作可課責原則

資訊隱私權的符擔性係針對當代社會主體生活的整體數位社會環境的設計與配置，應促進基本權利之實現。採取社會主體理論與隱私間隙理論之下，資訊隱私權應確保主體能夠抵抗來自其他環境因素的社會形塑力，以及透過日常實踐之玩之行為去改變、重塑對己有形塑力的外在環境，即確保抵抗、玩可發生的隱私間隙存在。Cohen 指出資訊隱私權因此須保障上述隱私間隙之存有與品質[289]，進而提出語義不連續（semantic discontinuity）、運作可課責（operational accountability）二項原則，具體化資訊隱私權的符擔性。

第一款 語義不連續原則

語義不連續原則主要是針對數位社會的監控問題而設，保障數位社會主體能夠有效地對抗數位社會中常態性地存在之對個人之積極塑造力。如本文在前所述，數位社會主體身處於廣泛存在加強版標準化監控與新興調節式監控操作的社會環境，而此二種數位監控的發生是源於監控操作中，政府與企業監控者建立嚴實的監控網絡社會結構，以及不斷發生的主體被精細地轉譯為數位資料的過程。語義不連續原則便是在防止、阻礙數位監控操作在監控網絡結構、資料轉譯的完整性[290]。

第一目 自我的不可計算性

[288] *See id.* at 1917-18.
[289] *Id.* at 21.
[290] *Id.* at 21.

doi:10.6342/NTU202500550

Cohen 認為，語義不連續原則的第一個實踐方法，是確保主體在實體環境和資訊層次上的「不可計算性」（incomputable）。Cohen 援引歐洲學者 Mireille Hildebrandt 提出的「不可計算的自我」（incomputable self）概念，即「自我」具有不可計算之本質。Hildebrandt 從二個面向證成此主張。從資訊學面向，由原子構成的真實世界之物件、事件、過程實際上無法被計算，被計算的僅是原子世界以數位資料型態表述之替代物。原因有二：一為機器學習等演算法「預測未來」的方法，是將過去的真實世界事物轉譯為可被機器處理的數位資料，計算出可能隱含的規則，作為推論的基礎，然而，每一次的轉譯／資料化過程，必然伴隨著真實世界部分的內容遺失（lost），數位資料型態之表述不可能等同於真實世界之真品；再者，縱算為了解決上述遺失的問題而將真實世界鉅細靡遺地轉譯、資料化，然而越高維度的計算、在數學上越難執行，是故完全、不遺落的轉譯與計算不具有實踐可能性[291]。

Hildebrandt 再從哲學、社會學等人文面向論證自我之不可計算性，此一面向的不可計算性源自於自我（self）的不確定性：自我認知／身分（identity）的雙重偶然性（double contingency），以及個人行為（act）與認知的關係性（relational）與生長（natality）性質[292]。

首先說明自我認同／身分的雙重偶然性。Hildebrandt 以社會學者 Paul Ricoeur 的「第三人稱視角（idem）與第一人稱視角（ipse）」理論，以及 George Herbert Mead 的「I 與 me」理論，建構出第二人稱視角。第三人稱視角是指主體居於他人、其他群體、社會等第三人角度稱呼（address）自己；第一人稱視角是指主體基於自我認知，對外的自我稱呼，涉及個人在社會的地位（position）。二者之間有「第二人稱視角」居間牽引著第一人稱與第三人稱視角的連動關係。第二人稱視角指主體／我從第三人的第一人稱視角觀看自我，建構與重構自我認知，根據該

[291] *See* Mireille Hildebrandt, *Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning*, 20 THEOR. INQ. LAW 83, 91-92 (2019).
[292] *See id.* at 87-93.

doi:10.6342/NTU202500550

認知做出或順應或反抗第二人稱視角的行動，再塑造與重塑他人、社會對主體／我的稱呼。上述自我認知／身分形塑與建構的過程所涉之第二人稱視角是基於不確定地預期（anticipation），而有雙重的偶然性。第一重的偶然性、不確定性在於主體從第三人的第一人稱視角對自我的觀看，是主體的預期、想像、猜測；第二重則在於主體做出的順應或反抗行動，會如何被第三人理解與詮釋，亦是基於主體的預測、想像、猜測。主體的自我認知／身分便在此過程中，不斷地形塑又重塑[293]。

另一項自我不可計算性的理由是個人認知與行為的生長性與關係性。先說明由 Hannah Arendt 提出之生長（natality）此項概念，人類從出生開始，受到好奇心與學習之需求驅動，不斷地探索、感知世界而持續地生長，延續至成人。而學習即是持續、反覆的生長歷程。相較於電腦程式，人類之學習有相互溝通從而持續創新（reinvent）的性質，電腦程式之學習能力有界限，在新的程式出現、出現無法偵錯（debug）的問題時，舊程式必須汰舊換新。而人類的學習則可透過個人與他人、社會常規之間來回不絕的溝通、校正而不停歇，此為個人行為與認知的持續生長性。而人類認知與行為的關係性則表示社會常規、環境與制度是由無數的個人行為與認知，透過反覆的相互溝通、校正集合所構成。因此，在人類認知與行為係由無數社會構成員，反覆持續地展示行動、相互學習、溝通與校正之下，認知與行為是不斷變動、持續發展、不確定的[294]。

Cohen 援引 Hildebrandt 的自我不可計算性作為主張語義不連續原則的依據，足以推翻「數位資料是客觀事實」之命題，並要求在進行個人／自我的轉譯、數位擷取時，應謹記自我之不可計算本質，正視甚至保留轉譯時的缺口、障礙、停止或跳出機制、不完全轉譯等阻礙[295]。

[293] *See id.* at 87-93.
[294] *See id.* at 87-93.
[295] *See* Cohen, *supra* note 18, at 21.

doi:10.6342/NTU202500550

首先，原子世界的事物不可能完全不遺漏地轉譯為數位資料並計算。再者，自我是不斷變動與校正而不確定的，個人行為在被轉譯為數位資料的當下，已經成為歷史紀錄，以過去的數位紀錄推論現實中持續生長的個人，終究不可能正確。最後，Hildebrandt 的自我認同／身分之第二人稱視角理論，可說明隱藏機器本質之人工智慧機器學習或機器人應有使用的限制，因為此類技術工具不可能以第一人稱視角詮釋主體，主體與披著人類外皮的機器互動時，無法以人類邏輯進行第二人稱視角之自我認知建構活動[296]。

第二目 公正的聚合

另一項 Cohen 提出的導引出語義不連續原則之主張，是挑戰「精準的個人化決策是符合人性尊嚴待遇」、「越多資料越好」命題的「公正的聚合」（just aggregation）原則。公正的聚合認為隱私權之保障應在資訊隱私面向禁止為人類行為賦加上高度理性化的人造框架，而在空間隱私面向提供供個人與集體隱身的庇護所（shelter）。證成公正的聚合之論證步驟是先拆解個人化決策等於合於人性尊嚴待遇之命題，理由有二，略為：數位資料形成的語義網（semantic web）雖然個人化，但決策的邏輯可能是制式化、將人類客體化的；個人語義網之缺漏處係由人口特徵剖繪推論的集體特徵填補的。因此帶出第二步驟的論證，所謂個人化決策實際上是虛構而不存在的，其根本為基於群體特徵剖繪的聚合式決定，重點是找出符合人性尊嚴要求的個人化與聚合式決策的條件。第三步驟是精準標定個人之個別化決策之技術基礎，是基於群體、人口特徵剖繪的聚合式決定，之所以能夠執行人口群體特徵剖繪的方法是個人在數位空間的透明化以及實體空間的曝露常規，並且發生數位資料跨脈絡的匯流（convergence）。是故，對於個人或特定群體之決定、判斷是否符合人性尊嚴之要求，重點不在於個人化或聚合式，而是找出符合人性尊嚴要求的個人化與聚合式決策的條件[297]。

[296] *See* Hildebrandt, *supra* note 291. at 92-93.
[297] *See* COHEN, *supra* note 241, at 251-52.

doi:10.6342/NTU202500550

因此，公正的聚合針對數位空間的透明、實體空間的強制曝露，以及資料匯流的問題，以個人資料之蒐集、使用、保存、移轉之限制，作為回應方式，至少必須阻斷跨脈絡的資料匯流。除此之外，Cohen 認為，以公正資訊行為作為基礎的資料受託人模型可以建立個人資料保護的基準[298]。

第二款 運作可課責原則

Cohen 提出的第二個隱私符擔性的規範原則是運作可課責（operational accountability）。運作可課責原則關注的是人類在實體環境的能動性，Cohen 在此所指之能動性不是個人在個別資料蒐集情境行使的告知同意權，而是指數位社會的公民、使用者，一般性地對於其被機讀的條件有置喙（have a say）的能力。而數位公民與使用者群體有影響人機互動、人類被機器讀取之環境與條件之前提與方式，是確保社會技術系統（sociotechnical system）運作的透明性與可問責性，規範的焦點指向資訊蒐用者與資訊蒐用整體環境的參與者之應負義務[299]。

為了證成數位社會應有運作可課責作為保障隱私之原則此一主張，Cohen 引用歐洲法學者 Mireille Hildebrandt 的「共同決定我們如何被讀取的權利」（the right to co-determine how we will be read），以及加拿大法學者 Lisa Austin 的「隱私關乎權力」（privacy is about power）理論，作為論證依據。Cohen 引用此二學者之理論的重點在於，指出數位社會的隱私保障應跳脫個人尺度，應從集體（collective）、強調社會參與者之連動關係（relational）作為設計規範的思考路徑[300]。

