《憲法解釋之理論與實務》第十二輯　蘇彥圖主編
臺北　中央研究院法律學研究所　法學叢書 (9)
民國 114 年 9 月，頁 187-235

科技正當法律程序的憲法意涵*

—— 美國判決與學說發展的檢視

劉靜怡**

摘 要

本文以「科技法律正當程序」為題，檢視美國法制中關於此一概念的判決和學說發展。本文首先分析正當法律程序的發展歷程，如何呈現出科技如影隨形的特色，進而以此為基礎，探討執法機關在面對各種科技的應用時，遭遇何種困境，以及這些困境導致哪些正當法律程序的爭議產生。接著，本文以美國政府的大規模監控計畫為例，分析正當法律程序在挑戰這類國家監控措施時，為什麼難以發揮保障人民權益的基本功能，同時，本文也以人工智慧時代的自動決策爭議，用來說明正當法律程序在人工智慧時代將遭遇何等挑戰。本文認為：在新興科技不斷發展下，正當法律程序保障的內涵已經呈現落伍或不足的現象，在面對當代的科技化與自動化社會脈絡時，必須將正當法律程序原則轉化成「科技正當法律程序」原則，並且嚴肅思考其所欲追求的憲法價值，是否正歷經一場前所未有的危機。

關鍵詞：科技正當法律程序、科技執法、大規模監控、自動化決策、人工智慧。

＊　本文曾刊登於專書《網路時代的隱私保護困境》，頁367-411（2021年）。〔責任校對：盧又瑄〕。

** 國立臺灣大學國家發展研究所特聘教授。

穩定網址：https://publication.iias.sinica.edu.tw/51716032.pdf。

目 次

壹、前言

在公法領域中，正當法律程序（due process of law）原則所提供的保障，向來是政府行使公權力之際，人民用以保障其基本權利的憲法防禦手段。然而，在各種行政措施與執法行為不斷科技化與自動化的當代趨勢下，政府固然得以藉此獲致節省成本、作成一致決定的好處，然而，相對地，在科技化與自動化的趨勢下，正當法律程序原則或許可以說是實質轉化成「科技正當法律程序[1]」（technological due process of law，或亦可稱為「科技化的正當法律程序」）所欲追求的憲法價值，卻遭遇越來越空洞化的危機，可能導致人民基本權利不保的窘境。

換言之，關於「正當法律程序」原則在美國當代憲法史上的角色，放在科技發展的脈絡下觀察，格外能夠凸顯出其在當代所面臨

1 關於「科技正當法律程序」此一用語，主要是借用自Danielle Keats Citron的多年前發表的論文，*see* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2007). 該論文的分析對象，主要是自動化決策的應用，在行政程序中的規則制定（rule-making）與行政決定（行政處分，adjudication）上可能扮演的角色，以及因此對於個人的正當法律程序權益所造成的衝擊，討論可行的解決之道。

的困境。這個「科技正當法律程序」的權利保護困境，從美國聯邦憲法增修條文（下稱美國憲法增修條文）第4條所要求的正當法律程序之發展歷程為背景，大致上可以從兩個面向來觀察，第一個面向是在滿足哪些條件的情況下，將達到侵害「合理隱私期待[2]」（reasonable expectation of privacy）的門檻，必須啟動法院令狀的要求。另一個面向則是美國憲法增修條文第4條所要求的「通知與評論」（notice and comment）此一行政程序參與層面的權利，在科技不斷發展的脈絡下，應該如何詮釋，才能充分落實其保障人民權利的功能。

首先，雖然美國憲法增修條文第4條提供法律正當程序的保障，殆無爭議，但是，美國聯邦最高法院針對何種政府行為會構成其憲法增修條文第4條所規定的搜索（search），因而必須以法院令狀為前提，卻經歷轉折。1920年代末期*Olmstead v. United States*這個判決所採取的「物理侵入原則[3]」（the physical trespass doctrine），持續居於主導判決方向的地位近四十年，直到1960年代中期的*Katz v. United States*的「隱私保護之合理期待[4]」（the reasonable expectation of privacy protection）出現，才使「合理隱私期待標準」成為憲法增修條文第4條搜索規定的判斷關鍵，亦即以個人隱私是否構成侵害為判斷標準，不再拘泥於必須構成物理性的有形侵入，才啟動法院令狀的要求。然而，此一判斷標準結合了美國聯邦最高法院的後續判決所發展出來「第三人原則[5]」（the third-party doctrine），使人民對於自己的通訊隱私所得主張的合理隱私期待，幾乎落空。

---

2 Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

3 Olmstead v. United States, 277 U.S. 438 (1928).

4 *Katz*, 389 U.S. at 347.

5 關於「第三人原則」的影響，請參見本論文「貳」、「參」與「肆」部分的相關論述，並可參見：李榮耕，科技定位監控與犯罪偵查：兼論美國近年GPS追蹤法制及實務之發展，臺大法學論叢，44卷3期，頁890（2015年）。

其次，隨著科技的進展與普及，無論是公私部門的監控行為，都已經成為常見的侵害權利現象，然而，或許直到Snowden事件爆發[6]之後，關於國家透過科技從事大規模監控的濫用行為，才受到比較明顯的重視，而國家監控行為，也是應該直接受到憲法檢視的監控類型，尤其是正當法律程序能否發揮節制國家監控行為、保障個人憲法權利的功能，在當前這個利用科技進行監控已成趨勢的時代中，格外值得探討。

再者，政府部門所運用得自動化系統對個人作成的決定，或者基於其可能秘密不公開的特性，或者基於其運作特性導致並無留存作成決定的相關紀錄（audit trails）的特性，會使行政機關事後無法重新審查系爭決定，因而破壞了行政法體系中關於聽證制度的基本要素[7]。即使這類自動化決策過程中踐行了某種聽證制度，職司重新檢視任務者，也可能會抱有AI不會出錯的偏見，因而空有制度卻徒勞無功。更進一步言之，即使人工智慧或自動化決策中的確有人參與其中，但因為參與者往往具有所謂的「自動化偏見」（automation bias）[8]，也就是人會傾向於認定人工智慧或自動化系統不會出錯，而行政部門未來的決策越來越仰賴自動化系統甚至人工智慧之後，此一偏見將更形嚴重，原因無他，因為人類可能越來越沒有能力去查證人工智慧或自動化系統是否犯下錯誤。甚至，就現有的成本效益分析而言，重新審查人工智慧或自動化決策的成本，可能遠大於其可能帶來的利益，也會成為加深自動化偏見的原因，更遑論現有的成本效益考量因素，可能並不充足，因此，對於如何解決此一自動化偏見困境，恐怕矯正效果有限、無力回天[9]。

---

6 關於Snowden事件的詳細始末，可參見GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE (2014).

7 *See* Citron, *supra* note 1, at 1253-54.

8 *Id.* at 1285-86.

9 *Id.* at 1254-55.

就行政法的日常體制，行政機關的決策經常涉及對個別人民的權益造成具體影響的決定（或者以「行政處分」的行政法概念來理解），此時會要求在程序上必須合乎法律正當程序的要求，以便保障個人的重要利益[10]。但是，人工智慧或自動系統決策的不透明化，卻會使正當法律程序所欲維護的程序保障價值，遭到掏空的命運。究其實際，甚至有學者認為，不但是行政機關對會對個別人民的權益造成具體影響的自動化決定，極可能會掏空正當法律程序原則中的核心，亦即憲法所賦予的程序保障，對於行政機關內部的規則制定（rule-making）程序來說，在行政決策自動化的趨勢下，也會有同樣的負面影響[11]。

舉例來說，正當法律程序原則所要求的個人受通知權（the right to be given notice），亦即要求行政機關在作成決定之前，必須滿足通知當事人的要求，而通知內容的範圍除了行政機關準備作成決定的事項以外，還應該包含支持系爭決定的證據，以及行政機關將如何作成決定的程序。受通知權此一要求的目的，明顯是為了讓當事人在受通知後可以表示意見，藉此避免行政機關的決定是基於錯誤事實作成，進一步也可避免造成適用錯誤法規的結果[12]。然而，大部分的自動化決策，並沒有充分滿足受通知權，例如美國國土安全部（United States Department of Homeland Security）針對禁飛名單（No-Fly List）的決定，便是典型的例子[13]。進一步言之，即使有些自動化決策形式上踐履通知程序，其通知內涵可能也並不充足適當，很可能欠缺支持自動化決定的理由，而且，如前所述，在自動化決策缺少稽核紀錄的情況下，更難以提供使當事人能夠藉以回應系爭決定的充足資訊。

---

10 *See, e.g.,* Londoner v. City and County of Denver, 210 U.S. 373 (1908).

11 Citron, *supra* note 1, at 1278-81.

12 *Id.* at 1282.

13 United States Government Accountability Office, Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public (Sept. 29, 2006), https://www.gao.gov/assets/a251884.html (last visited July 25, 2024).

以美國法為例，*Mathews v. Eldridge*[14]此一判決固然建立了關於正當法律程序的成本效益分析架構[15]，並且行之多年。然而，在人工智慧或自動化決策的脈絡下，卻可能難以適用。追究其原因，一方面是因為前述的自動化偏見，會使得負責聽證程序的行政機關人員比較不信任提出申訴或訴願的人民所持的主張，而且，申訴人或訴願人也沒有適當或足夠的資料，足以重建決策過程，證明人工智慧或自動化決策系統應當如何決策或作成怎樣的決定，才是正確的[16]。而且，類似No-Fly List這樣的自動化系統，自然會有系統秘密運作的先天限制，所謂公共安全或國家安全此一利益，不但被認為高於個人利益，此一利益也會導致被列入禁飛名單的個人完全無法得知如何被列入禁飛名單相關資訊[17]。

其實，上溯到憲法權力分立制衡原則的層次，檢視以人工智慧或自動化系統作成的行政機關決定，不難得出「課責性」（accountability）難以落實的結論。因為，行政機關透過人工智慧或自動決策系統的程式碼（code）而隱含的政策，難以為外界理解，甚至行政機關本身也無法偵測該系統內的運作，是否與實質上的政策互相悖離[18]。自動化系統無異於製造了新型態的授權結果，但無論是對授權起源的立法權、行政機關、民主政治甚或法治而言，恐怕都會帶來更多必須重新思考正當法律程序真正意涵的挑戰。

進一步言之，司法權原本針對行政機關作為審查的功能，在人工智慧與自動化決定的脈絡下，也可能會因此緊縮，受到相當衝擊。在此等決策脈絡下，法院無法檢視演算法的程式碼是如何變成行政機關所適用的規則或作成的決定，因此也就無法進行有效的審

14 Mathews v. Eldridge, 424 U.S. 319 (1976).
15 *Id.* at 333-35.
16 Citron, *supra* note 1, at 1283-85.
17 *Id*. at 1287.
18 *Id.* at 1295-96.

