論大規模政府監控之資訊隱私保障
—評析美國聯邦法院相關裁判 *

林昕璇
中央研究院

摘　要

本文旨在探討當國家嫻熟地結合大數據應用與公權力措施，形成非以特定人爲標的、未連結到明確終端目的之大規模監控時，對於個人資訊隱私權的衝擊影響。本文以憲法學及比較法學做爲論述基礎，提出概念類分「大規模政府監控」的數項要素，繼之以美國聯邦法院相關指標性判決之理論發展與實踐經驗作爲索解癥結的他山之石，反思資訊隱私在數位時代下的概念內涵與保障架構是否有重構之必要及如何成爲可能。

本文耙梳美國聯邦法院近年關於政府電信監控訴訟後發現，儘管巨量數據監控已大幅度改變人民對於隱私的認知與預設，2013 年爆發的史諾登揭密案深刻呈現出美國聯邦法院於八十年代奠基於公 / 私領域二分邏輯所確立之「合理隱私期待」與「第三人理論」理論框架的缺陷。本文進一步引介「馬賽克理論」作爲補充式的解釋取徑並予以評價。

林昕璇　中央研究院法律學研究所博士後研究員，研究領域爲憲法、資訊法、政府監控法制、數位人權及武裝衝突法。

* 作者感謝各位匿名審稿人對本文所提出的精彩精闢的問題與寶貴修改建議，令本文獲益匪淺，得以在修正後有更清楚成熟的立論與辯證。亦感謝季刊編輯委員會的寶貴修正建議與季刊編輯部的協助校訂。本文初稿曾在中研院法律學研究所主辦之「第十一屆憲法解釋之理論與實務研討會」上發表，復經作者增補修改完成。對於未能於文中妥善處理之部分，作者期待在未來研究中繼續反省思考。

（收件：2019/7/5，修正：2019/12/9，接受：2020/2/20）

本文的結論是，美國聯邦司法權眾聲喧嘩的訴訟爭議與理論辯難，不僅勾勒大數據時代保障資訊隱私的迫切性，更催生資訊隱私權的典範轉移，朝向更彈性且適應社會眞實脈絡的範式轉變。其活絡豐富之司法經驗對於建構一個更符合資訊隱私保障的法律機制尤具參考價值，足堪提供我國若干啓發性意義。

關鍵詞：大規模政府監控、大數據、資訊隱私權、美國聯邦憲法增修條文第四條、第三人理論、馬賽克理論

壹、問題緣起與研究主題

2013 年 6 月由英國衛報披露的史諾登（Edward Snowden）揭密案[①] 震驚全球，隨著國家挾其通訊科技的強大力量，對全民發動「大規模監控」（Mass Surveillance，又稱預防性監控、大眾監控）的崛起，標誌「全面監控國家」（National Surveillance State）[②] 時代已然到來。

此等預先將人民資料儲存彙整之行爲，結合數位科技的蓬勃發展與大數據運算能力，使國家得以透過各式監控手段，大規模、輕易地將零碎片段、無意義的個人資訊加以蒐集、彙整、分析、儲存，進而鉅細靡遺地拼湊出人民私生活的圖像，對個人隱私權的潛在侵害，自不待言。公部門以反恐及諜報蒐集等國家安全之名，對不特定人施以大範圍、地毯式的數據蒐集、分析與探勘，也成爲各國政府屢見不鮮的現象。據此，凡此等以「不特定人民」[③] 爲蒐集對象，

① 2013 年 6 月，英國《衛報》（*The Guardian*）及美國《華盛頓郵報》（*The Washington Post*），先後報導前美國國家安全局外包技術職員 Edward Snowden 揭發之弊案，根據其披露之資料顯示美國國家安全局（NSA）近年以美國公民與外國人爲標的，遂行大規模監聽。其中最具代表性者爲稜鏡計畫（PRISM），指出美國國安局以反恐之名，授權美國情報體系任意存取網路公司所保有用戶之數據資料。此事件震驚全球，遂引發美國與歐洲各國對政府大規模監控之高度重視和嚴肅論辯（Gellman and Poitras, 2013; Greenwald and MacAskill, 2013）。

② 「全面監控國家」（National Surveillance State）此一名詞，係由耶魯法學院憲法學教授 Jack Balkin 提出，指涉政府以提升行政效率和國防安全爲名，透過通訊監察、數據蒐集、大數據探勘分析等新興科技，找出並確認行政治理的問題所在與解決途徑的國家治理手段，係「資訊國家」（Information State）在現代行政國家面對數位化趨勢必然發展出的治理型態（Balkin, 2008:3-5）。

③ 所謂「不特定人民」係相對於「個人資料蒐集爲限」的概念區分，個人資料係指具有人別歸屬之特性，得以連結到個人的資料類型。按我國《個人資料保護法》第 2 條第 1 款，對於個人資料的定義：「自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料」。同時，根據經濟合作發展組織（OECD）1980 年訂定之《隱私保護與個人資料跨境流通原則》（*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*），則以「經識別或可識別而得以連結到其資料主體的資料的資料」，來對個人資料進行定義。二者在本質定義頗爲雷同，僅我國個資法同時以列舉方式羅列得列入個人資料的類型，

且「未明確連結終端目的」④ 的國家監控類型，與傳統上以個案或犯罪偵查等特定任務作爲目標的國家監控手段截然不同，對個人隱私的潛在威脅亦不可等同視之。循此，本文試圖思索一個核心問題，在國家發動針對不特定人、廣泛性的大眾監控，持續衝擊人民隱私權益的當下，司法者如何重新審視資訊隱私權概念內涵與保障譜系的開展、擴充與重塑，乃至於國家必須透過什麼樣的「體制」和「程序」對何種人民「權利內涵」予以規制？

以此爲思考起點，大規模監控在憲法學可能存在下列若干值得關懷的研究焦點。第一、「大規模監控」指涉之意義內涵及行爲特徵爲何？應循何種標準予以類型化？第二、伴隨網路與資訊應用技術的創新變革，國家監控行爲發展出許多有別於以往傳統的新形貌，改變了監控科技的運作模式，對於身處全面監控網絡中的人民來說，是否造成資訊隱私的基本權干預，從而觸動了憲法法律保留原則的需求？應訴求的保護標的及保護領域又爲何？第三、美國學理與實務判決往復交鋒的正反辨證與衍生而來的機制選擇，又爲法律規範與資訊政策的幽微交界處開拓什麼新的研究地景與啓示意義？

但同時亦以「可得識別該個人」作爲概括性要件；相對而言，「非以特定人個資爲限（非針對特定人民）」之資料蒐集，指涉國家也會透過蒐集社會群體所共同組合型塑而成的聚集性資料內容，藉以攫取、認識並掌握爲達成公共任務的事實背景與所需知識。往昔此類不具個人識別性的數據，由於數量過於龐大，且性質零碎散亂，人腦無法理解其所能夠呈現的意義而甚無利用價值。然而，此情形在科技高度發展的資訊社會脈絡下產生了驟變，蓋本來無意義而零碎的數據經過聚集性彙整後，再輔以大數據演算法，往往能夠形成有效強大的知識工具，爲政府行政管理所用，從而爲國家機器之權力行使帶來擴張強化的效果（OECD, 2013）。

④ 論者指出，將「是否明確連結到終端目的」作爲一種指標，界定國家監控的區別實益在於，傳統意義上的國家監控行爲，會存在某種明確的終端目的。譬如東德政府設立之史塔西（東德國家安全部 Ministerium für Staatssicherheit, MfS，由於 Staatssicherheit 一詞的縮寫，而通常被稱爲 Stasi），監控數以百萬計的人民，係以黨政思想控制爲其最終應用之目的。再如司法體系中以犯罪偵查爲蒐集證據爲目的所發動之通訊監察，便是典型的個案性、任務性國家監控行爲。相對而言，在資訊時代，持有資料量的增加所象徵的利益被更加地凸顯，資料價值的提升，國家蒐集資料的誘因亦日趨加強，因而逐漸產生自始並未連結到特定終端目的，而先行將資料予以蒐集、儲存，等待後續需要時再取用的國家監控類型（張君魁，2016:33）。

就上開疑義，美國聯邦最高法院於 2013 年首度針對由國際特赦組織美國分會提起，控告美國國家安全局依據《涉外情報監控修正法》（*FISA Amendments Act* of 2008）⑤ 執行的海外監控違憲之 *Clapper v. Amnesty International USA* ⑥ 一案作成判決。儘管在系爭案件中，最高法院最終否定原告的訴訟適格（Standing），但人民與法院互動交鋒的法律戰，已爲大規模政府監控的憲法論辯揭開了序幕。隨後進一步在 *American Civil Liberties Union v. Clapper*（以下簡稱 *ACLU v. Clapper*）、⑦ *Klayman v. Obama* ⑧ 等訴訟中，圍繞電信網路監控的執法界線和合憲與否的爭論，也彰顯美國實務上奠基於「合理隱私期待」（the reasonable expectation of privacy protection test）與「第三人理論」（the third-party doctrine）的隱私權保障譜系，面對由國家發動的常態性、系統性，甚至是跨國境的電信監控時，遭遇前所未有的挑戰，亦暴露其人權保障的潛在漏洞。

爲回應上開問題意識，本文架構安排如次：第貳部分擬從「大規模監控」此一新興國家監控模式出發，以勾勒出大規模政府監控在現代資訊國家中所展現的特徵、具體類型，及其與傳統國家監控行爲之區辨。並且分析國家機器結合大數據帶來資訊科技變革之情境脈絡，如何重構國家與個人間資訊權力的流動。第參部分試圖透過比較法文獻分析，耙梳史諾登揭密案後，美國公民自由聯盟（ACLU）、國際特赦組織（Amnesty International USA）等公民團體，如何透過美國聯邦憲法增修條文第四條（以下簡稱美憲增修條文第四條或增修條文第四條），推衍出政府監控行爲構成搜索而須適用法院令狀原則之憲法誡命，據以主張其具備主張憲法爭點的當事人適格（Standing），並挑戰美國國安局所發動的大型電話監控計畫之合憲性。第肆部分援引學說理論，主張並論證全面

⑤ Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub.L. No. 110-261, § 122 Stat. 2436 (2008).

⑥ Clapper v. Amnesty International USA, 133 S.Ct.1138 (2013).

⑦ American Civil Liberties Union v. Clapper, 785 F.3d 787 (2015); American Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724 (2013).

⑧ Klayman v. Obama, 957 F. Supp. 2d 1, 39 (2013).

數位監控國家的成形，及衍生而來的資訊隱私的典範轉移，同時提出本文見解，最後爲結論。

貳、大規模政府監控之類型化與行爲特徵

一、大規模國家監控之行為定性與類型化

（一）區辨標準——是否以「特定人的個資作為蒐集對象」及是否「明確連結至終端目的」

當大數據與國家權力連結，將根本性重塑國家監控行爲的基本形貌。有論者透過「是否以特定人之個資蒐集爲限」[⑨] 與「是否明確連結到終端目的」[⑩] 爲區別標準，將大規模監控類型化如下：[⑪]

---

⑨ 論者指出，以「是否以特定人的個資做爲蒐集對象」作爲類型化指標的目的係爲回應我國《個人資料保護法》第 2 條對於個人資料之界定。該條規定以「經識別或可識別而得以連結到其資訊主體的資料」作爲概括性的個人資料要件。相對於傳統意義下的「個人資料」蒐集，過往國家對於聚集性資料之取得，因數量過於龐大且技術不足，並不存在蒐集的誘因與動機。但這個現象在大數據時代有了相當大的轉變，蓋演算法、資料探勘（data mining）等應用科技使海量資料的分析判讀變得容易許多，伴隨而來的龐大資訊利益，成爲國家執行公共任務的知識之鑰。因此「是否以特定人的個資作爲蒐集對象」成爲區辨傳統監控與大規模監控之關鍵分水嶺，亦是推敲當代民主憲政體制如何回應此一新興國家權力的展演型態的思考樞紐（張君魁，2016:30-31）。

⑩ 論者指出，以「是否連結到終端目的」作爲另一參據指標的原因在於，絕大部分傳統認知上的國家監控行爲，幾乎都會明確地連結到終端目的，例如前述註（4）所提及的東德史塔西在蒐集人民資料時，就是以黨政思想控制爲其最終應用之目的，此一傳統國家監控，其終端目的非常明確（思想控制、犯罪偵查），亦鎖定特定的監控相對人。時至今日，大數據開啓膨大的新型態資訊利益，資料量擴增所象徵的利益被明確顯化，掌握公權力的國家自然不會對這些潛力無窮的新形態資訊利益無動於衷，毋寧更有強烈誘因在不具備任何終端目的之前提，甚至欠缺法律授權的情況下，蒐集個人抑或聚集性資料，發動所謂「政府大規模監控」（張君魁，2016:33-34）。

⑪ 更多有關以「是否以個人資料蒐集爲限」與「是否連結到終端目的」作爲建構大規模監控概念體系之參據指標的相關論述（張君魁，2016:29-34）。

表一　大規模政府監控之類型化一—以個資類型與蒐集目的區分

	明確連結至終端目的	非明確連結到終端目的
特定人的個資蒐集	個案性、任務性	預防性
不特定人之個資蒐集	單純知識生產型	流刺網型

資料來源：張君魁（2016:35）。

1. 個案性、任務性國家監控

個案性、任務性之國家監控行爲，係以「特定人的資料蒐集」與「明確連結到終端目的」兩個區別基準構成之國家監控類型。此種政府監控，目的係爲解決特定、個案性、任務性的公權力執行，透過國家權力啓動蒐集、近用個人資料、進一步利用該等個人資料、應用在其終端目的用途之上。因此在時間與空間上形成高度緊密的關聯性，以求該特定目的之達成（張君魁，2016:35）。具體而言，本於犯罪偵查與證據蒐集之目的所發動之國家監控，即屬典型之個案性、任務型國家監控行爲（張君魁，2016:35）。