Hildebrandt的共同決定我們如何被讀取的權利是來自於其引用 Irwin Altman的隱私的關係性（relational conception of privacy）。隱私之關係性與 Cohen 的隱私間隙理論相似，同樣認為隱私是定義與維持自我與他者的邊界。而主體的邊界管理是有賴於潛在（tacit）的知識之直覺、動態的活動，根據認知科學相關研究，主

[298] *See id.* at 253.
[299] *See* Cohen, *supra* note 18, at 21-22.
[300] *See* Cohen, *supra* note 18, at 21-22.

doi:10.6342/NTU202500550

體的邊界管理決策是即時、自動進行風險計算，主體作為社會構成員，快速地根據由文化與社會建構的人際關係與群體的屬性，直覺性做出隱私判斷。因此，如 Catherine Dwyer 的主張，對於主體而言，揭露個人資料的問題並非對個人資料之控制，而是不知揭露之後的後果，當資料蒐集與計算無所不在（pervasive computing），今日的數位主體無從知悉其他主體、社會參與者會根據資料作出如何的推論。因此 Hildebrandt 主張，主體應有可以預期、共同參與決定自己如何被環境讀取的權利[301]。

而 Lisa Austin 則去檢視、分析既有的社會技術系統，數位監控是如何形成、運作的，是哪些社會參與者握有相關權力（power），作為隱私保障規範的關注焦點。Austin 是從法學關於權力、權力濫用與法律保障之一般性原則，作為對於數位監控的執行者、形塑監控運作之社會與制度條件的其他社會參與者設計義務規範之正當性依據。Austin 認為傳統受憲法保障之隱私權範圍，包含對抗不合理之搜索扣押之侵入（trespass）類型。在此有二個特殊處：侵入法源自於私法、不合理之搜索扣押不需實際損害（harm）之發生。Austin 認為，在此法規範進入的正當性是失衡的權力關係。因失衡的權力關係而生的義務規範，亦可見於勞動法中。Austin 從而主張，由於個人資料蒐集使用所致之數位監控造成的權力失衡關係，國家應介入，對於數位監控者、形成數位監控之社會與制度條件的其他參與者，設有義務規範[302]。

Cohen 援引二位學者的主張，不論從主體作為社會構成員而應有之集體權利面向，抑或是數位監控之權力形塑與對於權力濫用可能性之節制，個人資料蒐集使用者以及形塑蒐集使用環境之其他參與者，應負有適當的透明性義務作為主體參與決策之依據和課責之基礎。

---

[301] *See id.* at 21-22; *See* MIREILLE HILDEBRANDT, SMART TECHNOLOGIES AND THE END(S) OF LAW: NOVEL ENTANGLEMENTS OF LAW AND TECHNOLOGY 102-03 (2015).

[302] *See* Lisa M. Austin, *Enough About Me: Why Privacy Is About Power, Not Consent (or Harm)*, *in* A WORLD WITHOUT PRIVACY: WHAT LAW CAN AND SHOULD DO? 131, 159-61 (Austin Sarat ed., 1 ed. 2014).

doi:10.6342/NTU202500550

第三節　理論分析

本文認為應選擇隱私間隙理論為機器學習時代的資訊隱私權典範。選擇理論的判準係根據該理論能否、如何回應自主控制典範無力處理的機器學習時代演算法問題。

在第二章本文整理出自主控制典範在機器學習時代發生的問題。首先是因現實條件而使資訊主體無法自主控制個人資料之問題：在揭露分享前之磋商能力不對等、揭露分享後因個人資料瑣碎化而生之無從追蹤與控制。其次為自主控制典範在預設上的問題：如上所述，自主決策的情境與框架是被建構出來的，個人資料蒐用者單方掌握著決策的條件，所謂自主實際上是被侷限的；此外，理性本身亦有限制，如本文在第二章整理的人類傾向以簡化心智處理複雜情況，以及人類過度樂觀等系統性心理偏誤。最後是機器學習應用於推論與預測分析產生的推論個人資料、主體與社會固著問題，前者指使用機器學習人格剖繪而在原有資料以外，產生新的同一主體、不同主體的個人資料，就該資料之自主控制權如何實踐；後者是機器學習進行預測分析並做出決策，造成個人被限制在預測分析之安排中，致使個人與社會之未來發展由機器決定、非人類的問題。

本節於第一項先就新興理論——信任理論與間隙理論之異同，觀察此二理論的特性。在第二項，則以本文以上提出的問題為主、學者對理論的評釋為輔，提出本文支持隱私間隙理論作為機器學習時代的資訊隱私權典範之主張及理據。

第一項 信任理論與間隙理論之分析

相較於自主控制典範，信任理論與間隙理論最明顯的特色是在不否定個人對個人資料的自主控制權之下，論證資訊隱私具有某種社會關聯性，以此主張應設有非由當事人磋商、具強制性的個人資料的蒐集使用規則。而二者的差異可再分從理論層次，以及規範層次說明。

doi:10.6342/NTU202500550

第一款 理論層次之分析

而在理論的層次，二者雖然都主張應在個人資料自主控制之外，擬定新的個人資料保護規則，論述的途徑卻迥然不同，信任理論之建構方法是從社會結構的面向，間隙理論則是從個人之主體性、自主面向。

簡言之，信任理論根據社會學之社會角色理論，以及對數位社會以數位資料為動能之觀察，論證資訊隱私——某種個人資料流動的規則——是一種維繫社會運作之必要社會結構，而驅動資訊主體願意承擔資料揭露所生的風險之脆弱性，是基於對揭露對象的信任。為維持數位社會的個人資料流動不輟，應保護資料主體對個人資料分享揭露的信任感，此為設置資訊隱私法規範的正當性。而資訊隱私之個人資料流動的規則作為社會結構之功能、面向，是著重於秘密保護、親密培養、自主實現與人性尊嚴保障的個人權利觀點，無法捕捉的。

相較於信任理論之現實面向分析取徑，間隙理論是以個人主體性、人格發展、自主的條件建構理論。間隙理論所主張的隱私權社會關聯性係上溯至主體之建構，間隙理論認為個人作為主體，是置身於社會當中，其自主之培育和實踐與社會密不可分。而主體性的養成、人格的發展、自主的培育與實踐，必須是個人擁有一私人領域、私人空間、隱私間隙為條件的，此一間隙使個人與其他個人、社會制度等他者互動時有所阻隔，個人保有自我定義、定義他人、反思試錯、形塑異見、對抗制度的可能性與空間。隱私間隙受到隱私權之保障，而隱私權的內涵不只是傳統的自主控制，因基本權利的實踐是在社會框架之下、基本權利亦屬存在於社會的事物，基本權利的保障內涵必須在意當代社會的環境條件，調整改變基本權利的內涵，使權利得以實踐，甚至積極打造有利於基本權實現的社會環境，以此推得基本權利的符擔性面向，個人資料保護權便從隱私權的符擔性演變而來，強調隱私權的實踐條件。

以典範變遷程度而言，本文認為信任理論僅是調整、強化既有資訊隱私權之

doi:10.6342/NTU202500550

典範。信任理論要求資訊受託人成為可信任的揭露對象，設置可信任的個人資料流動規範，所謂「可信任」的意義主要是依當事人自主磋商的結果，加上資訊流動脈絡之常規調整。此外，在資料受託人提供數位服務而設計產品、制定企業政策時，以使用者、資料主體的「最佳利益」控制資料受託人的可信任程度。整體來說，個人資料的蒐集使用規則仍是依當事人的磋商內容，以及各該資訊領域之行動者的實踐形塑的資訊常規決定。資訊受託人義務僅要求個人資料蒐集使用者加強告知義務、資料安全保護措施，以此強化資訊受託人的可信任度。對於跨單位、服務、平台、組織、脈絡的資訊流動，信任理論則要求資訊受託人作為具備專業技術能力者，為資料主體決定如何保持雙方磋商、主體信任的揭露條件。

而間隙理論則根本性地挑戰既有隱私權典範，並為隱私權重新定義。相較傳統理論，間隙理論從自主理論、基本權利理論至隱私權理論皆採取有別於傳統的見解。間隙理論根植於隱私最原始的概念——區分出私人領域，去討論區隔公私領域之間隙存在對於主體的意義，論述隱私間隙存在的必要性。而個人對於隱私間隙之保持，具有基本權利的地位。在涉及個人資料蒐集使用的面向，在 Cohen 的論述之下，受個人資料自主控制權與個人資料保護權保障。個人資料自主權是看重個人自由、依個人自由行使權能的面向（liberty-based、capability-based），個人資料保護權則是從基本權利實踐的環境條件——基本權利的符擔性——面向（affordance-based）建構，二者分從不同方向共同保障主體的隱私間隙存在。

第二款 規範層次之分析

在規範層次，信任理論認為資料主體與個人資料蒐集使用者之間，應成立資訊託管關係，資訊受託人應負如美國普通法對專業受託人要求負擔的諸項義務，並擬定一般性的資訊受託人義務，作為資訊受託人依循的行為準則，再設獨立的相關監管組織。而決定託管關係的範圍、受託人義務的內容與獨立監管組織的執法之原則是視當事人間的「信任」，根據雙方磋商時，資訊受託人誘使資料主體

doi:10.6342/NTU202500550

信任、資料主體授信的範圍與內涵，判斷是否成立託管關係，以及對於各資料主體之資料應保護的程度。具體來說，資訊受託人在處理個人資料、提供主體資訊服務時，應為資料主體、使用者之「最佳利益」執行其業務，將此原則謹記在心。當有爭議、衝突事件發生，最佳利益原則亦為資訊受託人為其行為辯護的說理方向。主張信任理論的美國學者認為能夠透過今日在美國聯邦交易委員會累積的有關個人資料蒐集使用者、數位服務提供者之爭議事件，逐步建立一般性的規範內容。並且資料受託人濫用當事人之信任的行為，構成聯邦交易委員會法第 5 條之不正行為。