查。即使法院勉力為之，可以認定演算法的程式碼的確轉化成行政機關適用的規則或作成的決定，但因為司法審查往往必須仰賴行政機關的詳細紀錄，才能確定行政機關是否濫用裁量權等等行政法上爭議的答案為何，人工智慧或自動化決策的程序能否滿足此一基本需求，導致司法機關難以發揮其節制行政機關的審查功能，不無疑問[19]。

本文主要以美國法制為探討對象。以下「貳」將先說明正當法律程序的發展歷程，如何呈現出科技如影隨形的特色。接著，本文「參」探討執法機關在面對各種科技的應用時，遭遇何種困境，以及這些困境導致哪些正當法律程序的爭議產生。「肆」則是以美國政府的大規模監控計畫為例，分析正當法律程序在挑戰這類國家監控措施時，為什麼難以發揮保障人民權益的基本功能。本文「伍」，則是將探討焦點轉移到人工智慧時代的自動決策趨勢，分析未來正當法律程序在此一趨勢下將遭遇何等面貌的挑戰。「陸」則是以本文上述內容之簡要歸納作為結論。

貳、「正當法律程序」的發展歷程：科技如影隨形的當代憲法發展史

如前所述，美國聯邦最高法院於1920年代末期*Olmstead v. United States*判決中所採取的「物理侵入原則[20]」（the physical trespass doctrine）持續主導判決方向近四十年，直到1960年代中期的*Katz v. United States*該判決的「隱私保護之合理期待[21]」（the reasonable expectation of privacy protection）出現，才轉而使「合理

19 *Id.* at 1297-1300.
20 *Olmstead*, 277 U.S. at 438.
21 *Katz*, 389 U.S. at 347.

隱私期待標準」成為增修條文第4條搜索規定的判斷關鍵，不再拘泥於必須構成物理性的有形侵入。

不過，更值得注意的是，在接下來的十多年時間裡，在*United States v. Miller*[22]和*Smith v. Maryland*[23]這兩個判決接連出現後，則是可以確定美國聯邦最高法院已經建立了所謂「第三人原則」（the third-party doctrine）。此一原則的核心，在於判斷個人資料在基於「自願」而提供給第三人，轉由第三人控制後，是否依然具有「合理隱私期待」。根據此一原則，只要個人將其資料提供給第三人（例如為其提供服務的金融機構或電信業者等）之後，其對於該資料便無合理隱私期待可言，所以也就不能援引美國憲法增修條文第4條的程序保障。換言之，根據上述判決，由於將其個人資料提供給該個人不再具有對本身資訊獨有的控制權時，也必須同時承擔第三方可能將該資料轉送或者提交給他人的風險，不能再認為該資訊有任何私密性質可言。雖然Antonin Scalia大法官曾於2012年在其主筆的*United States v. Jones*多數判決意見中指出，合理隱私期待原則與物理侵入原則兩者之間，應屬「並立」關係，並非「取代」關係[24]，也就是特別闡明美國憲法增修條文第4條的保護範疇，仍應涵蓋財產權和隱私權兩種權利類型，而實際上在個案適用時，則視其到底有無物理性的入侵，決定適用哪個原則，而Scalia大法官此一看法也為嗣後的*Florida v. Jardines*[25]與*Grady v. North Carolina*[26]兩個判決所援用，但是，整體而言，關於是否應該啟動法院令狀程序的判斷，在現行法上並無太大的變動，而上述判斷標準在科技現狀下是否符合法律正當程序保障的原始旨意，在美國的學說上則是依然爭執不休[27]。

---

22 United States v. Miller, 425 U.S. 435 (1976).
23 Smith v. Maryland, 442 U.S. 735 (1979).
24 United States v. Jones, 565 U.S. 400, 405-11 (2012).
25 Florida v. Jardines, 133 S. Ct. 1409 (2013).
26 Grady v. North Carolina, 135 S. Ct. 1368 (2015).
27 關於美國學者對上述判決的闡述，以及對正當法律程序發展趨勢的分析，*see*

就現狀而言，由於網路無處不在和遠端儲存的特性，導致執法人員無可避免地越來越仰賴資通訊科技（Information and Communications Technology, ICT）公司所儲存的資訊。舉例來說，由於許多主要的ICT公司都位於美國境內，因此導致全球的執法者甚或法院往往必須尋求美國政府的協助，才能順利取得其辦案所需的數位證據（例如美國境內的科技公司所掌握的電子郵件）。諸如此類的數位證據取得程序，往往速度緩慢而且程序不透明，長期以來，這類跨境資料取得，一直是許多國家的執法機關在取得有關其本國公民及其境內犯罪有關的必要證據時所面臨的基本困境。

雲端運算（cloud computing）趨勢的普及化，則是進一步加劇了此一困境的嚴重性。基於雲端運算仰賴網路儲存和近用資料的特性，等於是雲端服務供應商會讓個人資料在不同司法管轄區之中儲存與移動，因此，即使用戶和雲端服務供應商兩者是處於同一個司法管轄區之內，但是系爭資料可能會經過多個司法管轄區，而且，此種關於儲存與移動的實際情況，雲端服務的使用者和執法機關，通常並不知情。換言之，即使只是要取得某些電子郵件，執法機關也可能必須在數個國家啟動跨境資料取得的程序，此一程序對於起訴或審判來說，必然會造成拖延效果。而隨著雲端運算服務日趨普遍，跨境資料傳輸和繁瑣的跨境資料取得程序，很可能逐漸成為原則，而不再屬於例外[28]。

以2018年美國聯邦最高法院作成的*United States v. Microsoft Corporation*此一案件或判決[29]為例，在該案中，微軟公司拒絕服從

Kiel Brennan-Marquez & Andrew Tutt, *Offensive Searches: Toward a Two-Tier Theory of Fourth Amendment Protection*, 52 HARV. C.R.-C.L. L. REV. 103 (2017); Andrew G. Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547 (2017); Caleb A. Seeley, *Once More unto the Breach: The Constitutional Right to Information Privacy and the Privacy Act*, 91 NYU L. REV. 1355 (2016).

28 *See generally* Secil Bilgic, *Something Old, Something New, and Something Moot: The Privacy Crisis under the CLOUD Act*, 32 HARV. J.L. & TECH. 321 (2018).

29 United States v. Microsoft Corp., 138 S. Ct. 1186 (2018).

美國政府的搜索令，提供執法機關所需的通聯資料，因為該搜索令針對的資料，其實是儲存在愛爾蘭境內。2018年3月，當此一案件還在聯邦最高法院審理期間，美國國會所通過的「釐清海外資料使用法」（Clarifying Lawful Overseas Use of Data Act, CLOUD Act）經簽署成為正式生效的法律，儘管*Microsoft Ireland*案因CLOUD Act變成無判決實益，但這個案件卻顯示出跨境資料取得對隱私保護具有深遠影響的意涵。

根據第三人原則，針對自願向第三人提供的資訊，個人固然不得主張享有合理隱私期望，不過，根據美國聯邦最高法院2018年的*Carpenter v. United States*[30]判決，卻就取得個人的行動通信基地台位置歷史紀錄（historical cell-site records）此種資訊，認定其屬於第三人原則的例外。此一案件乃是涉及2010年12月至2011年3月這段期間，在Ohio和Michigan兩州發生一系列的搶劫案件，最後有4名男子在Detroit被捕，其中一名被捕者向FBI調查人員提供了15名共犯的姓名和幾個手機號碼，於是該案檢察官嗣後乃依「通訊紀錄法[31]」（Stored Communications Act, SCA）規定聲請並取得法院命令，要求MetroPCS和Sprint兩家電信公司提供本案原告Timothy Carpenter在兩個特定時段內的手機位置資訊（Cell-Site Location Information, CSLI），上述兩家電信公司根據此一法院命令要求，總共提供了12,898個位置資料，而該等資料顯示Carpenter當時就在四起搶劫案的現場，後來Carpenter在該案中被判有罪並遭判116年的有期徒刑。

在該刑事案件的審判過程，Carpenter曾嘗試以美國憲法增修條文第4條，排除CSLI資料成為該案有效證據。政府固然是根據通信紀錄法相關規定[32]獲得命兩家電信公司提供CSLI記錄的法院命令，

30 Carpenter v. United States, 138 S. Ct. 2206 (2018).
31 18 U.S.C. §§ 2701-12 (1986).
32 18 U.S.C. § 2703 (d) (1986).

但該規定僅要求聲請法院命令的執法機關應提出「合理的理由」（reasonable grounds）相信該記錄「與正在進行的調查相關且對該調查具有重要性」（relevant and material to an ongoing investigation），其所要求的證明標準，比聲請法院搜索票所要求的標準為低。同時，身為被告的政府，在這個案件中所主張的論點是，Carpenter的手機所發送的CSLI，是其自願提供給電信公司的，並成為電信公司正常商業紀錄的一部分，所以符合第三人原則，毋需踐履搜索令狀的要求。雖然此一類比邏輯看似一致，但是，此處值得質疑的是，究竟有多少手機用戶實際上知道自己手機會不斷地傳輸其位置資訊給電信公司？如果手機用戶根本不理解或不知道此一科技現實，究竟如何能夠合理地表現出是自願提供自己的位置資訊？

若是將*Carpenter*這個判決當成個案來觀察，其判決論理邏輯與結果對於所謂位置歷史紀錄以外的資料進行的搜索，其影響究竟如何，或許並不是非常清楚，尤其主筆此一判決意見的首席大法官John Roberts特別指出該判決適用範圍很窄[33]，更加深了此一不確定性。倘若*Carpenter*此一判決僅僅適用於行動通信的位置記錄資料，那麼美國憲法增修條文第4條的規定，很可能依然無法為電話通訊或電子通訊這類使用時同樣涉及提供給第三人的紀錄，提高正當法律程序的保障。如此一來，在網路環境下，美國憲法增修條文第4條便幾乎無法透過法律正當程序的要求，提供隱私保護。

在此一現狀，我們勢必應該發問的是：在現代科技的發展脈絡下，是否應該對正當法律程序此一憲法用以保障基本權利的程序性原則，予以某程度衡平性的調整[34]，使其在科技普及應用於日常生活的時代裡，實質上具有程序保障意義？

---

33 *Carpenter*, 138 S. Ct. at 2206. *See also* Susan Freiwald & Stephen Wm. Smith, *The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205 (2018).

34 *See, e.g.*, Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011).

除了*Carpenter*這個備受矚目的判決之外，美國聯邦最高法院在此一判決出現之前數年所作成的兩個判決，也顯示出司法者在面對現代科技不斷削減美國憲法增修條文第4條所提供的保護此一趨勢時，如何透過判決從事具有衡平意義的調整，以便確保正當法律程序所能發揮的人權價值。

首先，在2014年*Riley v. California*[35]此一判決中，聯邦最高法院縮小了「附帶搜索」（searches incident to arrest）的範圍。本案所涉及者同為手機資料，而且是司法者長期認可屬於美國憲法增修條文第4條例外情況的類型。該判決指出：手機的性質，與被逮捕者身上的其他物體不同。「手機」（cell phones）這類設備實際上等於是小型電腦，而且往往具有等同於相機、影音播放、錄影錄音、追蹤等等功能，手機這些和傳統物理證據之間的質量差異，是作成此一判決的法院將手機從合法逮捕的附帶搜索例外中予以排除的主因[36]。不過，值得一提的是，本判決並不因而禁止執法機關搜索手機，只要合法取得搜索令狀，則可以針對手機進行搜索。

其次，再往前回溯到2012年*United States v. Jones*[37]這個判決，聯邦最高法院則是指出，即使政府採用憲法制定者在制憲當時無法想像的現代科技（該案中所涉及的現代科技是GPS追蹤裝置）從事執法行為，只要其足以觸動增修條文第4條的門檻，就應該構成必須取得令狀的搜索。*United States v. Jones*這個判決所涉及的爭議，是警方在某一重大毒品案的偵辦過程中，為了取得被告與毒品交易之間的聯繫關係，在沒有取得搜索令狀的情況下，連續28天使用GPS設備追蹤系爭個案毒品罪嫌犯使用的車輛。政府認為將GPS追蹤設備裝在嫌犯Antoine Jones所使用的車輛上，藉此記錄該嫌犯在

