科技時代下之第三方原則
——以刑事偵查程序為核心*

劉耀明**

要　目

壹、前　言
貳、美國法上搜索概念之演進
　一、財產權基準至隱私權基準之流變
　　㈠財產權基準
　　㈡隱私權基準
　　㈢雙源保護之爭議
　二、隱私期待之合理性判斷
　　㈠主觀隱私期待
　　㈡客觀隱私期待
　　㈢合理隱私期待之評估要素
參、第三方原則概述
　一、第三方原則之源起及發展
　　㈠Katz案前之發展概況
　　㈡Katz案後之發展概況
　二、第三方原則之支持與批判
　　㈠支持見解
　　㈡反對見解
　　㈢Carpenter案局部限縮第三方原則適用範圍
肆、以風險分配概念建構第三方原則於科技時代下之適用判準
　一、科技發展與隱私保障之連動性
　　㈠馬賽克式監控
　　㈡大數據偵查
　二、馬賽克理論無法全面解決第三方原則所存爭議

DOI：10.53106/199516202025050037003

* 本文為行政院國家科學及技術委員會補助專題「科技時代下之第三人原則」（MOST 111-2410-H-015-008 -）研究案之成果，對於該委員會之補助，在此表達感謝之意。另對各審查委員不吝提供諸多寶貴意見，使本文內容得以更為周延及完整，謹致上最深之謝忱，惟相關文責，仍由本人自負，自不待言。

** 中央警察大學刑事警察學系專任助理教授，臺北大學法律學系法學博士。

投稿日期：一一二年十月二十七日；接受刊登日期：一一四年一月十四日

三、其他第三方原則之修正建議
㈠主觀隱私期待應降階為客觀合理性判斷之審查要素
四、應否適用第三方原則之風險分配評估要素
㈡評估要素
伍、結　語

摘　要

第三方原則認為，當人民自願將其所有之物品或資訊交予第三方時，即應承擔第三方將該物品或資訊再轉交予包含國家之他人的風險，而不得再主張就該物品或資訊擁有可合理期待之隱私。然在科技時代之下，人民在運用資訊設備之過程中將個人資訊交予第三方已屬生活中之常態，若貫徹第三方原則，對人民隱私權之維護可能有所不足。分析後，本文認為因第三方原則之本質在於風險分配，有其正當性，故仍有存在之必要，並提出七項評估要素，以供在科技時代下判斷相關偵查措施是否應適用第三方原則。

關鍵詞： 第三方原則、風險承擔理論、隱私權、合理隱私期待、令狀原則、監控社會

壹、前　言

在刑事訴訟領域，特定偵查作為應否受強制處分法定主義及令狀原則之拘束，考量重點主要涉及所侵害之基本權類型、侵害方式（公開或秘密）及侵害時間長短等因素，當綜合評估上述因素後，可認對人民基本權之侵害已逾相當程度時，即應有具體個別之授權基礎，不得援引我國刑事訴訟法第228條至第231條之一般授權條款為執法依據[1]，始符合強制處分法定主義之要求；而當侵害程度再提高，除須有個別授權條款外，原則尚應由客觀中立之法官進行事先審查，並以相當理由為發動門檻，方符合令狀原則之要求。

至於由美國聯邦最高法院所發展出之第三方原則（the third party doctrine），是指當個人自願將其所有之物品或資訊交予第三方時，即應承擔第三方將該物品或資訊再轉交予包含國家之他人的風險，而不得再主張就該物品或資訊擁有可合理期待之隱私權[2]，故在第三方原則之適用下，針對特定物品或資訊之隱私權的保障必要性將降低，以致國家由第三方處取得該物品或資訊，可不受令狀原則之拘束，甚至得以一般授權條款為執法依據。

問題在於，在科技時代下，幾乎已成為一般人日常生活必需品的智慧型手機或穿戴裝置等資訊設備，甚或用以建構智慧家居所必要的物聯網（internet of things, IoT）設備，皆不間斷大量蒐集使用者之相關資訊，並可能回傳至特定服務提供者之線上資料庫進行分析，以期提供符合個人化需求之良善服務，故一般使用者在利用資訊設備時，基本上皆知悉會向第三方業者提供個人相關資訊，以致存在適用第三方原則之外觀。另因儲存於第三方業者處之個人資訊，基本上多以數

1 林鈺雄，干預保留與門檻理論——司法警察（官）一般調查權限之理論檢討，政大法學評論，第96期，2007年4月，頁211以下。關於刑事訴訟法第228條至第231條之規定，究屬偵查作為之一般授權條款，或單純是任務指示規定，學說上存有不同見解，惟因此非本文探討之重心，故不進一步討論。

2 Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) (quoting Smith v. Maryland, 442 U.S. 735, 743-44 (1979)).

位資訊（digital information）形式存在，而數位資訊具備無限複製性及複製無差異性等特色[3]，故偵查機關能自第三方業者處取得與偵查對象之資訊設備中完全相同的資訊[4]；甚至在使用物聯網之狀況中，由於用戶端之資訊設備未必儲存相關資訊，故偵查機關也只能從第三方業者處取得所需資訊，以致物聯網形成用戶、偵查機關與業者間之三方關係[5]，而成為第三方原則之擅場[6]，例如，在美國一起發生於二〇一七年之命案中，因犯罪現場存在具錄音功能之物聯網裝置「Amazon Alexa」，美國法院即透過第三方原則，要求Amazon公司交出錄音資料[7]。在此狀況下，若仍一味適用第三方原則，是否可能掏空憲法對於隱私權之保障，即具疑義，而此亦被認屬科技時代下美國隱私權法制之核心缺點[8]。

至於我國是否有適用第三方原則之狀況，若依司法院釋字第293號解釋之解釋文所示：「銀行法第四十八條第二項規定『銀行對於顧客之存款、放款或匯款等有關資料，除其他法律或中央主管機關另有規定者外，應保守秘密』，旨在保障銀行之一般客戶財產上之秘密及

3　最高法院112年台上字第1650號刑事判決：「『數位證據』係指儲存於電磁紀錄載體，或是以數位方式傳送，所產生類似文書之聲音、影像及符號等，於審判中得用以證明待證事實之數位資訊證據，具有無限複製性、複製具無差異性、增刪修改具無痕跡性、製作人具不易確定性等特性。」

4　李榮耕，犯罪偵查中通訊內容的調取，國立臺灣大學法學論叢，第51卷第3期，2022年9月，頁760-761。

5　林鈺雄，科技偵查概論——干預屬性及授權基礎（下），月旦法學教室，第221期，2021年3月，頁45。

6　溫祖德，與談意見：以科技偵查跨境取得證據之研究——以美國法為中心（發言紀錄），檢察新論，第27期，2020年2月，頁208-211。

7　Crystal Bonvillian, *Did Alexa Witness Double Murder? Judge Orders Amazon to Turn over Device's Audio* (Nov. 15, 2018), DAYTON DAILY NEWS, https://www.daytondailynews.com/news/national/did-alexa-witness-double-murder-judge-orders-amazon-turn-over-device-audio/Th2auhV32yPAYro08Y7J0L/ (last visited: 2024.08.22).

8　溫祖德，調取歷史性行動電話基地台位置資訊之令狀原則——自美國Carpenter案之觀察，月旦法學雜誌，第297期，2020年2月，頁143-144。

防止客戶與銀行往來資料之任意公開，以維護人民之隱私權。」未因人民將金融相關資訊交予銀行，即降低隱私權之保護，與後述美國聯邦最高法院於United States v. Miller案[9]中之處理結果不同，故似可認我國無第三方原則之適用。然如論者所述，釋字第293號之個案背景，是議會向銀行調閱資料，與偵查機關向第三方業者調閱資料，未必可相互比擬，故無法單由釋字第293號，即推論我國不接受第三方原則[10]。若以調取通信紀錄、通訊使用者資料及網路流量紀錄為例，依通訊保障及監察法第11條之1之規定，並未採令狀原則，就此，若參考後述美國聯邦最高法院於Smith v. Maryland案[11]所提出之見解，即可能是適用第三方原則所得出之結果；另就通信紀錄中之位置資訊言，雖美國聯邦最高法院已於二〇一八年之Carpenter v. United States案[12]中，將調閱一定天數之歷史性基地臺位置資訊排除於第三方原則之適用範圍外，然我國於今（二〇二四）年修正上開通訊保障及監察法第11條之1之規定時，並未參酌Carpenter案之見解，暫不論此次修正是否妥適[13]，惟是否可認為我國目前所承認之第三方原則適用範圍，甚至較美國更廣，不無疑義。此外，如後所述，第三方原則之實質內涵，其實是風險分配問題，為「風險承擔理論」之下位類型，而風險承擔理論又為我國最高法院所明文承認[14]，故第三方原則在我國法下應仍有適用空間。

由於在現今強調以科技偵查措施對抗科技犯罪之際，偵查機關運

9 United States v. Miller, 425 U.S. 435 (1976).

10 李榮耕，前揭註4，頁794-795註115。

11 Smith v. Maryland, 442 U.S. 735 (1979).

12 Carpenter v. United States, 138 S. Ct. 2206 (2018).

13 我國通訊保障及監察法於本次修法前，針對未涉通訊內容之通訊資訊，同時存在保護不足及保護過度之狀況，本次修正未併同依隱私程度建立層級化之保護機制，殊為可惜，請參劉耀明，通訊監察之層級化事前管控機制，刑事法雜誌，第60卷第6期，2016年12月，頁39-41。

14 例如最高法院110年台上字第6095號刑事判決、最高法院104年台上字第503號刑事判決及最高法院100年台上字第4430號刑事判決等，皆以風險承擔理論為論述核心。

用科技設備追蹤或監視犯嫌，經常須借助第三方之力[15]，然在科技時代下，第三方原則之運用已於美國法上產生諸多爭議，故如何調和偵查公益與人權保障，以妥適運用第三方原則，應屬相當值得思考之議題。據此，本文擬以美國法之發展為借鏡，以分析如何在科技時代下判斷相關偵查措施應否適用第三方原則，而因第三方原則在美國法上，與合理隱私期待標準之操作密切相關，故在前言之後，本文將先藉由簡要說明美國法上搜索概念之演進，並帶出隱私期待合理性之審查方式，以作為後續討論第三方原則之基礎（貳）；其次介紹第三方原則之內涵、發展及相關批判（參）；再分析於科技時代下可用以審查應否適用第三方原則之相關評估要素（肆）；最後進行總結（伍）。

貳、美國法上搜索概念之演進

美國法上處理搜索之核心條文，為美國聯邦憲法第四修正案（以下簡稱「第四修正案」），依該條規定，人民就其人身、住所、文件及財物，有權拒絕政府不合理之搜索及扣押[16]，且一旦被認定構成該條意旨下之搜索，原則即受「令狀條款」（the warrant clause）及「合理條款」（the reasonableness clause）之規制[17]，若無令狀而為之，原

15 參考黃清德，警察機關要求私人提供資料協助追蹤監視的法律問題——以調閱電信資料及監視錄影資料為例，真理財經法學，第16期，2016年3月，頁7-9。

16 U.S. CONST. AMEND. 4 “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

17 林利芝，從美國最高法院United States v. Jones案分析美國政府運用GPS定位追蹤器探知個人位置資訊之適法性，月旦法學雜誌，第272期，2018年1月，頁178。

則會先被推定為不合理之搜索[18]，須透過證明個案並未構成搜索，或為合理之無令狀搜索，方可推翻違憲推定[19]。而因美國聯邦最高法院在個案中適用第三方原則之目的，主要即在將政府之取證行為認定非屬第四修正案下之搜索，以期不受相關規制，故第四修正案下之搜索意涵究竟為何，又如何判斷是否已構成搜索，對於正確理解第三方原則，有相當之關連性。因此，以下將簡要說明美國法上搜索概念之演進，再分析如何在隱私權基準下，判斷隱私期待是否具備合理性。

一、財產權基準至隱私權基準之流變

針對第四修正案下搜索之內涵，美國聯邦最高法院傳統認為其所保護者乃人民之財產權，但至Katz v. United States案[20]後，則轉向認為應以隱私權為保護標的，其後，雖於United States v. Jones案[21]中再次以財產權為判斷核心，惟至Carpenter案時，則又回到隱私權的判斷取徑。

㈠財產權基準

第四修正案保護人民不受政府不合理搜索及扣押之權利，源於英國之Wilkes v. Wood案[22]及Entick v. Carrington案[23]，該兩案皆涉及空白搜索票（general warrants）之使用，以及政治異議份子之言論自由保護爭議[24]。在Entick案中，Camden爵士指出，縱未造成任何實際損害，任何政府官員或第三方仍不得在未經許可之狀況下，侵入或占有他人財產[25]，而美國聯邦最高法院於一八八六年之Boyd v. United

18 *Carpenter*, 138 S. Ct. at 2221.
19 Riley v. California, 573 U.S. 373, 382 (2014).
20 Katz v. United States, 389 U.S. 347 (1967).
21 United States v. Jones, 565 U.S. 400 (2012).
22 Wilkes v. Wood, 98 Eng. Rep. 489 (1763).
23 Entick v. Carrington, 95 Eng. Rep. 807 (1765).
24 Neil Richards, The Third Party Doctrine and the Future of the Cloud, 94(6) WASH. U. L. REV. 1441, 1451 (2017).
25 Boyd v. United States, 116 U.S. 616, 627 (1886).

States案[26]初次探討第四修正案之意涵時，亦指出第四修正案之制定目的，主要在因應英國殖民時期慣用空白搜索票，以致嚴重侵害人民財產權，進而建立以財產權為核心之搜索扣押法理，此後，皆以政府是否物理性侵入第四修正案所列舉之「人身、住所、文件、財物」等保護領域，以判斷是否構成搜索[27]，且只要實際侵入憲法保護領域，縱僅分毫，亦屬搜索[28]。

上述以執法人員有無物理性侵入認定是否構成搜索之判準，學理上稱為「財產權基準」（the property doctrine）或「財產權侵害法則」（the trespass doctrine）[29]，而Olmstead v. United States案[30]則為採用財產權基準之典型，本案中，雖執法人員於戶外之電話線路安裝竊聽器以對被告進行監聽[31]，然美國聯邦最高法院仍以執法人員未實際侵入被告住所或其他財產，且監聽時轉錄之相關資訊，非得免受搜索或扣押之有形物，故判定未構成搜索[32]。

㈡隱私權基準

由於美國聯邦憲法並未明文保護隱私權，故雖在前述以保護財產權為主軸之Boyd案中，美國聯邦最高法院即指出第四修正案所保護者，包含人民之生活隱私（the privacies of life）[33]，然在二十世紀之大部分時間中，第四修正案對於自由及隱私之保護，主要仍是由財產

---

26 *Boyd*, 116 U.S. at 616.