資訊受託人的義務可分成二個類型：控制個人資料揭露條件的酌情揭露、誠實告知、保護資料安全義務，以及決定個人資料使用方式的忠實義務。第一類型中，酌情揭露義務是對資訊受託人將資料向外傳輸、再揭露之行為有所節制，確保資料是在符合資料託管關係當事人的期待下分享揭露；誠實告知義務則要求資訊受託人向資料主體、公眾告知其是否值得信任，如告知隱私條款、過去發生的隱私侵害爭議等；保護資料安全義務是加強資料安全保護措施，資料匿名性、特種資料的特別保護措施亦屬之。而決定資料使用方式的第二類型忠實義務，要求資訊受託人不能夠為自己利益而傷害授信、脆弱的資料主體，成為數位企業對使用者提供服務應遵守的行為準則，在有爭議時也應對此提出說理，以此節制資訊受託人之行為。

間隙理論主張的資訊隱私權保障方式，是在個人資料自主控制之外，另外在物質環境之運作上設置個人資料保護機制。二者共同確保個人與他者進行互動時，有邊界管理之呼吸空間存在。個人資料保護機制擴及所有會影響隱私之數位服務、工具的設計與配置決策。內容上包含語義不連續原則與運作可課責原則。

第二項 本文主張：以隱私間隙理論作為機器學習時代資訊隱私權典範

如本節開頭所述，本文採取隱私間隙理論作為機器學習時代的資訊隱私權典

doi:10.6342/NTU202500550

範。理由為（一）間隙理論體系較為完整；（二）直接調整物質環境之設計與佈局來資料隱私權保障之機制，更有效地解決自主控制典範無力解決的問題；（三）信任理論本身存在的問題。

首先，Julie Cohen 的隱私間隙理論從隱私權的理論面到具體規範的實踐面整體性的檢討與重構，清晰地說明隱私的概念、隱私與主體性發展和自主的關係、在基本權利層次建構隱私保障的權利體系。

間隙理論完整的體系有助於釐清本文在研究目的引用我國學者之研究而指出的三項問題：在理論層次回答資訊隱私與人格發展內在面向的關係、實踐層次捕捉個人資料外溢性問題，以及資訊隱私權與其他權利的關係。

有關資訊隱私與人格發展內在面向的關係，人格、主體性的自由發展必須確保主體有能夠重新定義自己與他人、進行批判性思考、形塑異見、擬定反動策略的私人領域存在，隱私間隙理論認為，前述私人領域之存在以主體保有隱私間隙為前提，即私人領域與社會結構之間存在的動態間隙，使主體能夠設定與他人的邊界、區隔出私人領域。隱私間隙的作用是防止社會的其他成員、社會結構過度侵犯主體設定的邊界，以及剝奪主體設定邊界的能力。若主體的隱私間隙被過度壓制而不復存，主體無法對抗社會結構的形塑，被框限在他人賦加的框架或模版活動，失去能動性與日常生活之偶然性。

而個人資料的外溢性係指個人資料透過橫向與縱向之串聯、聚合，以資料分析、相似性之比對，模擬出個人與群體的人格圖像，該人格圖像被用以建構對該個人與群體的其他個人之認識，因此，單一個人資料透過與其他資料之聚合、分析、比對，會產生更多的資訊。在間隙理論之下，個人資料的外溢性破壞個人設定邊界的能力，個人被套以他人製作的人格圖像來認識與理解。

間隙理論認為隱私權具有符擔性，並從著重個人自由之論述取徑、個人權能之論述取徑、符擔性取徑，分別建立不同的隱私保障取徑，在基本權利層次化為

doi:10.6342/NTU202500550

不同的權利。此外，確定隱私與人格發展、主體性維護的關係之後，亦較能夠區辨與其他權利之界線。

第二個採取隱私間隙理論的理由為直接調整物質環境之設計與佈局來資料隱私權保障之機制，更能夠有效解決自主控制典範無力處理的問題。

信任理論保障隱私的方式為提升既有自主控制典範下的公正資訊行為原則之保障強度，以及設置要求資料受託人以託管人之最佳利益為決策依歸的忠實義務。然而即便資料蒐用者依循加強的公正資訊行為原則，取得資料主體知情之同意、確保資料安全與即時性、限制資料揭露的程度與範圍，終究無法處理資料蒐用者對主體進行不當的人格剖繪與治理問題。而忠實義務所採之主體最佳利益原則，在主體與資料蒐用者知識與權力落差仍存在的情況下，是否符合主體最佳利益之論述，仍由蒐用者掌握；此外，因資料的潛能強大，公私部門依然能夠以不同的正當目的取用個人資料。

如 Cohen 所述，隱私不只是一項中性的社會結構，我們選擇的隱私概念代表著當代社會珍視的個人主體性與民主發展之價值[303]。個人與社會的穩定性與可預測性有其利益，如拘束人民內心的道德倫理、具強制力之法律規範、監視器等輔助規則實踐的技術工具，皆具有穩定社會的力量，人民因而得以預期他人行為與自己行為的後果，進而安排生活；社會亦因此依循一定規則穩定發展。然個人的發展與民主進展不可完全被凝結、被預測掌握，從而個別社會下的隱私權，代表對穩定與變動之間的調控，係具有規範性的，表示該社會留予個人與社會自由發展的空間[304]。因此，在間隙理論下隱私間隙之保有應直接成為物質環境的設計佈局的原則，在社會運作中自動地實踐。

另外，Cohen 對信任理論提出二項質疑。第一項質疑是針對資訊受託人的忠實義務——為主體最佳利益執行業務——之實踐可能性。Cohen 認為，對於數位

[303] *See* COHEN, *supra* note 241, at 149.
[304] See *id.* at 149.

doi:10.6342/NTU202500550

企業而言，特別是具有控制數位資訊環境能力之科技巨頭，其經營的方針是為企業本身、股東獲取商業利益，數位企業能否在產品競爭激烈的狀況下，堅忍不拔地謹記資料主體利益、犧牲商業利益，設計數位產品、制定經營策略，實在難以期待[305]。第二項質疑則是針對「可信任」的資訊常規之建構可能性，根據 Cohen 的說明，數位服務提供者依其提供之數位服務本質而應守之所謂資訊常規，實是某種商品安全規範。然而，商品安全規範的法理與數位服務的本質並不相合，商品安全規範係針對大眾市場商品——為大眾提供相同內容與品質之商品——而設，商品的內容與品質穩定、商品之間的區隔明顯，例如椅子、電鍋；而數位服務會根據使用者差異而提供不同、持續變動的服務內容，數位服務相較於傳統實體商品，本身的變動幅度顯著。如上所述，數位服務與傳統實體商品特性有相當的差異，在變動性大的數位服務脈絡下，是否能夠依個別數位服務的建構穩固的資訊常規，殊值可疑[306]。

[305] *See* Cohen, *supra* note 179.
[306] *See id.*

doi:10.6342/NTU202500550

第四章 機器學習時代的資訊隱私權之概念重構與保護機制

回到本文的研究議題：機器學習時代的資訊隱私權概念重構以及保護機制。本文在第三章整理、分析比較新興理論之後，選擇採取 Julie Cohen 的隱私間隙理論為重新建構資訊隱私權之典範理論。

相較於自主控制典範，間隙理論重新梳理了隱私的概念，並且以語義不連續原則與運作可課責原則擴張了資訊隱私權的保障領域，復以不同的論述取徑，建立資訊隱私權在基本權利保障層次的體系。

以下於第一節重新建構資訊隱私權，並於第二節說明機器學習係如何構成資訊隱私權的干預，以及干預的正當化條件作為保障機制。

第一節　資訊隱私權之重構

採隱私間隙典範的資訊隱私權在資訊隱私的概念、資訊隱私權保障體系、保障領域三個層次與自主控制理論不同。

在隱私間隙理論下，資訊隱私是主體保有管理與他人資訊邊界能力之空隙，資訊隱私權保障的不只是主體控管其資訊、阻絕或開放他人透過資訊認識主體的決定，而包含主體做出決定、設定資訊邊界的能力。資訊隱私權保障主體有做出資訊邊界管理之能力的空間存在。

肯認基本權利符擔性後，展開有別於自主控制典範的資訊隱私權利保障體系。有從自由為出發點之論述取徑、從主體的權能出發之論述取徑，以及著眼於物質環境的佈局與設計的符擔性取徑。三者共同保障主體的資訊隱私利益。

而從符擔性論述，資訊隱私權之保障要求物質環境的設計與佈局須符合二項原則。語義不連續原則切斷無縫的資訊串聯與流動，限制個人資料跨脈絡的流動，並依脈絡設計資料蒐用規則。運作可課責原則旨在提升資料主體在資訊環境的能

doi:10.6342/NTU202500550

動性，為資料主體與資料蒐用者之間建立課責關係，使資料主體具備課責能力，要求資料蒐用者為其行為所產生的結果負起責任，資訊環境運作的透明性化是基本的要求，公私部門的監控活動運作邏輯、資訊的接近使用規則、網絡運作的政策與通訊協定等資訊應開放予資料主體近用。

第一項 重新定義隱私與資訊隱私

在間隙理論之下，隱私為「社會主體與他人之間存在的呼吸間隙，使社會主體能夠參與邊界管理的過程」。依社會主體理論，主體置身於社會之中，不可避免地會與其他個人、組織、環境、制度等外在事物往來互動。這些外在事物具有社會形塑力，意即透過與主體的互動，去影響並形塑主體之思想和行為。而自我，是在區辨自己與他人的過程中逐漸形成，認識自我與他人的方式受到語言與文化影響。自我、主體性之發展，是在個人與外界互動、自我表述，以及遁回私人領域內反思、定義與重新定義自己與他人，此二過程之間來回往返而發生的，自我與主體性因此浮現。隱私便是讓主體得以往返於向外自我表述、回歸私領域定義與區辨人我之空間。