2. 單純知識生產性國家監控

單純知識生產型國家監控，是以「不特定人之個資蒐集」與「明確連結到終端目的」兩項參據構築的下位類型。政府部門藉由「匯聚性資料的蒐集」，輔以大數據演算法的分析處理，掌握行政治理所需知識，進而成爲國家權力進一步應用並連結（識別）到個人的手段，以促進行政權更有效的運作，對人民發揮更強的行政控制權（張君魁，2016:35）。例如，我國二十年來所建構的完整全民醫療紀錄數據（全民健康保險研究資料庫，2000）；衛生福利部自 101 年起開始推動的臺灣健康雲計畫（衛生福利部，2016）；上述計畫之下隸屬的四個子計畫包括加強個人健康紀錄和病例電子化交換系統建置的「醫療雲」；提升預防疾病觀念，與智慧型裝置結合，記錄健康狀況的「保健雲」子計畫；結合電子病例和實驗室傳染病通報系統，使得傳染病通報即時效率的「防疫雲」

等等均屬於國家係基於行政治理任務所需，明確連結至終端目的所發動的知識生產性國家監控之適例。

3. 流刺網型國家監控

流刺網型國家監控（dragnet surveillance），其特徵展現爲「未臻明確的終端目的連結」及「不特定人之個資蒐集」。美國媒體向以「流刺網型的國家監控」，指涉由史諾登案所揭發之美國國家安全局（National Security Agency，以下簡稱美國國安局或 NSA）長期監控美國境內電話紀錄等資料之廣泛蒐集現象（Kaufman, 2013; Kampmark, 2017）。根據史諾登在媒體上曝光的一系列 NSA 內部的機密文件，其中最具爭議的是「上游計畫」（UPSTREAM），以及「稜鏡計畫」（PRISM）。其運作方式是 NSA 長期以來在通訊公司架設秘密機房，使用通訊公司本身內建的乘載網際網絡的光纖來攔截、過濾及複製通訊內容（Greenwald and MacAskill, 2013; Sottek and Kopstein, 2013）；此一系列監控計畫的授權依據爲小布希政府於 2008 年通過之《涉外情報監控法修正案》（*The FISA Amendments Act of 2008*）中的 702 條款。根據該條款，美國情報機構只須憑藉司法部長（Attorney General）和國家情報總監（Director of National Intelligence）共同簽發的監聽命令即可向 Google、微軟、Facebook 或電信業者調閱國外用戶的通訊紀錄，繼而運用搜尋程式進行資料探勘的分析檢索萃取，滴水不漏地攫取任何可能涉及國家安全及反恐調查的情資（Greenwald and MacAskill, 2013; Sottek and Kopstein, 2013）。

4. 預防性國家監控

最後一個下位類型爲「預防性國家監控」。預防性國家監控行爲是由傳統國家監控在面臨到資訊科技能力與其所帶來的影響下，所形塑出來的結果。屬於新興國家監控行爲態樣。由於資訊本身利用價值陡升，提供國家實施預防性監控的誘因，「不再像過去以終端目的之緊密連結作爲主要開啓的原因，而

是在終端目的之需求尚未被觸發時，或僅具備模糊、不夠明確的關聯性時，便提前廣爲蒐集、儲存人民個人資料，以待後續『可能』之利用」（張君魁，2016:36-37）。

（二）區辨標準二—監控標的「是否為美國公民」及「是否於美國境內實施」

另一規模監控的類型化標準來自美國情報監控法。《涉外情報監控法》（*Foreign Intelligence Surveillance Act*，以下簡稱 FISA），其立法背景是尼克森政權水門案醜聞事件曝光後的全面反思，國會通過該法嚴格限制情報機構對於涉及美國公民以及美國長期居住的居民之通信進行監聽的權力。FISA 作爲反恐怖活動、反間諜活動、情報收集活動及祕密司法程序的一部基本法，對電信監控、物理性搜查、通信紀錄與通信追蹤、使用商務紀錄等秘密調查手段有全面性規定。

《涉外情報監控法》適用的主要對象固然爲外國勢力（Foreign Power）及外國勢力的代理人（Agent of a foreign power），惟 FISA1801（c）明文在獲取外國勢力或外國勢力代理人的情報過程中，如果資訊涉及某一美國人，仍須適用 FISA 取得法院令狀始得啓動監控程序。[12] 又根據 FISA1801（f）小節關於「電子監控」（electronic surveillance）之定義，不論是 1801（f）（1）款「通過電子、機械或其他監控裝置『獲取』有線或無線通信的內容」；抑或 1801（f）（3）款「通過電子、機械或其他監控裝置『意圖獲取』有線或無線通信的內容；與 1801（f）（4）款「在美國境內安裝或使用電子、機械或者其他監控裝置進行監控獲取訊息」。法律皆明文當通信發出者或預期的接收者是位於「美國境內的美國人」或者「位於美國境內之人」，即有 FISA 之適用，從而須遵守取得法院令狀之正當法律程序，以保障該個人的隱私合理預期（Donohue, 2014:786-91; Blum,

[12] 50 U.S.C. §1801 (c).

2009:275-80）。[13]

911 事件後，美國制定通過《愛國者法案》（*US Patriot Act*），根據 215 條款，擴大範圍至有體物（tangible things）。因此根據 FISA1861 條規範，爲偵蒐秘密情報活動、反恐行動及其商業交易來往，聯邦調查局可以申請使用包括書籍、紀錄、紙張、文件在內的有體物。[14] 嗣後 2008 年通過《涉外情報監控法修正法》（*FISA Amendments Act*）702 條款正式授權監控計畫於符合（1）不得針對資訊蒐集時身處於美國境內之人；（2）不得針對美國境外的美國公民；（3）倘若監控目的係爲取得合理相信位於美國境內之人，不得爲之；（4）若信號傳送者與潛在接收者均於信號蒐集時位於美國境內，不得爲之[15] 等條件下，得以毋須取得法院令狀授權由國家安全局逕行發動。換句話說，僅須憑藉司法部長（Attorney General）和國家情報總監（Director of National Intelligence）共同簽發的監聽命令，即可對境外非美國公民發動爲期一年的電信監控（Liu, Nolan, and Thompson II, 2014; Milanovic, 2015; Severson, 2015）。[16]

綜上所述，美國政府藉由《涉外情報監控法》、《愛國者法案》215 條款，及《涉外情報監控法修正案》702 條款構築之監聽網絡，從法條結構與適用來看係以（1）是否具有美國公民身分（2）監控實施地點是否爲美國境內兩項構成要件定其法規授權依據及應遵守之法定程序（Clarke et al., 2014）：

表二　大規模政府監控之類型化二—以公民身分及地理位置區分

	美國境內	非美國境內
美國公民	原 FISA 條文—需取得法院令狀	原 FISA 條文—需取得法院令狀
非美國公民	原 FISA 條文—需取得法院令狀	Section 702 of FAA—不需取得法院令狀

資料來源：作者自行整理。

[13] 50 U.S.C. §1801 (f) (1) (3) (4).
[14] 50 U.S.C. §1861.
[15] 50 U.S.C. §1881 a.
[16] 50 U.S.C. §1881 a.

（三）行為定性釐清

本節試圖檢視比較法文獻及美國法律體系對政府大規模監控之適用狀況，並抽繹出數個共通特性。此種政府監控模式的特徵爲：（1）各種後設資料（Metadata）的蒐集與儲存係由網路電信業者所爲，政府部門係以立法課與業者配合義務之所謂「搭便車」的方式利用該等資料。（2）由於電信網路之後設資料可供辨識、解讀、比對的效能極高，對政府部門若欲用以進行大規模且未必有特定指涉對象的情報工作能帶來極大的效益，換言之，通信資料儲存義務化下的儲存範圍，即便是未涉及通訊內容（non-content data）（亦即通訊實質內容以外）之後設資料，在如今都足以輕易令有權調取的公權力機制掌握並解讀出非常驚人的個人身分特徵（蔡宗珍，2014:26）。也因爲上述特徵，使得此類以後設（巨量）數據爲核心的新興政府監控模式，性質上屬於一般性、預防性措施，監控的手段主要是透過種種科技措施而掌握足以追索至特定人或可得特定之人的資料，進而分析判讀出種種目的資訊；監控的目的通常是基於如辨識、防治恐怖份子、預測恐怖攻擊行動、基於國安需求的情報蒐集等。正因如此，當代政府監控本於其「系統性」、「常規性」，以及「連結到多元終端目的」之資料取得行爲，所引發的法治國原則與人權危害疑慮，以及法制上對應的思考重點，也自然逐漸與過去的傳統監控模式有所差異，從而形塑出「大規模政府監控」的概念內涵與輪廓樣貌。

（四）小結

網路時代與資訊應用技術的創新與變革，令國家監控行爲發展出諸多細緻複雜的樣貌。本節試圖類型化大規模政府監控以便釐清其概念內涵和權力運作模式。第一種標準根據「是否以特定人之個資蒐集爲限」與「是否明確連結到終端目的」爲參據，區分出個案任務型、單純知識生產型、流刺網型及預防型等四個象限，藉以作爲定性大規模政府監控的概念工具。第二種則是根據美國涉外情報監控法及相關修正案，以是否爲美國公民，及監控實施是否發生於該

國境內之公民身分（citizenship）與地點（location）爲基準，界定各自應遵守之法源依據。前者的區別實益在於強調本文聚焦的「大規模政府監控」，係有別於針對範圍較小、較特定的犯罪嫌疑人與具體事件所爲的個案監控（targeted surveillance），凸顯政府藉助數位科技的電信監控，往往屬於以公權力爲後盾並遊走於法治灰色地帶的預防性監控措施，得以精準反映所謂「大規模監控」與傳統監控的本質差異。第二種區辨標準，則導源自美憲增修條文第四條規範搜索之要件與正當程序，國家必須對美國公民承諾做到最小限度的監管和最大程度保障。

二、大數據結合國家監控的加乘效應

（一）巨量數據蒐集、儲存與探勘之數字化記憶

與傳統數據相比，大數據[17] 的眞正新穎之處在於數據量（Volume）、時效性（Velocity）、多變性（Variety）的處理。[18] 被稱爲大數據預言家的 Mayer-Schönberger 認爲大數據泛指「資料量達一定相當規模所能創設新市場價值之科技模式，沒有一定的規模就無法實現，且這些事將會改變現有市場、組織、公民與政府間的關係（林俊宏〔譯〕，麥爾荀伯格〔原著〕，2014:14）」。美國國家科學基金會（National Science Foundation）則將大數據定義爲「大規模、多樣化地將源自文件、感應器、網路交易、電子郵件和點選流資料等一切現今或未來可得來源之數據系統性彙整分類的資訊技術（National Science Foundation, 2014）」。美國隱私法學者 Daniel Solove 在連結巨量資訊與隱私權的關連與侵

[17] 大數據也稱爲巨量資料、後設資料、海量資料等概念相類似的名詞。事實上，其並未特定指涉某種資訊應用方式，而係泛稱面對超越傳統資料庫所能處理的數位化資料，以大量（high-volume）、快速（high-velocity）且多樣化（high-variety）的資訊當作資產，對非常大規模（massive）且極度複雜的資訊，運用最新的機器學習和人工智慧，應用在電腦上的處理過程（Gartner, Inc, 2013; Howie, 2013）。

[18] 由上述註 17 的定義可知，大數據和過去行之有年的資料、處理、分析不同之處在於數據係巨量（volume）、多樣（variety）和可快速（velocity）的處理。

害態樣時，將數據利用的進程區分爲三個階段，依序是「資訊蒐集」、「資訊檢索比對階段」、「資料散佈至第三人階段」，最後綜合上開資料的交叉運用導致侵犯個人隱私的結果（Solove, 2006:477）。

依循 Solove 提出的侵害階段基準，首先，以大數據的「蒐集行爲」來說，其範圍可遍及客機訂票資訊，車子 GPS 定位器的回傳、工廠機器感應性讀數等，透過大數據對資料蒐集、儲存與分析的技術提升與成本下降，大爲擴充了可使用的數據量與多樣性（林俊宏〔譯〕，麥爾荀伯格〔原著〕，2014:141-45）；又以網路用戶的線上互動情形爲例，如使用者點擊的內容、搜尋關鍵字，乃至瀏覽頁面的停留時間等，此類向來被視爲資料廢氣（data exhaust），零碎、片段，看似無法利用而無價值的數據，一旦以量化方式呈現，將成爲大幅助益企業改善現有服務產品或開發新產品之重要根據（林俊宏〔譯〕，麥爾荀伯格〔原著〕，2014:158-61）。其次，在後設資料的分析比對階段，亦可能透過數據的「重新組合」和「目的外使用」兩種途徑衝擊資訊隱私（林俊宏〔譯〕，麥爾荀伯格〔原著〕，2014:151-53）。首先，「重新組合」最典型的例子即整合多個資料庫的勾稽運用，比如保險業者透過信用紀錄、瀏覽的網站、每日看電視的時間等生活行爲數據，可輕易標定高血壓、糖尿病或憂鬱症的高風險保戶（林俊宏〔譯〕，麥爾荀伯格〔原著〕，2014:83）；另一方面，「目的外使用」則意味著數據的價值已經不侷限在原始蒐集目的，而擴大至延伸用途以增加其後續散佈、利用的價值。具體而言，僅僅蒐集電腦使用者瀏覽網頁的搜尋關鍵字，行銷人員即可透過搜尋流量的觀察與數據分析，整合勾稽出消費者的喜好，進一步延伸用途至投放個人化廣告或促銷活動等商業行爲（林俊宏〔譯〕，麥爾荀伯格〔原著〕，2014:148-50）。誠如上述，數據的多樣巨量整合帶來潛藏的龐大商機和強大的監控動能，將誘發國家與私人業者後續對數據無止盡、無上限地予以分析、散佈、再利用的強烈動機，對人民資訊隱私與資訊安全造成相當程度的侵蝕。