35 Riley v. California, 573 U.S. 373, 433 (2014).
36 *Id.* at 446.
37 *Jones*, 565 U.S. at 400.

公共街道上的行蹤，不構成搜索或扣押，因為嫌犯Jones不能合理期待其在公共街道上的移動是具有隱私保護的。既然搜索和扣押公共街道上移動的資料不構成搜索，則當然不需要取得法院所發的搜索令狀。

然而，聯邦最高法院在本案中則是否定了政府上述主張。此一判決最重要的意義，便是從20世紀下半葉以來的*Katz*案分析架構出發之際，同時回歸早期普通法侵權原則的路線[38]，認為GPS設備裝在嫌犯Jones的車輛上這個連接關係本身，已經足以構成了搜索，因為它不但構成了對嫌犯Jones的私有財產予以侵犯的結果[39]，同時還包括尋找某些物品或資訊的企圖在內[40]。更值得注意的是，此一判決的多數判決意見指出，個人針對自己的所有物理性移動，都具有合理的隱私期待[41]。雖然該案多數判決意見並未明白指出「追蹤」在何時會變成「搜索」，但是，Samuel Alito大法官和其他三位大法官共同提出的協同意見書則明確指出本案其實不需要精確地指出追蹤構成搜索的時點，因為本案的追蹤行為達到四週之久，這一定已經構成搜索，應無疑問可言[42]。相對地，在本案中，Sonia Sotomayor大法官所提出的協同意見書，則是進一步指出聯邦最高法院應該揚棄第三人原則，認為第三人原則並不適合繼續在數位時代中援用，因為，在數位時代裡，幾乎每個人在日常生活中都會向第三人透露大量的個人資訊[43]。

在以上這兩個判決作為背景的脈絡下，檢視美國聯邦最高法院在*Carpenter*此一判決中所使用的分析架構，或可說是法院認為本案

38 參見：張陳弘，美國聯邦憲法增修條文第4條搜索令狀原則的新發展：以Jones, Jardines & Grady案為例，歐美研究，48卷2期，頁267-332（2018年）。
39 *Jones*, 565 U.S. at 404.
40 *Id.* at 408.
41 *Id.* at 403, 406.
42 *Id.* at 430 (Alito, J., concurring).
43 *Id.* at 417 (Sotomayor, J., concurring).

的案例事實同時符合GPS追蹤設備的特色，也符合第三人原則的特色。換言之，透過CSLI所為的追蹤，和*Jones*案中藉由GPS所為的追蹤相當，至於因上述追蹤所得的資訊，並非政府安裝追蹤設備所得，而是由被追蹤人自願提供給第三人的資訊，此處又與第三人原則相符。再加上前述*Riley v. California*判決中，聯邦最高法院認為透過長期追蹤而累積的大量資訊，違反了一般人在日常生活隱私中所擁有的隱私合理期待，更可推論出*Carpenter*此一判決的特色。

換言之，在*Carpenter*這個判決中，由於執法機關只需要從電信業者取得個人的CSLI，就可以達成對任何公民進行追蹤的目的，政府甚至毋須事先確定犯罪嫌疑人或執法對象，因為透過CSLI的取得，便可以追溯取得任何後來發現的犯罪嫌犯或違法者的所有行蹤資訊，其過程簡單而且幾無成本。因此，當美國聯邦最高法院以5：4的比數在*Carpenter*此一判決中作成違憲結論，多數判決意見拒絕將第三人原則延伸至CSLI資料時，其最重要的論據，應該就是認為CSLI資料與過去適用第三人原則的資料，不但質量不同，而且會使執法機關可以幾近完美地從事追蹤監視行為，正如同執法機關把電子腳鐐套到手機用戶腳上一般，因此，執行機關取得行動通信基地記錄應屬美國憲法增修條文第4條意義下的搜索，必須滿足搜索令狀的要求，方得為之。

最後，近年來由於恐怖主義盛行，導致各國政府紛紛以維護集體安全之名，強化監控，曾經因恐怖主義而受創甚深的美國政府，自然也不例外。然而，針對後911時期陸續出現的各種反恐立法，以提升行政效率或維護國家安全為名，授權政府進行極為廣泛的資訊蒐集與運用分析，以便達成充分監控的目標，司法者所面對的，便是應該以怎樣的正當法律程序予以規制，才能守住資訊隱私權保護的最後防線此一根本問題。2013年Edward Snowden透過媒體所揭露的美國國家安全局（National Security Agency, NSA）監控措施，不但監控美國國內人民的通訊內容，也對全球的通聯紀錄進行監

控，換言之，無論是否為美國公民，也不管其是否涉及任何不法行為，均屬NSA監控範圍之內，亦即此等監控措施乃是無差別（indiscriminately）的大規模（bulk）的資料蒐集計畫[44]。

因為政府具有強大的資訊掌控優勢，加上監控科技日新月異，因此，目前的監控模式與監控內涵，和傳統上的通訊監察模式與內涵均有相當差異。觀察近年來的判決發展，美國聯邦最高法院在面對大規模國家監控所引發的爭議時，似乎仍然很難擺脫「合理隱私期待」與「第三人原則」的傳統框架，亦即美國司法者對於當今新興監控模式對於隱私權所造成的風險，仍處於未能有效控管的消極應對狀態。由於根據第三人原則，一旦系爭資料被歸類為是個人主動提供給第三人，或者是已經流入公開領域中，即無從主張合理隱私期待並啟動正當法律程序保障，在此一邏輯下，現代監控架構下無時無刻進行的資料蒐集，及其後續的資料儲存、分類、分析、組合以及目的外利用等等，雖然無一不涉及侵害隱私的疑慮，但在目前美國聯邦最高法院仍然採用的立場下，根本無從釐清或解決[45]。

換言之，本於公私領域二元論所發展出來的合理隱私期待判斷標準和第三人原則，雖然仍屬美國聯邦最高法院遵循的判決邏輯，但在當代通訊與網路技術發展下，對於個人隱私的保障，幾乎已成掏空正當法律程序此一基本價值的魔咒。尤其是在公私部門各種系統性監控不但技術可行且漸成趨勢的當代情境下，美國聯邦最高法院如何面對正當法律程序保障的基本挑戰，值得關注。

另一方面，如前所述，就最近幾年的科技發展趨勢而言，因為大數據與人工智慧等科技的驅動，各種公私部門透過自動化系統對於個人作成種種決定，無論是其過程或結果，都可能涉及個人權利

---

44 *See generally* John Yoo, *The Legality of the National Security Agency's Bulk Data Surveillance Programs*, 37 HARV. J.L. & PUB. POL'Y 901 (2013).

45 *See generally* Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 NYU ANN. SURV. AM. L. 553 (2017).

無法受到充分保障的疑慮，這則是另一個正當法律保障程序受到科技運用衝擊的層面。此一層面的個人權利侵害疑慮，部分是出自於自動化系統決定的不透明不公開特性，部分則是因為其並無作成決定的相關紀錄可資稽核（audit trails）。以上兩者都會使行政機關在事後無法重新審查稽核自動系統所作成的決定，也因而會破壞原先行政法體系中的聽證制度精神。更棘手的是，即使在自動化決策下仍提供聽證制度，事後負責重新檢視或審查的行政機關，也極可能會抱著自動化系統不會出錯的偏見。同時，就現有的成本效益分析架構而言，重新審查自動化決策的成本，也可能遠大於其可能帶來的效益（這是因為現在的成本效益考量也是不足的）。在此一政府決策仰賴科技的應用趨勢下，我們應該如何看待正當法律程序的科技意涵，也是值得討論的重要議題。

參、科技應用下的執法困境與正當法律程序

由於至今仍然有效的第三人原則，事實上造成相當程度的隱私保護漏洞，美國國會早在1986年便立法通過「儲存通訊紀錄法」（The Stored Communications Act, SCA）。在美國聯邦立法體例上，SCA屬於電子通訊隱私法（Electronic Communications Privacy Act, ECPA）的Title II，規範內容為取得通訊服務供應商所儲存的通訊與記錄的限制規定[46]。相形之下，ECPA的Title I即監聽法（Wiretap Act）規範對象為即時通訊的截錄行為[47]，ECPA的Title III則是電話紀錄器法（Pen Register Act），主要是規範撥話記錄、監測和追蹤設備的利用[48]。此處值得注意的是，SCA的立法設計，乃是考量1986年當時電腦所執行的主要功能。所以，SCA僅兩類服務供應

46 18 U.S.C. § 2702 (1986).
47 18 U.S.C. §§ 2510-22 (1986).
48 18 U.S.C. §§ 3121-27 (1986).

商：一是電子通信服務（Electronic Communication Service, ECS）供應商，以及遠端計算服務（Remote Computing Service, RCS）供應商，原因無他，因為這兩者就是1980年代電腦使用的主要服務。依據SCA的規定，政府執法機關要強制ECS供應商提供儲存超過180天以上的資料，或者要求RCS供應商提供資料時，有以下三種程序上的選擇途徑，亦即搜索令（warrant）、傳票加通知（subpoena plus notice），稱為超級搜索令的§ 2703(d)命令（super search warrant）加通知等三種類型[49]。透過這些程序上的要求，SCA限制了政府或執法機關強迫網路服務供應商（Internet Service Providers, ISP）提供其客戶和訂戶資料的權限，也限制ISP自願向政府提供資料的空間。因此，SCA可以說是將隱私保護延伸到電子通訊紀錄上，透過立法模式填補因為第三人原則所造成的隱私漏洞，以便使美國憲法增修條文第4條的正當法律程序或多或少仍然可以發揮實質保護隱私的功能。

然而，近年來的科技發展，卻使得SCA的解釋適用變得相當複雜。就*Microsoft Ireland*案而言，其爭議焦點是§ 2703(d)中所規定的命令，究竟是指搜索令狀、傳票抑或是兩者的混合形式，其之所以具有區別實益，主要原因在於就SCA的域外適用而言，美國聯邦最高法院將會根據答案的不同而得出不同結論。究諸實際，本文以下所分析的美國新近通過的雲端立法，便是透過修改SCA的方式，授權政府執法機關可以強迫位於美國的網路服務業者提交儲存在另一個國家或司法管轄區的資料。

應該針對取得雲端儲存資料的方式與程序予以規範的主張，到*Microsoft Ireland*案出現之後，可謂達到臨界點。就*Microsoft Ireland*

---

49 *See* 18 U.S.C. § 2703 (1986). *See also* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1211 (2004); Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 387 (2014).

案的發展歷程來看，該案始於紐約南區地方法院的法官發出搜索令，要求Microsoft這家科技公司必須提供某客戶電子郵件帳戶的內容。由於該搜索令所要求的資料事實上是儲存在愛爾蘭境內，因此Microsoft乃訴請撤銷該搜索令狀。美國紐約南區地方法院依前述SCA的§ 2703規定（亦即SCA搜索令），否決了Microsoft的訴求，並且因為Microsoft拒絕執行搜索令中的要求，法院進一步判處Microsoft蔑視法庭罪。Microsoft隨後提出上訴，主張SCA搜索令應該受地域限制，美國聯邦第二巡迴法院支持Microsoft的主張，撤銷上述搜索令。本案再經上訴到美國聯邦最高法院，美國聯邦最高法院則發出移審令，決定受理本案[50]。

歸納起來，在上述雲端立法通過之前，各方對於跨境取得資料的看法，幾乎可說是天差地別。首先，主張政府或執法機關應該有權跨境取得資料的陣營，例如美國政府，即以「資料規避」（data evasion）此一擔憂為出發點，而美國聯邦最高法院首席大法官John Roberts和美國聯邦第二巡迴法院Gerard Lynch法官也顯露出類似立場。Roberts大法官曾經詢問Microsoft是否主張自己可以不受約束地將出自美國國內的通訊內容儲存在任何地方，並且告訴其用戶不必擔心美國政府會輕易地取得其通訊資料，因為這需要透過繁複的國際協議與合作程序，曠日廢時[51]。關於這個疑慮，本案前審的美國聯邦第二巡迴法院Lynch法官則是在其協同意見書中指出：如果SCA無法適用於海外的話，那麼Microsoft便可以透過選擇將其用戶資料儲存在其他國家境內伺服器上這種模式，來阻止美國政府取得其用戶資料的執法需求。如此一來，所謂隱私保護，將不再依賴傳統的司法監督，而是取決於私部門如Microsoft這類提供網路服務的公司的「商業決策」了[52]。

---

50 *Microsoft Corp*., 138 S. Ct. at 1186.