而間隙理論並未特意區別出資訊隱私作為獨立的概念或是隱私類型。本文認為可從「邊界管理」與隱私的功能試圖說明何謂資訊隱私。

間隙理論認為隱私間隙是浮動的，與主體與外在人事物的邊界管理活動有涉。此一浮動的隱私間隙概念來自於社會學者 Irvin Altman 的隱私觀點。Altman 認為不論在哪個文化之下，隱私是「動態性辯證」、「追求最佳化」、「多重機制」之主體設定與他人邊界的過程[307]。隱私有使主體能夠管理社會互動、建立與外在人事物互動的計畫與策略、發展並維持自我認同之三項功能[308]。而隱私規則會依個案所涉文化，而有不同的行為與心理上的機制來維持[309]。主體設定與他人邊界之機

[307] *See* Irwin Altman, *Privacy Regulation: Culturally Universal or Culturally Specific?*, 33 J. SOC. ISSUES 66, 67 (1977).
[308] *See id.* at 68.
[309] *See id.* at 68-69.

doi:10.6342/NTU202500550

制可能是透過語言文字（verbal）之表達或是行為暗示等（非語言文字，non-verbal），例如某甲以辦公室的門「關閉」、「打開」、「半開」之狀態，使其他社會成員知悉其與甲的互動界線[310]。

由此可知，主體透過此一設定與外在事物邊界的機制，決定與外在人事物的關係、互動程度，以及外在人事物對己之認識，區隔出私人領域。主體設定邊界的方式可以是身體上的、空間上的、資訊上的[311]。主體以身體邊界、空間邊界、資訊邊界之管理，在其置身的社會中區隔出私人領域，主體在私人領域中得以不受拘束地思辯、行動，定義自我與他人，建立對自己與對外在人事物之認識。而間隙理論下的隱私權，即是確保個人有動態性地維持邊界管理的能力，個人因此能夠去從事設定與他人之邊界的過程。

從前述內容可知，**資訊隱私應是主體能夠設定與外在人事物的資訊邊界之間隙，資訊隱私權保障個人有此間隙存在，確保個人保有動態性地設定與外在人事物的資訊邊界的能力。**

因此，在此資訊隱私概念之下，穿透主體設定與他人之資訊邊界，以及破壞主體以資訊性的策略控管他人對己之認識與互動關係之過程，屬於資訊隱私之侵犯。例如強迫揭露個人不願揭露之資訊，以及破壞合理隱私期待之個人資訊蒐集與串聯，如在未得個人同意下以跟追或錄影方式持續記錄個人在公共場所之活動，或者是使用具高度識別性之個人資料去串聯其他資料而拼湊個人圖像等。

除前述行為之外，間隙理論之資訊隱私的特別之處在於，隱私不是個人所設定的邊界，而是個人有動態性地維持設定邊界之能力的間隙、空間。在此理解下，破壞個人設定之邊界，係不尊重、違悖個人基於設定邊界之能力做成的決定，自屬隱私侵犯。然而更為幽微的隱私侵犯行為是直接剝奪個人設定邊界能力，諸如 1984 老大哥式之無所不在的監控、不同意即無法使用服務之取得使用者同意手法、

[310] *See id.* at 69-70.
[311] *See* Cohen, *supra* note 241, at 1908.

doi:10.6342/NTU202500550

以預決的細緻模板描繪主體之行為等。

第二項 資訊隱私權的不同保障取徑：以自由為出發點、以權能為出發點、符擔性取徑

間隙理論採取擴張的基本權利理論，認為基本權利的功能包含要求物質環境的佈局與設計應有助於權利之實踐，即基本權利符擔性理論。理由是物體的形狀、設計，或是物理世界的運行規則對主體的行為有規制（regulate）的作用，某些行為被激發、某些行為則被限制。而人造的物質環境之佈局、設計與運行邏輯實際上反映著社會結構背後的權力關係，不當的物質環境設計與佈局可能成為掌握高權者形塑、規訓主體的手段。基本權利符擔性理論認為透過物質環境之調整，確保個人基本權利的實踐、為主體賦能，進而平衡主體與掌控政治經濟高權者之間的權力關係。

採取基本權利符擔性理論之下，展開了新興的基本權利保障取徑，除了既有的以自由為出發點（自由取徑）、以主體權能為出發點（權能取徑）以外，發展出關注物質環境之設計與佈局的符擔性論述取徑（符擔性取徑）。分從不同的出發點論述，導引出不同的基本權利保障機制。

在資訊隱私的脈絡下，以自由為出發點論述出的資訊隱私保障機制在意的是，主體能夠自由、自主地設定自己與外在人事物的資訊邊界，以及有決定自己是如何被認識的自由，例如同意或拒絕他人取得個人資訊。如 Cohen 所言，以告知同意為核心的自主控制典範資訊隱私權，便是從此取徑論述出的資訊隱私保障[312]。

以主體權能出發的資訊隱私保障取徑，關懷主體保有設定資訊邊界能力之空間的基礎權能與物質資源。例如對資料蒐用之條件的知情權、資料錯誤之更正權、刪除權、資料外洩受通知權、拒絕自動化決策權等。

[312] *See* Cohen, *supra* note 18, at 20.

doi:10.6342/NTU202500550

而從符擔性取徑論述出的資訊隱私保障，係針對整體資訊環境的物質性條件的佈局與設計而言，必須確保個人在其生存的物質環境中能夠去管理與他人的資訊邊界，物質環境之設計與佈局須有滿足上述要求的限制（disabling）與賦能（enabling）要素。

符擔性取徑與自由取徑的關係是：二者皆係保障個人的隱私利益，符擔性取徑能夠透過對物質環境之要求輔助自由取徑保障機制之實踐。然而，若主體自願放棄資訊隱私間隙、同意資料蒐用者對其監控或自願受規訓，發生符擔性取徑與自由取徑之衝突。在此情形，由於資訊隱私間隙之保障係寫入、改變資訊環境的設計佈局，符擔性取徑原則上不受影響；另外，在資訊隱私概念已重構之下，資訊隱私權保障的不只是主體設定與他人資訊邊界之自由、自主決定，仍須確保主體保有能夠設定資訊邊界之空間存在。因此，主體自願放棄隱私間隙並不受到資訊隱私權之保障。

而符擔性取徑與權能取徑二者亦同樣地保障個人的資訊隱私利益，符擔性取徑也輔助權能取徑的實踐。然而二者實踐保障的方式不同，權能取徑在意是否設有保障資訊隱私的主體權能、各個主體是否皆具備行使權能的資源與能力。

如 Cohen 所述，透過此一擴張的基本權利理論，正能在概念上釐清資訊隱私權、個人資料自主控制權、個人資料保護權之關係，建構出較為完整、清晰的資訊隱私權利體系。Cohen 將資訊隱私權作為上位的概念，認為歐盟基本權利憲章第 7 條「隱私權」是從自由面向取徑所論述出的資訊隱私權保障，而第 8 條「個人資料保護權」從個人資料蒐集、處理、使用與保存之條件限制來保護個人資訊隱私，是從符擔性面向論述的資訊隱私權保障取徑[313]。

延續前述討論，Cohen 進一步表示，個人資料保護權並不會被資訊隱私權完全涵蓋。理由是個人資料保護權所保障的利益不限於個人的資訊隱私，另外會包

[313] *See* Cohen, *supra* note 18, at 20.

doi:10.6342/NTU202500550

含思想自由、集會自由、宗教自由等[314]。由此可知，若以歐盟基本權利憲章第 7 條與第 8 條為例來與隱私間隙理論對照，隱私間隙理論之資訊隱私權包含了個人資料自主控制之資訊隱私權，此為從自由面向之論述取徑，亦包含了個人資料保護權，此為從符擔性面向的論述取徑。惟如個人資料保護權之符擔性面向的資訊隱私權，透過個人資料之蒐用保護、資訊環境之設計限制，可能會保護到個人的其他自由與權利。

資訊隱私權的符擔性取徑是間隙理論在隱私概念之外，另一項與既有典範不同的關鍵。如前所述，符擔性取徑係要求資訊環境的設計佈局應保障主體的隱私，因此 Cohen 提出了資訊環境設計、佈局應守的二項原則，建構從符擔性取徑論述的資訊隱私權保障領域，即語義不連續原則與運作可課責原則。

第三項 資訊隱私權保障領域：語義不連續原則、運作可課責原則

如第一項所述，資訊隱私是主體能夠設定與外在人事物資訊邊界之間隙，主體透過限制與開放資訊性邊界，決定外在人事物對己之認識，與之互動、建立關係。資訊隱私權保障個人有此間隙存在，確保個人保有動態性地設定與外在人事物的資訊邊界的能力。

間隙理論認為在現代的資訊環境與規範結構之下，資訊隱私權之實踐有二個要件：語義不連續原則與運作可課責原則，構成資訊隱私權之保障領域。

語義不連續原則旨在對抗無縫隙與詳盡的資訊蒐集使用活動。實踐此原則的方式是在定義資訊法律關係、建構蒐集使用資訊之協定的制度性與技術性框架之中，設計具有複雜性的裂隙。而此複雜的裂隙應滿佈於社會主體的日常生活層裡，使主體在日常生活中，能保有不確定性、保有發生隨機與偶然事件的可能[315]。