（二）公私領域模糊化下隱私邊界的消融位移

資訊科技的研發趨勢，使得人們愈來愈無法界定社交網絡和網路場域究竟是一種公共領域還是私人領域，傳統上以「公共空間 v.s. 私人空間」、「公共資訊 v.s. 私人資訊」的二元對立框架所建構的「隱私權」概念涵攝與保障架構，在應對超國界、超法域的數位化網路情境中愈趨難以適用（劉靜怡，2012）。一方面，人們不斷在社交網絡的場域中公開個人資訊，而這一場域也在不斷形塑人們公開個人資訊的慣習，眞實與虛擬的界線不再清晰可辨（劉靜怡，2012:17-22）。另一方面，這一個場域仍有其邊界，各種社群網路軟體（social networking software）所生產的訊息主要面向自身的社交網絡，資訊仍階層化細分，並投放於具體群體予以散布流傳，而非全然是一種漫無疆界、漫無目的的公開透明狀態（袁夢倩，2015:58-59；劉靜怡，2012:4-8）。因此，網路毋寧成爲介於公共領域與私人領域之間的資訊權力運作場域，若其再配合大數據演算法強大且整合性的數據處理能量，從中衍生的隱私風險和規範困境顯得益發嚴峻。

（三）不平等的資訊流動強化政府監控

當今巨量資料與法學界具有相當影響力的牛津大學網路研究所教授 Viktor Mayer-Schönberger 指出：「在信息權力與時間的交會處，永不遺忘的記憶創造了時間和空間的『圓形監獄』[19]（林俊宏〔譯〕，麥爾荀伯格〔原著〕，

[19] 英國哲學家邊沁（Jeremy Bentham）1785 年提出「圓形監獄」的構想，該設計讓一個監視者位於中央的高塔，便可全景式監視所有犯人，而犯人無法得知是否正受到監視而不得不「自我監視」。法國哲學家暨社會學家傅柯（Michel Foucault）承繼邊沁的理論，認爲圓形監獄機制已不限於監獄或實體建築，而成爲現代國家權力掌握宰制人民的抽象工具。就此，溝通理論家甘迪（Oscar Gandy）則將圓形監獄的概念，進一步與大規模監控（Mass Surveillance）的操作邏輯類比，主張監控本身並不直接產生統治，監控之所以有效達成，並非取決於監控工具或監控組織的強大，反而是必須基於被監視者具有「反監控」和渴望自由的強烈欲望，並因擔心自由之喪失而對監視進行一種恐懼心理的自我再生產，監視才會發揮其統治效力，這也構成傅柯提出「全景敞視監獄」（Panopticon）的論證前提之一（林俊宏〔譯〕，麥爾荀伯格〔原著〕，2015:23；劉靜怡，2012:45）。

2015:167）」。一方面，數據規模的爆炸式增長、數據模式的高度複雜化以及數據背後隱藏大量的經濟與政治利益，其所表現出的數據整合與監控力量遠超以往。另一方面，學者指出，由於數據主體和數據控制者的資訊與力量對比關係顯不對稱，個人很難全面掌握大數據的運作模式，導致數據主體對於其個人資訊被利用的眞實狀況往往難以自主控制，也缺乏對數據控制者使用個人資訊進行監督的權力與能力（袁夢倩，2015:57），遑論建立一套關於資料使用與風險評估的法律模式節制國家監控高權。以 Google 爲例，用戶或許享受搜尋引擎爲資訊獲取帶來的巨大便利，但個人憑藉自身有限知識，對 Google 正利用戶網絡行爲數據進行廣告的營利方式一無所知（林俊宏〔譯〕，麥爾荀伯格〔原著〕，2015:114-21, 140-41），更難以理解 Google 是如何運用演算法精密分析用戶執行的每一項操作與指令，透過蒐集資料廢氣以達到改善現有服務或開發新服務之目的（林俊宏〔譯〕，麥爾荀伯格〔原著〕，2015:156-61）。如同 Schönberger 的觀察：「大型企業或政府，往往會利用資訊權力的差異來獲得資訊優勢。資訊權力接踵而至地從無權者流向有權者，從被監視者轉向監視者（林俊宏〔譯〕，麥爾荀伯格〔原著〕，2015:141）」。不僅如此，大數據的深度挖掘技術可以深度挖掘、比對、交錯分析網路數據背後的隱匿關聯，每一個數據單元，每一個字節片段，每一個人在網路留下的數位足跡（Digital Footprint），都是構成一個人「隱私的血肉」（袁夢倩，2015:56）。換言之，在使用者獲取網路服務的那一刻起，人們已經被系統性、自動化的「縫合」進一種顯失均衡的個人資訊交換機制當中，無意識地參與維持並再製既存的、不對稱的資訊權力分配。促成了大數據時代這一「超級圓形監獄」權力機制的形成（袁夢倩，2015:57）。

數位圓形監獄的形成，給予國家權力介入的可乘之機，形塑出一種全新型態，力量更爲無遠弗屆的社會監視系統，史諾登揭密案再一次清楚彰顯了公權

力如何透過法律授權依據，[20] 憑藉法規範誡命的權威性與拘束力，責令私部門如 Microsoft、Google、Facebook、Youtube、Skype 以及 Apple 等網路服務提供者，對用戶的電子郵件、網上聊天紀錄、電話通訊進行大規模的挖掘、疊加與整合，將散落於數位世界中那些本無意義、零碎的巨量數據予以系統化的權力使用。

上述數位資訊洪流引發的爭議反映技術變革如同雙刃劍，一方面爲人類社會帶來生活機能升級的美好藍圖，另一方面也觸發新的危機。同時直指了問題核心—國家權力與大數據科技相結合據以形構的當代政府監控模式，將以個人資料的「蒐集」、「檢索比對」、「散佈」三個行爲階段貫穿脈絡，而透過這三種監控手段的複合式運用，足以使有權立法調取或蒐集的公權力機關掌握並解讀出非常驚人的個人身分特徵，現有法律護衛資訊隱私的保障功能可說喪失殆盡。

三、小結

美國國安局之監控計畫，不僅揭露國家機器以自身擁有的調查權監控人民這個既存已久的現實，更彰顯國家公權力早已熟稔如何藉由法令的授權、課予私人電信業者儲存客戶通聯紀錄之配合義務，或者透過行政權的強力介入、利用通訊與網路業者所掌有之電信網路資料實施監控。

正因如此，有關資訊隱私的內涵重構與伴隨而來的體系反思，其必要性與重要性不言可喻。與傳統偵防手法不盡相同的大規模監控措施衍生之法律訴訟，究竟應該採取什麼樣的合法控制？而新興國家監控模式的分殊化所衍生的

[20] 此處所稱之法律授權依據，於 ISP 業者所持有之電信數據或其他電子紀錄部分，美國國會於 1986 年通過 *Stored Communication Act*，根據該法 Section 2703，政府可通過法院令狀，要求 ISP 業者提供儲存在外部伺服器超過 180 天以上的電子郵件或其他電子紀錄。但若是儲存於伺服器少於或等於 180 天時，則強制必須向法院聲請搜索令狀使得爲之。另一方面，出於反恐考量所採行的電子監控措施之法律授權依據爲《涉外情報監控法》（*Foreign Intelligence Surveillance Act*）。

傳統隱私邊界的消融位移，從基本權利保障的角度以觀，是否觸動新的憲法價值選擇、法律保留原則及法規範建置的迫切需求？本文以下將針對近年備受矚目的大型後設資料監控爭議，耙梳美國聯邦法院相關指標性判決之法理論據及發展趨勢，並加以評析。

參、美國聯邦法院有關國家大規模監控之判決趨勢

一、史諾登揭密案後美國實務判決發展

（一）授權依據與運作模式

2013 年 Edward Snowden 在英國衛報上揭露美國國家安全局正在對全球通聯紀錄，不論是否爲美國公民，亦不論公民是否涉及不法行爲而達合理懷疑門檻，皆進行無差別（indiscriminately）和大規模（bulk）的蒐集（Greenwald and MacAskill, 2013; Gellman and Poitras, 2013）。

如同前述，由美國國安局主導，並以抗制恐怖活動爲主要目的之政府監控計畫之授權依據，可追溯至 1978 年美國國會制定《涉外情報監控法》。在當時立法背景下，鑒於愈來愈多以保護國家安全爲由，濫用無令狀電子監控的行爲，若任無令狀之國內情報蒐集活動持續氾濫擴大，將侵害美國公民受美國聯邦憲法增修條文第四條所保障的權利（Solove and Schwartz, 2011:377-84）。故立法者透過制定《涉外情報監控法》（*Foreign Intelligence Surveillance Act*，以下簡稱 FISA），授權並規範行政部門在以蒐集外國情資爲目的時，對通訊所爲之特定電子監控行爲（Solove and Schwartz, 2011:384-87）。

根據該法，政府在進行涉外情報監控活動前，需取得令狀，並依據 FISA 設立涉外情報監控法庭（Foreign Intelligence Surveillance Court，以下簡稱 FISC），專責管轄此種涉外情報監控的申請與核准（Solove and Schwartz, 2011:384-87）。爲配合政府祕密活動，FISC 是以秘密程序運作，且以僅由政府部門列席表示意見之單方程序（ex parte）進行令狀批准審查（Solove and

Schwartz, 2011:385）。嗣後 FISA 歷經數次修正，在監控的標的上，陸續增加了關於物理搜索、電話撥號紀錄器、通訊追蹤器等通訊手段，至 1998 年，再擴增調取對象範圍至電信業者（common carrier）、儲存裝置、商業紀錄（business records）。[21]

在 FISA 授權下，美國國家安全局之大規模蒐集電話 metadata 計畫[22] 得以啓動。其蒐集模式原則上是情報分析人員，初步使用一些識別碼（Identifier），比如與恐怖活動相關聯的電話號碼、撥接時間、通話長短，透過查詢（Query）方式可獲得所需的涉外情報。[23] 其中，第一次查詢所使用的識別碼，通常被稱作種子資料（Seed），必須經過國家安全局底下的國土安全分析中心（Homeland Security Analytic Center）許可，判定該查詢之請求係有事實足認具有合理清晰的懷疑（Reasonable Articulable Suspicion, RAS）與外國恐怖組織有關，始能開始查詢（Kris, 2013:217-19; Solove and Schwartz, 2018:207-9）。而後種子（Seed）之利用分成三個步驟，第一步查詢僅能找出識別碼和與該種子資料有直接相關的 metadata，第二步接著找出與第一步直接相關的 metadata 和識別碼；同理可證，第三步找出與第二步直接相關的 metadata 和識別碼（Kris, 2013:217-19; Solove and Schwartz, 2018:207-9）。[24] 若以電話號碼爲例，情報分析人員會鎖定一個電話號碼當作種子資料，第一步查詢將找出該號碼於五年內所撥接的號碼，假設有 100 筆號碼，則第二步所能查詢出的結果，就是該 100 筆號碼五年內所撥接的電話號碼，假設又是 100 組，即可產生 1 萬筆號碼（Kris, 2013:217-

[21] ACLU v. Clapper, *supra* note 7, at 731-732 (2013).

[22] 所謂 Metadata，中譯又稱爲元資料、中介資料，其定義是「描述資料的資料（information about information）」，是最小之數據單位，用以支援如指示儲存位置、歷史資料、資料尋找、檔案紀錄等功能。對於資料的比對、辨識提供相當大的幫助，其類型包括通訊的時間、延續期間、地點、以及通訊雙方的電話號碼或電子郵件。在一般的通訊資訊中，後設資料指的是非訊息內容（non-content data），屬於訊息內容（content data）的相對概念（劉靜怡，2012:73）。

[23] Klayman v. Obama, *supra* note 8, at 16-17.

[24] *Id*. at 16.

19; Solove and Schwartz, 2018:207-9）。[25] 接著第三步就是找出 1 萬筆號碼五年內所撥接的號碼，若同樣是 100 組，則最終會勾稽出 100 萬筆電話號碼（Kris, 2013:217-19; Solove and Schwartz, 2018:207-9）。[26] 此種將數據整合成一個資料庫，再利用大數據勾稽的監控技術，使得橫跨不同電信網路仍可輕易地互相串聯，該資料庫成爲儲藏人民通訊記憶的寶庫，政府挾其國家高權享有追溯分析的優勢，進而發揮比以往更爲強大的監控能量。

本文以下將以案發後三個代表性判決爲主軸，嘗試分析美國法大規模政府監控計畫所衍生之法律爭點，探究當代資訊國家，如何借助大數據運算技術作爲一種治理模式，逐步侵蝕公民隱私的運作實態。

（二）Clapper v. Amnesty International USA 案的法律爭點與判決要旨

史諾登揭露美國政府部門長久慣行的監控暗箱後，國際特赦組織美國分部首先發難，提起訴訟爭執美國國安局根據 FISA 條款，對非美國公民之境外人士實施電信監控之行爲違憲。在 Clapper v. Amnesty International USA，以國際特赦組織美國分部爲首的民權組織主張：（1）《涉外情報監控法》2008 年修正案授權行政部門在私人公司協助下，得以蒐集、獲取美國境外非美籍人士的情報信息之規定，使得原告有客觀合理可能性其個人通訊情報遭到恣意搜集、分析與使用。[27]（2）該項修正將會使得原告必須付出更高的成本和過於沉重的手段（costly and burdensome measures）來確保其個資之隱蔽性，以避免遭到不當竊取。[28] 據此，原告主張《涉外情報監控法》2008 年修正案中之相關資訊蒐集的程序規定，違反美憲增修條文第四條要求法院對行政部門該項大規模資料蒐集計畫核發永久禁制令（permanent injunction）。[29]

---

[25] *Id*.
[26] *Id*.
[27] Clapper v. Amnesty International USA, *supra* note 6, at 1141-1142.
[28] *Id*. at 1142-1143.
[29] *Id*.