51 Transcript of Oral Argument at 48, *Microsoft Corp.*, 138 S. Ct. at 1186.

52 Microsoft Corp. v. United States, 829 F.3d. 197, 222 (2d Cir. 2016) (Lynch, J., concurring).

相對地，屬於反對陣營如Microsoft，為了淡化這種資料規避的疑慮，則是主張在該案中搜索令狀所要求的60,000筆資料中，其實只有54筆和儲存在國外的資料有關。而且，Microsoft還進一步主張，若要試圖阻止美國政府執法部門取得其電子郵件內容者，應該不會使用Microsoft所提供的服務，而是會刻意選擇特別承諾其儲存的資料屬於美國管轄範圍之外的網路服務供應商才對[53]。

CLOUD Act此一立法在美國聯邦最高法院的判決期限屆至的前兩個月，正式由美國國會通過，成為有效法律，其內容修訂了部分SCA的規定，明確允許使用搜索令去取得美國公司在外國伺服器上所儲存的電子通訊內容或資料。在此一立法生效後，美國聯邦司法部便針對Microsoft所持有的系爭資料，取得新的搜索令狀，而Microsoft也同意了以新的搜索令狀取代舊的搜索令狀。隨後，聯邦最高法院便裁定該案件已經沒有判決實益（moot），該案正式落幕[54]。

歸納言之，在CLOUD Act中，針對「跨境資料取得」此一需求，有兩個值得注意的規定，而且是過去美國通傳法制中未曾出現的新穎規定：首先，本立法針對「符合特定條件的外國政府」（qualifying foreign government）創設例外，允許繞過既有的雙邊司法互助協定（Mutual Legal Assistance Treaties, MLAT）程序[55]，符合條件的外國政府，是指與美國簽有行政協定（executive agreement），並已頒布法律為美國SCA所規範的業者提供CLOUD Act中所規定的「實質性和程序性機會」的國家。雖然截至2018年12月為止，美國政府尚未與任何國家簽訂任何這類行政協定，但未來若與各國達成協議並簽訂行政協定，外國政府將有三種自美國境內取得其所需資料的類型：一、是上述符合條件的外國政府將能夠

53 Transcript of Oral Argument at 48, *Microsoft Corp.*, 138 S. Ct. at 1186.

54 *Id.* at 1188.

55 關於透過雙邊司法互助協定取得境外雲端資料的說明，*see generally* Bilgic, *supra* note 28, at 328-31.

直接從美國公司取得資料，二、是曾與美國簽訂MLAT，但未簽訂行政協定的國家，仍然可以啟動MLAT的資料取得程序，三、和美國政府之間既無MLAT也未簽訂行政協定的國家，則必須透過「調查委託書」（letters rogatory）的方式取得美國境內的資料。

其次，CLOUD Act透過SCA的§ 2703此一規定的制定，解決了*Microsoft Ireland*案當中的核心爭議：根據§ 2713的規定，提供電信或網路服務的業者必須遵守SCA所規定的義務，無論系爭通訊、記錄或其他資料到底是位於美國境內或境外，皆然。換言之，CLOUD Act澄清了美國聯邦法律中原有的模糊地帶，並且也確認了SCA的境外適用範圍[56]。

不過，從另一方面來說，CLOUD Act的出現，卻也引發了至少三個隱私相關的爭議：首先，根據CLOUD Act的規定，乃是允許符合條件的外國政府幾乎毫無限制地取用美國境內的資料，其次，在排除不符條件的外國政府之際，同時也使得美國政府幾乎可以到處獲取資料，對外國政府而言，等於是創造了一種不受歡迎的「美國例外主義」（U.S. exceptionalism），其結果可能導致其他國家更致力制定所謂的「資料本地化法律」（data localization law），也就是立法強制要求凡是在本國境內所產生的資料，都必須儲存在物理上位於本國境內的伺服器上，這樣的法律，也將威脅到外國公民的數位隱私[57]。再者，此種讓全球政府均可和美國政府合作的結果，CLOUD Act也對其他國家保護其本國公民資料免受美國監視的努力，有所斲傷。從以上幾個層面來看，CLOUD Act並未解決*Microsoft Ireland*案的隱私爭議，但卻同時成為另一個隱私危機的開始，尤其是對外國公民的隱私保護來說，更是如此[58]。換言之，CLOUD Act對美國政府的好處相當明顯，也就是足以阻止網路業者

56 CLOUD Act § 103(a)(1) (2018) (codified at 18 U.S.C. § 2713).
57 *see generally* Bilgic, *supra* note 28, at 328-31.
58 *Id.* at 336-44.

隱藏美國政府想要取得的資料，但這個好處，卻是以犧牲外國公民的資料隱私為代價。

肆、大規模監控下失落的正當法律程序保障

究其實際，國家監控的類型繁多，從針對特定人進行資料蒐集的傳統監控，到未針對特定個人的全面性監控──或有稱為流刺網型的監控（dragnet surveillance）[59]，都會引發正當法律程序原則如何適用的疑慮。雖然國家監控大致上都是藉由國家權力的行使，進行個人資料的蒐集、處理和利用，但前者通常是對象特定且規模較小的監控措施，執行這類監控措施是基於某些個案的執法需求，甚至就執行期間而言，也比較明確而密集，往往在達成特定目的或特定任務解除之後，便停止監控[60]。相對地，全面性監控往往並未具有明確的目的，也未鎖定特定人，即可進行大量的個資蒐集行為，而這種執行模式類似流刺網運作方式的國家監控模式，其實正是Snowden事件中所揭露的NSA）針對美國境內通訊紀錄進行廣泛蒐集的監控模式[61]。

從當時媒體因為Snowden爆料而取得的一系列文件與資料內容來看，此種監控的運作模式，就是政府以NSA為運籌帷幄的核心，長期透過在通訊相關業者內部的網路攔截取得並複製無數的通訊內容[62]，並且根據「外國情報監控法」（Foreign Intelligence Surveillance

59 *See generally* Shahid Buttar, *Dragnet NSA Spying Survives: 2015 in Review,* ELECTRONIC FRONTIER FOUNDATION (Dec. 25, 2015), https://www.eff.org/deeplinks/2015/12/dragnet-nsa-spying-survives-2015-review.

60 參見：張君魁，論預防性國家監控之憲法界限，國立臺灣大學法律學研究所碩士論文，頁35（2016年）。

61 *See* generally Greenwald, *supra* note 6.

62 *Id.*

Act, FISA）的授權規定[63]，針對包括Microsoft、Google、Facebook、Youtube、Skype和Apple等網路業者所有的伺服器，要求其提供即時通訊等相關資訊，而針對這些網路業者提供的資訊，政府則是利用諸如搜尋程式等科技方法進行種種資料分析，希望藉此全面掌控任何可能危及國家安全或者涉及恐怖主義行動的相關資料[64]。

然而，究諸實際，除了Snowden事件所引發的關注之外，美國聯邦最高法院在2013年也曾經審理一個由國際特赦組織美國分部（Amnesty International USA）起訴控告NSA的案件[65]，並且陸續出現了*ACLU v. Clapper*[66]、*Klayman v. Obama*[67]等訴訟，以上這些訴訟的爭議重點，幾乎都是關於政府進行監控的執法要件為何，以及系爭監控是否違憲，並且彰顯出美國司法者長期以來以「合理隱私期待」和「第三人原則」當成是否啟動正當法律程序下之搜索令狀要求的判斷標準，在面對當代儼然成為常態的大規模系統性監控，甚至將監控對象擴及境外和非本國人民時，對於隱私權的保障，恐已成為相當明顯的規範漏洞。

首先，就*Clapper v. Amnesty International USA*這個判決的結果而言，雖然美國聯邦最高法院在這個判決中是以否定原告具有訴訟適格（standing）的方式作成判決，並未觸及本案控方即國際特赦組織美國分部「外國情報監控修正法」（FISA Amendments Act of 2008）所主張之美國政府執行海外監控違憲的實質爭議，然而，從這個判決出發，對於分析美國的司法者在面對國家大規模監控時，究竟採取何種應對模式，以及其所採應對模式是否適當，則不無幫助。

---

63 50 U.S.C. § 1861 (1978).

64 *See, e.g.*, DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 384-87 (4th ed. 2011).

65 Clapper v. Amnesty International USA, 133 S. Ct. 1138 (2013).

66 ACLU v. Clapper, 959 F. Supp. 2d 724 (2013).

67 Klayman v. Obama, 957 F. Supp. 2d 1 (2013).

究諸實際，在Snowden曝光揭露上述監控計畫與措施之前，美國政府的大規模監控計畫即行之有年。至於這些監控計畫的原始授權依據，也不是晚近之事，而是可以上溯到1978年美國國會通過的FISA[68]。當時之所以通過此一法律，主要是肇因於執法機關往往以維護國家安全的理由，濫用未取得法院令狀電子監控方法，方便其進行蒐集情報與資訊的執法行動。在當時的情境脈絡下，立法者認為，如果繼續放任沒有取得法院搜索令狀的國內情報蒐集活動不斷順著當時的情勢繼續氾濫擴大，將會侵害美國憲法增修條文第4條保障人民的隱私權利[69]，所以才有FISA此一立法，用以授規範政府蒐集外國情資時，針對人民通訊進行電子監控的執法行為[70]。

這部法律的主要規定，包括明定政府進行外國情報活動的監控，必須以取得令狀為前提，同時，本法也明定外國情報監控法院（Foreign Intelligence Surveillance Court, FISC）的設立及其功能，專責審理本法所規定之外國情報監控令狀申請與核准事宜[71]。值得注意的是，基於外國情報監控執行的秘密特質，FISC的審理程序不同於一般法院的公開程序，相對地，FISC原則上是以秘密程序的方式進行，同時是僅僅由政府機關出席表示意見的單方程序（*ex parte*）方式，針對令狀的批准與否進行審查[72]。

FISA通過之後至今，曾歷經多次修正，其修正內容大多是基於通訊科技發展而衍生出新的國家安全需求和情報蒐集必要性而來。而在九一一事件發生之後，美國國會更是迅速以反恐為名，通過「愛國者立法[73]」（USA Patriot Act）。此一立法通過之後，根據FISA的Section 1861規定，無論是針對秘密情報活動、基於反制國際恐

68 *See generally* SOLOVE & SCHWARTZ, *supra* note 64, at 384.
69 *Id.*
70 *Id.* at 384-87.
71 *Id.*
72 *Id.* at 385.
73 USA Patriot Act of 2001, Pub. L. 107-56, § 215, 115 Stat. 272, 287 (2001).