該原則的目標是破壞蒐集個人資料所建立出的語義網。今日建構語義網的資

[314] *See id*. at 22-23.
[315] *See* COHEN, *supra* note 241, at 239.

doi:10.6342/NTU202500550

料來自於不同時期、不同脈絡下蒐集的資料，並以人口剖繪技術所推論或預測之資料填補有缺漏之處。以過時、去脈絡、猜測而出的資料所拼湊出的個人資料語義網，實際上與真實存在的個人相去甚遠。因此，在語義不連續原則之要求下，資料的蒐集與使用脈絡之間需設有縫隙，將資料留予原脈絡中[316]。

語義不連續原則切斷個人語義網，將資料封鎖於原脈絡中，因此可切分出不同的個人資料蒐集使用情境，設置不同的資料蒐用規範，分別建立資料治理架構。Cohen 指出，在個別的資料蒐用情境，可依該情境之需求，決定個人化決策的精準程度，且依決策的精準程度設計資料蒐用的正當條件[317]。

舉例來說，在個人與一般的數位服務提供者之間，可認雙方成立資訊託管關係而設置一般性的資料受託人義務，作為基本的個人資料保護規範。而蒐用個人資料之利益較高，例如基於嚴重流行病防治、為資料主體身心健康之治療的資料蒐用情境，容許更高程度的個人化決策，然而亦須設有更高強度的資安要求、資料過期之刪除規定等。在以學術研究、社會福利等目的蒐集使用資料的情境，識別個人的需求低、跨脈絡的資料整合可能性高，因此應有更高的去識別化要求，或是在資料集內加入雜訊。在社群網絡平台，由於社群平台是使用者用來與他人互動的場域，平台不須為使用者設定資訊邊界，然可設特殊之個人資料傳遞限制，如禁止跨服務之資料傳輸，或是基於行銷目的販賣之資料需特殊的去識別化處理等。另外，在實體空間之資料蒐集，如監視器之設置，亦須符合語義不連續原則，例如限制監視器之密度、限制資料跨脈絡傳輸、要求線下傳輸、主體知悉監視器之存在等[318]。

資訊隱私權的第二個構成要件是運作可課責原則，其旨在提升資料主體在資訊環境的能動性。在自主控制典範下，資料主體影響資料蒐用者決策的方式是行

[316] *See id.* at 249-50.
[317] *See id.* at 253.
[318] *See id.* at 252-55.

doi:10.6342/NTU202500550

使知情後同意權。資訊與專業能力顯弱於蒐用者的主體，在資料蒐用者設計好的情境、基於其所提供之資訊與蒐用者磋商，若僅有知情同意原則，主體在資訊環境的能動性薄弱。Cohen 支持加拿大法律學者 Lisa Austin 的見解，Austin 認為現代個人生存之社會，其結構性基礎關係並不是雙方當事人磋商、同意的契約關係，而是基於權力關係所建構的。因此，Cohen 給出的解方是「課責關係」。在課責關係中，資訊環境的運作過程參與者／經營決策者必須對於其所造成的結果負起責任，而受到資訊環境運作、設計決策所影響的主體，應有課責的能力。此一課責關係之法理是源自於資訊社會成員之間的相互尊重[319]。

建立課責關係的前提是資訊環境運作的透明。資訊社會下的主體之生活深受數位技術的操作者、設計者、相關企業的經營者之決策影響，而如人類與自然環境、宇宙萬物之關係，由於人們的生活與這些環境事物密不可分、受其牽動，從而我們致力於洞悉其運作法則。主體與資訊環境之關係亦如是，主體應知悉、洞悉資訊環境運作的實際情況與規則[320]。

為了確保主體在資訊環境中的課責能力，數位技術與服務的提供者、操作者、設計者、相關企業的經營者等，須提供三種類型資訊。第一種類型是公私部門監控活動的運作邏輯與實際情況，特別是人口剖繪的分類與排序資訊。除了資料的使用目的、其他資料處理者、資料的正確性外，個人資料被蒐用情境的運作邏輯、特定資料在該情境發生作用的方式、提供其他資料如何對結果產生影響、分類與排序使用者的邏輯等。第二類資訊是關於網際網絡的資訊可近性的資訊。現代，私人企業是資訊近用服務的主要提供者，平台與演算法支配著數位網絡空間的資訊可近性，搜尋引擎或社群平台應使其篩選、排序資訊的邏輯透明，然為保護私人企業的營業秘密，可由專家或獨立監管機關查核，不須對外公開相關資訊。第三種是網絡運作政策、協定的透明開放，數位網絡的運作政策與通訊協定

[319] *See* Cohen, *supra* note 18, at 22.
[320] *See* COHEN, *supra* note 131, at 234-35.

doi:10.6342/NTU202500550

對資訊社會主體的影響力大，該政策與協定之制定，應開放主體參與的可能性[321]。

第二節 機器學習之資訊隱私權保障機制

除了資訊隱私權概念之重構之外，本文的另一項研究主題為機器學習的資訊隱私權保障機制。機器學習是現代關鍵的數位資訊技術，改變資訊的蒐集使用方式，對個人的資訊隱私造成影響。本節首先於第一項說明機器學習的運作原理與應用。第二項為機器學習如何構成資訊隱私權之干預。最後是資訊隱私權應有之保障機制。

第一項 機器學習

在數位資料是資訊的主要型態之現代社會，個人使用數位化資訊工具與其他個人、政府單位、私人企業互動間，持續產生數位資料。機器學習即是現代使用電腦等機器處理數位資料的關鍵技術工具。

在本質上，機器學習是一種演算法，演算法是「一連串、有次序的指示操作（instruction），將資料輸入後執行演算法而得到輸出結果[322]」。機器學習演算法具有兩項特色：機器執行、藉由資料學習。過去，演算法是人類寫出、再以人力或使用計算機、電腦等工具執行。然，人腦計算與儲存資訊的能力與效率有限，因此人類藉助電腦等機器之力，處理更多的資訊、執行更複雜的運算、解決更困難的問題。而學習的方式上，人類是累積經驗、歸納出理解事物的規則，而機器學習的方式，除了人類調整修正以外，因電腦的儲存與計算能力、資料化技術越加強大，現代的機器學習技術最關鍵的一項變化毋寧是能夠在巨量的資料當中探索出人類知識範圍外的規則、演算法模型，即資料探勘（data mining）。透過資料探勘建構演算法模型，並且再以持續餵入新的資料而調整、修正該模型，達到類似

[321] *See id.* at 235-38.
[322] *See* ALPAYDIN, *supra* note 2, at 2.

doi:10.6342/NTU202500550

於人類學習的效果[323]。

機器學習是以統計原理，在大量的資料當中，找出資訊之間的關聯性、為資訊分類與排序，可以用於描述現狀，或是推測未來。例如購物網站分析過去消費者購物資料，發掘啤酒與尿布時常同時出現在同次的購物清單中，因此對將啤酒加入購物車的消費者投放尿布廣告。另一種機器學習的應用是模版辨識（pattern recognition），模版辨識是以資料之間的相似性進行分類與排序，為資料集內的資料分類並製作模版，例如信用評等系統、臉部辨識、語音辨識、光學字元辨識、醫學診斷系統等[324]。

機器學習廣泛地被公私部門使用，例如警察單位使用臉部辨識系統[325]、採用精準醫療系統之社會福利措施、雇主在勞動場域採用員工評鑑系統、醫療機器人等。機器學習不只輔助決策者做成決定，也會直接與使用者互動、再蒐集使用者資料繼續修正互動方式。

舉例說明，自閉症兒童之照護機器人是協助患有自閉症之兒童練習人際互動的數位工具，在此情境使用機器人的好處是能夠重複同樣的人際互動模式，並避免人類照護者的情緒波動刺激自閉症兒童的不良反應。該照護機器人根據過去診療自閉症兒童所取得之資料，如兒童的家庭背景、在校表現、生理狀態、醫療紀錄等，加上專業醫療人員之知識，建構基本的互動模型。機器人與自閉症兒童進行互動時，將持續蒐集兒童反應資料，如肢體、眼神、口語的反應，給予不同的互動行為回饋，同時持續修正互動模型[326]。

再舉一例說明，美國在 2015 年由歐巴馬政府提出的精準醫療倡議（Precision Medicine Initiative）計畫，試圖建立更為精準、經濟的健康保險服務，依人群的

[323] *See id.* at 1-3.
[324] *See id.* at 3-9.
[325] 參見 Frank Pasquale（著），李姿儀（譯）（2023），《二十一世紀機器人新律：如何打造有 AI 參與的理想社會？》，頁 195，左岸文化。
[326] *See* Eduardo Castelló Ferrer et al., *RoboChain: A Secure Data-Sharing Framework for Human-Robot Interaction*, (2018), https://arxiv.org/abs/1802.04480 (last visited Jan 7, 2025).

doi:10.6342/NTU202500550

背景、生活狀況、基因資料等，提供不同的健康保險。判斷健保內容的方式是以一百萬名自願參與計畫者的過去的醫療紀錄、參與計畫期間的就醫紀錄與行為評估、基因樣本、日常生活紀錄等資料，建置資料庫並建構模型[327]。

第二項 機器學習對資訊隱私權之干預

回顧 Cohen 提出的數位資訊網絡社會下的隱私干預活動：資訊性的標準化監控、空間性的暴露、主體協助監控與自我監控、調節式監控。以巨量資料為基礎之機器學習在上述隱私干預活動中發揮作用，或是加強干預的強度。機器學習建構與修正演算法的基礎是大量的資料，因此加速了資料化的現實、強化既有之監控，同時帶來新的資訊隱私干預類型：機器學習的怪異。