本案聚焦於此類國家新興監控模式下的受害者，究須主張其所受損害的具體和直接至何種程度，方可認爲具備當事人適格（Standing）？就此程序門檻，法院最終認定原告不能僅因一連串之可能推測（speculative chain of possibilities），而害怕成爲受監控之目標，此種高度懷疑的恐懼（highly speculative fear），尚不足以構成確定、具體、實質且即將發生的損害，從而以不具備當事人適格駁回原告訴訟，最後也就未能針對國安局之大規模電信監控措施是否違反美憲增修條文第四條之實體爭點予以審酌。[30]

（三）Klayman v. Obama 案的法律爭點與判決要旨

Klayman v. Obama 一案中，原告以其爲威訊公司（Verizon Communications）之用戶身分，控告美國國安局、司法部（Department of Justice）、總統、司法部長和國家安全局局長等人，連同私人電信業者之威訊公司、Google、Microsoft、YouTube、AOL 及 AT&T 等網路、電信服務提供者。[31] 原告主張 FISC 法院對於大規模蒐集電話數據之許可，已逾越 FISA 的法定授權範圍，理由爲該數據蒐集行爲與國家安全調查無關，FISC 無權許可，而有認爲該計畫違反憲法增修條文第一、第四及第五條所保護之個人權利。因此請求法院核發暫時禁制令（preliminary injunction），請求停止該計畫的蒐集行爲。[32]

法院認爲 FISA 雖未賦予第三人對於法院依第 1861 條所下之命令有司法審查權，惟 FISA 亦無明文禁止第三人對該命令不得提起司法審查之限制，因此認爲除非立法者以清楚明確之方式，明示其預先排除司法審查之企圖，否則應肯認原告有對監控命令提起司法審查之當事人適格。[33] 因此，本案國家安全局

[30] *Id*. at 1148-1150.
[31] Klayman v. Obama, *supra* note 8, at 10-11.
[32] *Id*.
[33] *Id*. at 24-25.

蒐集美國公民電話 metadata 之行爲，因與個人核心之憲法權利有關，法院仍可審酌該計畫是否違反增修條文第四條所保障之權利，以決定是否核發暫時禁制令。[34]

循此，法院首先闡明暫時禁制令的四個核發要件，分別是（1）原告勝訴之可能性（likelihood of success on the merits）、（2）若不核發禁制令是否造成原告遭受不可回復之損害（irreparable injury）、（3）核發禁制令是否對其他利害關係人造成實質損害及（4）核發禁制令是否促進公共利益。[35] 首先，就原告是否受有損害部分，法院說明該蒐集計畫可拆解爲「電話 metadata 之蒐集」與「後續查詢過程中所進行之數據分析」兩個行爲，兩者均必須存在特定、具體、實質且即將發生之損害，始有理由作出禁制令。[36] 值得注意的是，本件法院與前揭 Clapper v. Amnesty Int'l USA 一案立場相異，其認爲本案在數據蒐集部分，由於有史諾登在衛報揭露的新聞在先，且事件爆發後政府隨之解密並證實 2013 年 4 月 FISC 確實有核准國家安全局蒐集威訊電信（Verizon Communications）用戶的電話 metadata，有別於 Clapper 案的高度懷疑，本件原告係有確切證據相信威訊電信之用戶數據已被蒐集達七年且儲存達五年，存在持續被蒐集的連續事實。[37] 又針對後階段之分析數據部分，法院以兩個理由論證該分析數據行爲已具備增修條文第四條中「搜索」之行爲特質。首先，法院提及本案數據分析行爲，不似 DNA 或指紋資料庫，係以單一快照（snapshot）方式記錄個人數據，本案國安局大規模蒐集電話 metadata 的資料庫每日即時更新，不啻令政府更容易取用該數據達到重複、大規模、秘密監控人民不公開事務之目的。[38] 其次，每次監控取得之數據可保留五年，並得查詢、分析調查該些未經調查目標同意之數據。儘管政府提出 Smith v. Maryland 一案揭櫫之「第

[34] *Id*. at 7-9.
[35] *Id*. at 25.
[36] *Id*. at 26.
[37] Id.
[38] *Id*. at 28-29.

三人理論」（the third-party doctrine）[39] 予以抗辯，主張當事人自願撥出之號碼應欠缺合理隱私期待，然法院以兩案時空背景和運用技術不同爲由，拒絕援用第三人理論於本案。[40] 綜合上述理由，法院認定此大規模蒐集電話 metadata 計畫構成增修條文第四條所謂「搜索」，[41] 自當受到第四條規範取得令狀授權始得爲之。

結論上，Klayman 法院認爲國家安全大規模蒐集電話 metadata 之計畫，構成不合理搜索，從而認定原告具有核發暫時禁制令的勝訴可能性，且若不核發，恐致原告遭受不可回復之損害，故法院許可核發暫時禁制令。[42] 又法院強調即使本案的作成將與許多判決先例相衝突，法院仍本於美憲增修條文第四條經歷過無數法院先例累積而成之原始初衷，目的係爲了對抗政府恣意侵犯個人安全及鞏固隱私保障，衡酌再三最終認爲現實上難以想像有比大規模蒐集電話 metadata 這種系統化、無差別地對幾乎所有美國公民，持續性蒐集並保留長達五年個人數據的秘密監控計畫，更加侵害人民隱私的國家行爲，從而肯認該計畫侵犯隱私之程度，自當落入增修條文第四條的保障範疇。[43]

惟值得注意的是，在哥倫比亞特區地方法院作出判決後，該案後續上訴至哥倫比亞特區巡迴上訴法院。[44] 法院以原告 Klayman 等人無法舉出足夠的勝訴可能性，亦無法說明受有任何實質性的損害及勝訴利益（likelihood of success

[39] 在 Smith v. Maryland 案，美國聯邦最高法院確立所謂「第三人理論」（The third-party doctrine），藉以處理個人資料轉手於第三人後是否仍具有合理隱私期待之判斷原則。該理論認爲一旦個人將其資訊交給（爲其提供服務）企業（即第三人）時，當事人得合理預期此個資會藉由該第三人散布，該提供資料的個人對於該資料即喪失合理隱私期待，從而不適用美憲增修條文第四條所提供的程序保障。請參考 Smith v. Maryland, 442 U.S. 735（1979）；United States v. Miller, 425 U.S. 435（1976）（劉靜怡，2012:48, 2010:206；李榮耕，2015:890）。

[40] Klayman v. Obama, *supra* note 8, 30-37 (2013).

[41] *Id*.

[42] *Id*. at 42.

[43] *Id*. at 41-43.

[44] Obama v. Klayman, 800 F.3d 559 (2015).

on the merits）爲由，不符合暫時性禁制令核發之要件，從而認定政府並未違反增修條文第四條，原告確定敗訴。[45]

（四）ACLU v. Clapper 案的法律爭點與判決要旨

與 Klayman v. Obama 起訴背景類似，ACLU v. Clapper 由美國公民自由聯盟（American Civil Liberty Union）與紐約公民自由聯盟（New York Civil Liberties Union），同樣以其爲威訊用戶爲由，質疑國家安全局電話 metadata 蒐集計畫之合法性，對國防部長、司法部長、國家安全局及其安全服務中心，以及參與該計畫之執行部門與人員提起訴訟。[46]

程序上，ACLU 案之法院首先處理違憲審查時，原告必須具有特定、具體且即將發生之損害之當事人適格要件。政府引用 Clapper v. Amnesty Int'l USA 一案抗辯，認爲原告僅有高度懷疑之恐懼，尚難謂有具體損害發生。然法院援引 Amidax Trading Group v. S.W.I.F.T. SCRL，[47] 認爲僅須表明資訊被政府獲取，即係證明受有損害之事實，故法院認定原告確因政府大量蒐集電話有關之 metadata 而受有損害，具備當事人適格。[48]

就大量蒐集電話 metadata 計畫是否違反美憲增修條文第四條的實體爭點，法院以 Katz v. United States [49] 判決先例提出之合理隱私期待爲標準，檢視該監控計畫是否構成美國憲法增修條文第四條規定之「搜索行爲」。政府再次援用 Smith 案之「第三人理論」，主張個人對自願揭露予第三方的資訊不具有正當的

---

[45] Klayman v. Obama, 805 F.3d 1148 (2015).
[46] ACLU v. Clapper, *supra* note 7, at 749-750 (2013).
[47] Amidax Trading Group v. S.W.I.F.T. SCRL, 671 F.3d 140 (2d Cir. 2011).
[48] ACLU v. Clapper, supra note 7 at 737-738 (2013).
[49] 1967 年美國聯邦最高法院在 Katz v. United States 一案明確揭示隱私權保障在於「個人」，而非「地方」。最值得關注的是，Harlan 大法官在本案撰寫的協同意見書，提出一個受到後續判決廣泛採用的「合理隱私期待」理論，藉以判斷是否構成美憲增修條文第四條所定之「搜索」而須適用法院的令狀原則要求。詳參 Katz v. United States, 389 U.S. 347（1967）。

隱私期待。[50] 法院認爲即使本案之蒐集計畫所產生的隱私顧慮與 Smith 案不盡相同，惟電信用戶既然知悉電信業者有設備可長久記錄其撥號，用戶對所撥打之號碼即無正當的隱私期待，儘管大數據的應用科技使得數據蒐集規模變得龐大，但法院認爲其並不影響資訊所有人自願提交資訊予第三方之本質。[51]

最終綜合考量該蒐集計畫，雖範圍涵蓋幾乎所有人民，惟此計畫目的係爲找出難以察覺的恐怖活動所必要之設計，且經過 FISA 第 1861 條授權，關於發動監控要件之政府必須表明「正當理由認爲其所蒐集之有體物與授權調查具備相關聯性（relevant）」一節，原告爭執其「相關性」要件設定過於浮濫不確定，惟法院認爲只要是可延伸（bear on）或可合理引導其他事務進行延伸調查者，均可認爲具備相關聯。[52] 再者，由於此類大型監控計畫是爲標定隱微之恐怖活動所必要之設計，政府不可能預先知悉何人之電話 metadata 會連結至反恐資訊之特性，爲發揮反恐偵查的即時性和預防未來攻擊之功能，應認其不致於逾越法規授權範圍。[53]

二、美國聯邦法院大規模政府監控訴訟判決評析

（一）自願揭露即喪失合理隱私期待已與時代脫節

根據上開討論，美國聯邦法院關於大規模蒐集電話 metadata 的訴訟，泰半圍繞系爭監控計畫，是否僭越增修條文第四條所保護的隱私權，而構成不合理搜索這個核心爭議上。本文細究 Clapper v. Amnesty International USA、Klayman v. Obama 和 ACLU v. Clapper 等案，發現法院反覆擺盪於當事人適格、授權明確性等程序面上的疑義，始終未能針對實體爭議審查系爭監控措施是否構成「不合理搜索」從而牴觸增修條文第四條。不約而同地，Klayman

[50] ACLU v. Clapper, *supra* note 7 at 749-750 (2013).
[51] *Id*. at 752.
[52] *Id*. at 746-748.
[53] *Id*.

和 ACLU 兩案中，政府部門均援引 1979 年以來聯邦最高法院於 Smith v. Maryland [54] 和 U.S. v. Miller [55] 之先例所確立的「第三人理論」，認爲人民既然已經同意將資料交予電信業者或商業組織等第三方，即喪失合理隱私期待，無從再主張其政府行爲違反憲法增修條文第四條。此一穩如磐石的見解，若套用在目前飛速發展的數位科技情境下，對於個人通訊隱私權利的保障，顯然構成嚴重漏洞。

誠如 Leon 法官於 Klayman 案判決指出，往昔第三人理論據以確立之指標判決 Smith（1979）、Miller（1976）等案作成背景是在 80 年代，當時的國家監控行爲僅是短時間、針對特定犯罪嫌疑人，安裝一次性、對目標回報數據的撥號紀錄器等傳統認知下的犯罪偵查手段，與今日國安局動用大數據應用科技，以每日每時每刻、全面且無差別的儲存電話 metadata 不同，顯示警察和電信業者的關係已改變。[56] 其次，Smith 案的爭議是警方爲調查犯罪，在特定人及有限目的下所安裝撥號紀錄器的個人電話，是否有權進行數據蒐集的問題。[57] 反觀在 Amnesty International USA、Kalyman、ACLU 等近年一連串爭執各種巨量數據監控計畫的爭訟中，情境已轉變爲國安局每日蒐集人們數以萬計的電信數據，大量儲存、且未來可不斷有效探勘數據資訊的程度；若再搭配每日更新，留存時效長達 5 年之數據儲存與再利用，對隱私和資訊自由造成的潛在威脅自然不可同日而語。[58]

針對美國隱私權典範過於陳舊之弊，美國學界亦早有論者提出批判。資訊隱私法學者 Daniel J. Solove 主張美國實務界應揚棄以往以私密 / 公開與否爲界，以及制式二元邏輯下的私隱觀念所建構的「合理隱私期待」與「第三人理論」

[54] Smith v. Maryland, 442 U.S. 735 (1979).
[55] United States v. Miller, 425 U.S. 435 (1976).
[56] Klayman v. Obama, *supra* note 8, at 30-37 (2013).
[57] *Id*. at 31-35 (2013).
[58] *Id*.