怖活動的需求，或者是調查與美國人無關的外國情報資訊，聯邦調查局都可以申請使用基於USA Patriot Act的Section 215所取得的「有體物」（tangible things）[74]，惟該等申請必須具備合理理由，同時，由於這些透過政府監控所取得的個人資訊，乃是未經個人同意而取得的資訊，在依法執行本法規定的監控時，也必須符合「最小化程序」（minimization procedures）的要求。

此外，同樣值得注意的是，FISA修法[75]之後，將受監控對象的範圍，從原始規定中的「美國公民」擴張至「非美國公民」，而此一修法結果在正當法律程序的意涵下，便是執法機關在針對非美國公民啟動監控措施之際，毋須向FISC法院取得令狀，相對地，根據FISA對於非美國公民進行監控，則是由聯邦司法部長（Attorney General）和國家情報主任（Director of National Intelligence）兩者共同簽發監聽命令，即可針對境外非美國公民進行長達一年的電信監控[76]。再者，根據FISA的授權，NSA也可以執行大規模的蒐集metadata的計畫，並且進一步從這些metadata出發，進行進一步的資料蒐集與分析，將結果不斷整合成資料庫，並以大數據等科技進行利用，使得政府能夠據以進行監控。

更重要的是，如前所述，這類大規模監控計畫，事實上早已行之有年，但因為其具有秘密運作的特質，再加上FISC的審理程序依法不必公開，因此，一般社會大眾對此種大規模監控計畫所知相當有限，一直到Snowden事件發生後，才陸續出現政府監控措施遭到挑戰的現象，也才陸續出現針對國家監控措施進行審理的法院判

74 50 U.S.C. § 1861 (2001). *See also* David Kris, *On the Bulk Collection of Tangible Things*, 7 J. NAT'L. SECURITY L. & POL'Y 209 (2014).

75 Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, § 122 Stat. 2436 (2008).

76 *See generally* Daniel Severson, *American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change*, 56 HARV. INT'L L.J. 465 (2015).

決。而這些涉及大規模政府監控的判決，其內容正足以顯現出當代借助各種資訊科技從事治理的趨勢，其實是個隱私權逐步遭到侵蝕，而正當法律程序原則難以發揮保護基本權利功能的趨勢。

美國聯邦最高法院所作成的*Clapper v. Amnesty International USA*[77]判決，是Snowden事件後由國際特赦組織美國分部首先發難的結果。本案起訴原告是國際特赦組織美國分部，其起訴爭執的重點則是NSA根據FISA上述規定，針對不具有美國公民身分的境外對象進行電信監控，該行為應屬違憲。原告主張：FISA在2008年修正之後，授權執法機關在私人公司協助下，可以蒐集並且取得美國境外不具有美國籍之通聯對象的相關資訊和情報，導致原告在沒有客觀合理的期待可能性下，便遭遇其個人資訊和通訊遭到恣意蒐集、分析和利用使用的結果，而且，系爭規定將導致原告必須付出比過去更高的成本，以及必須採取負擔過於沉重的手段（costly and burdensome measures），確保其個資與通訊的隱密程度，以保護其個資與通訊免於不當近用的命運。因此，原告主張上述修法規定中關於資訊蒐集程序的規定，違反美國憲法增修條文第4條，原告因此主張法院針對政府的大規模資料蒐集計畫，核發永久禁制令（permanent injunction）[78]。

本案在審理過程中的主要爭執焦點，在於這類國家大型監控計畫下的原告，到底應該針對其所受的損害，如何主張與證明的問題。尤其是原告所受損害之具體程度和直接與否，應跨過怎樣的門檻，才足以認定其具備「當事人適格」（standing）？聯邦最高法院的判決結果，是認定原告基於一連串的可能性推測（speculative chain of possibilities），擔心自己成為受監控對象，是具有高度猜測性質的恐懼（highly speculative fear），僅是如此，仍不足以構成確

77 *Clapper*, 133 S. Ct. at 1138.
78 *Id.* at 1142-43.

定、具體、實質且即將發生的損害，因此以原告不具當事人適格而駁回此一訴訟。由於在程序要件的當事人適格此一爭點上即遭否決，法院自然未就NSA從事大規模監控的作法是否違反美國憲法增修條文第4條此一實體爭點進行審理[79]。

同樣地，在*Klayman v. Obama*[80]這個判決中，也引發當事人適格與法院應否核發禁制令的爭議。本案原告以Verizon Communications這家電信公司的用戶身分，同時以政府與私部門業者為被告，主張其透過大規模電話通訊攔截與分析的方法，違法執行一個秘密的政府監控計畫[81]。至於被告範圍，在政府方面包括總統、NSA及其局長、聯邦司法部（Department of Justice）及其部長等，在業者被告方面，除了Verizon Communications之外，還包括Google、Microsoft、YouTube、AOL以及AT&T等網路業者。在本案中，原告主張FISC針對大規模蒐集電話資料的許可令，逾越FISA規定的授權範圍，因為此種大規模資料蒐集措施，與維護國家安全之調查無關，所以FISC不該發給許可令，而此一無權卻發給許可令的作法，導致大規模監控計畫違反美國憲法增修條文第1條、第4條及第5條的規定。基於上述主張，原告主張法院應該發出暫時禁制令（preliminary injunction），命令政府停止系爭資料蒐集行為[82]。

針對當事人適格的爭議，法院認為根據FISA的規定，應該足以肯認原告具備針對系爭法院許可監控的命令提起司法審查的當事人適格[83]。據此而言，本案所涉之NSA蒐集美國公民電話metadata的措施，既然有侵害個人憲法權利的疑慮，法院自可針對系爭措施是否違反美國憲法增修條文第4條進行檢視，決定是否核發暫時禁制令[84]。

---

79 *Id.* at 1148-50.
80 *Klayman*, 957 F. Supp. 2d. at 1.
81 *Id.* at 10-11.
82 *Id.*
83 *Id.* at 24-25.
84 *Id.* at 7-9, 24-25.

不過，在本案中，法院採取與前揭美國聯邦最高法院在*Clapper v. Amnesty International USA*一案相反之見解。簡言之，作成*Klayman v. Obama*案的美國聯邦最高法院，認為既然有Snowden在衛報揭露的新聞，而隨後美國政府也證實2013年4月FISC的確核准NSA去蒐集Verizon Communications用戶的電話metadata，因此，在長期持續蒐集電信公司用戶資訊的事實，無可爭執[85]。至於針對NSA針對蒐集所得資訊進行分析，該法院則是認定系爭分析行為已構成美國憲法增修條文第4條的「搜索」。理由在於NSA在本案中之分析行為，和一般的資料庫分析行為不同，而是以拍下快照（snapshot）方式隨時進行記錄並每日即時更新，這種作法使政府更容易利用因此取得的人民秘密通訊資料，進行重複不間斷的大規模秘密監控[86]。加上透過此種監控方式所取得的資料，依法均可保留五年，可以隨時針對這些資料從事未經資料當事人同意的查詢與分析，所以，即使美國政府的抗辯，是以*Smith v. Maryland*這個判決所確定的第三人原則為依據，主張資料當事人對於自己自願撥出的電話號碼等資料欠缺合理隱私期待，作成此一判決的聯邦法院依然以本案的時空與科技脈絡，和*Smith v. Maryland*當的時空背景與科技使用方式並不相同為論據，認為本案不應適用第三人原則[87]，亦即法院認為上述大規模監控構成「搜索」，應有法院令狀之授權，始得為之。換言之，系爭計畫既然構成美國憲法增修條文第4條的不合理搜索，所以原告在本案中要求法院核發暫時禁制令，應以原告具有勝訴可能性為由，予以許可，以免原告遭受不可回復之損害，此即法院在本案中許可核發暫時禁制令的主要論據[88]。

值得注意的是，在這個美國哥倫比亞特區地方法院的判決中，即使本案的論證與判決結果，與過去的判決先例並不一致，但是該

85 *Id.* at 26.
86 *Id.* at 28-29.
87 *Id.* at 30-37.
88 *Id.* at 42.

法院仍以美國憲法增修條文第4條的原始目的是為了節制政府恣意侵犯個人隱私權益，而系爭大規模監控的系統化、無差別化特性，事實上可以說是侵害全體美國公民隱私為由，所以應該認定其落入美國憲法增修條文第4條的範疇[89]。不過，本案在上訴至美國哥倫比亞特區巡迴上訴法院之後，該上訴法則一反上述一審法院的認定，認為原告無法充分證明勝訴可能性，也無從證明其所受之實質損害為何，不符暫時性禁制令核發要件，乃廢棄原判決並發回地方法院更審[90]。該地方法院更審後於2017年維持先前巡迴上訴法院的上述認定，駁回原告請求，原告於是上訴，2019年巡迴上訴法院再度維持地方法院更審的駁回決定。

另一個與*Klayman v. Obama*的背景相仿的案件，則是*ACLU v. Clapper*。這個案件是由美國知名的兩個民權組織即美國公民自由聯盟（American Civil Liberty Union, ACLU）和紐約公民自由聯盟（New York Civil Liberties Union, NYCLU）擔任原告提起訴訟，同樣是在Snowden揭發NSA監控計畫之後，起訴主張NSA蒐集Verizon Communications用戶的電話metadata違憲[91]。本案法院在處理原告必須合乎特定、具體且即將發生之損害此一當事人適格要件的程序爭議時，受控的美國政府引用*Clapper v. Amnesty International USA*此一判決，主張原告僅是具有高度懷疑的恐懼而已，並不足以構成具體損害發生的要件。但是，本案法院卻引用*Amidax Trading Group v. S.W.I.F.T. SCRL*[92]，指出僅須表明資訊遭到政府部門取用，便合乎證明受有損害之事實此一要求，因而認定本案的原告滿足當事人適格的要件[93]。

---

89 *Id.* at 41-42.
90 Obama v. Klayman, 800 F.3d 559 (D.C. Cir. 2015).
91 *ACLU*, 959 F. Supp. 2d at 749-50.
92 Amidax Trading Group v. S.W.I.F.T. SCRL, 671 F.3d 140 (2d. Cir. 2011).
93 *ACLU*, 959 F. Supp. 2d at 737-38.

接著，在實體爭點方面，本案法院則是以*Katz*案的合理隱私期待標準，並且適用第三人原則，否決個人對於自願揭露給第三方的資訊具有正當的隱私期待可言[94]。換言之，本案法院認為雖然本案系爭監控計畫涉及的隱私與過去判決先例所涉及者不盡然相同，但電信服務使用者既然知悉電信業者的設備足以長期紀錄其撥號對象，使用者即無正當的合理隱私期待，甚至，本案法院也認為政府監控的規模，並不影響第三人原則的適用[95]。再者，本案法院綜合考量系爭監控計畫所追求的目的，認定其基於反恐的需求，在政府不可能預先知悉哪些電話的metadata會與反恐資訊有關的情境下，為了使反恐偵查具有即時性，以便預防未來的恐怖攻擊，所以其所採取的監控措施應仍屬法規授權範圍內[96]，加上本案中尚無證據足以證明政府有超出原始反恐目的的系爭資訊使用行為，而且既有法制中已有立法監督和行政監督兩者，並有FISC此一司法審查機制，所以並未違反美國憲法增修條文第4條[97]。

伍、人工智慧時代自動決策下前景不明的法律正當程序

就如何將自動化運用於公部門的決策此一討論而言，並非始於近年來的人工智慧熱潮，究其實際，行政機關過去長期以來其實就相當依賴電腦為其進行分析資訊，例如藉由電腦系統針對特定施政措施進行的本益評估，應是早已行之有年。在人工智慧時代中，其不同之處在於對電腦的依賴可能會擴張到許多新的用途上，例如警察部門的決策。換言之，警察部門可以使用具有預測功能的執法工

94 *Id.* at 749-50.
95 *Id.* at 752.
96 *Id.* at 746-48.
97 *Id.* at 757.