27 王兆鵬，重新定義高科技時代下的搜索，月旦法學雜誌，第93期，2003年2月，頁167-168。

28 Silverman v. United States, 365 U.S. 505, 510-12 (1961); *Carpenter*, 138 S. Ct. at 2213.

29 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，國立臺灣大學法學論叢，第44卷第3期，2015年9月，頁881。另「財產權侵害法則」亦有譯為「非法侵入私人財產法則」，參見林利芝，前揭註17，頁179。

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

31 *Id.* at 456-57.

32 *Id.* at 466.

33 *Boyd*, 116 U.S. at 630.

權之觀點進行理解[34]。因此，一般認為是聯邦最高法院在一九六七年之Katz案中，表示第四修正案所保護者為人，而非地點[35]；且由相關判例觀察，第四修正案亦應包含對隱私權之期待後[36]，方肯認隱私權屬第四修正案之保護標的[37]。

與Olmstead案之場景相似，在Katz案中，執法人員在被告經常用以進行賭博交易之電話亭外，安裝監聽及錄音設備[38]，然如Brandeis大法官於Olmstead案之不同意見書中所述，財產權基準之判斷方式過於僵化，當隨著科技進步，政府將可能得以不具物理性侵入之方式，揭露住所中最為隱私之資訊，卻未觸發第四修正案之保護[39]，故美國聯邦最高法院在Katz案放棄採用財產權基準，以期對隱私保護進行更靈活之分析[40]，進而，聯邦最高法院除指出第四修正案之保護範圍不限於有形物體，而及於口頭對話等無形利益外[41]，並表示封閉之電話亭如同住所，是個人得享有合理隱私期待之處所[42]，且不論以電子或物理方式侵入，皆可對隱私權造成顯著侵害[43]，故用以進行監聽之設備是否實際侵入電話亭牆面，無涉搜索之判定[44]。

針對Katz案為何將長久以來所建立之財產權基準轉變為隱私權基準，論者指出，主要是因科技進步已超越制憲者之預想，物理性侵入憲法保護領域，已非國家獲取個人資訊之必要途徑，縱人民拉下窗簾

34 *Carpenter*, 138 S. Ct. at 2239.
35 *Katz*, 389 U.S. at 351.
36 *Id.*
37 *Jones*, 565 U.S. at 406-08.
38 *Katz*, 389 U.S. at 348.
39 *Olmstead*, 277 U.S. at 473-74 (Brandeis, J. dissenting).
40 H. Brian Holland, A Third-Party Doctrine for Digital Metadata, 41(4) CARDOZO L. REV. 1549, 1555 (2020).
41 *Katz*, 389 U.S. at 353.
42 *Id.* at 360.
43 *Id.* at 362.
44 *Id.* at 353.

或低聲細語[45]，甚至用盡一切方法，可能也無法阻止政府以科技設備探知其生活私密[46]，亦即，原得以住所等憲法保護領域形成之保護網已然失效[47]，以致財產權基準已不足以保護第四修正案之權利，故美國聯邦最高法院只能修正搜索意涵，以符合人民對隱私期待之動態變化[48]。進步言之，在財產權基準下，原則以公、私領域作為是否受第四修正案保護之明確分界，然科技之發展，卻逐漸模糊公、私領域之區分，以Katz案所涉及之電話為例，電話之發明，使人們不須親自見面，即可與遠方之人低聲交談[49]，在Olmstead案判決時，全美僅不到40%之家庭使用電話，然後續發展突飛猛進，電話迅即成為社會不可或缺之一部分，故聯邦最高法院只能被迫重新思考Olmstead案之立場[50]，並使個人尋求隱私保護之資訊，縱處於公眾領域，亦有受憲法保障之可能性[51]。

㈢雙源保護之爭議

在Katz案前，美國聯邦最高法院皆以財產權基準審查是否構成搜

45 以人民可拉下窗簾以保護自身隱私，故認為使用望遠鏡不會構成搜索之美國州法院判決，如：People v. Arno, 90 Cal.App.3d 505, 153 Cal.Rptr. 624 (1979) (use of binoculars to view eighth floor office to observe pornographic materials not a search since viewable by naked eye from a better vantage point); Commonwealth v. Williams, 262 Pa.Super. 508, 396 A.2d 1286 (1978) (use of binoculars to see into home not a search because suspect could have closed curtains), rev'd in part, 494 Pa. 496, 431 A.2d 964 (1981).

46 王兆鵬，前揭註27，頁179；林利芝，前揭註17，頁179；溫祖德，GPS定位追蹤監視之立法論，載台灣2019年聯合國反貪腐公約專題學術研討會實錄論文集，2019年11月，頁234。

47 Michael W. Price, Rethinking Privacy: Fourth Amendment Papers and the Third-Party Doctrine, 8(2) J. NAT'L SEC. L. & POL'Y 247, 259 (2016).

48 Ash Wold, Katz in the Digital Age: Why the Katz Subjective Prong Must Be Restrenghtened, 52(1) SW. L. REV. 174, 176 (2023).

49 Price, *supra* note 47, at 259-60.

50 *Id.* at 261.

51 *Katz*, 389 U.S. at 351.

索[52]；在Katz案後，於一九六七年至二〇一二年間，則幾乎皆以隱私權基準理解第四修正案，並審查執法人員於個案中之行為是否構成搜索[53]，然此狀況於二〇一二年之Jones案產生鬆動。

Jones案涉及執法人員在不具有效令狀之狀況下，將GPS安裝於Jones所駕車輛之底盤，以追蹤其行跡，在蒐集二十八天後，獲得多達2,000多頁之車輛移動資訊[54]。起訴後，Jones聲請排除以GPS所獲取車輛位置資訊之證據能力，然哥倫比亞特區地方法院僅排除車輛進入緊鄰Jones住家之停車場的位置資訊，未排除於公共道路上之位置資訊，並依相關證據判定Jones與其他共犯成立共同運輸毒品罪，惟該判決遭哥倫比亞特區巡迴上訴法院撤銷[55]。

哥倫比亞特區巡迴上訴法院於判決中指出，個人於步出家門時，並非即捨棄其隱私，如美國聯邦最高法院於Katz案中所表明，只要是個人試圖保護之隱私，縱於公共場域，亦可能受憲法保護[56]，故在未取得有效授權之狀況下，以GPS揭露個人行動之全部及模式資訊，已違反第四修正案[57]。

上訴後，雖美國聯邦最高法院大法官一致同意本案該當搜索行為，但理由卻相當分歧。Scalia大法官主筆之多數意見指出，雖Katz案將隱私權納入第四修正案之保護範疇，但未同時將原已承認之財產權排除其外，故Katz案是在原財產權基準外，再納入隱私權基準，並未窄化第四修正案之射程範圍[58]。而因物理性侵入憲法保護領域在第四修正案通過時，即屬搜索之範疇，故本案執法人員於Jones所駕車輛之底盤上安裝GPS，已該當物理性侵入，應構成搜索[59]，如此，方能提

52 Wold, *supra* note 48, at 175; *Olmstead*, 277 U.S. at 466.
53 李榮耕，前揭註29，頁886。
54 *Jones*, 565 U.S. at 403.
55 *Id*.
56 United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010).
57 *Id.* at 558, 568.
58 *Jones*, 565 U.S. at 407-08.
59 *Id.* at 404-05.

供至少與第四修正案通過時相同程度之保護[60]。

至於Scalia大法官何以在長久改採隱私權基準後，又再度以財產權基準處理第四修正案之爭議，並主張財產權及隱私權皆在第四修正案之保護範圍內，若參考其於二〇一三年之Florida v. Jardines案[61]中所述，主要是因同時以財產權及隱私權為保護標的，可使案件之處理較為簡單[62]，亦即，若確定已物理性侵害財產權，即可認定構成搜索，無須再判斷是否侵害可合理期待之隱私權[63]。就此，論者指出，在多數案件中，不論採用財產權基準或隱私權基準，對於是否構成搜索之判斷，影響並不大，但在科技時代下，由於偵查機關得以非物理性侵入方式獲取所需個人資訊，故採隱私權基準以擴張搜索概念，較能即時回應保護人民基本權之需求[64]；另在實際面向上，因富者所擁有之財產權較多，故當以財產權為保護源頭時，可能產生擁有更多財產權之富者受到更多保護之歧視性結果[65]。

此外，當以財產權基準處理GPS偵查之議題時，論者指出，由於單純「貼附」GPS於車輛底盤之行為，與傳統認定之物理性「侵入」有異；且所取得者，乃車輛之外觀移動路徑，並非車輛內所蘊含之資訊，故將遭質疑未構成搜索，因此，與其認定Jones案是重回財產權基準，不如說是新創一種不甚關心財產權是否確遭侵入或破壞的物理性侵入標準[66]。而若以物理性侵入特定財產領域之最終目的仍在取得資訊而論[67]，論者認為Jones案之實質內涵乃「單源雙軌」，亦即，第四修正案下之搜索所保護者，仍為單源之隱私權，只不過以財產權基準

60 *Id.* at 411.

61 Florida v. Jardines, 569 U.S. 1 (2013).

62 *Id.* at 11.

63 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，第48卷第2期，2018年6月，頁298-299。

64 李榮耕，前揭註29，頁887-889。

65 張陳弘，前揭註63，頁301-303。

66 張陳弘，前揭註63，頁299-300。

67 張陳弘，前揭註63，頁315。

及隱私權基準之雙軌途徑進行保護[68]。

二、隱私期待之合理性判斷

與財產權基準是以物理性侵入為判準不同，在隱私權基準下，判斷個人所主張者是否屬第四修正案所保護之隱私權，須通過Harlan大法官於Katz案之協同意見書中所提出的雙重檢驗，亦即：*1.*個人須具體展現出其主觀上對於隱私之實際期待；*2.*該主觀期待須被社會（準備）承認具合理性[69]，若不符任一要件，即非屬第四修正案所保護之隱私權，縱對之造成侵害，亦不構成第四修正案下之搜索[70]，而不受第四修正案之相關規制，論者稱此判準為「雙叉法則」（two-pronged test）[71]。

至於Harlan大法官提出合理隱私期待標準之論據，因其並未引用任何權威見解，故論者指出可能是彙整相關判決先例之結果，亦即，主觀隱私期待是源於「自願揭露」（voluntary-exposure）行為，將被認定是自願放棄第四修正案之保護的相關案例[72]；而客觀隱私期待則源於Hester v. United States案[73]中，檢驗相關場域是否為社會所肯認之隱私空間，並指出敞地（open filed）不在保護之列的見解[74]。

㈠主觀隱私期待

雙叉法則的第一階層，是檢驗個人是否具體展現出其主觀上對於

---

68 張陳弘，前揭註63，頁271-272。

69 *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

70 李榮耕，論偵查機關對通信紀錄的調取，政大法學評論，第115期，2010年6月，頁119。

71 李榮耕，你好，我不好——得一方同意的通訊監察及近年最高法院相關判決簡評，月旦法學雜誌，第174期，2009年11月，頁185；Charlie Brownstein, Confronting Carpenter Rethinking the Third-Party Doctrine and Location Information, 92(1) FORDHAM L. REV. 183, 191-92 (2023).

72 Orin S. Kerr, Katz Has Only One Step: The Irrelevance of Subjective Expectations, 82(1) U. CHI. L. REV. 113, 123-25 (2015).

73 Hester v. United States, 265 U.S. 57 (1924).

74 Kerr, *supra* note 72, at 123.

隱私之實際期待。雖稱主觀隱私期待，然是指個人之客觀行為所反映的主觀意願，並非真正評量個人之主觀意圖[75]，故檢驗之重點，在於個人所展現欲阻隔他人窺視其隱私之客觀行為[76]，如司法院釋字第689號解釋理由書所述：「不受侵擾之期待已表現於外」，即強調主觀期待之外顯性。

㈡客觀隱私期待

雙叉法則的第二階層，是檢驗個人對隱私之主觀期待，是否被社會（準備）承認具合理性。至於考量社會觀感之理由，可能在於隱私本是源於社會演進過程所生之概念，故其價值須考量社會脈絡方能正確理解[77]。

有爭議者是，究竟何人可代表社會判斷個案中之主觀隱私期待是否合理？例如，在後述之Miller案中，雖美國聯邦最高法院以第三方原則判定個人交予銀行之資訊不具合理隱私期待，然依相關研究調查顯示，一般大眾卻認為政府蒐集個人與銀行間之交易往來資訊，已對隱私權造成相當高之侵害[78]，而此類與一般大眾認知脫節之判斷結果，則引發對司法系統公平性之擔憂[79]。

然而，應注意者是，若過度偏重社會通念，而忽略隱私應有之規範意義，亦可能不利於隱私權之保障[80]。以科技發展對隱私權之影響而言，可分為直接與間接兩種面向，前者，如司法院釋字第689號解

---

75 張陳弘，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，2018年12月，頁99。

76 Kerr, *supra* note 72, at 127.

77 張陳弘，前揭註63，頁325；張陳弘，前揭註75，頁107。

78 Christopher Slobogin & Joseph E. Schumacher, Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society", 42(4) DUKE L.J. 727, 740 (1993).