原則，廣泛地承認公共場所中亦存在隱私的容許性，藉以限制政府資訊蒐集行爲，確保並擴大人民對個人資訊之掌控能力，免於在資訊應用時代中受到侵害（Solove, 2010:1525-27）。他認爲，倘若系爭政府資訊蒐集行爲（information gathering），有導致維護民主自由所涉合理重要性（problems of reasonable significance）疑義時，即應受增修條文第四條規範（Solove, 2010:1527-38）。而此處所謂「合理重要性問題」，則指涉侵害隱私或者抑制人民言論或集會自由；可能阻礙人民暢所欲言的表意自由，或者放任政府未受適當控制監督而恣意取得人民個資時等，包括但不限於對民主自由精神造成弊害之行爲（Solove, 2010:1528）。而在正當法律程序的面向上，他建議釋憲者應從資訊蒐集的行爲效果來形構監督管制手段，衡酌系爭數據蒐集行爲的頻繁度、於政府監控行爲階段進程發揮的功能、最後手段性和監控對象是大規模或個案性等面向，重新省思增修條文第四條令狀原則的適用性問題（Solove, 2010:1528-29）。

學者 Laura K. Donohue 回顧聯邦最高法院與增修條文第四條相關判決，指出在 1970 年代和 1980 年代創建的學理已經與當今數位社會的運作法則脫節。亦即，第三人理論、自願揭露法則所仰賴的（a）私人與公共空間；（b）個人數據與第三方數據；（c）內容數據與非內容數據等二元對立的隱私典範，套置於數位資訊社會情境根本無從適用，從而法院必須重新考慮美憲增修條文第四條的理論內涵，以建構更有效益的規範框架，否則勢將逐漸架空該條所欲達成的保障意旨（Donohue, 2015:553）。

（二）法院見解浮動凸顯隱私保障之缺漏偏誤

承上，現代資訊國家挾其統治高權的秘密監控，在啓動目的、鎖定客體、時間長短、儲存分析、後續散佈使用等各個面向上，其規模和形式，早已與傳統國家通訊監控行爲相異，而產生本質上的改變。

美國聯邦法院圍繞大規模國家監控的合憲性及合法性審查，從 ACLU v. Clapper 與 Klayman v. Obama 兩案見解反覆浮動以觀，似仍囿於「合理隱私期

待」以及「第三人理論」之傳統見解，未能因時制宜地調整古典公私領域二元對立框架下隱私的概念內涵與保障範疇。

循此，美國針對國家大規模監控對隱私權造成的隱憂，雖迭有訴訟爭執，惟聯邦法院對相關爭議仍顯得保守。換言之，根據第三人理論及其衍伸之自願揭露法則，一旦資料係屬人民主動提供予第三人，或放置到公開空間，即不得主張有合理隱私期待的主流見解來看，將使資訊隱私所得以保障的範圍大爲限縮，或是根本性地錯失個人資料得以有效保護的時點。然而現代國家監控之資料蒐集行爲，有相當大的可能性會與後續的資料「儲存分析」、「重新組合」甚至「目的外使用」相結合，導致侵害隱私權的行爲地散落分布於不同階段當中，而有就後續行爲予以單獨個別評價之必要。換言之，縱使人民在最初時間同意提供予國家監控單位爲蒐集，也未必當然表示後續之資料利用行爲就不再形成人民隱私之威脅（張君魁，2016:76）。

（三）第三人理論的鬆動

值得注意的是，美國聯邦最高法院於 2018 年 6 月做成 Carpenter v. United States [59] 案，推翻過去「第三人理論」的技術性解釋。本案源於 2011 年間之通訊門市連續搶劫犯，當時美國執法單位爲取得包括本案上訴人 Timothy Carpenter 在內共 15 名共犯的行動電話紀錄，檢察官依據《儲存通訊紀錄法》（*Stored Communications Act*, 1986）請求法院核發命令（court order），以取得被告包含電話號碼通聯紀錄，銀行和信用卡明細等紀錄。[60] 另一方面，本案上訴人 Carpenter 主張行動電話定位資訊（cell-site location information, CSLI）的取得並未基於法院令狀（warrant），違反美憲增修條文第四條保障人民免於受無理搜索或扣押之權利。[61]

[59] Carpenter v. U.S., 138 S.Ct. 2206 (2018).
[60] 18 U.S.C. 2703 (d).
[61] Carpenter v. U.S., *supra* note 59, at 2209.

美國聯邦最高法院於 2018 年以五比四票數，爲鬆動「第三人原則」取得突破性進展。法院指出相較於交通工具的 GPS 追蹤紀錄，CSLI 紀錄更可能因行動電話的隨身性而有更大的隱私侵害疑慮，本案藉由累計嫌疑人 127 天內的行動電話定位資訊，CSIL 所具備的「詳盡（detailed）、編年網羅式（encyclopedic）且得毫不費力取得（effortlessly compiled）」的特徵，[62] 位置信息會不斷記錄存取於美國所有 4 億台設備，當今唯有不持有手機之人方能倖免於如此持續不間斷（tireless）且全面（absolute）的監控網絡之外。[63] 不啻「已全面性涵蓋行動電話持有者動向、時間戳記的資料剖繪了個人生活面貌，亦得串聯勾稽出其家族性、政治上、專業上、信仰上以及性向方面的關聯」。[64]

法院更特別強調 CSLI 紀錄具「追溯特質」（retrospective quality），蓋 CSLI 紀錄多爲持續性紀錄，更使得該個人移動資訊在現今數位行動電話無所不在而完全曝光，政府在取得之證據基礎上，也能輕易憑恃元數據的大量額外疊加而建構出一個人清晰的移動歷程。[65] 法院也特別比附援引前案 United States v. Jones 指出，與 GPS 定位追蹤是特定犯罪嫌疑人後方才啓動蒐集數據不同，CSLI 的蒐集使得某特定人一旦被標定爲犯罪嫌疑人，其人在過往五年每日、每時、每刻、每分、每秒的生活追跡資訊都可隨時不經增修條文第四條令狀原則之拘束爲執法機關召喚調取。[66] 因此，法院裁示本案中應嚴格適用「第三人理論」，但也併同強調本案僅屬個案性例外，並非意味著從此放棄傳統判例法原則，也彰顯聯邦最高法院逐漸趨向彈性，傾向視個案所涉數據類型決定是否落入增修條文第四條的保障範疇。[67] 從本案判決理由顯見，隨著數位通訊監控工具的擴張與多樣化，聯邦最高法院愈益迫近檢視政府大規模監控的運作

[62] *Id*.
[63] *Id*. at 2218.
[64] *Id*. at 2217-2218.
[65] *Id*.
[66] *Id*. at 2218.
[67] *Id*. at 2220.

特徵、和傳統監控的相異處，以及可能構成的潛在隱私危機。法理論述上，一方面沿襲 United States v. Jones 協同意見書中 Sotomayor 大法官對於數位科技地殼變動（seismic shifts in digital technology）肇生的理論反思與典範轉型，[68] 並再次清楚指明當代政府數位監控係奠基於「常規性」、「持續性」、「累加堆疊」和「追溯特質」的運作特徵。

三、小結

承上述，美國聯邦最高法院目前就大規模政府電信監控的司法實務操作判準，仍相當程度植基於古典公私領域二元論的「合理隱私期待」與「第三人理論」。上開基準套用在大數據與互聯網加乘助長的政府監控的情境脈絡下，對於個人通訊隱私權利的保障，似乎顯得處處制肘，而有不敷時代需求之憾。回應來自學界與地方法院的質疑聲浪，聯邦最高法院 2018 年 6 月 Carpenter v. United States 一案爲「第三人理論」的適用帶來突破性進展，不僅承認公共場所亦有主張合理隱私期待的彈性空間以外，更從「公共場所的合理隱私期待」、「資訊堆疊可能形成的隱私侵害」以及「metadata 的追溯特質」三個面向鬆動第三人理論的嚴格適用。由美國聯邦最高法院吹響的典範轉移的革命號角，將對過往謹守「第三人理論」的電信監控的資訊隱私解釋取徑帶來多大程度的修正與撼動，值得後續觀察。

肆、全面監控國家下資訊隱私的典範轉移與本文見解

一、全面數位監控國家的成形

數位時代的隱私權，逐漸打破古典將住家作爲隱私界線的公私領域二元標準，科技介入人們生活的方式，愈趨於無形且天羅地網，再也不復以往只是肉

[68] *Id*. at 2219.

眼觀察或物理方式的侵入模式，加之大數據應用，使國家對資料蒐集、儲存與分析的能量大幅提升與成本下降，擴充了可使用的數據量與多樣性。大數據應用科技固然有其正面的影響力，使得充足的資訊可以增加市場效率、優化政府決策，但也可能導致國家挾其強大的監控能量而引發資訊濫用和侵蝕人民資訊隱私的危機。資訊主體無知和有意見流入公私部門的個人資訊，令資訊主體在記憶—遺忘之預設倒轉的資訊社會裡嚴重喪失對於涉己資訊的控制力（林俊宏〔譯〕，麥爾荀伯格〔原著〕，2015:129-40；蘇慧婕，2016:505），最終導向資訊權力的不平等流動（林俊宏〔譯〕，麥爾荀伯格〔原著〕，2015:140-41；蘇慧婕，2016:505），國家將在永不遺忘的「數位圓形監獄」裡（林俊宏〔譯〕，麥爾荀伯格〔原著〕，2015:167），無所顧忌地以大規模監控模式執行公共任務，正當化隱私權的侵蝕。美國憲法學者 Jack Balkin 描述的全面監控國家（National Surveillance State）預言已然成眞（Balkin, 2008:3-5）。

意識到國家監控能量擴增與資訊權力傾斜的滑坡效應，歐盟法院於 2014 年 5 月率先爲沸騰已久的「被遺忘權」（Right to be Forgotten）[69] 描繪基本輪廓，傾向以承認被遺忘權爲起點，替歐盟公民建構一個隱私普世之權利對抗來自國家之侵害。其認爲，要在永不遺忘的網路世界和電信通訊場域中，有效保障人格發展自由，就必須揚棄傳統個資保護「公開資訊不受保護」、「自願揭露資訊不受保護」之公私二分思維（蘇慧婕，2016:509）。重新引入資訊價值的生命週期，肯定同一公開資訊的價值會隨著系爭資訊的內容、時間和情境的流逝、保障需求和衝突強度而浮動，因此適當賦予資訊主體有事後更新或限縮該資訊開放程度的權利（蘇慧婕，2016:505-10）。質言之，綜觀歐洲人權法院與歐盟法院分別對歐陸法制透過「權利導向」（right-dominated）模式與創設實定法權利之「被遺忘權」的雙軌途徑，強化其認爲隱私保護的核心在於個人尊嚴（dignity）的維護，包括其對個人「形象」、「姓名」、「聲譽」資料等進行理性判斷之自主決定（許炳華，2015:150）。

[69] 有關「被遺忘權」作爲一項實體基本權利之性質與定性，國內已有諸多豐富文獻探析（蘇慧婕，2016:505；許炳華，2015:127-34；徐彪豪，2015:50-70）。

相對而言，美國法制基於隱私權之發軔係出於對抗國家之一種自由價值（liberty），有鑑於美憲增修條文第一條基於觀念自由市場（Marketplace of ideas）的理念，明定「國會不得制定剝奪言論自由或出版自由的法律」，原則上難以制定要求網路服務提供者進行自我審查進而實現公民「被遺忘權」之法案（Rosen, 2012:88），也導致司法者多所節制，而不願意實質審查政府蒐集人民巨量數據之合憲性與合法性。

隱私法學者 Joel Reidenberg 觀察歐美相異的發展指出，歐洲和美國的政府情報監控法已經來到資訊隱私的轉折點。Reidenberg 提出三項提案包括（a）數據保存期限必須與數據近用的規範強度互相配合（Reidenberg, 2014:606-7）；（b）政府對個人資訊的取用與蒐集必須記錄在案並依循一定法律程序對人民公開（Reidenberg, 2014:607）；（c）政府人員必須對資訊不當監控之行爲負擔個人法律責任（Reidenberg, 2014:607-8）。如此一來，方能緩解當前各國對以國家安全爲名發動的政府監控所導致之缺乏公眾監督、違背公開政府理念乃至斲傷民主的負面效應（Reidenberg, 2014）。

Joel Reidenber 的論點與學者 Laura Donohue 的主張若合符節。Laura Donohue 指出美國於全球網絡的佈建與監控，根本性的挑戰增修條文第四條及其主流理論建構的資訊隱私典範。傳統上來說，聯邦調查局（Federal Bureau of Investigation, FBI）及中央情報局（Central Intelligence Agency, CIA）僅能分別於法規範制度內蒐集情報，且往昔刑事司法執法系統（criminal law enforcement）與情治系統（intelligence agencies）各自蒐集的數據之間，猶如存在一道隱形防火牆般涇渭分明，不得互相流用，美國學說與實務向以「the wall」稱之。然而 911 恐攻後，國家安全恐怖主義任務組合警力（Joint Terrorism Task Force）此一聯邦層級的整合性反恐組織成立，[70] 致使這道防