具，使用機器學習技術來強化他們關於自己管轄區域內未來犯罪的預測[98]。另外，美國也已經開始運用警察執法時隨身使用的照相機（body camera）所拍得的影片，當作訓練資料來強化機器視覺演算法，以便精進其執法效能。這類利用人工智慧執法的措施，不但有隱私疑慮，而且就執法的課責性而言，也會遭致課責不足的批評[99]。

其次，近年來人工智慧也已經逐漸為本身就以維護人民權利的部門如法院等機構，用來決定判決時的刑期長短或者假釋與否等決策，雖然這些機構多少仍然透過針對其所使用的人工智慧科技或演算法進行風險評估的方式，當作保護人民權利不受侵害的機制。但是，即使如此，依然無法確保其利用人工智慧決定刑期長短與保釋可能性時，不至於因此正當化甚或放大了某些長期存在的偏見，而這種使用人工智慧決定刑事處分內涵的模式，也使得對判決與假釋等決策的監督與審查，因為其更加不透明的特性而產生更高的難度[100]，這是個值得關切法律制度與司法體系的法學研究者嚴肅思考的議題。

究其實際，人類心靈活動本身就有複雜性和不透明性，而其正是目前人工智慧模仿的對象[101]，也正是此一不透明的心靈活動。假使未來政府決策或私法判決對不透明的人工智慧依賴逐漸升高，甚至連法律的解釋適用都依賴人工智慧的分析時，那麼，在科技上與法律上如何解決此一不透明特性所帶來的課責與規範難題，就是難以迴避的分析對象了。

---

98 *See* Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633 (2017).

99 *See, e.g.,* Drew Harwell, *Facial Recognition May be Coming to a Police Body Camera Near You*, WASHINGTON POST (Apr. 26, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/04/26/facial-recognition-may-be-coming-to-a-police-body-camera-near-you/?utm_term=16e4a05a6d81.

100 *See, e.g.*, ELECTRONIC PRIVACY INFORMATION CENTER, AI IN THE CRIMINAL JUSTICE SYSTEM, https://epic.org/algorithmic-transparency/crim-justice/ (last visited Nov. 12, 2018).

101 *See* Peter Margulies, *Surveillance by Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights*, 68 FLA. L. REV. 1045, 1065-66 (2016).

隨著AI的發展，政府機關開始使用AI來進行決策與處理事務，因此也衍生了一系列的爭議。例如，論者不乏提出這樣的看法：在民主社會中，政府自然是應該由人類親自治理，而不是直接委由人工智慧和演算法去從事治理行為，否則，如此一來，將會衍生出違背民主治理的基本原則、欠缺課責性以及造成電腦霸權這些質疑[102]。以美國行政法上的「禁止授權原則」（non-delegation doctrine）[103]為例，當行政機關的決定是由人工智慧的輔助作成時，即不免必須分析正當程序、禁止差別待遇與決策透明度的爭議。換言之，在人工智慧時代下，行政機關如何才能確保自己在依賴人工智慧當作自動化決策的工具時，不至於遭遇違法的挑戰，並且讓機器學習的結果不會導致政府失控的結果，以及確保機器學習的運作過程不至於違背法律的核心理念，讓機器學習能夠在提高政府機關的行政管制效率時，也符合行政法基本原理原則的要求。

---

102 *See, e.g.*, Cary Coglianese & David Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105 GEO. L.J. 1147 (2017).

103 就美國行政法的發展歷史來看，法院最初是認為國會不得將憲法所賦予之立法權，授權給行政機關以行政命令的方式，去補充法律的不足之處，也就是所謂的「禁止授權原則」（non-delegation doctrine），可參見美國聯邦最高法院1892年的判決，也就是Field v. Clark, 143 U.S. 649 (1892)。隨著時代的演變與行政管制事務複雜性的增加，因為絕對的禁止授權很難符合實際需要，美國聯邦最高法院終於在J.W. Hampton, Jr. & Co. v. United States, 276 U.S. 394 (1928)一案中，提出「明確原則」（intelligible principle，亦可翻譯成明白易懂之原則，或清晰原則）畫出立法授權的界線所在，藉以舒緩禁止授權原則所造成的嚴酷限制。換言之，倘若立法機關在進行立法授權時，附有明白易懂的原則，即可為之。如此一來，禁止授權原則的內涵，便不再是所謂的「禁止」，而是轉而成為有條件之授權原則，也就是只有在不符明確原則的情況下，才禁止國會授權。雖然美國學界對於明確原則爭辯不休，但是，在Whitman v. American Trucking Association, Inc., 531 U.S. 457 (2001)。這個判決中，美國聯邦最高法院的多數意見，依然認為禁止授權原則適用之際，應該以明確原則當作判斷基準，司法者並未禁止授權原則。關於學界對禁止授權原則和明確原則的批評，*see* Steven F. Huefner, *The Supreme Court's Avoidance of the Nondelegation Doctrine in* Clinton v. City of New York*: More than "A Dime's Worth of Difference"*, 49 CATH. U. L. REV. 337 (2000); Eric A. Posner & Adrian Vermeule, *Interring the Nondelegation Doctrine*, 69 U. CHI. L. REV. 1721 (2002).

機器學習雖然具有許多優點，例如預測發展趨勢和提高決策準確度等優勢，但是，如前所述，機器學習也具有「黑箱」（black box）的本質，也就是無法得知在提供了資料給演算法之後，到底決策如何作成、該決策和所提供資料間之間關係究竟如何等等內涵，究諸實際，這樣的機器學習特色，和行政法的基本原理原則之間有重大關聯性。近年來美國各州利用演算法當成行政管制措施與決策的工具，並藉以評估行政管制措施或施政的風險等，越來越常見[104]。至於在聯邦政府層級，無論是環保署、郵政總局、海洋大氣署和食品藥物管理署等部會，也都採用這種行政管制工具。換言之，許多行政機關都認知到巨量資料或大數據的重要性。更進一步而言，機器學習因為自我學習、黑箱本質及縮短或繞過人類決策的特性，與其他數據工具相較之下，功能更為強大，也因此更受到美國地方與聯邦行政機關的青睞。例如使用機器學習協助行政機關進行風險預測，便是常見的運用類型。這種自動化決策固然具有比過去準確的特性，而且所花費的資源也比較少，但是，機器學習的特色，自然也包括同時減少了人類實質涉入的空間，並且難以解釋行政管制結果背後的具體理由。

可以想見的是，在行政機關沒有裁量空間的行政管制領域裡，使用演算法來進行判斷，以及用人工智慧履行制定規範的任務，具有相當吸引力，但是，若是人工智慧成熟到可以順利運用在行政機關需要行使裁量權的決策上，則可能是更吸引人之處。一般而言，在透過人工智慧科技制定行政管制規範時，機器學習至少到目前為止應該依然無法直接處理行政管制規範中複雜的面向，理由在於要理解行政管制規範背後的規範意旨，往往並不是透過機器學習單純

104 *See, e.g.*, STEPHEN GOLDSMITH & SUSAN CRAWFORD, THE RESPONSIVE CITY: ENGAGING COMMUNITIES THROUGH DATA-SMART GOVERNANCE (2014); Bechara Choucair, Jay Bhatt & Raed Mansour, *How Cities Are Using Analytics to Improve Public Health*, HARV. BUS. REV. (Sept. 15, 2014), https://hbr.org/2014/09/ how-cities-are-using-analytics-to-improve-public-health/ [https://perma.cc/R26N-7RU2].

的預測功能，就可以達成任務，而且，機器學習所產出的預測，也無法直接適用到預估行政管制規範在個案上的影響或解釋個案中的因果關係，也就是仍然很難完全取代人類在行政管制規範中的參與必要性。更何況，將機器學習運用於行政管制領域時，機器學習所需的資料，仍然必須先由人類蒐集、選擇與輸入，設定機器學習的目標，並且由人類參與判斷最終演算結果，無法將這一連串的必要過程予以自動化，否則難以想像。此外，如何蒐集到數量足夠的龐大資料，作為人工智慧的「學習資料」（learning data），也是另一個相當大的挑戰。姑且不論上述有關機器學習在轉變行政管制面貌上會遭遇哪些挑戰，當機器學習涉及取代人類判斷時就容易產生爭議，也會引起是否符合行政法與憲法的基本原則的質疑。

使用人工智慧或機器學習科技來從事行政管制，除了在學界已經廣泛討論的倫理與隱私爭議[105]之外，還有可能會涉及逾越授權的爭議，亦即無論是在憲法層次，或是在立法層次與行政層次，都可能有此一方面的疑慮。除此之外，本文所關切的正當法律程序，恐怕也會成為人工智慧時代行政管制領域的重要議題之一。

授權給非人類而是機器去從事行政行為，對法院來說，由於很難直接將機器和人類等同視之，所以，就禁止授權原則[106]的觀點來看，會產生不少典型的公法爭議，其中恐怕以在諸如此類由機器學

105 Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 96 (2014); Roger Allan Ford & W. Nicholson Price II, *Privacy and Accountability in Black-Box Medicine*, 23 MICH. TELECOMM. & TECH. L. REV. 1, 3-4 (2016); Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1170-71 (2015); Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 395-97 (2014); Neil M. Richards & Jonathan H. King, *Three Paradoxes of Big Data*, 66 STAN. L. REV. ONLINE 41, 42-43 (2013) [hereinafter Richards & King Three Paradoxes]; Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63, 65 (2012).

106 *See, e.g.*, Cass R. Sunstein, *Nondelegation Canons*, 67 U. CHI. L. REV. 315, 322 (2000).

習支持的行政管制模式下，究竟是否有能夠符合權責原則要求的人類扮演最終的把關角色，最為關鍵[107]。或許，若是行政機關要使用機器學習系統去處理行政管制上的法規選擇問題，在確保其客觀性與一致性之餘，至少要符合禁止授權原則的要求，畢竟，至少就目前而言，機器學習科技對於行政管制領域而言，應該只是行政管制工具之一而已，與其他憲法允許使用的行政管制工具並無不同，所以也不該脫逸於禁止授權原則的規範之外。

就國會立法層次的授權而言，主要爭議焦點應該在於機關對於機器學習演算法的依賴程度，是否會超出國會透過立法文字賦予行政機關的授權。以美國行政法的判決當作觀察對象，固然法院對於行政機關可以使用哪些管制工具協助其作成管制決定，向來仍賦予行政機關相當程度的選擇空間，可以基於其管制需求、管制能量和不同層級機關的特性，在立法授權範圍內行使一定的裁量權[108]，然而，由於司法機關過於尊重行政機關行政管制決定的質疑從未間斷且日漸強烈[109]，所以，不能排除若有觸及禁止授權原則的紅線，法院還是可能會斷然否決行政機關採取機器學習行使行政管制權力所得的管制結果，甚至，也不能排除日後國會可能會立法禁止特定機關或所有機關在某些行政管制事項或領域上從事授權。

除了禁止授權原則如何解釋適用之外，正當法律程序所提供的憲法保護，在人工智慧時代中將出現何種面貌，則是更值得關切。究諸實際，從個人權利保護的觀點來看，在人工智慧時代裡，行政

107 *See, e.g.*, Cary Coglianese, *Presidential Control of Administrative Agencies: A Debate over Law or Politics?*, 12 U. PA. J. CONST. L. 637, 646 (2010); Cary Coglianese, *The Emptiness of Decisional Limits: Reconceiving Presidential Control of the Administrative State*, 69 ADMIN. L. REV. 43 (2017).

108 *See, e.g.*, David J. Barron & Elena Kagan, *Chevron's Nondelegation Doctrin*e, 2001 SUP. CT. REV. 201 (2001).

109 *See, e.g.*, Ronald A. Cass, *Vive la Deference?: Rethinking the Balance Between Administrative and Judicial Discretion*, 83 GEO. WASH. L. REV. 1294, 1319-26 (2015).