79 Brownstein, *supra* note 71, at 204.

80 劉定基，從美國法的觀點評司法院大法官釋字第六八九號解釋——以新聞自由、言論自由、隱私權的保障與衝突為中心，興大法學，第11期，2012年5月，頁218。

釋所示，私人活動將因科技發展而更易於被他人所監控或揭露；後者，主要指可能影響一般人對於隱私權之想法及立場，亦即，社會大眾可能認為，由於個人之相關資訊已因科技發展而易於被取得，故個人不得再主張任何權利[81]，因此，若純以社會通念判斷隱私期待是否合理，在科技時代下，確實可能產生疑慮。而林子儀及徐璧湖大法官於釋字第689號之部分協同意見及部分不同意見書中所述：「根據美國憲法之實務經驗，在運用隱私之合理期待判斷準則以判斷系爭之不受干擾自由是否存在時，必須謹慎，切不能忽略在**判斷當事人主觀期待是否屬合理期待時，必須是以社會已形成為當為規範，而非以當時社會多數人之觀點，作為判斷之基礎**；否則將改變該準則原來提供合理界定隱私權保障範圍之功能，反而成為不當減少隱私權保障之憑藉。」深值省思。

㈢合理隱私期待之評估要素

雖Katz案所提出之合理隱私期待測試（the reasonable expectation of privacy test），可依Harlan大法官之雙叉法則進行檢驗，然因「合理隱私期待」之意涵究竟為何，美國聯邦最高法院並未明確闡釋，僅指出可能與財產法或社會認可相關[82]，以致迄今仍混沌不明[83]。

至於美國聯邦最高法院用以評估期待是否合理之要素，論者歸納指出有四種具主導地位之評估模型，亦即：*1.* 機率模型（probabilistic model），此模型考量個人資訊被他人或警察知悉之可能性，機率愈低，即愈可能具合理之隱私期待[84]，另判斷重點主要取決於理智之人預期其隱私可被維持之機會，故當執法人員以違反習俗或社會期待之方式，而揭露理智之人可期待隱蔽之資訊時，即違反隱私之合理期

81 李榮耕，前揭註29，頁929-930。

82 Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978).

83 Orin S. Kerr, Four Models of Fourth Amendment Protection, 60(2) STAN. L. REV. 503, 504-05 (2007).

84 *Id.* at 506.

待[85]；*2.*隱私事實模型（private facts model），此模型聚焦於被蒐集資訊之性質，而非蒐集方式，當執法人員蒐集特別具保護必要性之個人資訊時，即可能違反隱私之合理期待[86]；*3.*實證法模式（positive law model），此模型審酌執法作為是否涉及財產法或第四修正案以外之實證法，若隱私另獲實證法之保護，隱私期待即可能具合理性[87]；*4.*政策模型（policy model），此模型直接衡量執法作為應否受第四修正案之拘束，以避免濫權[88]。

於實際個案中，因無任一模型可用於解決所有爭議，故美國聯邦最高法院經常混搭各種模型進行評估[89]，而雖同時採用多種模型，會使合理隱私期待之意涵欠缺明確性及可預測性，然亦具使第四修正案之適用更為靈活的益處[90]。至於為何以運用之靈活性為首要考量，原因與違反第四修正案之結果有關，亦即，第四修正案對執法作為施加合理性之要求，並以證據排除為後盾，當個案中之執法作為被認定違反第四修正案時，隨之而來者，即是證據排除，然證據排除卻可能導致犯罪者逍遙法外，以致須付出極大之社會成本，如何因應，即須審慎思考，就此，因第四修正案之適用，基本上可劃分為是否構成搜索，以及搜索是否合理兩大區塊，且當認定構成搜索後，若無搜索令狀，基本上會被推定不具合理性，除非能證明個案中存在緊急或取得有效同意等特殊例外，以反證具合理性，否則，即須面對證據排除之後果，然能否反證合理性並非明確規則，不利執法人員於個案中進行快速評估，故迫使聯邦最高法院將重心置於是否構成搜索之階段，並將執法作為區分為是否適用第四修正案之不同類別，再以合理隱私期待劃定界限，亦即，當個案中之執法作為未涉合理隱私期待之干預

85 *Id.* at 530-31.
86 *Id.* at 506.
87 *Id.*
88 *Id.*
89 *Id.* at 507.
90 *Id.*

時，即不受第四修正案之拘束，及其所伴隨之證據排除效果[91]。

據上可知，美國聯邦最高法院不採單一模型以評估隱私期待是否合理，主要是價值判斷後之考量，亦即，第四修正案之制定目的在於避免過度之警察監控，故合理性之評估與利益平衡相關，須於防止執法人員濫權之同時，也賦予其偵查犯罪所需之適當權力[92]。而如後所述，因適用第三方原則之目的，主要在於解除隱私期待之合理性，以利執法人員得於不適用令狀原則之狀況下，即可取得偵查犯罪所需資訊，故第三方原則，亦應屬價值判斷後之產物。

參、第三方原則概述

雖有論者指出，由涉及第三方原則之案件不斷被提起爭訟，可知此項原則尚未獲得完善處理及理解，亦未被充分理論化[93]，然由後述美國聯邦最高法院於Miller案指出，縱相關資訊之揭露是基於有限之目的，且揭露者相信其對第三方之信任不會遭到背叛，第四修正案仍不禁止政府透過第三方獲取他人向其揭露之資訊[94]；以及於Smith案所示，對自願移轉予第三方之資訊，不具合理隱私期待[95]，皆可謂已定義經典之第三方原則意涵[96]。而由個人自願揭露予第三方之資訊，即不具合理隱私期待之論點觀察，第三方原則乃由合法隱私期待（legitimate expectation of privacy）及自願揭露兩項要素構成，其中，自願揭露之概念在於，當個人自願與第三方共享資訊時，即應承擔該資訊再被轉交予他人之風險，社會不會肯認對此等資訊之主觀隱私期

91 *Id.* at 527-29.

92 *Id.* at 526-27.

93 Stephen E. Henderson, After United States v. Jones, After the Fourth Amendment Third Party Doctrine, 14(2) N.C. J.L. & TECH. 431, 434-35 (2013).

94 *Miller*, 425 U.S. at 443.

95 *Smith*, 442 U.S. at 743-44.

96 Eunice Park, Objects, Places and Cyber-Spaces Post-Carpenter. Extending the Third-Party Doctrine Beyond CSLI: A Consideration of IoT and DNA, 21 YALE J.L. & TECH. 1, 18 (2019).

待具合理性，進而，即不再受第四修正案之保護[97]。

只是，在科技時代下，人們於日常生活中無可避免須將個人資訊交予第三方業者[98]，以期在合理範圍內使用現代科技設備，故若過度強調第三方原則之適用，無疑會弱化科技時代下之隱私權保障。而因如論者所述，隱私是一種抽象且變動中之概念，將隨科技之進步而改變[99]，故第三方原則在美國聯邦最高法院作成Carpenter案判決後，已觸發了變動的契機。為瞭解在科技時代下究應如何看待第三方原則，以下將就第三方原則之源起、發展及相關批判進行說明。

一、第三方原則之源起及發展

第三方原則亦有稱為「第三人理論」、「第三人法則」、「第三人原則」或「第三方假設」（the third party assumption），由於實質內涵涉及風險分配議題，可認屬「風險承擔理論」（the assumption of risk rule; the assumption of risk doctrine）之下位概念[100]。與第三方原則性質類似者，尚有公眾揭露原則（the public exposure doctrine），兩者皆以自願揭露原則（the knowingly expose to the public rule）為出發點，認為當個人自願向第三方或公眾揭露相關資訊時，即不得再主張具可合理期待之隱私權，只是，一般在討論第三方原則時，多涉及向特定少數人揭露個人資訊，故強調交付資訊者應承擔該資訊再被移轉予他人之風險；而公眾揭露原則因涉及向不特定之公眾揭露個人資訊，既公眾皆已知悉，即無所謂資訊會再被移轉予不知情者之問題[101]。以下，分就Katz案前後，簡要說明美國法上關於第三方原則之

97 *Carpenter*, 138 S. Ct. at 2216.

98 *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring).

99 林利芝，前揭註17，頁188。

100 參考李榮耕，前揭註70，頁119-120。

101 例如在United States v. Lee案中，執法人員駕駛海岸巡邏艦尾隨涉嫌走私之Lee至離岸約24英里的合會點後，以探照燈照射走私船甲板，並發現裝載非法酒精之箱子，雖Lee主張其已試圖退至太平洋中央，以隱蔽其行動，然法院仍認為，因Lee已將違禁品暴露於可見範圍，故未構成第四修正案之搜索，請參

發展狀況。

㈠Katz案前之發展概況

第三方原則發展自一系列個人向線民揭露犯罪資訊之案件[102]，並與風險承擔之概念相關[103]，例如，美國聯邦最高法院在On Lee v. United States案[104]中指出，被告向線民陳述自身犯罪資訊而被線民錄音存證，因該錄音已得對話當事人一方（即線民）之默許，故無須取得令狀[105]；在Lopez v. United States案[106]中指出，被告欲向政府官員行賄，卻遭該官員錄音存證，被告應承擔該官員日後於法庭上複製兩人對話之風險[107]；在Hoffa v. United States案[108]中指出，認為不會被友人出賣之信任，不受第四修正案保護[109]，故當個人向其友人透露私密資訊時，即應承擔被友人出賣之風險[110]；在Lewis v. United States案[111]中指出，雖住所受第四修正案之全面性保護[112]，且臥底緝毒人員是以隱瞞真實身分之方式，而二次受邀進入被告住所完成毒品交易[113]，然與同涉執法人員以隱瞞身分方式進入被告辦公室之Gouled v. United States案[114]相較，Gouled案之執法人員在進入辦公室後，即秘密竊取

United States v. Lee, 274 U.S. 559, 560-61, 563 (1927).

102 Peter C. Ormerod & Lawrence J. Trautman, A Descriptive Analysis of the Fourth Amendment and the Third-Party Doctrine in the Digital Age, 28(2) ALB. L.J. SCI. & TECH. 73, 110-11 (2018).

103 *Smith*, 442 U.S. at 745; *Miller*, 425 U.S. at 443; *Carpenter*, 138 S. Ct. at 2220.

104 On Lee v. United States, 343 U.S. 747 (1952).

105 *Id.* at 753-54.

106 Lopez v. United States, 373 U.S. 427 (1963).

107 *Id.* at 439.

108 Hoffa v. United States, 385 U.S. 293 (1966).

109 *Id.* at 302.

110 *Id.* at 303.

111 Lewis v. United States, 385 U.S. 206 (1966).

112 *Id.* at 211.

113 *Id.* at 206-08.

114 Gouled v. United States, 255 U.S. 298 (1921).

與犯罪相關之私人文件[115]，然Lewis案之執法人員並未見聞或取走任何非被告自願向其揭露之事物[116]，亦即，被告是自願向執法人員揭露犯罪資訊及事證，隱瞞身分僅是促使被告說出其願意或渴望向任何有意購毒者陳述之資訊，並未侵害隱私權，故未構成第四修正案意涵下之搜索[117]。

㈡Katz案後之發展概況

在Katz案後改以合理隱私期待說明個人應承擔向線民揭露犯罪資訊之風險的第一例，為United States v. White案[118]，美國聯邦最高法院於該案明白指出，當被告自願相信線民並與之對話，即須承擔線民身上配有無線電或錄音設備並與政府分享資訊之風險，而無合理隱私期待可言[119]。

至於在其他案類中，如Katz案所強調，因第四修正案所保護者為人，並非地點[120]，而Harlan大法官於Katz案之協同意見書亦指出，住所雖值得保護，然若個人自願將其物品、行為或談話曝露於公眾可清楚察知之處，即顯示其主觀上並無隱藏意圖，故不受隱私權保護[121]，因此，縱屬位於身體、住所、文件或財物等憲法保護領域內之資訊，若個人自願向公眾揭露，亦不受保護。以下，分就第四修正案所列舉之保護領域進行說明。

1. 身　體

由於個人對身體內所含之資訊具合理隱私期待，並無爭議，故任何對身體以物理性接觸方式所為之取證行為，皆該當搜索；且在美國聯邦最高法院近期之判例發展下，「身體」之意涵已被擴張至衣服、

115 *Id.* at 304.
116 *Lewis*, 385 U.S. at 210.
117 *Id.* at 210-12.
118 United States v. White, 401 U.S. 745 (1971).
119 *Id.* at 751-52.
120 *Katz*, 389 U.S. at 351.
121 *Id.* at 361 (Harlan, J., concurring).

口袋中之物件、襯衣及襪子等身體之延伸物[122]，另在Grady v. North Carolina案[123]中，針對政府強制要求經判決確定之性侵犯穿載GPS設備以進行監控之作法，美國聯邦最高法院亦以GPS已物理性地「接觸」於個人身體之上，且目的是為取得身體所產生之資訊，而認定構成搜索[124]。

雖Grady案與Jones案相同，皆將物理性「侵入」擴及於「接觸」[125]，並將身體移動資訊納入身體之保護範疇，然因Grady案涉及以科技設備接觸身體，故當以不具物理性侵入之科技監控方式取得身體移動資訊時，似無法直接援引Grady案作為認定構成搜索之論據。因此，針對公開之身體移動資訊，能否適用第三方原則或公眾揭露原則，仍應視個案狀況而定，而此，將涉及後述之馬賽克理論。

2.住　所

由於個人有退至家中，以免受不合理之政府干預的權利[126]，故住所為第四修正案極為核心之領域[127]。雖Alito大法官於Jardines案之不同意見書中指出，個人對於自屋內飄散至戶外之資訊（大麻氣味），無法主張合理隱私期待[128]，然該案多數意見指出，警方在未得屋主默許之狀況下，攜帶緝毒犬至門廊外嗅聞有無大麻氣味，已物理性侵入住所，應構成搜索[129]。雖該案多數意見是以財產權基準切入，然論者指出，以未得屋主默許為判斷要件，亦與屋主對其門廊是否存在可不被警方攜帶緝毒犬嗅聞之合理期待有關[130]，此外，因大麻氣味已自屋內飄散至戶外，故亦與能否適用第三方原則或公眾揭露原則有關。

122 張陳弘，前揭註63，頁286-288。
123 Grady v. North Carolina, 135 S. Ct. 1368 (2015).
124 *Id.* at 1370-71.
125 張陳弘，前揭註63，頁312。
126 *Silverman*, 365 U.S. at 511.
127 *Jardines*, 569 U.S. at 6.
128 *Id.* at 23-24 (Alito, J., Dissenting).
129 *Id.* at 11.
130 張陳弘，前揭註63，頁314。

另在相關科技追蹤設備之使用上，論者指出第三方原則為影響United States v. Knotts案[131]及United States v. Karo案[132]之判決結果的重要因素[133]。在Knotts案中，美國聯邦最高法院指出，被告於公共道路上之行車軌跡為公眾清楚可見之資訊，不具合理隱私期待[134]，且因偵查人員既得於公開場所以目視方式進行跟監，則縱使用電子監控設備，亦無不同[135]。然於Karo案中，由於以電波發送器所取得之資訊，包含於住所內移動而未揭露予第三方或公眾之非公開資訊，仍具合理隱私期待，故聯邦最高法院認定構成搜索[136]。