[70] 聯合恐怖主義特遣部隊（JTTF）係各聯邦、州和地方執法機構共同構築而成的反恐行動團體。其職責包括刑事犯罪的調查如電匯欺詐和身份盜用。JTTF 組成的機構包括聯邦執法機構，如聯邦調查局（FBI）、美國特勤局（USSS）、緝毒局（DEA）、酒精、煙草、

火牆隨之土崩瓦解（Seamon and Gardner, 2005:321-22; Scheppele, 2004:1038; Donohue, 2016:158-59; Cate and Dempsey, 2017:20）。美國國內所有人民情資，犯罪執法與打擊國際恐怖組織的資料庫自此可以互相流用，這不僅放任公民個人資訊可以無所節制地被政府機構大規模且無差別地調取、勾稽、整合與分析，個人公私生活將無所遁形地爲政府機構所汲取獲知，危殆結社自由、言論自由、信仰自由，乃至正當法律程序等重要民主法治國原則的負面效應不言可喻（Donohue, 2016:159）。

我國學者劉靜怡從宏觀視角探詢資訊隱私的憲法保障之發展方向。她主張，吾人於進行資訊法規範的制定與解釋之際，應清楚認知到網路科技情境下的「第三人」無處不在且處於無時不刻在蒐集分析個人資訊，倘若不將焦點拉回憲法正當程序保障的原始關切，僅流於機械化地操作「第三人理論」與「自願揭露法則」的後果，將導致執法者得以輕易規避個人隱私保護的基本要求，或動輒濫用公權力的藉口，對於網路電信服務使用者而言，是最大的隱私隱憂（劉靜怡，2012:49），也會成爲國家機器趁隙而入的漏洞所在。從這個觀點來看，史諾登案正是美國法長期以來理論與實際狀況脫節錯位的最外顯展示。

二、逐步架空民主監督之科技民主赤字

學者強調民主監督及民主課責之重要性，蓋近用和取得與通訊監察計畫及措施相關的資訊，往往是人民對抗來自於政府之潛在權利侵害的捍衛堡壘（劉靜怡，2017）。揆諸實際，資訊接近使用權限不平等的結果，人民與公權力機關的資訊利益對立與潛在鴻溝不僅無法弭平，更將日益擴大。因此美國自史諾

火器和爆炸物局（ATF）、美國移民與海關執法局（ICE）、美國郵政檢查局（USPIS）、美國法警局（USMS）、聯邦空軍服務局（FAMS）、美國外交安全局（DSS）、海軍刑事調查局（NCIS）、美國陸軍刑事調查司令部（CID）、美國空軍特別調查辦公室（OSI）、美國海關與邊境保護局（CBP），以及州和地方之執法機構。

登揭密案以降的美國聯邦各級法院判決，儘管立場仍曖昧模糊，惟從各審級法院法官致力於個人隱私通訊權利遭到侵害與否的個案裁量與法律論證，均彰顯監控科技的司法監督仍有其必要性及重要性。

學者亦指出數位監控的惡用或濫用是一種對民主的貶損，最直觀的理解來自於未有詳密之組織與程序規範下，公民自身涉己資訊常規性且無差別地爲國家所汲取，倘若未能被賦予充分通暢的反對意見表達之機會或者異議申訴之制度性管道，則足以侵蝕人民與政府間之信任關係。尤有甚者，政府機關未踐行當事人同意原則和建構適當退出機制下，逕行交由第三人或第三機關之目的外使用，資訊蒐集部門權力行使與內在權力結構關係得以逃遁於任何政治問責或公眾辯論之外，恐傷害「權」「責」之間的動態平衡。若再高懸國家安全、反恐情資整合等重要公共利益之名，則更容易以「安全國家」（Security State）爲名，行「科技獨裁」之實（Haggerty and Samatas, 2010:10-11）。此外，從各種科技法律與政策的審議思辨以觀，又因欠缺數位社會中各個公民構成員充分的介入參與對話論辯，則該等以預測型演算法與統計概率等科學評價之方式自動化分類個別之個人爲不同群體之作爲，惟恐造成社會定序（Social Sorting）的歧視烙記，最終導致學者 Haggerty and Samatas 聲稱的「科技民主赤字」危機（Technical Democratic Deficit）（Monahan, 2010:105-6; Haggerty and Samatas, 2010:10）。

三、資訊隱私保障的典範轉移

回應改革呼聲，史諾登案後至今六年，學者 Helen Nissenbaum 提出得以更貼近個案事實的進行分析的「情境脈絡完整性」（Privacy as contextual integrity）理論，主要在破除傳統隱私權討論裡，從「私密 / 公開」二元對立出發的論述基礎適用於巨量電信數據蒐集的情境中。Nissenbaum 認爲，政府無差別監控所反映的社會與科技環境迥異於以往，主要呈現在資訊主體分享資訊的

自願性（Voluntariness）；[71] 元數據收集者匯總、存儲、組合和分析這些數據的能力（Capability），和大眾對於元數據提供之預設風險（Assumption Risk）。除此之外，學者 Kift 與 Nissenbaum 亦比較第三人理論此一判決先例的適用背景，與當今盛行之巨量數據蒐監控模式的差異。茲分別詳列如下表三及表四（Kift and Nissenbaum, 2017:352-67）。

Nissenbaum 更強調，將情境脈絡完整性的理論框架適用於國家安全局監控後，國安局在訴訟中提出「由於數據區分爲內容數據（content data）與後設數

表三　Metadata 主宰的數位化下資訊傳輸模式之變化比較表

	社會與科技情境之變遷	對資訊流之衝擊	規範性啓示
自願性（Voluntariness）	電信服務使用者即便明知業者取得 metadata，但因其並沒有其他合理的替代手段不予提供，故可判斷其對第三人資訊分享並非出於自願。	改變資訊流的傳遞原則。	削弱「業務紀錄相對於私人紀錄應享有較低度保障」之規範原則。
能力（Capability）	Metadata 的持有者擁有大幅擴增的數據匯集、儲存整合與分析能力。	改變資訊流的屬性（Attribute）。	Metatdata 本身即足以揭露包含敏感信息的內容通訊紀錄。故 metadata 不能再被定位爲非內容的非敏感數據。
預設風險（Assumption Risk）	由於監控科技的進步，人民具備更多預設認知自身的 metadata 將被輕易攫取的風險。	將引進更多行爲主體（Actors）進入原本備受侷限的資訊流。	自由開放的社會中，溝通式 metadata 應該享有更強度的法律保護，俾免於被警方輕易取得。

資料來源：Kift 與 Nissenbaum（2017:352-53）。

[71] 學者 Nissenbaum 提出三重測試，用於評估第三方資訊分享是否出於自願（voluntariness）。首先，當事人是否自願地與第三方共享資訊；第二，當事人是否有不這樣做的替代方案；第三，該替代方案是否合理（Kift and Nissenbaum, 2017:258）。

表四　傳統形式監控與大型政府監控之情境脈絡比較表

	聯邦最高法院 Smith v. Maryland （1979）	美國國安局巨量電話數據蒐集計畫 Bulk Telephony Metadata Collection Program （2013）
適用情境	特定刑事偵查個案	國家安全之反恐目的
信號發送者	特定犯罪嫌疑人	所有註冊電話號碼之電信用戶
信息來源	撥出之電話號碼	撥出與接收的號碼電話、數據、時間和通話持續時間。其他通話識別碼（例如：國際移動用戶識別碼、國際移動設備識別碼等），和任何電話卡號碼
授權依據	無	愛國者法案 215 條

資料來源：Kift 與 Nissenbaum（2017:359）。

據（metadata），故而人民對後設數據並不存在合理隱私期待」的抗辯事由，顯然違反了語境完整性分析（Kift and Nissenbaum, 2017）。

若干美國隱私法學者轉而從組織暨程序保障功能的角度出發，試圖以程序規範誡命回應大規模政府監控的管制需求，制度設計的參據歸納如表五（Cate and Dempsey, 2017:23）。

四、大規模政府監控的資訊隱私保障取徑初探

（一）馬賽克理論的引介援用

馬賽克理論（Mosaic Theory）乃一連串資訊自由法案件爭議中所建構之理論，本係美國聯邦最高法院用以處理國安資訊公開爭訟所習用的理論，美國實務與臺灣實務均已採行，[72] 國內亦已有學者引介之（張陳弘，2016, 2018a）。美國憲法學者 David Pozen 歸納 1920 年至今的司法裁判經驗證據，指出此一

[72] 學者張陳弘將我國司法實務操作合理隱私期待標準歸納爲三大取徑，其中關於公共場域之活動如公共道路上的行車途徑，台灣高等法院 104 年度易上字第 352 號刑事判決指出一般理性之人應可預期其活動隨時得被不特定人看見，而難謂具有社會所接受的客觀合理期待。惟若此些活動被長時間且密集延續地蒐集、記錄而分析出新的個人資訊時，則有受合理隱私期待保護之可能（張陳弘，2018a:95-96）。

表五　組織暨程序保障功能導向下的制度設計參據

規範事項	規範路徑
法源依據	a. 憲法位階：憲法是否承認隱私權？或者任何限制國家自私人獲取數據的底線原則？ b. 法律位階：是否存在實定法規範該等國家監控行爲？ c. 一般原理原則：「國安通訊監察程序」與「刑事偵查程序」資料庫流用之禁止。
規範標的	內容（content data）與非內容數據（non-content data）之取得應有寬嚴程度之規範要求
規範對象	針對特定人（targeted）之監控與非針對特定人之監控（bulk access）應各有發動之法源依據
資料後續使用之嚴格監管	a. 法律應明定其所蒐集數據之後續使用、保存與揭露之基準 b. 法律應明定資料留存之年限
民主課責與監督機制	建置針對政府監控計畫之行政監督、司法監督及立法專責監督單位，確保該等機制符合公開透明和民主課責。
公私協力模式	課予私人電信業者制定內部規範予客戶概括性保護之義務

資料來源：Cate 與 Dempsey（2017:23）。

理論形成，主要的背景與冷戰與後冷戰時期頻發的國安資訊公開訴訟密切相關。面對層出不窮來自公民團體與新聞工作者的情報資訊公開請求，於 Halkin v. Helms、[73] Halperin v. CIA [74] 等案，乃至聯邦最高法院的代表性案例 CIA v. Sims，[75] 以最高法院爲首的各級法院均有志一同適用馬賽克理論（The Mosaic Theory）裁示「我們必須承認每個微小單一的情資，就像一塊拼圖，即便其本身並不顯得那麼重要，但其得再與其他單一情資拼湊下，進而整合爲一個更爲全面的圖畫，這副圖畫將可能使得覬覦美國國土安全的恐怖份子有機可趁，成爲有心人士掌握並危及美國國家安全的狙擊目標」。[76] 對應於政府監控的情境，

[73] Halkin v. Helms, 598 F.2d 1, 8 (D.C. Cir. 1978).
[74] Halperin v. CIA, 629 F.2d 144, 148 (D.C. Cir. 1980).
[75] CIA v. Sims, 471 U.S. 159 (1985).
[76] Halperin v. CIA, *supra* note 74, at 150.

馬賽克理論可理解爲：透過統計分析技術，對隱私的穿透力將可能產生大於單純個別個資的相加效果（即 1+1 可能產生大於 2 的加乘效果）（Pozen, 2005）。Alito 與 Sotomayor 大法官分別於 Jones 案的協同意見書中，不約而同地展現借鏡馬賽克理論的痕跡，令美憲增修條文第四條的判例法指引出一條方法論上的新取徑（張陳弘，2016）。

本文認爲，根據前開分析，無論是美國學理從實體法上重新檢視何謂「合法」與「非法」監控，抑或在正當法律程序的面向上，敦促立法嚴格明定監督政府監控行爲的民主課責機制，一個顯而易見的發展趨勢是，傳統基於「公開 / 保密」作爲隱私核心保障內涵之二元概念所建構的合理隱私期待，已逐漸遭受到美國聯邦法院因案制宜之鬆動，或至少恐難直接一律取法傳統判例法則或無差別一體適用，而有重構資訊隱私保障典範的必要。未來對於巨量數據監控的憲法解釋取徑上，儘管目前美國司法實務尚未趨同發展出一套可茲遵循的明確準則，惟從 Alito 及 Sotomayor 兩位大法官在 United States v. Jones 的協同意見書內容，併同美國聯邦最高法院 2018 年作成 United States v. Carpenter 一案所呈現的文字脈絡和司法論證，實蘊含美國法實務欲擴大延伸「馬賽克理論」勾勒出新的解釋取徑的跡象。

（二）美國法發展經驗的本土化重構初探

政府仰仗資訊應用科技，通過常態性大型監控計畫，對人民進行大規模、無差別而持續性監控，加上各種資料庫的建立與運用，逐漸成爲同時出現在公部門與私部門的常態，人民的數位足跡唾手可得所衍生的隱私衝突，在各國已是方興未艾且屢見不鮮。臺灣亦不例外。公務機關對部門所持有巨量資料之應用分析實態並不乏見，譬如衛福部健保署建置全民健康保險資料庫，對外提供各界申請學術研究使用；又如警政與戶政或其他國家型資料庫之串連應用；2020 年我國政府爲遏制新冠病毒之蔓延，頻繁使用電子監控的手段追蹤確診病患等等，皆屬適例。在憲法民主國原則下，都必須逐一接受法律保留原則、授

權明確性原則與比例原則的檢驗。其中，針對健保署爲學術研究，而於原始目的外「大規模強制利用」人民健保個資建置資料庫的行爲，經最高行政法院於106年度判字第54號判決合法，引致我國學者質疑，[77] 全案業已由台灣人權促進會提起釋憲聲請。[78] 理由洵爲各該主管機關適用個資法時混淆「組織法」與「行爲法」的法制框架，與目的外使用和資料當事人同意原則的規範扞格外，層出不窮的對於法律保留原則及授權明確性原則的曲解，實已碰觸到違憲與否的灰色地帶。