機關依靠機器學習系統做出判斷與決定，有無可能違反憲法所要求的正當法律程序原則，可能更值得關注。以美國行政法為例，依據*Mathews v. Eldridge*[110]此一判決中所建立的標準，法院認為，政府如果要僅依據書面文件的審查，未經事前聽證程序而針對人民權益事項作成判斷，針對這類行政程序，檢驗其是否滿足正當法律程序的標準，除了人民的權益必須受到該行政決定的影響，以及衡量透過系爭程序錯誤剝奪人民權益風險和提供額外或替代程序予以保障的可能利益外，關於因該程序所帶來的政府利益，包含所涉及之政府功能、政府財政與行政負擔，都應該考量在內。該判決也指出正當法律程序是具有彈性的，可以根據特別情況需求提供正當法律程序以保護人民權益。

根據上述檢驗標準，當機器學習科技運用在行政程序中時，到底能促進怎樣的政府利益，就有檢視必要。例如機器節省大量聽證程序所需耗費的經費，或者運用機器學習作成決定，和以人類作成決定相較之下，可以更容易避免錯誤剝奪人民權益，那麼採用機器學習科技，就可以說是具有促成正當法律程序之價值。同時，如果機器學習作成的行政決定錯誤率夠低，法院針對仰賴該演算法系統作成的決定，似乎也沒有理由僅僅因為行政機關運用演算法從事行政管制而加以反對。然而，這是否表示行政機關仰賴機器學習做判斷時，不需要由獨立超然的分析專家來擔任檢驗角色，或者是在仰賴機器學習制定管制規範之前，應該先通過專家諮詢委員會審查，或者至少必須通過同儕審查，都是人工智慧時代具有研究價值的治理議題。更值得注意的是，是否滿足正當法律程序的要求，必須要從系統的運作過程及其運作結果來判斷，但是，截至目前為止，依然沒有任何成熟而固定的判斷標準可言，唯一可以確定的，或許是，若是透過演算法所作成的決定，可以避免人類所製造的偏誤，

110 *Mathews*, 424 U.S. 319, 323-25.

而得到優於人類判斷的結果，應該就可以滿足正當法律程序的要求。所以，未來關於人工智慧或機器學習在正當法律程序原則下可能衍生而值得探討的議題，應該是個豐富的公法寶藏。

整體而言，姑且不論機器學習或AI科技可能引發的資訊隱私保護問題，早已是受到關注的議題[111]，例如，Neil M. Richards與Jonathan H. King兩人在多年前的合著論文中便已指出，大數據演算科技應用到線上行為時，可能便是意味著「隱私的終結」（the end of privacy）[112]，因為這類技術可以假借要讓數百萬的線上使用者的行動更加透明且提升效率之名，對掌握權力者完全公開，但是，相對地，掌握權力者相對於一般使用者來說，卻是藏身於神秘與不透明之中。因此，論者主張應該嚴肅考慮引入新的規範形式，讓大數據與人工智慧等仰賴演算法的科技，得以公開受到政府的管制、稽核，甚或在必要時，對掌握演算法權力者施以管制與懲處，也就成為美國法學界關注的研究議題[113]。例如Danielle Keats Citron提倡「科技的正當程序」（technological due process）[114]，或者Oren Bracha和Frank Pasquale兩人主張美國應該創設一個全新的政府機關，例如稱為「聯邦搜尋委員會」（Federal Search Commission）[115]，職司檢視搜尋黑箱並確認是否因之發生不當或不法的操控，都是在此一人工智慧時代特有的研究議題下，所提出的具體主張。

換言之，仰賴演算法作成決策，主要挑戰之一在於如何確保適當的透明度，以符合課責要求。舉例而言，倘若行政機關作出的決

111 *See generally* Ryan Calo, *Peeping HALs: Making Sense of Artificial Intelligence and Privacy*, 2 EUR. J.L. STUD. 168 (2010).

112 *See* Richards & King, Three Paradoxes, *supra* note 105.

113 *See* Neil M. Richards & Jonathan H. King, *Big Data and the Future for Privacy*, *in* RESEARCH HANDBOOK ON DIGITAL TRANSPORTATIONS 272 (F. Xavier Olleros & Majlinda Zhegu eds., 2016).

114 *See* Citron, *supra* note 1.

115 *See* Oren Bracha & Frank Pasquale, *Federal Search Commission - Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149 (2008).

定，其唯一理由是機器學習結果建議如此決定，那麼，是否可以算是適當的判斷，以及其判斷理由是否可以上述機器學習結果當作唯一解釋，均不無疑問。畢竟，行政機關作成決定時，必須說明理由，而在機器學習的情境下，為了滿足此一要求，行政機關必須解釋其在機器學習上所使用的預設與方法，而法院也必須在獲得合理合法的解釋時，才能履行把關行政機關決定的責任，因此，關於機器學習之使用，是否應該要求行政機關揭露其選擇、方法、輸入變量等等，揭露程度與範圍又該多大，在人工智慧時代，也是依然討論法院針對行政機關作為的實質審查對象、程度與範圍時，難以迴避的問題。然而，不可否認的是，除了提供決定理由之外，還必須負擔揭露義務，對於仰賴人工智慧或機器學習作成決定的行政機關而言，恐怕非常難以徹底實踐。究竟應該用何種適度保護個人資料的方法揭露，並且避免資訊過度揭露，當然也是人工智慧時代下正當法律程序原則必須回答的一系列問題。

無論上述各種主張孰優孰劣，以及何者可採，這些論爭至少告訴我們，人工智慧科技對公法研究所帶來的衝擊，就是一連串嶄新的差別待遇與正當法律程序爭議。的確，從歷史經驗來看，傳統的行政管制系統，往往有過度僵化、官僚、沒有彈性以及速度緩慢而難以適應新現實等傾向。無論人工智慧應用的未來規範方向如何，法律規範在面對人工智慧的「預測」和「決策」特色時，都應該嚴肅以對。以前面所舉的各個例子而言，人工智慧科技預測出來的結果與或者因此作成的各種決策，倘若被認為可以當成社會福利或健康保險的決策基礎，或者當成大規模監控的工具，甚至可以當成行政決定甚或刑事處罰的依據時，應該如何落實「正當法律程序」的基本要求[116]？甚至，以人工智慧科技從事預測和決策「過程」是否及應該如何規範？在法律規範面向上，應該如何評價在人工智慧所

116 *Cf.* ANDREW G. FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017).

導引出來的預測和決策「結論」？對於「人」在這類預測和決策中的參與程度，是否及應該如何要求？換言之，「人」在這類人工智慧所導引的預測和決策過程中，究竟應該扮演何種角色，才能維護正當法律程序原則所要維護的憲法價值，恐怕是終極問題。

歸結起來，恐怕不難發現，當公部門運用人工智慧或機器學習科技時，演算法其實占據相當核心的地位，因此，應該採取怎樣的規範模式，追求以「負責的演算法」（accountable algorithms）作成決策結果，應該是探討正當法律程序原則如何落實時的重點。換言之，在人工智慧與機器學習應用上的「解釋」與「透明」所要確保的決定公正性，如何落實，尤其，法制設計上應該如何容許個人在符合一定條件時，選擇「退出」由人工智慧作成的決策，可能都是「負責的演算法」應該涵蓋的範疇。

從正當法律程序所強調的程序保障觀點來看，在可見的未來，隨著機器學習和演算法變得越來越複雜，當其應用在行政管制領域時，大致上會面臨兩個主要困難，也就是「可預測性」（predictability）和「可解釋性」（explainability）這兩個困境。然而，從行政管制歷史來看，可解釋性和可預測性的規範，並不是全新的行政管制問題。在極其複雜的系統上應用的科技，早已面臨這些挑戰，例如藥物的研發便是典型的實例。當某一公司開始開發這些藥物時，對於「為什麼會證明有效」的假設，也往往帶有高度猜測成分。其次，即使藥物在其預期的用途上，被證明為有效，也很難預測其副作用，例如，當Pfizer發現Viagra是治療性功能障礙的有效方法時，事實上是將Viagra當成治療心臟病的藥物進行研發，同樣地，Rogaine是先將治療高血壓的藥物Loniten上市之後，才被發現其具有促成頭髮再生的功能，都是療效和副作用很難預測的知名實例[117]。

117 *Id.* at 102-03.

其實，人類也是很難預測及解釋的。例如，當我們以法律提供某些誘因（incentives）或權利（entitlements），企圖改變被管制者的行為時，也很難預知其是否有效，即使有效，也不見得能預測所有的附帶效果。進一步言之，基於人工智慧和機器學習的上述特性，預測難度可能更甚於此。換言之，倘若某一演算法的可預測性不足，那麼該演算法就可能比我們所知道的更危險，如果該演算法的可理解性不足，那麼要知道如何糾正其有問題的演算結果，則是難上加難。究其實際，很可能連要探知哪個產出結果可能有問題的，也非常困難。更何況，有許多演算法不但是運作方式不透明，甚至還可以受到商業機密的法律保護。如此一來，若要確保演算法的應用不偏離正當法律程序的要求，必然要面對演算法的責任難以衡量、演算法的責任難以追查、人的責任難以歸咎等等難以迴避的困難問題。

綜合本文所述，若要確保人民在人工智慧或自動決策時代的正當法律程序權益，則必須確保提供給人民的，是有效的受通知權保障，而此一保障則必須建立在前述的稽核紀錄上。完整的決策系統稽核紀錄，不但是司法審查不可或缺的要素，也可以幫助減少行政機關克服「電腦不會出錯」的自動化偏見。

不過，值得注意的是，要達成上述基本目標，首先需要行政機關建立起人工智慧或自動化決策系統可能會出錯的基本認知，同時，行政機關也必須負擔起詳細解釋其決定的責任，尤其是其為什麼仰賴人工智慧或自動化決策系統作成決定。再者，有效的救濟程序，更是科技時代的正當法律程序原則必須確保的底線，而這就可能必須重新檢視在科技時代或已不合時宜的成本效益分析架構，以確保人民在科技時代仍能行使有效的聽證權。

陸、結論

2016年美國執法機關在調查一起大規模槍擊案時，曾經向聯邦法院提出聲請獲准，命令蘋果公司必須協助執法人員進行搜索，解鎖其產品即蘋果手機，當時蘋果公司執行長Tim Cook發表公開聲明反對法院的命令，主張系爭命令將創下負面前例，並且呼籲美國社會應該公開討論資訊安全性等問題[118]。此一公開聲明再度引發社會大眾注意到執法需求、公共安全、新興科技和隱私保障等數者之間錯綜複雜關係的重要性。但是，即使如此，嗣後美國國會罕見地出現兩黨合作促成、以保護人民電子郵件通訊免於監控的「電子郵件隱私法草案」（Email Privacy Act），仍因適逢大規模槍擊案的發生，該草案從未曾在參議院進行投票[119]。這類因為新聞事件的出現而導致隱私權保護的立法決策起落不定的現象，備受詬病[120]，但不幸卻正是在新興科技不斷發展下已經過時或不足的正當法律程序保障所面對的當代社會脈絡，導致科技（化）正當法律程序的法制，遲遲難以完善建構。

從另一個角度來看，美國憲法增修條文第4條的正當法律程序原則，過去一個世紀以來的發展軌跡，幾乎是由科技發展的陰影所鋪成的。在各種行政措施與執法行為不斷科技化與自動化的當代趨勢下，政府除了不斷強調科技執法之名外，也以追求效率、節省成本、作成一致決定等好處，不斷嘗試引進人工智慧或自動化決策於行政程序之中。然而，相對地，在本文所討論的科技化與自動化的

---

118 Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), https://www.apple.com/customer-letter/.