至於就空中監視是否構成搜索部分，論者指出，因住所上空並非住所本身，自其上空飛越，不存在物理性侵入行為，故美國聯邦最高法院於California v. Ciraolo案[137]及Florida v. Riley案[138]中，判斷是否構成搜索之重點，並非有無物理性侵入，而是住所是否具開放性或不具隱蔽性[139]，亦即，縱在住所之範圍內，然若個人就相關物品未為遮蔽，以致使其揭露於公眾目光之下，仍不具合理隱私期待。

3. 文　件

論者指出，第四修正案對於「文件」之保護，可展現出對於思想、言論及通訊自由之重視，而第三方原則之創設，則擴張政府依法強制揭露私人文件之權力[140]。

首先，在商業文件部分，雖如前述，第三方原則是發展自一系列

131 United States v. Knotts, 460 U.S. 276 (1983).
132 United States v. Karo, 468 U.S. 705 (1984).
133 金孟華，GPS跟監之程序適法性——從美國United States v. Jones案談起，裁判時報，第68期，2018年2月，頁26-27。
134 *Knotts*, 460 U.S. at 285.
135 *Id*. at 281-82.
136 *Karo*, 468 U.S. at 716-17.
137 California v. Ciraolo, 476 U.S. 207 (1986).
138 Florida v. Riley, 488 U.S. 445 (1989).
139 張陳弘，前揭註63，頁281-282。
140 張陳弘，前揭註63，頁279。

個人向線民揭露犯罪資訊之案件，然因第三方原則之最廣泛輪廓，是至Miller案後方成形[141]，故有論者認為Miller案是美國聯邦最高法院創設第三方原則的真正源頭[142]。在該案中，檢察官為偵查被告逃漏稅捐之犯行，調取被告之註銷支票、存款條及對帳單等銀行紀錄，美國聯邦最高法院就上開調取行為是否構成搜索，指出由於上開資料乃銀行之紀錄文書，被告並無所有或持有之權利；且支票並非機密內容，僅是商業交易中之交換工具，故被告僅具有限之合理隱私期待，既被告已自願將其揭露予銀行，即應承擔銀行再將資訊移轉予國家之風險，最後判定未構成搜索行為[143]。

其次，在與通訊有關之資訊部分，美國聯邦最高法院於Smith案中指出，電信用戶在撥打電話時，主觀上已自願將電話號碼傳送至電信公司之交換系統以完成撥號，故對所撥打之電話號碼，並無主觀之隱私期待；另因電信用戶知悉電信公司會記錄其撥打之電話號碼，以作為電信公司之各種商業用途，故縱電信用戶對所撥打之電話號碼主張具主觀隱私期待，社會也不會承認其期待具合理性，因此，電信用戶須承擔電信公司將電話號碼轉交予警方之風險[144]。

4.財　物

在隱私權基準之下，第四修正案保護「財物」之核心，並非該財物本身所具有之財產權利益，而是該財物在封閉狀況下所內存之資訊，故欲成為第四修正案所保護之「財物」，除與當事人適格理論有關之「所有或持有」要件外，尚須屬於具「隱蔽」性質之封閉容器[145]，如美國聯邦最高法院於Minnesota v. Dickerson案[146]中指出，若

141 Ormerod et al., *supra* note 102, at 111.

142 *See, e.g.*, Jillian Chambers, Carpenter, the Fourth Amendment, and Third-Party Workarounds, 53(1) CONN. L. REV. 183, 190-91 (2021); Price, *supra* note 47, at 264; Wold, *supra* note 48, at 177.

143 *Miller*, 425 U.S. at 443.

144 *Id.* at 742-44.

145 張陳弘，前揭註63，頁283-284。

146 Minnesota v. Dickerson, 508 U.S. 366 (1993).

將財物置於可讓他人一目瞭然之開放視野處，即因不具隱蔽性而無法主張可合理期待之隱私權[147]。

二、第三方原則之支持與批判

由上述第三方原則之源起及相關發展可知，第三方原則與合理隱私期待之認定息息相關[148]，並涉及憲法保護領域之範圍議題。有疑義者是，雖隱私之內涵主要在於「不受干擾」（to be let alone）之權，未必與秘密等同，故美國聯邦最高法院早期將「隱私」與「秘密」劃上等號，進而以公、私領域作為得否主張合理隱私期待之判準[149]，在現今已被認為無法有效保護人民之隱私權，然何以在Katz案改採隱私權基準後，聯邦最高法院卻仍透過Knotts案及Karo案，建立偏向財產權基準之公、私領域區分標準，以處理合理隱私期待議題[150]？就此，主要原因可能是當個人資訊處於第四修正案所列舉之憲法保護領域時，因屬個人能自主支配而可要求不受干擾之私人場域，故推定於此範圍內之資訊皆具合理隱私期待[151]；反之，當個人自願將其資訊置於遠離憲法保護領域之場域，而使特定第三方或公眾得以輕易探知時，則推定不具隱私之合理期待，如Knotts案即以政府所取得者為公開場所之位置資訊，而認定不具合理隱私期待。據此，以個人將其資訊置於公領域或私領域，作為應否承擔資訊外洩風險之判準，有相當之道理。

只是，在科技時代來臨後，為符合生活所需，個人須大量將其資訊交予第三方業者；且政府得借科技之力，在公領域大量蒐集個人資

147 *Id.* at 375.

148 Lucas Issacharoff & Kyle Wirsha, Restoring Reason to the Third Party Doctrine, 100(3) MINN. L. REV. 985, 987 (2016).

149 黃楷中、呂明龍、沈芳伃，找到你／妳了——淺論GPS偵查犯罪之合法性，司法新聲，第131期，2019年7月，頁86、90。

150 Fabio Arcila Jr., GPS Tracking out of Fourth Amendment Dead Ends: United States v. Jones and the Katz Conundrum, 91(1) N.C. L. REV. 1, 38-39 (2012).

151 參考蔡彩貞，定位科技在刑事司法程序之運用與人權保障——以利用GPS追蹤為中心，裁判時報，第65期，2017年11月，頁72-73。

訊，並於彙整分析後，形成個人完整圖像，此乃過往不可想像之事，以致一般皆認為，主張僅置於憲法保護領域之私領域內的資訊，方具合理隱私期待之見解，已無法適用於科技時代。

針對合理隱私期待標準究應如何調整之問題，有論者區分公、私領域進行說明，指出在屬憲法保護領域之私領域，若個案中之資訊是以物理性侵入方式取得時，即推定已侵害可合理期待之隱私權；若未有物理侵入手段，則實質判斷是否侵害可合理期待之隱私權；至於在遠離憲法保護領域之公領域，則因不存在可供物理侵入之空間，故只能實質判斷是否侵害可合理期待之隱私權[152]。

審究上述論者之說明，其實是價值判斷後之風險分配結果，只是較符合科技時代之需求。然須注意者是，此種風險分配既為推定，即得舉反證推翻，例如，縱在屬憲法保護領域之私人住所，若個人自願打開住所窗戶，而使公眾得直視屋內空間時，在公眾可視之範圍內，亦將成為與社會共享之空間，無由要求他人須閉目不視或繞道而行，以成就此種個人隱私[153]，亦即，當個人對其自身資訊有掌控能力，卻自願將資訊提供予特定第三方或公眾知悉時，即須自行承擔資訊外洩之風險[154]，而此，即為第三方原則之核心所在。

由此觀之，第三方原則之內涵在於調整針對隱私保護所設定之風險分配，應有其正當性，然論者指出，研究第四修正案之學者卻對第三方原則既愛又恨[155]，並未完全接受，何以如此，應有探究必要，故以下將簡要介紹支持及反對者之見解，以及美國聯邦最高法院首次明白限縮第三方原則適用範圍之Carpenter案。

152 張陳弘，前揭註63，頁271-272；張陳弘，前揭註75，頁104。

153 張陳弘，前揭註75，頁105。

154 參考李榮耕，前揭註4，頁796。

155 Orin S. Kerr, The Case for the Third-Party Doctrine, 107(4) MICH. L. REV. 561, 563 (2009).

㈠支持見解

支持者之論據，主要有二，第一較偏向財產權益面向，亦即，持有個人所交付資訊之第三方，多為該資訊所附著之資料的持有人及所有人，故當然有權自由決定是否將資訊再移轉予他人[156]，此見解乃上述Miller案之論據，亦為後述Carpenter案之不同意見書所採用的見解[157]。

第二則為因應科技犯罪面向，如論者指出，在科技變遷之時代，若無第三方原則之適用，將使犯罪者利用第三方服務進行犯罪，並隱藏於第三方之後，以減少接受公開監視之可能性，故適用第三方原則，可在個人隱私與追訴犯罪之公益間，取得一定平衡[158]。以近期發生之United States v. Gratkowski案[159]為例，被告Gratkowski使用比特幣支付自兒童色情網站下載資料之費用，執法機關為調查相關交易資訊，以大陪審團傳票向比特幣交易所Coinbase公司調取相關資訊，並以自Coinbase公司取得之資訊聲請搜索票獲准，且在搜索被告住所後，發現存有相關證據之硬碟，針對上述執法作為，被告主張未依搜索票取得比特幣交易相關資訊，已違反第四修正案之要求[160]，然聯邦第五巡迴上訴法院仍以第三方原則為由，拒絕將隱私保護擴及至儲存於比特幣區塊鏈上之公開資訊，以及比特幣交易所保存之個人資訊[161]。就此判定結果，論者即認為可發揮阻止潛在犯罪者利用虛擬貨幣進行非法交易之效果[162]。

156 CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 157 (2008).

157 *Carpenter*, 138 S. Ct. at 2230 (Kennedy, J., Dissenting), 2247 (Alito, J., Dissenting).

158 Kerr, *supra* note 155, at 575-77; Holland, *supra* note 40, at 1550.

159 United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020).

160 *Id.* at 309.

161 *Id.* at 312-13.

162 Daniel Penn, The Fifth Circuit, Fourth Amendment, and the Third-Party Doctrine: Two Takeaways from the Court's First Ruling on Bitcoin Privacy, 24(1) SMU SCI. & TECH. L. REV. 125, 133 (2021).

㈡反對見解

由於第三方原則之適用可能嚴重弱化第四修正案之保護能力[163]，故提出後即引起立法者抵制，例如，美國國會為回應Miller案，通過「1978年財務隱私權案」（the Right to Financial Privacy Act of 1978）；為回應Smith案，通過「撥號追蹤法」（the Pen Register Act）[164]。

至於反對者之見解，自理論層次而言，有指出因第三方原則之基本假設是個人將其資訊交予第三方後，第三方就該資訊即有再移轉予他人之可能性，然究應以何種程度之可能性為適用前提，並非無疑，特別是在移轉可能性極低之狀況中，更可認已顯示出個人對該資訊之主觀隱私期待具合理性；另當將資訊交予第三方後，雖可認對該人已放棄隱私權，然能否等同認定對所有人亦皆放棄隱私權，則有疑義[165]。

上述論點，其實與第三方原則之源起與發展有關，此因，如前所述，第三方原則源於一系列執法機關藉由被告誤信其他罪犯、臥底或線民，而取得相關犯罪資訊之案件，因此，論者認為，第三方原則可謂是以一系列信任不值得信任之人的個案為基礎[166]，並要求揭露者自行承擔選擇信任虛偽朋友之後果[167]，然美國聯邦最高法院卻將虛偽朋友之案例，疊加至合理隱私期待之檢驗上，並運用至商業關係中，其

163 Elspeth A. Brotherton, Big Brother Gets a Makeover: Behavioral Targeting and the Third-Party Doctrine, 61(3) EMORY L.J. 555, 559 (2012).

164 *Id.* at 576.

165 李榮耕，前揭註4，頁796-797。就此，最高法院100年台上字第6422號刑事判決之意旨，似可資參照：「『已洩漏之秘密不為秘密』，係針對洩漏或交付秘密對向行為之收受者而言，除該對象行為之收受者為公眾外，若該收受者將秘密洩漏或交付予其他不應知悉秘密者，仍應成立犯罪。」

166 Eang L. Ngov, *More Than Friends: Recognizing Dichotomous Relationships in the Third Party Doctrine* 8 (2023), https://ssrn.com/abstract=4357446 or http://dx.doi.org/10.2139/ssrn.4357446 (last visited: 2024.08.22).

167 *Id.* at 5.

妥適性如何，即非無疑[168]，故鑑於當資訊在合法之商業或專業關係中揭露時，接收資訊之企業或個人，多受法律規範、行業規範及企業聲譽等因素之拘束，而可被一般人相信遭其背叛之風險甚低，進而，即應仍具合理隱私期待[169]。

此外，亦有可對應上述支持者見解之反對理由。首先，就偏向財產權益之面向而言，Marshall大法官於Smith案之不同意見書中指出，隱私並非一次性之商品交易，當個人基於一定目的而將相關資訊交予第三方或電信業者時，並不當然同時接受該資訊可再因其他目的而揭露予他人[170]。另論者亦指出，個人將資訊交予銀行或電信業者時，應可期待其僅於營業之必要範圍內使用該資訊，且使用目的是為提供所需服務，故第三方原則應適度修正及限縮[171]。而若以論者將個人行動軌跡比擬為具創作性之「著作」觀察，由於著作權應歸屬於創作該行動軌跡者所有，相關業者持有該等資訊，僅是創造者之非專屬性授權[172]，故交付資訊之行為，不代表完全失去財產權益。

其次，就因應科技犯罪面向而言，論者指出，是否真實存在會於犯罪前慮及以第三方作為逃避查緝手段之「理性」犯罪者，值得懷疑[173]。另縱認第三方原則在過往有其道理，但在科技時代之下，個人大量使用悠遊卡等交通運輸票證、信用卡、第三方支付工具、電信或網路服務等各式第三方服務，以致第三方持有大量個人資訊，在此種狀況下，透過片斷性資訊（segmental information）之比較及分析，即可形成集合性資訊（collective information），進而拼湊出完整個人圖

168 *Id.* at 8-9.

169 *Id.* at 11-12.

170 *Smith*, 442 U.S. at 749 (Marshall, J., Dissenting).