資訊性的標準化監控是以蒐集個人資訊，依循特定規則將個人特徵化、分類、排序並給予評鑑，依評鑑結果對個人、群體進行治理，達成規訓目的之監控活動。將機器學習的模版辨識應用在分析、辨識特定人口群體之特徵，依特徵製作人口模版的人口特徵剖繪，並依人口群體給予不同的評鑑結果，是數位社會的標準化監控的基礎操作。對於個人的資訊隱私而言，個人資料之蒐集直接涉及主體對資訊邊界管理的決定；再者，以預先製作的人口模版套加於主體之上，以模版中的特徵填補對主體的認知、作為認識主體的依據，減損主體控制資訊邊界的能力。

空間性的暴露是監控者在實體與虛擬的空間設計監控系統、建立空間使用規範，讓受監控者在空間中感到暴露，產生心理上的不安全感，而自動地依循監控者的規則行動。如前所述，機器學習技術被公私部門廣泛地使用，個人在數位與實體空間的活動持續被資料化、資料化的精細度更高，這些資料可能被抽離脈絡、歸入個人的數位檔案，成為其他社會成員認識的基礎。例如雇主在網路「肉搜」求職者的公開資料、形成粗略的印象，對於具有某些喜好或特徵之求職者給予負

[327] *See* ALEX PENTLAND, ALEXANDER LIPTON, & THOMAS HARDJONO, BUILDING THE NEW ECONOMY: DATA AS CAPITAL 162-65 (2021).

doi:10.6342/NTU202500550

面評價，人們可能因此改變其在網路空間的行為、形塑良好形象[328]。個人的資料被蒐集、抽離脈絡使用、無法決定可近用者等，影響人們的資訊隱私。

再，藉由機器學習技術提供精緻、貼近個人喜好與需求的個人化服務，馴化主體、使之無法抗拒地交出個人資料、過度投入數位服務之使用甚至成癮，並且自願依從被套加的人口模版活動，屬於數位社會的調節式監控、主體自我與協助監控的模式，干預主體的資訊隱私權。上述個人化服務包含搜尋引擎、社群平台內容推播、購物平台推薦、數位廣告推播等，能夠透過使用者背景資料、互動回饋資料，即時修正提供的服務貼近使用者的需求與偏好，增加使用者的黏著度。而在主體自我與協助監控部分，除前述個人可能追求取得更好的社會評價，修正改變在數位空間的行為之外，美國社會學者 Shoshana Zuboff 指出青少年使用社群平台服務時，為了取得同儕或群眾的認同，改變自己的生活、身材、行為而符合能夠在社群平台上取得「讚」的樣子。此外，Zuboff 提到已有研究認為社群平台業者為了增加使用者的黏著度，以吃角子老虎機的設計機制為原型，誘使個人無意識地持續使用社群平台，難以抽身而幾近成癮[329]。

另一項專屬機器學習技術造成的資訊隱私權干預是「機器學習的怪異」。機器人、機器學習創造了某種理論上不存在但實際上卻存在的怪異事物（creepiness），其以人性、類似人類的外觀或設計，來掩蓋實為雜亂、人類難以理解的邏輯與算式之本質，破壞了「人」與「非人」之分野。自我的生長是一社會的、持續辯證的過程，主體會從與其他人事物的互動所得到的回饋、從他人的視角來感知自我、建構自我認知。而人類與機器、自動化邏輯互動，必須消化機器的怪異、人力無法理解或想像的邏輯、「觀點」，干擾自我形構的過程。機器的理性並不等於人性。主體形塑、認識自我與他人的方式之一，是想像自己是如何被他人理解的，而決定互動。因此，對主體而言，無法知悉其與無法理解的機器

[328] *See* PASQUALE, *supra* note 158, at 20.
[329] 參見 Shoshana Zuboff（著），溫澤元等（譯）（2020），《監控資本主義時代（下卷）：機器控制力量》，頁 720-754，時報。

doi:10.6342/NTU202500550

邏輯互動之下，會被如何理解，進而無法決定互動方式、設定資訊邊界[330]。

第三項 符擔性取徑之機器學習的資訊隱私權保障機制

隱私間隙理論主張，確保個人在資訊社會中能夠維持足夠的隱私間隙之條件。資訊隱私權保障個人以語義不連續對抗無縫的個人資料蒐集使用，以及有參與決定資訊社會運作的結構與規則之過程、數位資訊網絡社會應有運作結果究責之機制，是為資訊隱私權之權利內容：語義不連續原則與運作可課責原則之保障。因此就上述機器學習運作所構成之資訊隱私權干預結果，政府應積極設置符合資訊隱私權保障之機器學習相關規範制度。以下詳述之。

重申語義不連續原則與運作可課責原則之內涵。Cohen 表示，語義不連續原則是為了阻礙對主體與社會之無縫隙的讀取和操弄，採取干擾、中斷或抽回資訊流的策略，其正當性在於自我之不可計算性，以及反對越精準越好迷思之公正的聚合。而運作可課責原則係將資料蒐用行為與活動之品質與性質加入資訊隱私規範的焦點，並且讓個別使用者與社群有參與決定自己如何被解讀的決策過程[331]。

從本節第二項內容可知，機器學習是結合整體數位資訊網絡社會技術系統而為運作的，從而 Cohen 主張，機器學習相關規範之客體是對於隱私有影響力之資訊環境整體的設計決策者，包含構成與運行社會技術系統之公私部門監控集團，如軟體系統供應商、硬體設施營運商、建構與運作網絡數位環境之各參與者，以及資料經濟所依從之商業模型決策者等[332]。

Cohen 整理學者們對相關問題的解方，提出四個層次的設計資訊隱私保護機制之建議：一般性機制、數位服務提供者之組織程序規範、外部監督機制，以及建立在意資訊隱私的職業倫理與社會文化之方法。

---

[330] *See* Cohen, *supra* note 18, at 13-14.
[331] *See id*. at 24-25.
[332] *See id.* at 25.

doi:10.6342/NTU202500550

第一款 一般性隱私保護機制

在一般性資訊隱私保護機制上，Cohen 原則上支持多數學者主張的差分隱私（differential privacy），然而 Cohen 不滿足於此，而主張應有強制性的干擾資訊流之設計，以及數位服務與產品應有強制中斷使用的機制存在。所謂差分隱私是指根據資料蒐集使用之目的而決定蒐集的精緻程度，適時地增加資料集的雜訊，限制識別性，例如以流行病之防治與藥品的分配為目的之蒐用價值會高於為行銷目的之蒐用，前者可容許更精細的資料蒐集分析。惟 Cohen 認為個人資料之蒐用目的五花八門、個個可與正當公益連結，亦難知悉多精細才符合目的[333]。

Cohen 表示，除差分隱私之外，資訊系統與產品的設計應設有強制的限制資訊流與中斷服務使用作為一般性的隱私保護機制。限制資訊流之設計係指原則上禁止跨裝置、跨平台、跨部門、跨業者或跨脈絡之資料流通，且此禁止流通是寫入系統或產品的運作規則中的。此外，數位產品與服務在使用時，應設置中斷使用之機制，中斷或轉向使用者過度投注之注意力，以及緩和使用者與自動化工具背後之非人性邏輯互動的密度。另外，對於將主體套入資訊框架或模板之操作，Cohen 提出代碼混淆（obfuscation）的解方，在差分隱私框架下，根據個別情境的資料蒐集使用目的，限制資料集中個人資訊的使用可能性，調整精準決策的精準程度[334]。

第二款 內部組織程序與外部監管機制

在構成資訊環境之系統與服務提供者的內部組織程序規範部分，Cohen 整理幾項學者提出的規範建議。首先是要求企業將隱私監理納入公司的風險管理一環。再者是在設計產品與服務時，限制跨脈絡之資料流通，例如跨裝置、跨產品或服務、跨部門等。最後是將隱私保護內化為設計產品與服務、內部經營、人員訓練

[333] *See id.* at 28.
[334] *See id.*at 28-29.

doi:10.6342/NTU202500550

所依從的價值。

另外，就數位系統、服務或產品提供者之營運是否符合資訊隱私權保障的要求，Cohen 指出有內外部之監理機制存在。內部可設組織之審查委員會（Institutional Review Board），主要功能在於協助組織做出符合資訊隱私規範要求之決策，成為組織之諮詢單位，參與產品與服務之設計流程，並審核組織之決策是否符合隱私保障要求。然非所有服務提供者皆有資力設置內部監管機制，Cohen 建議可建立外部隱私專家組織為中小企業、新創事業等無力自營內部機制之數位產品服務提供者提供資訊隱私法遵服務[335]。

第三款 建立在意資訊隱私之職業倫理與社會文化

Cohen 亦對相關職業倫理與社會文化之形塑提出建議方案。在數位資訊技術專業領域層面，應擬定培育專業人才的教育原則，以及制訂相關的倫理守則與指引。此外，透過規範之制定與遵循，區隔並揭露不符合資訊隱私權保障要求之組織行為與活動，改變使用者對於「好的數位服務與產品」之判斷標準，喚醒個人與社群在意資訊隱私之意識，並接受為隱私保障而設的數位服務中斷與不效率等機制。逐步扭轉不利隱私保障之商業模式[336]。

[335] *See id.*at 25-27.
[336] *See id.* at 27-28.

doi:10.6342/NTU202500550

第五章 結論

現代機器學習的技術基礎是以數學、統計原理在巨量的資料探索不在人類所知範圍內的規則，建立演算法模型，協助人類處理資料與問題。人們在日常生活與數位服務與工具互動產生資料，資料在數位網路之間傳輸、聚集，公私部門蒐集大量的人類資料，以機器學習的關聯性分析、模版辨識操作，將蒐得的資料當作個人特徵描述個人，分類與排序資料、製作人口模版，建構替代現實世界的「真實」。