119 *See* Erin Kelly, *Senate Derails Bill to Rein in E-mail Surveillance*, USA TODAY (June 9, 2016), https://www.usatoday.com/story/news/politics/2016/06/09/senate-derails-bill-rein-email-surveillance/85641196/.

120 *See, e.g.*, Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 632-33 (2017).

趨勢下，或許，正當法律程序原則實質上已經轉化成必須迫使我們以「科技正當法律程序」原則的角度來分析與思考的狀態，亦即我們不得不思考和分析正當法律程序所欲追求的憲法價值，是否正歷經一場空洞化的危機甚或戰役。

如同本文的分析，美國憲法增修條文第4條基於正當法律程序所要求的搜索令狀原則，在當代法院見解趨勢下，對於個人隱私所提供的保護，實屬有限。首先，長期以來，美國聯邦最高法院在諸多不同的脈絡下，都認為凡是當事人自願提供給第三人的資訊，便無法再享有美國憲法增修條文第4條所保護的合理隱私期待。甚至，縱使當事人最初提供給第三人的資訊，是以限制目的或私密方式提供給第三人，也無例外。*Smith v. Maryland*這個指標性的判決，認定個人對於自己撥打的電話號碼沒有合理隱私期待，理由即是其所撥打的號碼此一資訊，是自願提供給電信公司，所以政府可以取得。同樣的論理邏輯，也可能出現在網路通訊的相關資訊上，例如網址、網站、電子郵件等等，均可能因此不受美國憲法增修條文第4條的正當法律程序保障[121]。雖然，如前所述，此一論理邏輯，近年來曾遭到自由派Sotomayor大法官的反對，批評這種解釋合理隱私期待的方式，根本無從處理數位時代的爭議[122]，學說見解中抱持類似立場者也所在多有[123]，但是，在聯邦最高法院近期所作成之關於通訊資料的*Carpenter*判決，法院依然拒絕重新檢視第三人

121 *See also* Michael Pollack, Taking Data, 86 U. CHI. L. REV. 77, 85-86 (2019).

122 *Id.* at 86-87.

123 *See, e.g.*, LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND SURVEILLANCE IN A DIGITAL AGE (2016); Marko Milanovic, *Human Rights Treaties and Foreign Intelligence: Privacy in the Digital World*, 56 HARV. INT'L L.J. 81 (2015); Peter Ormerod & Lawrence J. Trautman, *A Descriptive Analysis of the Fourth Amendment and the Third- Party Doctrine in the Digital Age*, 28 ALBANY L.J. SCI. & TECH. 73 (2018). Joel R. Reidenberg, T*he Data Surveillance State in the United States and Europe*, 49 WAKE FOREST L. REV. 583 (2014); Ira S. Rubenstein, *Privacy Localism*, 93 WASH. L. REV. 1961 (2018); Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681 (2018).

原則，認為該案仍應適用第三人原則。可以預見的是，除非美國聯邦最高法院在關於第三人原則的解釋適用上，明顯朝向願意積極維護人民在科技時代中所得享有的正當法律程序此一基本權益的方向發展，否則，人民關於合理隱私期待的期待可能性，恐怕仍有一段相當漫長的不合理路程，有待跋涉[124]。尤其是在這類案件中扮演第三人角色的電信業者與網路業者，往往很少挑戰政府的執法方式，或者即使提出挑戰也未能獲致成功結果[125]，更使這個隱私保護的漏洞難以填補，導致正當法律程序保障的徹底落實，更是難以樂觀期待。

124 *See* Pollack, *supra* note 121, at 88.
125 *Id.* at 88-89.

參考文獻

1. 中文部分

李榮耕（2015），科技定位監控與犯罪偵查：兼論美國近年GPS追蹤法制及實務之發展，臺大法學論叢，44卷3期，頁871-969。

張君魁（2016），論預防性國家監控之憲法界限，國立臺灣大學法律學研究所碩士論文。

張陳弘（2018），美國聯邦憲法增修條文第4條搜索令狀原則的新發展：以Jones, Jardines & Grady案為例，歐美研究，48卷2期，頁267-332。

2. 外文部分

Barron, David J., and Elena Kagan. 2001. Chevron's Nondelegation Doctrine. *The Supreme Court Review* 2001:201-265.

Berman, Emily. 2017. When Database Queries Are Fourth Amendment Searches. *Minnesota Law Review* 102:577-638.

Bilgic, Secil. 2018. Something Old, Something New, and Something Moot: The Privacy Crisis under the CLOUD Act. *Harvard Journal of Law & Technology* 32:321-355.

Bracha, Oren, and Frank Pasquale. 2008. Federal Search Commission - Access, Fairness, and Accountability in the Law of Search. *Cornell Law Review* 93:1149-1210.

Brennan-Marquez, Kiel, and Andrew Tutt. 2017. Offensive Searches: Toward a Two-Tier Theory of Fourth Amendment Protection. *Harvard Civil Rights-Civil Liberties Law Review* 52:103-144.

Calo, Ryan. 2010. Peeping HALs: Making Sense of Artificial Intelligence and Privacy. *European Journal of Legal Studies* 2:168-192.

Cass, Ronald A. 2015. Vive la Deference?: Rethinking the Balance Between Administrative and Judicial Discretion. *George Washington Law Review* 83:1294-1329.

Citron, Danielle Keats. 2007. Technological Due Process. *Washington University Law Review* 85:1249-1314.

Coglianese, Cary. 2010. Presidential Control of Administrative Agencies: A Debate over Law or Politics?. *University of Pennsylvania Journal of Constitutional Law* 12:637-650.

——— 2017. The Emptiness of Decisional Limits: Reconceiving Presidential Control of the Administrative State. *Administrative Law Review* 69:43-82.

Coglianese, Cary, and David Lehr. 2017. Regulating by Robot: Administrative Decision Making in the Machine-Learning Era. *Georgetown Law Journal* 105:1147-1223.

Crawford, Kate, and Jason Schultz. 2014. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review* 55:93-128.

Donohue, Laura K. 2016. *The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age.* Cambridge, MA: Oxford University Press.

——— 2017. The Fourth Amendment in a Digital World. *Annual Survey of American Law* 71:553-686.

Ferguson, Andrew G. 2017. The "Smart" Fourth Amendment. *Cornell Law Review* 102:547-632.

——— 2017. *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York, NY: NYU Press.

Ford, Roger Allan, and W. Nicholson Price II. 2016. Privacy and Accountability in Black-Box Medicine. *Michigan Telecommunications and Technology Law Review* 23:1-44.

Freiwald, Susan, and Stephen Wm. Smith. 2018. The Carpenter Chronicle: A Near-Perfect Surveillance. *Harvard Law Review* 132:205-235.

Goldsmith, Stephen, and Susan Crawford. 2014. *The Responsive City: Engaging Communities Through Data-Smart Governance.* San Francisco, CA: Jossey-Bass.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State.* New York, NY: Metropolitan Books.

Huefner, Steven F. 2000. The Supreme Court's Avoidance of the Nondelegation Doctrine in *Clinton v. City of New York*: More than "A Dime's Worth of Difference". *Catholic University Law Review* 49:337-428.

Kerr, Orin S. 2004. A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It. *George Washington Law Review* 72:1208-1243.

——— 2011. An Equilibrium-Adjustment Theory of the Fourth Amendment. *Harvard Law Review* 125:476-543.

——— 2014. The Next Generation Communications Privacy Act. *University of Pennsylvania Law Review* 162:373-419.

Kris, David. 2014. On the Bulk Collection of Tangible Things. *Journal of National Security Law and Policy* 7:209-296.

Kroll, Joshua A., Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson, and Harlan Yu. 2017. Accountable Algorithms. *University of Pennsylvania Law Review* 165:633-705.

Margulies, Peter. 2016. Surveillance by Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights. *Florida Law Review* 68:1045-1118.

Milanovic, Marko. 2015. Human Rights Treaties and Foreign

Intelligence: Privacy in the Digital World. *Harvard International Law Journal* 56:81-146.

Ohm, Paul. 2015. Sensitive Information. *Southern California Law Review* 88:1125-1196.

Ormerod, Peter, and Lawrence J. Trautman. 2018. A Descriptive Analysis of the Fourth Amendment and the Third- Party Doctrine in the Digital Age. *Albany Law Journal of Science & Technology* 28:73-149.

Pollack, Michael. 2019. Taking Data. *University of Chicago Law Review* 86:77-141.

Posner, Eric A., and Adrian Vermeule. 2002. Interring the Nondelegation Doctrine. *University of Chicago Law Review* 69:1721-1762.

Reidenberg, Joel R. 2014. The Data Surveillance State in the United States and Europe. *Wake Forest Law Review* 49:583-608.

Richards, Neil M., and Jonathan H. King. 2013. Three Paradoxes of Big Data. *Stanford Law Review Online* 66:41-46.

——— 2014. Big Data Ethics. *Wake Forest Law Review* 49:393-432.

——— 2016. Big Data and the Future for Privacy. Pp. 272-290 in *Research Handbook on Digital Transformations*, edited by F. Xavier Olleros & Majlinda Zhegu. Cheltenham: Edward Elgar Publishing.

Rubenstein, Ira S. 2018. Privacy Localism. *Washington Law Review* 93:1961-2050.

Schwartz, Paul M. 2018. Legal Access to the Global Cloud. *Columbia Law Review* 118:1681-1762.

Seeley, Caleb A. 2016. Once More unto the Breach: The Constitutional Right to Information Privacy and the Privacy Act. *New York University Law Review* 91:1355-1385.

Severson, Daniel. 2015. American Surveillance of Non-U.S. Persons:

Why New Privacy Protections Offer Only Cosmetic Change. *Harvard International Law Journal* 56:465-514.

Solove, Daniel J., and Paul M. Schwartz. 2011. *Information Privacy Law*. 4th ed. New York, NY: Wolters Kluwer Law & Business.

Sunstein, Cass R. 2000. Nondelegation Canons. *University of Chicago Law Review* 67:315-343.

Tene, Omer, and Jules Polonetsky. 2012. Privacy in the Age of Big Data: A Time for Big Decisions. *Stanford Law Review Online* 64:63-69.

Yoo, John. 2013. The Legality of the National Security Agency's Bulk Data Surveillance Programs. *Harvard Journal of Law & Public Policy* 37:901-930.

Constitutional Implications of Technological Due Process of Law:

An Analysis of American Law

*Ching-Yi Liu**

Abstract

This Article focuses the idea of "technological due process of law" and examines its developments, including theorie and court decisions, in the American legal system. This Article first analyzes the doctrinal development of due process of law and how it presents the characteristics of being constantly followed and surrounded by technologies. With this understanding, it further explores the difficulties law enforcement agencies encounter when facing the application of various technologies, and the due process of law dilemmas and controversies that have arisen from the difficulties. This Article takes the U.S. government's large-scale surveillance program as an example to analyze why the principles of due process of law cannot anymore fulfill its fundamental function of protecting people's rights. At the same time, this Article also uses the controversies over automated decision-makings to illustrate the due process of law challenges in the age of artificial intelligence. This Article proposes that as the protections provided by the principles of due process of law have become outdated and insufficient, the principle of due process of law must be transformed into "the principle of technological due process of law" and only by doing so, we are capable of seriously considering whether the constitutional values it

* Distinguished Professor, Graduate Institute of National Development, National Taiwan University.

was designed to pursue are experiencing unprecedented crisies in the coming automated society.

KEYWORDS: technological due process, technology-assisted law enforcement, mass surveillance, automated decision-making, artificial intelligence.