171 李榮耕，前揭註70，頁138-139；李榮耕，前揭註4，頁799。

172 王郁霖，智慧聯網時代下數位監聽與第三方保密義務之衝突——以包裹式授權契約為中心，月旦刑事法評論，第10期，2018年9月，頁90以下。

173 Erin Murphy, The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr, 24(3) BERKELEY TECH. L.J. 1239, 1241-45 (2009).

像，並掌握個人隱私[174]，故適用第三方原則，將對隱私權產生重大侵害風險，能否確實平衡個人隱私與追訴犯罪之公益，即具爭議。如Sotomayor大法官於Jones案之協同意見書即指出，合理隱私期待之操作，應重視人們能否合理預期其於公開場所之活動，會被政府全面記錄分析，並進而掌握其私生活、政治及宗教信仰等資訊，若無法預期，仍應肯認具合理隱私期待[175]；另因在科技時代下，個人於日常生活中交予第三方業者之資訊甚多，故第三方原則可能不適用於科技時代，而應重新思索其於科技時代下保護個人隱私之可行性及適法性[176]。因此，不乏論者指出，至少應認為第三方原則不適用於大量儲存數據及共享資訊之科技時代[177]。

㈢Carpenter案局部限縮第三方原則適用範圍

由於美國聯邦最高法院於Katz案中指出，個人故意向公眾揭露之資訊，縱位於住所或辦公室中，亦不屬第四修正案之保護範疇；反之，個人尋求隱私保護之資訊，縱位於公眾得觸及之處所，亦可能受憲法保護[178]，故論者指出，Katz案之核心作用，在於破除以公、私領域作為得否受第四修正案保護之傳統判準[179]，只是，Harlan大法官所提出之雙叉法則，由於建立第三方原則等因素，而持續被不當運用[180]，亦即，透過以第三方原則解除已向第三方揭露之個人資訊的合法隱私利益，最終使合理隱私期待之檢驗，又重回公、私領域區分之單一判準[181]。惟此狀況，在Jones案、Riley v. California案[182]及

174 李榮耕，前揭註4，頁797。

175 *Jones*, 565 U.S. at 416 (Sotomayor, J., Concurring).

176 *Id.* at 415, 417-18.

177 *See, e.g.*, Price, *supra* note 47, at 299; Tricia A. Martino, Fear of Change: Carpenter v. United States and Third-Party Doctrine, 58(2) DUQ. L. REV. 353, 369-70, 375-76 (2020).

178 *Katz*, 389 U.S. at 351-52.

179 Holland, *supra* note 40, at 1557-58.

180 Wold, *supra* note 48, at 177-78.

181 Holland, *supra* note 40, at 1599.

Carpenter案判決陸續作成後，已有鬆動傾向[183]。

首先，在Jones案中，雖政府所蒐集者，乃被告已向公眾揭露之車輛行經軌跡，然因執法人員於安裝GPS及後續更換電池之過程中，被認定已侵入第四修正案所保障之財物（即車輛）[184]，故仍被認定構成搜索行為，易言之，Jones案已展現出只要非法侵入憲法保護領域，縱最終蒐集者為已向公眾揭露之資訊，仍構成搜索行為[185]。

其次，在Riley案中，雖檢方主張得對受拘捕被告之手機進行附帶搜索，以取得儲存於手機本身及雲端上之數位資訊，然美國聯邦最高法院基於與一般實體物品相較，數位資訊對執法人員之人身安全幾乎不可能構成威脅；且搜索手機可獲得之資訊數量及性質，與搜索一般實體物品毫無相似之處[186]，故判定附帶搜索不合法。論者指出，本案雖未直接論及第三方原則，然其分析技術發展，並重新解釋既往判例[187]，對顛覆公、私領域判準具重大意義，亦即，若法院嚴格適用第三方原則，則被告對存放於雲端硬碟中之數位資訊，可能無法主張合法之隱私利益，然Riley案選擇檢視允許無令狀附帶搜索所欲追求之利益平衡，認定在此情形中，個人之隱私利益，更勝於確保執法人員安全及防止證據湮滅之國家利益[188]，並基於對存取龐大數據及任意行使公權力之擔憂，而限制對受拘捕者之手機進行附帶搜索[189]。

最後，Carpenter案涉及國家以法院命令（court order）而非搜索票（search warrant）向第三方之電信服務提供者，調取被告使用電信服務之基地臺位置資訊（cell site location information, CSLI）的事件。雖當手機連結至基地臺，即會自動生成帶有時間戳記，而被稱為基地

182 *Riley*, 573 U.S. at 373.
183 Holland, *supra* note 40, at 1573-74.
184 *Jones*, 565 U.S. at 403-04.
185 Holland, *supra* note 40, at 1577.
186 *Riley*, 573 U.S. at 386.
187 Brownstein, *supra* note 71, at 197-98.
188 Holland, *supra* note 40, at 1581.
189 *Id.* at 1587.

臺位置資訊之紀錄[190]，且當產生之位置資訊愈多，就愈易於用以定位手機使用者之位置[191]，然因一般人皆知悉包含基地臺位置之通信紀錄，是透過手機使用電信服務後必然產生之資訊，且該等資訊是由電信服務提供者所持有，故在第三方原則之適用下，國家取得該等資訊，似無須受令狀原則之拘束。

然而，Carpenter案意識到在科技時代下，天平已過度傾向執法者一方[192]，故詳細討論第三方原則，並重新定義其意涵[193]。以Miller案及Smith案所要求之「自願揭露」、「供第三方利用」及「於正常業務範圍內使用」三項要件而言[194]，雖Carpenter案符合後兩項要件，但就手機用戶向電信業者傳遞使用手機之相關資訊，是否屬自願揭露，則有疑義。就此，美國聯邦最高法院指出，人們基於各種理由使用手機，手機已是參與現代社會生活之必要工具，人們幾乎可謂已喪失是否使用手機之選擇權，且手機只要處於開機狀態，為使用相關電信服務，必然須持續連結至基地臺，故手機基地臺位置資訊之揭露，僅須用戶開啟手機，無須再有其他積極之肯定作為，因此人們不太會意識到位置資訊正在被蒐集[195]。此外，第四修正案之主要目的在於防止過度侵害隱私權之警察監控，以避免人民遭受政府恣意侵入個人私生活領域[196]；且當適用第三方原則時，雖會降低隱私期待之合理性，但未必皆降低至無法適用第四修正案之程度[197]。而因手機已是科技時代下人民之生活必需品；且為提供完善服務，電信業者所架設之基地臺數量大幅增加，以致透過基地臺進行三角定位可獲知之手機位置資訊愈

190 *Carpenter*, 138 S. Ct. at 2211.
191 *Id.* at 2211-12.
192 Wold, *supra* note 48, at 185.
193 *Carpenter*, 138 S. Ct. at 2216-17, 2219-22.
194 Steven Arango, Cloudy with a Chance of Government Intrusion: The Third-Party Doctrine in the 21st Century, 69(4) CATH. U. L. REV. 723, 728 (2020).
195 *Carpenter*, 138 S. Ct. at 2220.
196 *Id.* at 2214.
197 *Id.* at 2219.

趨精準，在多數人皆手機不離身之狀況下，當國家調閱大量通信紀錄時，即可有效分析出手機使用者之日常生活作息及人際交往狀況等不欲人知的隱私，故使用手機對於人民而言，就如同自行戴上電子腳鐐，而國家則可藉由調取通信紀錄達到幾乎完美程度之監控[198]，進而浮現第四修正案對政府濫權干預之擔憂[199]。因此，為有效因應偵查措施借科技之力所帶來的變化，應要求國家於調取包含基地臺位置資訊之通信紀錄時，原則須取得法院所核發之搜索票後方得為之，以期由法院於事前以較嚴格之相當理由門檻進行審查，進而避免國家之過度監控。

由上述判決意旨可推論出，美國聯邦最高法院試圖從兩個面向縮減第三方原則之影響力。第一是降低向第三方揭露資訊後對隱私期待之合理性所造成的影響，在過往，只要向第三方揭露資訊，原則即會適用第三方原則而無法再主張合理隱私期待，然Carpenter案判決引用Riley案之見解指出，揭露資訊雖會降低隱私期待之合理性，但未必降低至完全不具合理性之程度[200]，故當個人交予第三方之資訊的私密程度愈高，由於原本之期待合理性甚高，縱因揭露而降低合理性，仍愈有機會能主張依舊具備可合理期待之隱私權。

第二則是直接限縮第三方原則之適用範圍，如論者指出，美國聯邦最高法院鑑於基地臺位置資訊對於手機使用者而言，具備「深度揭露性」、「全面觸及性」及「蒐集資訊之自動性及不可避免性」等特性[201]，而決定限縮第三方原則之適用範圍。而此面向其實與第三方原則之立論基礎，亦即「自願揭露原則」有關，特別是蒐集資訊之「不可避免性」部分，已彰顯個人向電信業者交付相關位置資訊，並非

198 *Id.* at 2218.

199 *Id.* at 2222.

200 *Riley*, 573 U.S. at 392.

201 溫祖德，前揭註8，頁139-140；溫祖德，偵查機關調取歷史性行動電話基地臺位置資訊之合憲性審查——從美國聯邦最高法院判決檢視我國法制，政大法學評論，第167期，2021年12月，頁193。

「自願」，而是迫不得已之故。只是，聯邦最高法院亦指出，Carpenter案之判決意旨僅適用於該案非常狹猛之個案事實[202]，且明確指出此判決之意旨不適用於商業紀錄、即時性位置及監視錄影器等傳統監控科技或工具所取得之資訊[203]，並非全面廢棄第三方原則。

雖Carpenter案僅是有限縮減第三方原則之適用範圍，然論者仍指出，狹隘之判決與狹隘之後果並不等同，Carpenter案可謂已徹底改變第三方原則[204]，而使第三方原則具突破性之發展[205]，並使消費者於使用相關智慧產品或服務時，對其個人資訊仍可主張具合理隱私期待[206]；且其正視取得長期位置資訊與是否構成第四修正案下之搜索的關連性，對未來諸多科技偵查措施之使用，亦具重大啟示[207]。

肆、以風險分配概念建構第三方原則於科技時代下之適用判準

由上述討論可知，第三方原則在美國法上發展已久，且在傳統偵查上，不論採用財產權基準或隱私權基準，皆可發揮評定偵查行為是否構成搜索之效用，然在科技發展之下，由於對隱私保護之需求相應提升，故對第三方原則提出批判者不在少數，而美國聯邦最高法院更直接於Carpenter案中限縮第三方原則之適用。

雖Carpenter案判決同時指出該案僅是有限度地適用，然在科技時代下，個人將資訊交予第三方業者已是生活中之常態，此非該國立憲者或提出第三方原則時所能預見，故第三方原則在科技時代下究應何

202 *Carpenter*, 138 S. Ct. at 2220.

203 *Id*.

204 Arango, *supra* note 194, at 725-26.

205 林其樺，數位時代個人隱私界線怎麼畫？——從美國Carpenter v. United States案淺介行動電話定位資訊之隱私合理期待，科技法律透析，第30卷第11期，2018年11月，頁11。

206 同前註，頁15。

207 溫祖德，前揭註201，頁219。

去何從，並非無疑。自結論上而言，本文認為第三方原則主要在處理風險分配問題，尚無完全廢棄之必要。至於論者指出馬賽克理論為科技時代下適用第三方原則之解方，本文則保守看待。以下將簡要說明科技發展與隱私保護之關連性，並解釋何以馬賽克理論無法完全解決第三方原則於科技時代下之適用爭議，以及簡介目前論者所提第三方原則之修正建議，最後提出本文認為在決定是否適用第三方原則時，可資考量之評估要素。

一、科技發展與隱私保障之連動性

誠如美國聯邦最高法院於Kyllo v. United States案[208]中所述：「若堅持憲法第四修正案對人民隱私權之保護程度完全不受科技進展影響，實過於愚蠢。[209]」而我國司法院釋字第689號解釋理由書亦指出：「現今資訊科技高度發展及相關設備之方便取得，個人之私人活動受注視、監看、監聽或公開揭露等侵擾之可能大為增加，個人之私人活動及隱私受保護之需要，亦隨之提升。」故隱私保護與科技發展存在連動關係，須與時俱進[210]，進而，當科技越進步，司法實務及學術界即更致力於隱私權之提升[211]，如美國聯邦最高法院於Carpenter案中，將個人得主張合理隱私期待之範圍擴及於公開場域；以及於Riley案中，將手機內存資料排除於附帶搜索之範圍外，皆為適例。以下，簡要說明科技偵查措施之特性，以呈現其與傳統偵查手段之差異，而有提升隱私保障之必要性。

㈠馬賽克式監控

科技偵查與傳統偵查最大之不同，在於可藉由科技進行長期性、連續性及累積性之資訊蒐集，並於取得大量個人資訊後，再以科技設

208 Kyllo v. United States, 533 U.S. 27 (2001).

209 *Id.* at 33-34.

210 *See* United States v. Warshak, 631 F.3d 266, 285 (6th Cir. 2010).

211 許炳華，大數據時代下隱私權之保護——可能之影響暨對策，興大法學，第20期，2016年11月，頁172。

備進行分析及使用，進而揭露個人私生活圖像，致使個人隱私產生系統性曝露於外之高度危險[212]。就此，除論者指出GPS挾現代科技之力，突破過往以空間所建構之堡壘，並在長期且持續之監控下，穿透時間屏障，如鬼魅般刺探個人日常生活隱私外[213]；在路口監視器之使用上，因我國之監視錄影系統早已滲入日常生活，大街小巷中幾乎無所不在，只要一出家門，一舉一動即可能進入監視器之監控範圍[214]，且透過比對及分析監視器畫面，即可將被拍攝者之五官等特徵連結至特定個人，進而成功突破匿名性[215]；此外，由於衛星具跨國界、精準測量定位追蹤及日益精密之空照解析度等特性，故被廣泛運用於軍事探測、科學研究、交通導航及犯罪偵查等各種領域，若將之與路口監視器等系統進行結合，更可達全面監控之程度[216]，且個人幾乎無法抵抗。

因此，雖美國聯邦最高法院於Carpenter案中並未質疑以監視錄影器（security cameras）等傳統監控科技或工具所取得之資訊[217]，然在科技時代下，國家可能以各種科技手段長期且持續性地蒐集受監控者之集合性資訊，而形成馬賽克式之監控[218]，應為不得不面對之現象。

㈡大數據偵查

國家除可能利用各種科技工具進行馬賽克式監控外，誠如論者所述，科技時代快速發展之技術雖豐富人們之日常生活，但人們也因此

212 溫祖德，前揭註46，頁225。

213 蔡彩貞，前揭註151，頁65。

214 許福生，我國運用監視錄影系統法制規範之回顧與展望，中央警察大學學報，第46期，2009年6月，頁14。

215 黃清德，前揭註15，頁41-42。

216 蔡達智，衛星監控資訊作為法庭證據之實證研究——以高等以上法院裁判為中心，科技法學評論，第5卷第1期，2008年4月，頁64。

217 *Carpenter*, 138 S. Ct. at 2220.