就此，我國學者邱文聰提出「資訊隱私應有的憲法保障強度與多階層比例原則之構想」，其認爲「人性尊嚴與尊重人格自由發展」是資訊隱私此一權利的本質核心範疇，應得到高強度的憲法保障，故主張國內現行大規模研究用途健保資料庫建置行爲的憲法保障而言，應進一步仿照大法官建構之「職業自由三階段理論」的多階段比例原則並且適用「最嚴格之審查標準」，以作爲衡量資訊隱私限制的準據（邱文聰，2018:42-43）。

本文認爲，除了上述我國學者邱文聰指出的嚴格審查標準，美國學理之「情境脈絡完整性理論（privacy as contextual integrity）」及「民主自由所涉合理重要性理論（questions of reasonable significance）」，在具體操作上，雖有失之主觀模糊而難以預測之虞，然而大規模政府監控所觸發的資訊隱私議題，實際上仍不脫數位資訊場域，因應資訊時代的挑戰變遷下，每個公民主體對於自身隱私邊界的重新集體協商與共識整合的多元價值權衡過程，落實於我國釋憲實務中，終究仍須回到闡釋比例原則時，如何衡平「國家行爲之公益目的」與「人民隱私權益之捍衛護守」此一槓桿操作的涵攝過程（張君魁，2016:145-46）。

---

[77] 關於中央健康保險署（原爲健保局）將其掌有之國民健保資料，委託國家衛生研究院建置「全民健康保險研究資料庫」，再對外提供各界申請學術使用所引發的個資侵害爭議與相關訴訟評析，詳見張陳弘（2018b）；邱文聰（2018）。

[78] 關於台灣人權促進會就健保資料庫案提起釋憲案之新聞稿，請參考台灣人權促進會（2017a），另有關釋憲理由書全文，請參考台灣人權促進會（2017b）。

具體而言，釋憲者在闡釋我國憲法第 12 條之通訊隱私及第 22 條之資訊隱私暨個人資訊自決權時，須將臺灣人民對科技生活的認知與想像轉化爲客觀價值取捨，融入到比例原則的解釋過程。在這個層次上，本文認爲，「民主自由所涉合理重要性理論」強調我們應對一個不受適當民主監督，恣意取得人民個資的數據利維坦與嚴重失衡的資訊權力結構關係抱持戒愼恐懼的嚴正態度，對資訊國家下法治國原則的護守具有憲法誡命式的先導價值。其次，「情境脈絡完整性理論」跳脫了區分「公開 / 非公開」的制式二分窠臼，主張巨量數據的資訊流通活動在資訊主體分享資訊的自願性（Voluntariness）；元數據收集者匯總、存儲、組合和分析這些數據的能力（Capability），和大眾對於元數據提供之預設風險（Assumption Risk）已與往昔傳統監控大相逕庭，更加貼近資訊場域實踐經驗的規範性論證，都是釋憲者在解決基本權法益衝突或基本權法益與其他憲法價值衝突時足以參考借鏡、比較法制可以「入駐」之處。然而爲避免其流於主觀而難以預測，本文進一步主張以「馬賽克理論」爲輔助的適用原則。

馬賽克理論的應用價值，不僅可充分凸顯大型政府監控的主要蒐集標的乃屬於 metadata 此種片段零碎、無法識別特定人的元數據，當事人或許不介意此一單元數據被蒐集使用，但一旦經過系統化、常規化及連結多目的用途的堆疊累積，搭配現行以過度僵化的「告知後同意機制」爲基本規範框架的個人資料自主權概念，[79] 將使得人民的隱私利益於國家安全或行政治理的大纛下銷蝕殆盡。其次，由於後設資料與政府大型監控計畫的核心難題，係在大數據的數位洪流下，國家與公民之間的資訊不對稱以及資訊接近使用權限嚴重失衡的結果，導致當事人的資訊隱私潛在侵害性不僅存在於「資訊取得階段」，後續「包

[79] 學者劉定基呼應包括 Fred H. Cate 教授在內的多位美國隱私法學者指出，現行各國法制通用的「告知、同意」制度，在實際操作上是將保護個人資料的重責大任幾乎完全交由當事人承擔，個人資料的蒐集者與使用者一旦取得當事人同意，形同取得後續使用、傳輸、整合、散布與流通完全通行證，而不再受到法律拘束，顯然已不符合當今數位科技情境，而有重新檢討的必要（劉定基，2017:277-300）。

括分析、處理與散布的資訊使用階段」更不受時間、空間的拘束。就此，馬賽克理論的提出，正可用以反思及調控個人資料不斷堆疊、整合分析後所可能在後續使用階段推演出新的隱私傷害的可能性，進而修正資訊隱私保護的司法論證和判斷標準。

在 Web2.0 的時代，巨量數據監控成爲近年來國家權力取得人民通訊與活動資訊的管道中，最受重視也在實際應用上最爲活躍的通訊監控手段。而本文側重著墨之 2013 年至 2015 年的 Klayman v. Obama 案及 ACLU v. Clapper 案，乃至 2018 年的 Carpenter v. United States 案，法律爭點逐漸收窄聚焦於後設資料（metadata）在大數據所驅動、日益強大的檢索比對系統下，導致國家權力與人民資訊自主決定權之間的嚴重資訊落差應如何折衝權衡安全與隱私利益的難題。爰此，本文主張美國實務所採用的「馬賽克理論」作爲巨量數據監控洪流下的把關手段。解釋論上，倘若 metadata 經過一定的組合，可從細微片段中拼湊出個人生活圖像時，此時應考慮該國家資訊蒐集及使用行爲該當於「搜索」，需遵守法院令狀原則始得爲之，反之，若仍存於片段狀態，尚難拼湊出個人時，則仍可繼續適用合理隱私期待與第三人理論。考量我國已有判決引用馬賽克理論，在法制繼受上也可較迅速爲我國實務所接受與具體操作。

伍、結論—索解癥結的他山之石

本文以比較憲法爲研究途徑，反思當政府嫻熟地結合科技力量，構成非以特定人爲標的、未連結到明確之終端目的之「國家全面監控」，公民資訊隱私作爲一項基本權利的挑戰與因應。爲能更清楚呈現筆者的想法與觀點，試將前開討論節要整理，臚列如下：

一、當代資訊國家下人民 VS. 國家的數位落差

數位時代下，公民權利與國家權力呈現出極嚴重的武器不對等與資訊落

差。2013 年史諾登揭密案將美國國安局歷時年久的反恐監控計畫曝光於眾，以 ACLU 爲首的公民團體起訴之 Clapper v. Amnesty International USA、ACLU v. Clapper、Klayman v. Obama 等案泰半圍繞於系爭行爲是否構成美憲增修條文第四條之「搜索」而須以法院令狀爲之？當事人是否具有當事人適格？等法律爭點，美國聯邦法院雖隱微意識到國家與公民間的資訊權力流動模式，與往昔傳統監控模式已大相逕庭，但囿於遵循先例原則（Stare Decisis），[80] 仍預設了自願揭露法則與第三人理論的立場，而未能進行理論適用上的變革。

二、大規模政府監控的類分區辨有助於釐清其合法界線

本文認爲數位監控已是當代資訊國家不可避免的行政治理模式，故試圖進一步將大規模政府監控予以類分辨正，目的係爲了思考，哪一些監控模式已經侵害到重大基本人權與隱私權堪稱嚴重而不堪容忍，故需強化其正當法律程序與民主監督？哪些類型侵害密度尚不致於過大，故不需要高強度的民主監督？凡此法律辯難，都是巨量數據監控的法規範領域，後續值得深思的議題，而這些問題都必須以政府監控模式之類型化，作爲後續民主監督與權利保障機制開展之思考肇端。承此，本文歸納的第一種分類標準爲「是否以特定人之個資蒐集爲限」與「是否明確連結到終端目的」，其區別實益在於精準標定出所謂大規模監控是由國家挾其統治高權，執行以非特定人個資蒐集爲客體、且未連結至終端目的的「無差別」全面數位監控。於此同時，根據美國《涉外情報監控法》提出之第二種判準，以「公民身分（Citizenship）」與「監控實施地點（Location）」爲參據，扣準法律授權依據定其容許性及合法性，乃是目前美國法學者在論述政府監控議題時的慣用分類。

[80] 判決先例原則（Doctrine of Stare Decisis），又稱因循先例、遵循先例原則，在普通法體系的法官造法（judge-made law）過程中，爲維持判決的穩定性（stability）與可預測性（foreseeability），法官原則上應該尊重已經形成的判決先例，法院在確認某項判例（precedents）「具備不得排除具拘束力的先例」，以及「需參考具說服力的先例」兩項構成要素時，即應該根據該判例要旨，作出類似判決。詳參 Sprecher（1945）。

三、巨量數據監控時代下資訊隱私的典範轉移

本文續而考察大規模政府監控於美國聯邦法院訴訟的發展軌跡與學說理論變遷發現，傳統植基於合理隱私期待與公私領域二元對立論的資訊典範，已無法有效地解釋並解決巨量數據所帶來的一連串法律挑戰。爲回應風險遽增的巨量數據監控，隱私法學者 Paula Kift 與 Helen Nissenbaum 的「情境脈絡完整性理論」與 Daniel Solove 的「民主自由所涉合理重要性（questions of reasonable significance）」判準，皆可謂應運隱私概念的範式轉移而生的理論產物。進一步言，Helen Nissenbaum、Daniel Solove 以及 Laura Donohue 強調法院應充分認知到大規模政府監控與傳統監控兩者在蒐集情境、截收者、預設風險、和收集數據期間、長短等監控手段的差異性，以此爲衡量參數而發展出不同程度的管制需求。Daniel Solove 以及 Laura Donohue 倡議返歸憲法增修條文第四條的原意考察「搜索」之規範性義涵。相對於重構憲法解釋的思考路徑，學者 Fred H. Cate 與 James X. Dempsey 則訴諸正當法律程序，主張整合法源依據、規範標的、規範對象、資料後續使用之監管機制、民主課責與監督機制和公私協力模式等關聯要素，進行規範建置的拓勘與修正。

四、馬賽克理論的啟示性意義

從美國法實踐經驗，不難看出主戰場已轉移到後設數據（metadata）的法律評價及其與美憲增修條文第四條相容性的闡釋。故本文進一步深化馬賽克理論於處理此類爭議的應用價值。本文主張當今 Metadata 的監管失靈與外溢現象，係引致公民資訊隱私潰堤失守卻又無從主張權利救濟的關鍵因素。馬賽克理論恰可用以反思傳統典範之不足，並漸進式地調控當代政府監控係取決於「大規模」、「無差別」之治理邏輯衍生而來的諸多弊端。同時，不僅於資料蒐集階段，後續資訊輾轉流通及再利用之數個階段內人民隱私利益有被侵害之虞時，馬賽克理論亦可成爲司法解釋論上俾資依循的基石底蘊。

總結而言，美國聯邦法院與學理間眾聲喧嘩的交鋒論爭，不僅勾勒出資訊

隱私落實保障的困難性及迫切性，也預示了資訊隱私權的典範轉移已是大勢所趨。因應政府監控的全球擴張，大數據結合政府監控動能下對個人隱私領域範圍的認知重構、國家安全、行政治理、與資訊科技生活的價值選擇，於美國聯邦司法權的運作場域中交疊成錯綜複雜的法益競合與角力，其活絡豐富之理論與實踐對於建構一個更符合資訊隱私保障的法律機制尤具參考價值，足堪提供我國若干比較法借鏡。

參考書目

全民健康保險研究資料庫（2000）。https://nhird.nhri.org.tw/。2020/04/17。

(National Health Insurance Research Database (NHIRD) [2000]. https://nhird.nhri.org.tw/ [accessed April 17, 2020].)

台灣人權促進會（2017a）。〈你知道健保資料庫要釋憲了嗎（釋憲聲請書簡易版）〉。https://www.tahr.org.tw/news/NHRI-constitution-apply-short。2020/04/20。

(Taiwan Association for Human Rights [2017a]. "Press Release of TAHR Filing for Judicial Interpretation of the Health Insurance Database." https://www.tahr.org.tw/news/NHRI-constitutionapply-short [accesses April 20, 2020].)

_____（2017b）。〈健保資料庫案釋憲理由書全文〉。https://www.tahr.org.tw/news/2136。2020/04/20

(_____ [2017b]. "Full Statement of Judicial Interpretation of the National Health Insurance Research Database Case." https://www.tahr.org.tw/news/2136 [accessed April 20, 2020].)

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〉，《台大法學論叢》，第 44 卷，第 3 期，頁 871-969。

(Rong-geng Li [2015]. "GPS Surveillance and Criminal Investigation: A Lesson from United States v. Jones." *National Taiwan University Law Journal*, Vol. 44, No. 3:871-969.)

林俊宏（譯），麥爾荀伯格（原著）（2014）。《大數據—「數位革命」之後，「資料革命」登場：巨量資料掀起生活、工作和思考方式的全面革新》。台北：天下文化。

(Mayer-Schönberger, Viktor [2014]. Jun-hong Lin [trans.]. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Taipei: Commonwealth Publishing.)

_____（2015）。《大數據隱私篇—數位時代，「刪去」是必要的美德》。台北：天下文化。

(_____ [2015]. Jun-hong Lin [trans.]. *Delete: The Virtue of Forgetting in the Digital Age*. Taipei: Commonwealth Publishing.)