機器學習製作的人口模版所想像、模擬出的人格圖像成為公私部門認識個人、人口群體的基礎。該人格圖像被賦加的特徵資訊，被用來填補在原資料集內的個人未被取得的資訊；不在原資料集的個人，亦可能因具備特定與人格圖像相同的特徵，被歸屬在該人格圖像所描述人口群體之下，而被賦加特定人格圖像。

機器學習被應用於數位社會的監控活動。人口模版是剪除、忽略群體內個人差異，將多元、具有能動性的個人標準化為以抽象化、一般性描述人口特徵而製成的人口模版，是監控者依群體進行差別評價、治理的關鍵素材。機器學習技術能夠透過新取得的資料與被監控者的回饋，持續修正人口模版、調整與被監控者的互動方式、設計適宜於特定主體的規訓手段，以個別化治理與規訓達成集體監控的目標。數位監控者以上述機器學習技術為基礎，決定「優良」、「合規」、「不良」之人格圖像，依其在實體與數位空間的支配力設計空間的規矩、設置情蒐機制，使受監控者感知到其行為活動可能被蒐集為評價的素材，希望取得良好評價或懼怕受不利對待而自動地依從數位監控者設計的空間規矩。另外，仿人性的數位服務與工具成為數位監控者的凝視機制，使用者與之互動時，轉換至宣稱為人、實為機器之視角，猜想在機器邏輯下，自己是如何被觀看，以此建構自我認知與決定互動行為。而因數位服務是個人進入數位空間、與其他社會成員建立連結的入口，加上服務提供者以增加使用者的黏著度為目標來設計使用方式與機制，個

doi:10.6342/NTU202500550

人難以脫離數位監控。

面對前述機器學習之運作與應用，以個人資料自主控制理論為典範的資訊隱私權失去實踐可能性，亦無法保障個人的人格自由發展。在資料蒐用前之決策階段，資料主體與資料蒐用者之間存在知識與權力落差，資料主體無法理解複雜艱澀的資訊隱私保障政策、無法確認資料蒐用者的資訊隱私保障能力；單一資料縱向串聯主體的其他資料或橫向串聯其他個人資料後產生新資訊之個人資料外溢效果，使主體無從評估同意資料蒐用後的風險；另外，主體受限於資料蒐用者給定的決策框架，磋商成本高、不同意即無法使用數位服務，資料主體不具有蒐用決策之自主性。而因數位社會中個人與數位服務與工具的互動頻繁，大量的個人資料在無法確知身分、難以盡數的資料蒐用者之間傳遞、累積、分析使用，資料主體同意資料蒐集使用之後，無法追蹤資料的使用狀況，難以控制個人資料；此外，機器學習聚合、串聯資料建構演算法模型、製作人口模版，資料主體縱然要求資料蒐用者刪除、停止處理資料，亦無從消除資料已發生的外溢效果。

數位監控者在數位與實體空間部署情蒐活動與機器凝視工具等監控機制，促使主體追求成為能取得好評價的人格；此外，監控者依其製作的人口模版，將具有相同特徵的主體歸入模版，並對被歸屬於不同模版的主體提供個人化服務，使之凝著於模版中。此類監控操作皆取得主體之同意、係主體自願依從，自主控制典範之資訊隱私權無法捕捉到上述監控操作對人格發展造成的侵害。

立基於社會主體理論，Julie Cohen 提出隱私間隙理論重構隱私的概念。社會主體理論反駁古典自由主義設想的生而自主、理性的理想主體，認為主體性係主體在其置身的社會中與其他主體、物質環境、社會規範互動中而逐漸發展、浮現的。主體依循既有的社會結構安排生活、從事人際互動、認識自己與他人，主體性在此過程受社會結構之影響而形塑。然而，若容任社會結構恣意對主體施加形塑力，將使主體單一化、失去能動性，社會失去多元與活絡的動能而僵固，故須

doi:10.6342/NTU202500550

確保主體在社會結構下的能動性。

隱私，便是主體保有管理與他人邊界能力的動態空間／間隙，是確保主體能動性、主體性自由發展、培育自主理性的主體之要件。在隱私間隙中，主體能夠定義與重新定義自己與他人，反思與批判既有的社會規範，進而策動改變社會結構的行動，以此確保社會結構下主體的能動性與自主性。

主體透過身體、空間、資訊的邊界管理，決定自己被他人認識的方式與程度、與他人建立關係。資訊隱私是主體保有管理與他人資訊邊界的能力之隱私間隙，而資訊隱私權即是對個人資訊隱私之保障。

以確保主體保有對抗社會結構形塑力的空間為目標的資訊隱私權，發展出從物質環境之設計與佈局為出發點去論述基本權利保障之符擔性取徑。有別於從自由或主體權能為出發點之論述取徑，符擔性取徑要求主體置身的物質環境應具備足以確保基本權利之實踐的賦能或限制要素，以改變物質環境之設計佈局為主體賦能，進而調整社會結構背後的不對等權力關係。

機器學習時代的數位監控，係由數位監控者以資料傳輸流建構起廣泛的監控網絡，利用機器學習技術處理大量資料、製作人口模版，再對主體進行個別化治理。透過此一過程產生監控者與被監控者之間的知識與權力落差，個別被監控者無從以一己之力對抗數位監控者集團。

從而機器學習時代的資訊隱私權保障以語義不連續原則與運作可課責原則為要件。語義不連續原則旨在建立資料傳遞網絡之間的縫隙，阻斷監控者集團之間無縫隙的資料流。縫隙應存在於不同的數位監控者、監控者組織內的部門、數位服務之間。而個別數位服務之運作亦應設有中斷或暫緩機制，阻斷個人資料之蒐集以及主體過度投入的注意力，緩解主體過於頻繁地與機器邏輯互動而造成的主體性發展損害。

doi:10.6342/NTU202500550

運作可課責原則要求資料蒐集使用者為其行為產生的結果負起責任，轉換承擔資料蒐集使用風險發生之主體，透過個別的損害發生與課責關係，確保個人在資料蒐集使用關係中的能動性，而不只是告知與同意。而有效的課責以資料蒐用之透明性為前提，數位監控活動的運作實況與邏輯原則上應對個人與公眾透明，網絡通訊協定等政策之決策過程，亦應使個人、使用者社群能夠參與。

具體而言，從符擔性取徑論述的機器學習時代資訊隱私權保障，要求構成整體資訊環境之個別資料蒐用者依循語義不連續原則與運作可課責原則設計數位服務、擬定組織內隱私保障政策，並設置相關的監管機制，重塑數位社會之隱私保障文化。

doi:10.6342/NTU202500550

參考文獻

一、 中文文獻

Douglas E. Comer（著），鄭王駿等（譯）（2019），《電腦與網際網路國際版》，全華。

Frank Pasquale（著），李姿儀（譯）（2023），《二十一世紀機器人新律：如何打造有 AI 參與的理想社會？》，左岸文化。

Shoshana Zuboff（著），溫澤元等（譯）（2020），《監控資本主義時代（下卷）：機器控制力量》，時報。

王志弘（2015），〈拼裝都市論與都市政治經濟學之辯〉，《地理研究》，62 期，頁 109-122。

王德瀛（2020），〈簡評加州消費者隱私保護法－規範重點與其對美國隱私保護的影響〉，《科技法律透析》，32 卷 3 期，頁 19-27。

王澤鑑（2012），《人格權法：法釋義學、比較法、案例研究》，自版。

呂胤慶（2021），《公部門中的人工智慧—人為介入作為正當使用人工智慧的必要條件》，國立臺灣大學法律學研究所碩士論文。

李榮耕（2022），〈刑事程序中人工智慧於風險評估上的應用〉，《政大法學評論》，168 期，頁 117-186。

李震山（2011），〈論資訊自決權〉，氏著，《人性尊嚴與人權保障》，頁 709-756，元照。

林子儀（2015），〈公共隱私權〉，收於：國立臺灣大學法律學院（編），《馬漢寶講座論文彙編，第五屆》，頁 7-62，財團法人馬氏思上文教基金會。

doi:10.6342/NTU202500550

林建中（1999），《隱私權概念之再思考—關於概念範圍、定義及權利形成方法》，國立臺灣大學法律學研究所碩士論文。

邱文聰（2009），〈從資訊自決與資訊隱私的概念區分－評「電腦處理個人資料保護法修正草案」的結構性問題〉，《月旦法學雜誌》，168 期，頁 172-189。

--------（2018），〈人工智慧相關法律議題芻議〉，收於：劉靜怡（編），《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》，元照。

--------（2020），〈第二波人工智慧知識學習與生產對法學的挑戰——資訊、科技與社會研究及法學的對話〉，收於：李建良（編），《法律思維與制度的智慧轉型》，頁 135-166，元照。

陳起行（2000），〈資訊隱私權法理探討——以美國法為中心〉，《政大法學評論》，64 期，頁 297-341。

翁逸泓（2022），〈資料治理法制：歐盟模式之啟發〉，《東海大學法學研究》，64 期，頁 55-116。

孫森焱（2020），《民法債編總論上冊》，自版。

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。

--------（2018），〈隱私之合理期待標準於我國司法實務的操作—我的期待？你的合理？誰的隱私？〉，《法令月刊》，69 卷 2 期，頁 82-112。

--------（2022），〈美國加州消費者隱私保護法制之最新發展與比較法啟示〉，《當代法律》，6 期，頁 24-39。

黃銘輝（2009），〈法治行政、正當程序與媒體所有權管制－借鏡美國管制經驗析論 NCC 對「旺旺入主三中」案處分之合法性與正當性〉，《法學新論》，17 期，

doi:10.6342/NTU202500550

頁 105-149。

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。

劉定基（2009），〈欺罔與不公平資訊行為之規範—以美國聯邦交易委員會的管制案例為中心〉，《公平交易季刊》，17 卷 4 期，頁 57-91。

--------（2013），〈析論個人資料保護法上「當事人同意」的概念〉，《月旦法學雜誌》，218 期，頁 146-167。

--------（2017），〈大數據與物聯網時代的個人資料自主權〉，《憲政時代》，42 卷 3 期，頁 265-308。

--------（2023），〈資訊的保鮮期限？──論被遺忘權幾個待解的習題〉，《政大法學評論》，174 期，頁 217-263。

劉靜怡（2006），〈言論自由：第六講：言論自由、媒體類型規範與民主政治〉，《月旦法學教室》，42 期，頁 34-44。

鄭詠綺（2023），《論歐盟社群媒體平台精準投放之管制架構：以私生活權之保障為中心》，國立臺灣大學法律學研究所碩士論文。

蘇慧婕（2022），〈歐盟被遺忘權的內國保障：德國聯邦憲法法院第一、二次被遺忘權判決評析〉，《臺大法學論叢》，51 卷 1 期，頁 1-65。

二、 英文文獻

Ackoff R. L. (1999). *Ackoff's Best: His Classic Writings on Management.* Wiley.