218 *See* Orin S. Kerr, The Mosaic Theory of the Fourth Amendment, 111(3) MICH. L. REV. 311, 312-14 (2012).

付出向第三方揭露個人資訊之代價[219]，不論使用諸如手機、筆電、平板等各種資訊設備，皆持續記錄個人的生活點滴，且相關資料除記錄於個人之資訊設備外，亦通常同步儲存於電信業者處，甚至上傳雲端備份，在此狀況下，經由大數據之比對分析，已可產出超越片斷性資訊價值加總之集合性資訊，而若再輔以AI科技，將使整體社會轉變為一個有機的「巨大資料庫」（以下簡稱「巨庫」），且最終，將形成一個橫跨現實世界與虛擬世界之「有機融合體的跨巨庫」，當國家利用跨巨庫進行犯罪偵查時，可達成聚沙成塔之成效，使國家得以片斷性資訊之集合，成功推論個人完整圖像[220]，而此種透過大數據進行犯罪偵測及預防之作法，最終則可能形成監控社會[221]。

二、馬賽克理論無法全面解決第三方原則所存爭議

上述科技偵查之特性，特別是彙集大量資訊以形成個人私生活完整圖像部分，與馬賽克理論密切相關。馬賽克理論建構自一連串本用於處理應否許可人民要求政府公開相關資訊之資訊自由法案件，且發展之初，主要目的是在防止人民請求公開涉及國家安全之機密文件[222]，其理念在於，運用統計分析技術以整合個別資訊，將產生超越將單一資訊加總之效果[223]，亦即，量變可能導致質變[224]。在國家安全領域，馬賽克理論存在已久；司法領域，則首見於一九七二年之

219 Martino, *supra* note 177, at 375-76.

220 劉芳伶，從跨巨庫觀點論刑事訴訟法新設「科技設備監控處分」之定性與規制——以「GPS科技之利用」為檢討中心，月旦法學雜誌，第306期，2020年11月，頁115-116。

221 林其樺，前揭註205，頁15；溫祖德，前揭註6，頁210。

222 David E. Pozen, The Mosaic Theory, National Security, and the Freedom of Information Act, 115(3) YALE L.J. 628, 630-33 (2005); 張陳弘，前揭註63，頁292。

223 Jace C. Gatewood, District of Columbia Jones and the Mosaic Theory—In Search of a Public Right of Privacy: The Equilibrium Effect of the Mosaic Theory, 92(3) NEB. L. REV. 504, 506 (2014).

224 *Maynard*, 615 F.3d at 562.

United States v. Marchetti案[225]；至於刑事判決，則由華盛頓州最高法院在State v. Jackson案[226]中開啟引用馬賽克理論之先河，而Jones案之二審判決United States v. Maynard案[227]，更是首次正式使用「馬賽克理論」名稱，並援引該理論內容以認定警方在無合法搜索票之情形下，進行GPS偵查已侵害人民可合理期待之隱私權的指標性案件。

由於馬賽克理論認為大量資訊在進行關連性分析後，能產生價值遠高於個別資訊加總之綜效[228]，故將馬賽克理論納入偵查行為之規制時，即不應以單一時點進行片斷觀察，而須將諸多片斷集合成一個整體，再判斷是否侵害可合理期待之隱私權[229]。例如就個人於公開場所之活動而言，雖一般人可觀察到他人於公開場所之單次活動，然因個人資源有限，難以有效監控他人之整體性活動，但當以國家力量進行整體性之資訊蒐集時，片斷之活動資訊將質變為可揭露個人隱私之完整圖像[230]，故Knotts案指出全天候之監控與單次性之監控，應適用不同之憲法原則[231]，有其道理所在；而林子儀大法官於司法院釋字第603號解釋之協同意見書中指出：「隨電腦處理資訊技術的發達，過去所無法處理之零碎、片斷、無意義的個人資料，在現今即能快速地彼此串連、比對歸檔與系統化。當大量關乎個人但看似中性無害的資訊累積在一起時，個人長期的行動軌跡便呼之欲出。誰掌握了這些技術與資訊，便掌握了監看他人的權力。故為因應國家和私人握有建立並解讀個人資訊檔案的能力，避免人時時處於透明與被監視的隱憂之中，隱私權保障的範圍也應該隨之擴張到非私密或非敏感性質的個人資料保護。」更值得參考。由此可知，Carpenter案將監視錄影器等傳

225 United States v. Marchetti, 466 F.2d 1309 (1972); Gatewood, *supra* note 223, at 523.

226 State v. Jackson, 76 P.3d 217 (Wash. 2003).

227 *Maynard*, 615 F.3d 544.

228 蔡彩貞，前揭註151，頁64。

229 劉芳伶，前揭註220，頁114-115。

230 溫祖德，前揭註46，頁236-239。

231 *Knotts*, 460 U.S. at 283-84.

統監控科技或工具所取得之資訊，直接排除於該案意旨之適用範圍外[232]，是否適宜，尚值討論。

由於在馬賽克理論之操作下，原已向公眾或特定第三方揭露，而被認已不具合理隱私期待之個人資訊，將有因資訊量之疊加而重新被社會肯認具隱私期待合理性的可能，故馬賽克理論被認為可用以反制第三方原則，或創設第三方原則之例外[233]。只是，雖論者參考Carpenter案之見解，指出第三方原則應限縮適用於揭露有限資訊之狀況，當交予第三方之資訊具備「深度揭露性」、「全面觸及性」及「蒐集資訊之自動性及不可避免性」時，即應排除第三方原則之適用，並肯定個人仍享有合理之隱私期待[234]，以期在隱私及自由之保護與政府利益間取得平衡[235]。然論者亦指出，由於適用馬賽克理論，以事先建立蒐集多少數量或何種性質之資訊，方會質變為搜索的框架為前提[236]，然Carpenter案就此並未清楚指明，仍待司法進一步解釋[237]，故馬賽克理論遭受不夠明確之批判[238]。

以Carpenter案為例，因偵查機關在該案中聲請調閱基地臺位置資訊之天數，分別是向Sprint公司調取七天、向MetroPCS公司調取一五二天[239]，故有論者認為Carpenter案之判決意旨能否適用於調閱六天以下之基地臺位置資訊，尚存疑義[240]。另縱不論量之門檻不夠明確的問題，由於馬克賽理論主要在處理隱私期待是否合理之議題，故針對應

232 *Carpenter*, 138 S. Ct. at 2220.

233 許炳華，前揭註211，頁158。

234 溫祖德，前揭註201，頁231-232。

235 Stephen E. Henderson, Carpenter v. United States and the Fourth Amendment: The Best Way Forward, 26(2) WM. & MARY BILL RTS. J. 495, 531 (2017).

236 Kerr, *supra* note 218, at 326, 333.

237 溫祖德，前揭註8，頁143。

238 Kerr, *supra* note 218, at 329; Issacharoff et al., *supra* note 148, at 1001.

239 United States v. Carpenter, 819 F. 3d 880, 888, 890 (6th Cir. 2016).

240 Margot E. Kaminski, *Carpenter v. United States: Big Data Is Different* (July 2, 2018), THE GEO. WASH. L. REV., https://www.gwlr.org/carpenter-v-united-states-big-data-is-different (last visited: 2024.08.22).

以何人之標準進行合理性衡量的爭議，於此處同樣存在，因此被批判指出，若完全交由法官決斷，可能產生以特定法官之意志取代社會規範之結果[241]。

此外，由於馬賽克理論以資訊大量彙集為前提，而Carpenter案所排除適用之商業紀錄及即時性位置資訊[242]，在一般狀況下，卻未必有大量資訊彙集之狀況。先就商業紀錄言，在科技時代下，部分穿戴裝置之使用目的在於記錄使用者之心跳、血壓或血糖等可能較位置資訊更具私密性之健康狀況[243]，並提供予第三方業者，以利其提供適切服務，若國家調閱此類資料，仍須大量取得方可排除第三方原則之適用，對於隱私之保護，顯有不足之處。其次，就即時性之位置資訊言，以我國近年討論相當熱烈之M化車為例，由於其精準度可達1公尺[244]，並具垂直定位功能，故可用以推知手機使用者位於室內之即時性位置資訊，在此種狀況下，國家使用本質屬虛擬基地臺之M化車迫使手機向其註冊，並取得手機相關資訊，有無適用第三方原則之餘地，似存疑義，此因，雖純就技術外觀而言，M化車等虛擬基地臺之使用，是強制手機向其註冊，以取得手機之IMEI及IMSI等資訊，並鎖定手機所在位置，未向第三方業者調取相關資料，故似無第三方原則之適用，然論者指出，由於一般手機用戶皆知悉，不論其是否位於室內，當手機開機後，即會自動搜尋基地臺並與之連結，而M化車偽裝為真實基地臺之本質，就如同臥底人員一般，若參考上開美國聯邦最高法院之相關判例，當自願向臥底人員揭露資訊時，即不受第四修正案之保護，則縱用戶不知其手機所連結者，其實是政府之虛擬基地

241 *Carpenter*, 138 S. Ct. at 2246 (Thomas, J., Dissenting).

242 *Id.* at 2220.

243 參見許炳華，穿戴式科技發展下隱私權保護之探討，財產法暨經濟法，第63期，2021年3月，頁161以下。

244 林鈺雄，科技偵查概論——干預屬性及授權基礎（上），月旦法學教室，第220期，2021年2月，頁56。

臺，仍有適用第三方原則之可能性[245]。就此，若採肯定見解，因在實際執行上，M化車一般僅被用以取得較真實基地臺定位更為精確之位置資訊，並非用以大量取得位置資訊，故無法以馬賽克理論因應，進而，即不受令狀原則之拘束。至於我國今年修正刑事訴訟法時新增之第153條之2，則偏向採否定見解，依該條規定，當使用M化車等探知「行動通訊設備之位置、設備號碼或使用之卡片號碼」之科技方法時，未區分實施調查之時間長短，皆明確採用令狀原則進行規範。

三、其他第三方原則之修正建議

針對如何於科技時代下修正第三方原則，除上述馬賽克理論外，論者亦已提出諸多可參酌之建議，以下，簡要介紹四種修正方案。首先，有認為第三方原則之適用應回歸財產權基準，以期最佳實踐第四修正案之制定目的，亦即，在個案中，先判斷所取得之資訊是否屬個人財產？若否，則系爭資訊是否須侵入財產方能取得？當上述兩項問題有任一肯定時，即構成搜索[246]，以期大幅限縮第三方原則之適用範圍[247]。而在採用上開方式時，應將「財產」之關注重心，由現行之占有（possession）轉為控制（control），亦即，縱將相關資訊交予他人占有，只要個人對該資訊仍具控制權限，即可認仍具財產利益[248]；另為因應科技時代之來臨，應將「侵入」概念擴及於資訊設備，以將執法機關自行或透過業者協助，而自遠端存取資訊設備之行為，認定已構成侵入[249]。此見解之出發點涉及財產權之認定，本為第三方原則肯否見解中所涉及之爭議；另就個人是否仍保有控制權限，仍應進行個案評估。

---

245 Kristi Winner, From Historical Cell-Site Location Information to IMSI-Catchers: Why TriggerFish Devices Do Not Trigger Fourth Amendment Protection, 68(1) CASE W. RES. L. REV. 243, 270 (2017).

246 Brownstein, *supra* note 71, at 214-15.

247 *Id.* at 222.

248 *Id.* at 215-16.

249 *Id.* at 216-17.

第二，有提出以「利益競爭測試」（competing-interests test）作為修正第三方原則之新分析框架，操作上，先就個人及第三方之競爭利益賦予獨立價值，其中一方為個人資訊之自主利益，另一方為第三方與政府共享資訊之自主利益；其次衡量兩項利益，以進行客觀合理性評價，此時，當前者之利益優於後者時，即無第三方原則之適用[250]。另在處理第一步驟時，須依三項指導原則進行評估，第一，若第三方是依政府之強制命令而提供資訊時，因第三方本質上只是政府之手足延伸，無自主利益可言，故無第三方原則之適用[251]；第二，當第三方為法人等企業實體時，其自主利益通常較第三方為自然人時為低[252]；第三，當第三方為法人時，個人利益始終優先，而當第三方為自然人時，再依個案狀況具體衡量[253]。若依此見解，因目前較具爭議之案件，多為政府向第三方業者強制調閱個人資料，可能導致皆無第三方原則適用之結果。

第三，有認為當個人資訊由第三方業者控制時，能否主張合理隱私期待，應取決於：㈠消費者是否瞭解相關技術之設計，本須第三方業者之介入；㈡消費者是否具備有意義之機會，以選擇不與第三方業者共享資訊[254]。在此前提下，使用穿戴式或語音控制等智慧型設備、物聯網，或私人基因檢測等服務所生資訊，因消費者幾無選擇餘地，故無第三方原則之適用[255]。此見解其實涉及第三方原則之核心，亦即「自願揭露」之認定，並以有無拒絕揭露資訊之機會，作為是否該當自願揭露之判準，故最終仍須回歸有無選擇餘地之評估。

最後，有認為自動化技術之出現，是迫使Carpenter案重新評估第三方原則之因素，故第三方原則之適用，須在能反映第四修正案保護

250 Brotherton, *supra* note 163, at 592.
251 *Id.* at 592-93.
252 *Id.* at 593.
253 *Id.* at 594-95.
254 Park, *supra* note 96, at 6.
255 *Id*.