邱文聰（2018）。〈被淘空的法律保留與變質的資訊隱私憲法保障—評最高行政法院一零六年度判字第五四號判決與相關個資法條文〉，《月旦法學雜誌》，第 272 期，頁 32-44。

(Wen-tsong Chiou [2018]. "The Principle of Legal Reservation Undermined and the Constitutional Protection of Informational Privacy Attenuated: On the Supreme Administrative Court Decision 106/54 and Personal Information Protection Act." *The Taiwan Law Review*, Vol. 272:32-44.)

徐彪豪（2016）。〈被遺忘權近期發展—歐盟法院判決週年後回顧與本土觀察〉，《科技法律透析》，第 27 卷，第 11 期，頁 50-70。

(Piao-hao Hsu [2016]. "Recent Development of Right to Be Forgotten: Revisit After Anniversary of EUCJ Ruling on Google Spain Case and Observations on Local Evolvement." *Science and Technology Law Review*, Vol. 27, No. 11:50-70.)

袁夢倩（2015）。〈被遺忘權之爭—大數據時代的數字化記憶與隱私邊界〉，《學海》，第 4 期，頁 55-61。

(Meng-qian Yuan [2015]. "The Right to Be Forgotten: Digital Memory and Privacy Boundaries in the Age of Big Data." *Xuehai*, No. 4:55-61.)

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

(Chun-kuei Chang [2016]. *On the Limitation of Preventive Surveillance in the Constitution*. Unpublished master thesis, College of Law, National Taiwan University, Taipei.)

張陳弘（2016）。〈已公開個人資料的隱私保護可能—司法陽光網引發的隱私保護爭議〉，《法令月刊》，第 67 卷，第 9 期，頁 143-64。

(Chen-hung Chang [2016]. "Privacy Protection for Publicly Available Personal Data- Privacy Protection Issues of Sunshine Judiciary Website." *The Law Monthly*, Vol. 67, No. 9:143-64.)

_____（2018a）。〈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》，第 69 卷，第 2 期，頁 82-112。

(_____ [2018a]. "The Application of the Reasonable Expectation of Privacy Test in Taiwan: My Expectation? Reasonable in Your View? Whose Privacy?" *The Law Monthly*, Vol. 69, No. 2:82-112.)

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

(_____ [2018b]. "Controversy over Information Privacy Arising from the Taiwan National Health Insurance Database: Examining the Taiwan Highest Administrative Court Judgment No. 106-Pan-54." *Chungyuan Financial & Economic Law Review*, Vol. 40:185-257.)

許炳華（2015）。〈被遺忘的權利—比較法之觀察〉，《東吳法律學報》，第 27 卷，第 1 期，頁 125-63。

(Pin-hua Hsu [2015]. "Right to Be Forgotten: Observations from the Perspectives of Comparative Law." *Soochow Law Review*, Vol. 27, No. 1:125-63.)

蔡宗珍（2014）。〈政府監控概觀—兼淺析歐盟 2006 年強制儲存通信紀錄指令〉，《台灣法學雜誌》，第 244 期，頁 25-29。

(Tzung-jen Tsai [2014]. "An Overview of the Government Mass Surveillance: Analysis on EU Compulsory Storage of Communication Records Directive 2006." *Taiwan Law Journal*, Vol. 244:25-29.)

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》，第 42 卷，第 3 期，頁 265-308。

(Ting-chi Liu [2017]. "The Principle of Information Self-determination in the Era of Big Data and IoT." *The Constitutional Review*, Vol. 42, No. 3:265-308.)

劉靜怡（2010）。〈新興科技與犯罪—以美國法制之通訊隱私程序保障爲論述中心〉，《刑事政策與犯罪研究論文集》，第 13 卷，頁 199-217。

(Ching-yi Liu [2010]. “Emerging Technologies and Crimes: Centered on the Protection of Communication Privacy Procedures in the US Legal System.” *Proceedings of Criminal Policy and Crime Research*, Vol. 13:199-217.)

_____（2012）。〈社群網路時代的隱私困境—以 Facebook 爲討論對象〉，《台大法學論叢》，第 41 卷，第 1 期，頁 1-70。

(_____ [2012]. “The Privacy Dilemma in the Social Networking Age: With a Focus on Facebook.” *National Taiwan University Law Journal*, Vol. 41, No. 1:1-70.)

_____（2017）。〈通訊監察與民主監督—歐美爭議發展〉，《歐美研究》，第 47 卷，第 1 期，頁 43-106。

(_____ [2017]. “Surveillance and Democratic Supervision: Reflection on Tendencies in Development in Europe and the United States.” *EurAmerica: A Journal of European and American Studies*, Vol. 47, No. 1:43-106.)

蘇慧婕（2016）。〈歐盟被遺忘權的概念發展—以歐盟法院 Google Spain v. AEPD 判決分析爲中心〉，《憲政時代》，第 41 卷，第 4 期，頁 473-516。

(Hui-chieh Su [2016]. “The Evolving Right to Be Forgotten: An Analysis of ECJ’s Google Spain v. AEPD Decision.” *The Constitutional Review*, Vol. 41, No. 4:473-516.)

衛生福利部臺灣醫療雲專題報導（2016）。〈臺灣健康雲—爲國人營造無所不在的健康資訊環境〉。https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvMC8xMDA3OC8wNDVmZmI5MC1kNDJkLTQxNzAtYTZmMC0zN2Q5YWYwMzBiN2IucGRm&n=6Ie654Gj5YGl5bq36Zuy77yN54K65ZyL5Lq654ef6YCg54Sh5omA5LiN5Zyo55qE5YGl5bq36LOH6KiK55Kw5aKDLnBkZg%3D%3D&icon=..pdf。2020/04/17。

(Special Report on MOHW’s Taiwan Health Cloud [2016].“Taiwan Health Cloud-To Create a Ubiquitous Health Information Environment for People.” https://ws.ndc.govtw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvMC8xMDA3OC8wNDVmZmI5MC1kNDJkLTQxNzAtYTZmMC0zN2Q5YWYwMzBiN2IucGRm&n=6Ie654Gj5YGl5bq36Zuy77yN54K65ZyL5Lq654ef6YCg54Sh5omA5LiN5Zyo55qE5YGl5bq36LOH6KiK55Kw5aKDLnBkZg%3D%3D&icon=..pdf [accessed April 17, 2020].)

Balkin, Jack M. (2008). “The Constitution in the National Surveillance State.” *Minnesota Law Review*, Vol. 93, No. 1:1-25.

Blum, Stephanie Cooper (2009). “What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform.” *Boston University Public Interest Law Journal*, Vol. 18:269-314.

Cate, Fred H. and James X. Dempsey (2017). *Bulk Collection: Systematic Government Access to Private-sector Data*. New York: Oxford University Press.

Clarke, Richard, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, Peter Swire, and The President's Review Group On Intelligence and Communications Technologies (2014). *The NSA Report: Liberty and Security in a Changing World*. New Jersey: Princeton University Press.

Donohue, Laura K. (2014). "Bulk Metadata Collection: Statutory and Constitutional Considerations." *Harvard Journal of Law & Public Policy*, Vol. 37, No. 3:757-900.

_____ (2015). "The Fourth Amendment in a Digital World." *NYU Annual Survey of American Law*, Vol. 71:553-685.

_____ (2016). *The Future of Foreign Intelligence*. New York: Oxford University Press.

Gartner, Inc., IT Glossary (2013). https://www.gartner.com/it-glossary/big-data (accessed April 20, 2020).

Gellman, Barton and Laura Poitras (2013). "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program." *Washington Post*. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.bb51889ec36e/ (accessed April 21, 2020).

Greenwald, Glenn and Ewan MacAskill (2013). "NSA Prism Program Taps into User Data of Apple, Google and Others." *Guardian*. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (accessed April 20, 2020).

Haggerty, Kevin D. and Minas Samatas (2010). "Surveillance and Democracy: An Unsettled Relationship." In Kevin D. Haggerty and Minas Samatas (eds.), *Surveillance and Democracy* (pp. 1-16). London: Routledge.

Howie, T. (2013). "The Big Bang: How the Big Data Explosion Is Changing the World." *Microsoft UK Enterprise Insights Blog, Microsoft News Center*. https://news.microsoft.com/2013/02/11/the-big-bang-how-the-big-data-explosion-is-changing-the-world/ (accessed April 20, 2020).

Kampmark, Binoy (2017). "The Merry Life of Dragnet Surveillance." *International Policy Digest*. https://intpolicydigest.org/2017/05/27/merry-life-dragnet-surveillance/ (accessed April 20, 2020).

Kaufman, Brett Max (2013). "A Guide to What We Now Know about the NSA's Dragnet Searches of Your Communications." *ACLU*. https://www.aclu.org/blog/national-security/guide-what-we-now-know-about-nsas-dragnet-searches-your-communications (accessed April 20, 2020).

Kift, Paula and Helen Nissenbaum (2017). "Metadata in Context – An Ontological and Normative Analysis of the NSA's Bulk Telephony Metadata Collection Program." *I/S: A Journal of Law and Policy for the Information Society*, Vol. 13, No. 2:333-72.

Kris, David S. (2013). "On The Bulk Collection of Tangible Things." *Journal of National Security Law & Policy*, Vol. 7:209-95.

Liu, Edward C., Andrew Nolan, and Richard M. Thompson II (2015). "Overview of Constitutional Challenges to NSA Collection Activities." *Congressional Research Service*. https://fas.org/sgp/crs/intel/R43459.pdf (accessed May 20, 2020).

Milanovic, Marko (2015). "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age." *Harvard International Law Journal*, Vol. 56:81-146.

Monahan, Torin (2010). "Surveillance as Governance: Social Inequality and the Pursuit of Democratic Surveillance." In Kevin D. Haggerty and Minas Samatas (eds.), *Surveillance and Democracy* (pp. 91-110). London: Routledge.

National Science Foundation (2014). "Critical Techniques and Technologies for Advancing Big Data Science & Engineering." *National Science Foundation*. https://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf14543 (accessed April 20, 2020).

OECD (2013). "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." *OECD*. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed April 20, 2020).

Pozen, David (2005). "The Mosaic Theory, National Security, and the Freedom of Information Act." *Yale Law Journal*, Vol. 115:628-79.

Rosen, Jeffrey (2012). "The Right to Be Forgotten." *Standard Law Review Online*. https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/ (accessed April 20, 2020).

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

Scheppele, Kim Lane (2004). "Law in a Time of Emergency: States of Exception and the Temptations of 9/11." *University of Pennsylvania Journal of Constitutional Law*, Vol. 6:1001-83.

Severson, Daniel J. (2015). "American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change." *Harvard International Law Journal*, Vol. 56, No. 2:465-514.

Seamon, Richard Henry and William Dylan Gardner (2005). "The Patriot Act and the Wall between Foreign Intelligence and Law Enforcement." *Harvard Journal of Law & Public Policy*, Vol. 28:319-464.

Solove, Daniel J. (2006). "A Taxonomy of Privacy." *Pennsylvania Law Review*, Vol. 154, No. 3:477-560.

_____ (2010). "Fourth Amendment Pragmatism." *Boston College Law Review*, Vol. 51:1511-38.

Solove, Daniel J. and Paul M. Schwartz (2011). *Information Privacy Law*. New York: Aspen Publishers.

_____ (2018). *Privacy, Law Enforcement, and National Security*. New York: Wolters Kluwer Publishers.

Sottek, T. C. and Josh Kopstein (2013). "Everything You Need to Know about PRISM- A Cheat Sheet for the NSA's Unprecedented Surveillance Programs." *Verge*. http://www.theverge.com/2013/7/17/4517480/nsa-spying-prismsurveillance-cheat-sheet (accessed April 20, 2020).

Sprecher, Robert A. (1945). "The Development of the Doctrine of Stare Decisis and the Extent to Which It Should Be Applied." *American Bar Association Journal*, Vol. 31:501-9.

Reclaiming Informational Privacy under Government Mass Surveillance: An Assessment of the U.S. Federal Courts Cases

Hsin-hsuan Lin

Abstract

This article seeks to discuss the impact on privacy of personal information when the state couple big data technology with public measures to conduct massive metadata surveillance without targeting specific persons or having a specific purpose to surveil. Methodologically, this article employs constitutional law and comparative legal analysis to critically examine litigation in the U.S. triggered by government mass surveillance and establishes a conceptual category of "government mass surveillance," which exhibit several elements. This is followed by an examination of the theoretical development and practical experience drawn from several seminal cases of the U.S. Federal Courts.

This article found that the treasure trove of litigation in the U.S. Federal Courts have significantly changed people's perceptions and presumptions of privacy. The 2013 Snowden disclosures profoundly revealed that the federal judiciary of the U.S. is confronted by the inherent defects and deficiencies embedded in the theoretical framework of "reasonable expectations of privacy" and "third-party doctrine," which was established in the 1980s and based on the dichotomy of the public / private domain. This article further introduces the "mosaic theory" as a supplementary interpretative approach and evaluates its enlightening significance.

This article concludes that the rigorous debate between the U.S. federal court's judgment and American legal scholarship not only outlines the difficulty and urgency

Hsin-hsuan Lin is a post-doctoral researcher at Institutum Iurisprudentiae, Academia Sinica. Her research interests include constitutional law, information law, government surveillance, digital rights, law of armed conflicts.

of reclaiming informational privacy in the era of big data, but also dictates a paradigm shift in our expectation of informational privacy toward a less standardized and more flexible interpretation. These insightful lessons should inform Taiwanese courts as they respond to prevailing issues presented by government mass surveillance.

Keywords: government mass surveillance, big data, informational privacy, the Fourth Amendment of the U.S. Constitution, the third-party doctrine, the mosaic theory.