Acquisti, A. & Grossklags, J. (2005). Privacy and Rationality: A Survey. In *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation* (pp. 15-29). (Privacy

doi:10.6342/NTU202500550

and Technologies of Identity: A Cross-Disciplinary Conversation). Springer Science and Business Media, LLC.

Advisory Committee on Automated Personal Data Systems of Department of House, Education, and Welfare (1973). Records, Computers, and the Rights of Citizens. https://www.justice.gov/opcl/docs/rec-com-rights.pdf.

Alpaydin, E. (2014). *Introduction to Machine Learning*. The MIT Press.

Altman, I. (1977). Privacy Regulation: Culturally Universal or Culturally Specific?. *Journal of Social Issues, 33*(3), 66-84.

Austin, L. (2014). Enough About Me: Why Privacy Is About Power, Not Consent (or Harm). In Sara, A. (Eds.), *A World without Privacy: What Law Can and Should Do?* (pp. 131-189). Cambridge University Press.

Balkin, J. M. (2016). Information Fiduciaries and the First Amendment. *UC Davis Law Review, 49*(4), 1183-1234.

Bamberger, K. A. & Lobel, O. (2017). Platform Market Power. *Berkeley Technology Law Journal*, 32, 1051-1092.

Barocas, S. & Nissenbaum, H. (2014) Big Data's End Run around Anonymity and Consent. In Lane, J., Stodden, V., Bender, S. & Nissenbaum, H. (Eds.), *Privacy, Big Data, and the Public Good* (pp. 44-75). Cambridge University Press.

Burdon, M. & Andrejevic, M. (2016). Big Data in the Sensor Society. In Sugimoto, C. R., Ekbia, H. R. & Mattioli M. (Eds.), *Big Data Is Not a Monolith*. The MIT Press.

Carey, P. (2018). *Data Protection: A Practical Guide to UK and EU Law.* Oxford University Press.

doi:10.6342/NTU202500550

Cohen, J. (2012). *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice.* Yale University Press.

-------- (2013). What Privacy Is For?. *Harvard Law Review, 126*, 1904-1933.

-------- (2019). Turning Privacy inside Out. *Theoretical Inquiries in Law*, 20, 1-31.

-------- (2024). How (Not) to Write a Privacy Law. https://knightcolumbia.org/content/how-not-to-write-a-privacy-law.

Crawford, K. & Schultz, K. (2013). Big Data and Due Process：Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review, 55*, 93-128.

Desouza, K. C. & Smith, K. L. (2014). Big Data for Social Innovation. *Stanford Social Innovation Review, 2014*, 39-43.

Fairfield, J. & Engel, C. (2015). Privacy as a Public Good. *Duke Law Journal, 65,* 385-457.

Federal Trade Commission (2014). Data Brokers: A Call for Transparency and Accountability.

Ferrer, E. C., Rudovic, O., Hardjono, T. & Pentland, A. (2018). *RoboChain: A Secure Data-Sharing Framework for Human-Robot Interaction,* https://arxiv.org/abs/1802.04480.

Fried, C. (1968). Privacy. *The Yale Law Journal, 77*(3), 475-493.

Froomkin, A.M. (2019). Big Data: Destroyer of Informed Consent. *Yale Journal of Law & Technology, 21*(3), 27-54.

Fuster, G. G. & Scherrer, A. (2015). *Big Data and Smart Devices and Their Impact on Privacy*. European Parliament.

doi:10.6342/NTU202500550

https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf.

Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal, 89*(3), 421-471.

Goffman, E. (1959). *The Presentation of Self in Everyday Life*. Anchor Books.

Gupta, S. B. & Mittal, A. (2017). *Introduction to Database Management System.* Laxmi.

Hildebrandt, M. (2014). *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology.* Edward Elgar Publishing.

-------- (2019). Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning. *Theoretical Inquiries in Law, 20*(1), 83-121.

Hirsch, D. D. (2016). Privacy, Public Goods and the Tragedy of the Trust Commons: A Response to Professors Fairfield and Engel. *Duke Law Journal Online, 65*, 67-93.

-------- (2020). From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics. *Maryland Law Review, 79*(2), 439-505.

Koops B. J. & Gahic, M. (2021). Unite in Privacy Diversity: A Kaleidoscopic View of Privacy Definitions. *South Carolina Law Review, 73*, 465-499.

Krasnow, E. G. & Goodman, J. N. (1998). The "Public Interest" Standard: The Search for the Holy Grail. *Federal Communications Law Journal, 50*(3), 605-635.

Lazaro, C. & Métayer, D. L. (2015) Control over Personal Data: True Remedy or Fairytale?. *SCRIPTed, 12*(1), 3-34.

Lubarsky, B. (2016). Re-Identification of "Anonymized" Data. *Georgetown Law Technology Review, 1*, 202-213.

doi:10.6342/NTU202500550

Lynskey, O. (2015). *The Foundations of EU Data Protection Law.* Oxford University Press.

Matsumi, H. & Solove, D. J. (forthcoming 2025). The Prediction Society: Algorithms and the Problems of Forecasting the Future. *University of Illinois Law Review*.

Miller, A. R. (1971). *The Assault on Privacy: Computers, Data Banks, and Dossiers.* University of Michigan Press.

Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information.* Harvard University Press.

Pentland, A., Lipton, A. & Hardjono, T. (2021). *Building the New Economy: Data as Capital*. The MIT Press.

Prosser, W. L. (1960). Privacy. *California Law Review, 48,* 383-423.

Regan, P. (2020). A Design for Public Trustee and Privacy Protection Regulation. *Seton Hall Journal of Legislation and Public Policy, 44*(3), 487-513.

Richards, N. M. (2013). The Dangers of Surveillance. *Harvard Law Review, 126*, 1934-1965.

Richards, N. M. & Woodrow, H. (2016). Taking Trust Seriously in Privacy Law. *Stanford Technology Law Review, 19*, 431-472.

-------- (2019). The Pathologies of Digital Consent. *Washington University Law Review, 96*(6), 1461-1503.

-------- (2021). A Duty of Loyalty for Privacy Law. *Washington University Law Review*, *99*, 961-1021.

Schwartz, P. M. (1999). Privacy and Democracy in Cyberspace. *Vanderbilt Law Review,*

doi:10.6342/NTU202500550

52, 1609-1702.

Schwartz, P. M. & Peifer, K. (2017). Transatlantic Data Privacy Law. *The Georgetown Law Journal, 106,* 115-179.

Solove, D. J. (2006). *The Digital Person: Technology And Privacy in the Information Age*. NYU Press.

-------- (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review, 154*, 477-560.

-------- (2008). *Understanding Privacy*. Harvard University Press.

-------- (2023). The Limitations of Privacy Rights. *Notre Dame Law Review, 98*(3), 975-1036.

-------- (2024). Murky Consent: An Approach to the Fictions of Consent in Privacy Law. *Boston University Law Review, 104,* 593-639.

Solove, D. J. & Schwartz P. M. (2024). *Information Privacy Law.* Aspen.

Solove, D. J. & Woodrow, H. (2024). Kafka in the Age of AI and the Futility of Privacy as Control. *Boston University Law Review, 104*, 1021-1042.

Solow-Niederman, A. (2022). Information Privacy and the Inference Economy. *Northwestern University Law Review, 117*(2), 357-454.

Tene, O. & Polonetsky, J. (2013). Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property, 11*(5), 240-273.

Viljoen, S. (2021). A Relational Theory of Data Governance. *The Yale Law Journal, 131*, 573-654.

doi:10.6342/NTU202500550

Waggins C., & Jones, M. L. (2023). *How Data Happened: A History from the Age of Reason to the Age of Algorithms*, W. W. Norton & Company.

Waldman A. E. (2018). *Privacy as Trust: Information Privacy for an Information Age*. Cambridge University Press.

-------- (2022). Privacy, Practice, and Performance. *California Law Review, 110*(4), 1221-1280.

Warren, S. D. & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193-220.

Westin A. F. (1967). *Privacy and Freedom*. Ig Publishing.

Woodrow, H. & Solove, D. J. (2015). The Scope and Potential of FTC Data Protection. *Washington Law Review, 83*(6), 2230-2300.

Zuboff, S. (2018). *The age of surveillance capitalism : the fight for a human future at the new frontier of power*, Public Affairs.

doi:10.6342/NTU202500550