人民不受政府恣意侵害之目的下，進行利益平衡[256]。在此原則下，判斷是否適用第三方原則，應採取三階段之平衡檢驗，亦即：㈠確認系爭個人資訊所蘊含之隱私利益的強度及合法性；㈡考量向第三方揭露個人資訊，會使合法隱私利益受到何種程度之削減；㈢進行個人隱私利益與政府利益之平衡[257]。由於此論者提出之建議甚為詳盡，殊值參考，故再擇要說明如下。

在第一階段確認系爭個人資訊所蘊含之隱私利益的強度及合法性時，須考量所產生及蒐集之資訊的性質，以及政府自聚合元數據（aggregated metadata）中擷取個人資訊之能力[258]。

在資訊性質之分析上，另須考量政府獲取全面歷史性資訊，以及無差別蒐集及保存資訊之因素[259]。前者，在元數據密集技術（metadata-intensive technologies）之使用，已為科技時代之日常的狀況下，不論使用網頁瀏覽器、手機或智慧家電等資訊設備，皆會自動產生、蒐集及儲存大量資訊，故應思考此種涉及敏感資訊之全面性檔案（comprehensive dossier）存在本身，可能即屬一種無可避免、且將導致政府濫權干預之監控型態[260]。後者，鑑於相關業者於提供服務時，可能無差別地全面蒐集及儲存其用戶使用服務之資訊，故應思考相關資訊之蒐集，是否具上述特性，甚至已達個化程度，而逾越社會之預期[261]。

在自聚合元數據中擷取個人資料之能力上，主要與相關資訊得揭露生活隱私之程度有關，就此，可考量下列八類敏感性資訊進行審酌，亦即：*1.*預算或商業交易等財務資訊；*2.*與辯護人面談等法律事務資訊；*3.*各種就醫之身心健康資訊；*4.*與性取向、交往狀況或活動

256 Holland, *supra* note 40, at 1585.
257 *Id.*
258 *Id.* at 1588.
259 *Id.*
260 *Id.*
261 *Id.* at 1588-89.

有關之資訊； *5.* 涉及家庭之相關因素； *6.* 涉及職業領域之相關因素； *7.* 涉及政治傾向之相關因素； *8.* 涉及宗教信仰之相關因素[262]。

最後，當進行上述評估時，須就揭露敏感資訊之可能性及機率進行調查[263]。在可能性之調查上，僅要求抽象認定，例如，手機基地臺位置資訊可能得用以擷取個人之政治、宗教信仰或性習慣等資訊[264]。在機率之調查上，須考量資訊之精確及（或）詳盡程度，例如，是否帶有時間戳記，以及定位之精準程度等；此外，亦須考量資訊之數量及（或）密度，例如，涉及之時間越長且持續密度越高，即越可能洩露敏感資訊[265]。

在第二階段中，依Carpenter案之見解，縱有揭露行為，隱私期待之合理性亦未必削減至不受第四修正案保護之程度，而於評估因揭露所生之削減效果時，須考量揭露之自願性，以確認個人是否確實願與他人共享資訊，此時，由Carpenter案及Riley案之意旨觀察，使用會產生資訊之相關設備或服務，對於參與現代社會生活之必要程度；以及使用者在使用設備或服務過程中，控制資訊自動產生及傳送予第三方業者之能力，為關鍵評估要素[266]。前者，如Riley案指出，手機已是日常生活中之一部分[267]，甚至可謂已成為人類身體之成分[268]，故有將近75%之智慧手機用戶表示，在大多數之時間中，手機皆在距其不到5英尺之範圍內，且有12%之用戶承認，甚至在淋浴時，亦使用手機[269]；另如Carpenter案指出，人們已被迫隨時攜帶手機，不論在其穿越公共道路，或進入私人住宅、診間、政治總部或其他可能揭露隱私之處

262 *Id.* at 1589-90.
263 *Id.* at 1590.
264 *Id.* at 1590-91.
265 *Id.* at 1591-92.
266 *Id.* at 1592-93.
267 *Riley*, 573 U.S. at 385.
268 *Id.*
269 *Id.* at 395.

所[270]。後者，參酌Carpenter*r*案之意旨，須考量下列三項子因素，亦即[271]：*1.*相關資訊是否為自動生成，如用戶除開機外，無須採取進一步之確認行為；*2.*使用設備或服務所進行之活動種類，以及產生相關資訊之比例；*3.*是否可能在不放棄使用設備或服務之前提下，減少或完全拒絕相關資訊之傳遞[272]。

在第三階段進行平衡時，應考量第四修正案確保個人隱私免受恣意侵害及過度警察監控之意旨[273]，以Carpenter案而言，其考量身體活動紀錄可能揭露個人之敏感資訊，且手機基地臺位置資訊提供精確且詳盡之行動軌跡紀錄，又具長期且高密度蒐集之特性，故產生遭政府恣意追溯監控之風險[274]。

四、應否適用第三方原則之風險分配評估要素

由上述討論可知，馬賽克理論所處理者，主要是將某些因適用第三方原則或公眾揭露原則，而被認不具合理隱私期待之資訊，在大量彙集後，質變為具合理隱私期待之整體資訊，並無法完全處理第三方原則在科技時代下所可能造成之管制漏洞。不過，馬賽克理論確已凸顯科技發展對隱私保護所可能產生之影響，且傳統認為已公開之資訊即不得主張合理隱私期待之理論，可能有修正之必要[275]。而其他修正建議，雖切入點未盡相同，然基本上皆具參考價值，只是前三者所提出之修正建議，尚須考量個人揭露資訊之目的、資訊之性質及數量、揭露者對於該資訊之隱私期待、有無相關實定法之保密規定、政府需求及社會規範等評估要素[276]，而最後一種修正建議，則已詳列眾多可

270 *Carpenter*, 138 S. Ct. at 2218.
271 Holland, *supra* note 40, at 1594.
272 *Carpenter*, 138 S. Ct. at 2220.
273 Holland, *supra* note 40, at 1594.
274 *Id*. at 1594-95.
275 張陳弘，前揭註63，頁292-293。
276 *See* Stephen E. Henderson, Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too, 34(4) PEPP. L.

納入審酌之評估要素，明顯較為完整。

針對第三方原則之修正，本文認為，第三方原則乃風險承擔理論之下位概念，其提出及適用涉及風險分配議題，仍有存在之必要性，只是在決定是否將風險分配予交付資訊之個人承擔時，不宜以是否「知悉」會將個人資訊交予第三方為斷，且應將合理隱私期待標準中之主觀隱私期待，納為審查隱私期待是否具備合理性的要素之一，而無獨立檢驗之必要。以下，將先敘述應將主觀隱私期待納為客觀合理性判斷之審查要素的理由，再說明各種得用以決定個案是否適用第三方原則之評估要素，以期適當調整第三方原則於科技時代下之適用範圍，進而兼顧人權保障及追訴犯罪所需[277]。

㈠主觀隱私期待應降階為客觀合理性判斷之審查要素

雙叉法則之第一階層檢驗，主要涉及個人所展現欲阻隔他人窺視其隱私之客觀行為[278]，而因「客觀行為」是否足以阻絕他人窺探，須以社會觀點為斷，故在實際運作上，雙叉法則之主觀分支已流於形式，客觀分支通常方為檢驗是否發生搜索之唯一判準[279]。如論者指出，美國多數法院於操作合理隱私期待標準時，或未提及主觀標準；或僅提及而未實際運用；或有運用，但不影響結論，故可謂合理隱私期待標準已化約為客觀合理期待之單一檢驗步驟[280]。

針對第三方原則與主觀隱私期待之關係，由於當個人自願將其相關資訊交予第三方時，自交付行為之客觀面向解讀，似無法認定其主觀上對該資訊具有隱私期待，故在第三方原則之適用下，原則會被認

REV. 975, 989 (2007).

277 若參酌美國聯邦最高法院於Katz案所提見解，第四修正案之保護重點為「人」，而非「地點」，則以下所提相關評估要素，亦可用以分析我國今年修正刑事訴訟法新增之第153條之3中，相關「空間」是否「具隱私或秘密合理期待」之判斷。

278 Kerr, *supra* note 72, at 127.

279 Wold, *supra* note 48, at 174.

280 Kerr, *supra* note 72, at 114.

定因欠缺主觀隱私期待，而不得主張具備可合理期待之隱私權[281]。就此，雖有論者認為，第三方原則已取代主觀隱私期待之分析，故建議應恢復主觀隱私期待分析之原始力量，以納入權利受侵害者之聲音，並避免第四修正案之分析，淪為發現罪證時之事後偏見[282]，然其主張揭露資訊僅為是否具備主觀隱私期待的考量因素之一，其他諸如個人是否採取相關保護措施、共享資訊是否為使用相關設備之必然結果、個人真正意識到與他人共享資訊之程度等，皆應納入考量[283]，似亦偏向客觀合理性之評估。

此外，若不將主觀隱私期待降階為客觀合理性判斷的審查要素之一，又強調當不符主觀隱私期待之要件時，即不具備可合理期待之隱私權，在科技時代下，無疑會導致隱私權保障之弱化。此因，如前所述，科技發展可能影響一般人對於隱私權之想法及立場，亦即，在隱私期待之客觀合理性判斷上，一般人可能認為相關個人資訊已因科技發展而易於被取得，故個人不得再主張任何權利[284]，就此，或可參酌司法院釋字第689號解釋之意旨進行反制，亦即，因個人不受侵擾之權利，會隨科技之進展而衰弱，故相關法制須與時俱進，以提供適當保護，在此規範層面上，即可認為客觀合理性之判斷不致受科技發展影響，甚至可謂在科技發展之下，應適當提高合理性之評斷結果。然在主觀隱私期待之判斷上，由於個人會隨科技發展，而對使用資訊設備會將個人資訊交予第三方之狀況更為瞭解，以致可能在使用資訊設備後，即無法再主張具主觀隱私期待，此時，若再將主觀隱私期待視為能否主張合理隱私期待之前提判準，無疑將侵蝕隱私權之保障範圍，例如，曾有美國判決指出，因一般網路使用者皆知悉上網即可能遭受駭客攻擊，故在連線使用網路當下，就無法再對個人電腦內存資

281 李榮耕，前揭註29，頁890。

282 Wold, *supra* note 48, at 185-86.

283 *Id.* at 188-89.

284 參考李榮耕，前揭註29，頁929-930。

料主張具主觀隱私期待[285]，即為適例。

據上，本文認為，當進行合理隱私期待之檢驗時，雖仍可保留主觀隱私期待之檢驗要素，然應將其降階為客觀合理性的評估要素之一，不再是主張合理隱私期待之先決要件。

㈡評估要素

雖Carpenter案具開創性，並朝現代隱私權之正確方向邁進[286]，然其除同時指出僅是有限適用外[287]，亦未提出明確之操作標準[288]，而是將相關限制保留予個案中之獨特事實[289]。鑑於在科技時代下，與Carpenter案類似之狀況甚多，許多技術皆允許進行與手機基地臺位置資訊相同、甚至更具侵入性之監視[290]，故如何在科技時代下就是否適用第三方原則提供較具全面性之評估要素，即有探討必要。就此，鑑於隱私權是一種仍在形成及改變之動態概念[291]，會隨時代之演進而更易其內涵[292]，故如Harlan大法官於White案之不同意見書中所強調，隱私之期待是否合理，應取決於已內化在過去及現在之相關規則、風俗及價值中的規範[293]，因此，隱私期待之合理性審查，並非單純機械式計算個人維持其特定資訊秘密之可能性[294]，而應自憲法保障人民不受國家恣意侵害之精神出發，以進行價值取向之判斷[295]，且在考量隱私

---

285 United States v. Matish, 193 F. Supp. 3d 585 (E.D. Va. 2016).

286 Wold, *supra* note 48, at 183.

287 *Carpenter*, 138 S. Ct. at 2221.

288 Paul Ohm, The Many Revolutions of Carpenter, 32(2) HARV. J.L. & TECH. 357, 369-70 (2019).

289 Tonja Jacobi & Dustin Stonecipher, A Solution for the Third-Party Doctrine in a Time of Data Sharing, Contract Tracing, and Mass Surveillance, 97(2) NOTRE DAME L. REV. 823, 862-63 (2022).

290 *Id*.

291 李榮耕，前揭註70，頁118。

292 林利芝，前揭註17，頁187。

293 *White*, 401 U.S. at 786 (Harlan, J., Dissenting).

294 李榮耕，前揭註29，頁944。

295 李榮耕，前揭註29，頁945。

保護之同時，因犯罪者在科技時代下可能利用第三方服務進行犯罪，並隱身於第三方之後[296]，故如何提升偵查人員使用科技措施反制之能力，以與犯罪者利用科技以遂行犯罪之狀況取得平衡，亦為不得不納入考量之要素。

因此，本文認為隱私期待之合理性判斷，其實是一種價值權衡議題，而適用第三方原則以降低隱私期待之合理性，也是價值判斷後之結果，並以風險承擔為實質內涵。關於風險承擔理論，發展自侵權行為法，承擔風險者基本上會獲得特定利益，以作為承擔風險之回報，故若無利益，即無風險承擔；此外，僅當瞭解包含可能之後果及其發生之可能性等風險，且有能力接受或拒絕風險時，方會真正承擔風險[297]，並通常以合約或其他方式明確同意接受損害風險，或明確表明其接受風險之意願，以甘冒可能造成之損害[298]，因此，唯有個人知悉風險並自由且自願承擔風險，方有風險承擔理論之適用，若個人是基於不得已之因素方接受風險，即不在適用範圍[299]。據此，「知悉」風險與「自願承擔」風險，乃不同層次之議題，例如，知悉出外散步可能發生車禍，不代表願意承擔因單純散步即被汽車撞擊之風險[300]；又如縱國家向全民宣告雖拉上窗簾，國家仍可窺視，亦無人會接受人民自此須承擔被國家監視之風險，因此，知悉風險，實與願否承擔風險不同[301]。

296 Kerr, *supra* note 155, at 575-77.

297 Brotherton, *supra* note 163, at 577.

298 *Carpenter*, 138 S. Ct. at 2263 (Gorsuch, J., Dissenting).

299 陳聰富，自甘冒險與運動傷害，臺北大學法學論叢，第73期，2010年3月，頁157。

300 Richard A. Epstein, Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations, 24(3) BERKELEY TECH. L.J. 1199, 1204 (2009).

301 *Id.* at 1206. 另可參見臺灣高等法院花蓮分院109年上字第43號民事判決：「英美法所稱『自甘冒險行為』，常見於運動比賽受傷案例之討論。以比較法觀點，自甘冒險得排除加害人之損害賠償責任，美國通說上認需符合二項要件：⑴被害人知悉危險，且對於該危險進行評估；⑵被害人自願面對該危險。」

而如前所述，不論第三方原則或公眾揭露原則，皆以自願揭露為出發點，並認為當個人自願向第三方揭露資訊時，方須承擔第三方將資訊再移轉予他人之風險，故是否適用第三方原則，亦應以風險承擔理論之第二層次，亦即「自願承擔」之判斷為核心，當事人是否知悉風險，不過是自願承擔風險之前提。

若以Carpenter案於排除第三方原則之適用時，所要求之「深度揭露性」、「全面觸及性」及「蒐集資訊之自動性及不可避免性」三項要素觀察[302]，其實「蒐集資訊之不可避免性」方為真正的唯一判準，至於其他兩項要素，不過是判斷個人是否基於「不可避免」方將資訊交予第三方之評估要素，亦即，當交付之資訊愈具深度揭露及全面觸及性，愈可推論個人是因不得已方交付。

以下，將介紹本文在參考美國聯邦最高法院進行合理隱私期待之四種檢驗模型後，認為在科技時代下，可用以判斷是否適用第三方原則之七項評估要素，其中，第一項至第六項，主要與估評個人是否出於自由且自願而將資訊交予第三方相關；第七項則涉及防止國家濫權之政策性考量。惟須先行說明者有二，其一，聯邦最高法院於United States v. Jacobsen案[303]指出，若相關偵查作為僅會顯示是否存在違禁物之資訊，而不會顯示其他私密事項時，不構成搜索[304]，依此判決之意旨，人民應不得對僅會顯示違禁物資訊之偵查作為主張合理隱私期待，自無再探討是否適用第三方原則以降低隱私期待合理性之必要。

其二，針對以信賴為基礎之職業，因國家甚至須盡力促成及保護個人願向第三方提供相關資訊，故應形成第三方原則之外在界限，例如，論者認為縱個人將其資訊告知醫師，國家仍不得主張第三方原則而任意蒐集醫療資訊[305]；另憲法法院112年憲判字第9號判決亦指出：

302 *Carpenter*, 138 S. Ct. at 2223.

303 United States v. Jacobsen, 466 U.S. 109 (1984).

304 *Id.* at 115-20.

305 Michael Gentithes, App Permissions and the Third-Party Doctrine, 59(1) WASHBURN L.J. 35, 40 (2020).

「未將律師或辯護人與被告、犯罪嫌疑人、潛在犯罪嫌疑人間基於憲法保障秘密自由溝通權之行使而生之文件資料（如文書、電磁紀錄等），排除於得搜索、扣押之外，於此範圍內，與憲法第15條保障律師之工作權及憲法第16條保障被告之訴訟權之意旨不符」，雖此憲法判決非自隱私權之角度思考，但仍舊涉及個人將資訊交予第三方後，是否即無法主張合理隱私期待之議題。基本來說，本文認為至少就刑事訴訟法第182條所定得行使拒絕證言權之職業，因整體社會已在價值判斷後，肯認個人縱將相關資訊交予第三方，仍受保護[306]，故應無適用第三方原則以要求其承擔資訊外洩風險之餘地。

1. 是否有放棄隱私之客觀行為

放棄隱私可能有兩種類型之客觀行為，其一是自願拋棄、棄置或放棄其所持有之物品，此時，即不得再主張具合理隱私期待[307]。至於是否放棄，依美國聯邦第四巡迴上訴法院於United States v. Small案[308]所述，應考量個人之言語、舉止及其他「客觀」面向之因素[309]，與個人主觀意念無涉。至於將目前一般人經常使用之電子郵件長期留存於第三方業者之伺服器，是否該當隱私之放棄，論者指出，在時代進步之下，數位資訊儲存設備之成本降低，相關第三方業者提供使用者大量網路儲存空間，以期提高使用其服務之黏著度，且因數位資訊不具形體，可無限複製，與有形物不同，故個人將數位資訊儲存於第三方業者之通訊系統上，更類似於存放在個人檔案夾或資料庫中，並不當然能解釋為棄置[310]。

其二是自願與他人共享所持有之物或資訊，例如，當「數人對同

306 刑事訴訟法第182條：「證人為醫師、藥師、心理師、助產士、宗教師、律師、辯護人、公證人、會計師或其業務上佐理人或曾任此等職務之人，就其因業務所知悉**有關他人秘密之事項**受訊問者，除經本人允許者外，得拒絕證言。」

307 李榮耕，前揭註4，頁777-778。

308 United States v. Small, 944 F.3d 490 (4th Cir. 2019).

309 *Id.* at 502.

310 李榮耕，前揭註4，頁778-780。

一處所均擁有管領權限之情形，如果同意人對於被搜索之處所有得以獨立同意之權限，則被告或犯罪嫌疑人在主客觀上，應已承擔該共同權限人可能會同意搜索之風險[311]」；另當使用者自行於電腦安裝點對點（peer-to-peer, P2P）連線軟體，以共享電腦中之資訊時，因已允許他人隨意進入其設備中取得資訊，自應承擔資料外洩風險，而不得主張具合理隱私期待[312]。惟應注意者是，與他人共享資訊之行為，雖會降低隱私期待之合理性，但是否適用第三方原則，仍應考量個案中之其他事實，以綜合評斷。

此外，若參考論者所述，應區分是將資訊揭露予公眾或特定對象，前者主觀上難再認有隱私期待；後者因多僅是雙方合法交易之附隨行為，仍有主張合理隱私期待之可能性[313]，可知揭露對象之人數多寡，亦將影響個人是否放棄其隱私之認定。

2.交付個人資訊是否為生活所必需

個人縱有將相關物品或資訊交予第三方之客觀行為，然若屬從事生活所必需之相關活動的附隨行為時，應否認定屬不得已之行為，而排除第三方原則之適用，應審慎評估。此因，在現代生活中，人們須不斷向諸如銀行、網路或交通等第三方業者提供個人資訊，方能取得各式服務，故若認只要向第三方提供個人資訊，即不得享有可合理期待之隱私權，並不合理[314]，例如，Brennan大法官於Miller案之不同意見書中指出，個人向銀行等業者揭露個人資訊，並非全然自願，而是參與現代生活所無可避免[315]；另Marshall大法官於Smith案之不同意見書亦指出，除非放棄使用電話服務，否則，個人無法完全排除接受監控之風險，故在實際層面上，個人可謂幾乎無選擇是否承擔此風險之

311 最高法院104年台上字第503號刑事判決。

312 United States v. Perrine, 518 F.3d 1196 (10th Cir. 2008).

313 Susan W. Brenner & Leo L. Clarke, Fourth Amendment for Shared Privacy Rights in Stored Transactional Data, 14(1) J.L. & POL'Y 211, 257-59 (2006).

314 李榮耕，前揭註29，頁944。

315 *Miller*, 425 U.S. at 451 (Brennan, J., Dissenting).

可能性[316]。而在科技時代下，相關資訊設備之使用已與一般人之生活密切結合，且為有效使用資訊設備及第三方服務，將個人資訊交予第三方業者，通常亦是無從選擇之結果[317]，從而破壞風險承擔之基本假設[318]，故能否謂在交付後即不具隱私之合理期待，實存爭議。

此外，在科技時代下，偵查機關除透過向第三方調閱，以取得偵查目標之個人資訊外，亦可能自行利用科技設備取得。以個人於公共場所之活動資訊而言，若結合馬賽克理論，即有主張具合理隱私期待之可能性，至於國家能否主張適用第三方原則或公眾揭露原則，重點則在個人曝露其行蹤，是否為生活所必需而不可避免。

以利用路口監視器取證為例，我國政府機關所設置之監視器密度甚高，且普遍附有車牌辨識功能，只要輸入特定車牌資訊，即可取得該車輛於數個月內行經監視器涵蓋範圍內之運行軌跡，而因政府機關所設置之監視器位置皆有依法公告，故當人民步出家門時，應可推定已知悉其使用交通工具之行蹤將被國家所掌握；甚至，當監視器密度夠高時，即能直接達到定位目的[319]，若結合衛星影像辨識，監控範圍更廣[320]，而若再結合人臉辨識功能，威力更為強大[321]，故進入受監視區域，可能涉及是否默示同意向公眾交付個人資訊之爭議。就此，因雖個人處於公共場所與非公共場所中之隱私期待合理程度不同，但並無法據以認定人民自願出現於公共場所，即代表自願放棄個人隱私[322]，畢竟，步出家門乃經營日常生活所必需，而一般人對路口監視器之監控，實難以抵抗，故向公眾揭露個人於公開場所之活動，有時

316 *Smith*, 442 U.S. at 750 (Marshall, J., Dissenting).

317 DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 73 (2010).

318 Price, *supra* note 47, at 267.

319 李榮耕，前揭註29，頁876註8。

320 蔡達智，前揭註216，頁70-71。

321 施育傑，科技時代的偵查干預處分——兼論我國法方向，月旦法學雜誌，第306期，2020年11月，頁167-168。

322 許華孚，錄影監視系統在控制犯罪運用的省思，犯罪學期刊，第12卷第1期，2009年6月，頁17。

乃無可避免之事，當不得認只要一出家門而進入監視器之監視範圍內，即無隱私期待可言[323]。

若以我國今年修正刑事訴訟法時新增第153條之1之內容分析，其第3項是以實施調查時間之長短，區分以科技方法追蹤被告或犯罪嫌疑人位置，應否受令狀原則之拘束，故顯已蘊含馬克賽理論之意旨，問題在於，除條文中明示之全球衛星定位系統外，究竟如何解釋該條所定其他「非以辨識個人生物特徵之科技方法」？若純就文義解釋，除人臉辨識技術因明顯屬個人生物特徵，故不得以本條為授權基礎外，調閱eTag資訊、使用車牌辨識或衛星影像辨識等方法，特別是調閱監視器畫面，應否受本條規制，重點在於是否屬「科技方法」，就此，若依法務部於二〇二〇年九月八日以法檢字第10904527940號函公告之「科技偵查法」草案，草案第3條主要規範秘密實施監看及錄影等偵查作為，其立法理由指出：「調取已存在之監看、與聞、測量、辨識、拍照、錄音、錄影資料作為證據，例如調取路口監視器畫面，係依據刑事訴訟法等規範及授權為之，亦非本法之適用範圍」，明確將調閱已存在之監視器畫面定性非屬「科技偵查法」之處理範圍，則或可推論調閱監視器不屬科技方法；另若依行政院院會於二〇二四年五月通過之「科技偵查及保障法」草案，草案第2條第1項與刑事訴訟法第153條之1第1項之規範內容相似，皆使用「得使用全球衛星定位系統或其他非以辨識個人生物特徵之科技方法」之用語，而其立法理由第1點則指出：「衛星定位雖為目前最普遍之即時追蹤位置技術，但追蹤位置之科技方法或技術種類甚多，無論偵查機關是否**以衛星定位系統或其他科技方法**實施追蹤位置或定位之調查，均應遵守本條規定。[324]」並未明確排除調閱監視器之偵查作為；至於若依法務部於法案三讀通過時所整理之內容，刑事訴訟法第153條之1之立法

323 許福生，前揭註214，頁16-17。

324 行政院網站，科技偵查及保障法草案，https://www.ey.gov.tw/File/5B7977D4D8ABA5DC?A=C，造訪日期：2024年8月22日。

理由第3點指出：「衛星定位雖為目前最普遍之即時追蹤位置技術，但追蹤位置之方法或技術種類甚多，無論是否**以衛星定位系統、無人機或其他科技方法**實施追蹤位置或定位之調查，均應遵守本條規定。[325]」亦僅將無人機偵查納入本條規範標的，並未明確排除調閱監視器之偵查作為，故調閱監視器是否屬本條之「科技方法」，尚待司法實務建立可資參考之見解，惟若考量現行偵查實務在監視器之調閱上，已逐漸引進人工智慧之協助，則可預期在不久之將來，調閱及分析監視器畫面之能力將大為提升，進而，在有效維護隱私權之面向上，對科技方法採取較廣寬之解釋，或較為適當。

3. **第三方之背景及於個案中之地位**

如前所述，第三方原則是源於一系列以自然人為虛偽朋友之案例，故論者批判Miller案及Smith案忽略人們對潛在犯罪者與對銀行或電話公司等合法企業間，存在信任上之差異，並指出在法律規範、行業規範及企業聲譽等因素之考量下，個人縱向合法企業或專業人士揭露資訊，仍可主張合理之隱私期待，故是否適用第三方原則，應取決於第三方之背景[326]。就此，涉及本文前述認為當第三方在法律上具拒絕證言之權利時，應成為第三方原則之外在界限的見解，故縱構成自願揭露，亦不應適用第三方原則；反之，則須衡量其他要素，以決定揭露資訊之自願屬性。

另因第三方原則是源於一系列「人與人」對話之背景[327]，故當接收資訊者為自動化機器而非人類時，因基本上不存在機器會將資訊轉交予政府之風險，故究有無第三方原則之適用，即生疑義[328]。就此，美國聯邦最高法院於Smith案中指出，當個人自願向電信公司傳遞撥號資訊，並於正常業務過程中，將該資訊揭露予電信公司之設備時，

---

325 法源法律網，https://db.lawbank.com.tw/GetFile.ashx?pfid=0000373766，造訪日期：2024年8月22日。

326 Ngov, *supra* note 166, at 10.

327 Richards, *supra* note 24, at 1467.

328 Holland, *supra* note 40, at 1570.

亦應承擔電信公司將該資訊再轉交予執法機關之風險[329]，進而將第三方原則之適用範圍，擴及至將資訊揭露予自動化設備之情形[330]。針對此爭議，本文亦贊同聯邦最高法院之結論，此因，自動化蒐集資訊之設備，不過是第三方業者設置用以輔助其遂行業務之工具，對是否適用第三方原則，不應產生影響，否則，將有利用此要素規避執法之可能性。

至於第三方之角色定位為何，亦可能影響個人將物品或資訊交予第三方是否屬不可避免之判定。例如，當將郵件交由郵務公司傳遞[331]或透過電信公司進行通話[332]時，不論郵務公司或電信公司，皆非資訊接收者，而是資訊傳遞者，與Miller案中之支票及存款單等資料，本就是要交予銀行，並不相同，故美國聯邦最高法院並未適用第三方原則，以調降通訊者之隱私期待合理性[333]。另在科技時代下，因電子郵件已大幅度承擔過往實體郵件或電話通訊之功能[334]，且在個人透過電子郵件進行溝通之過程中，相關第三方業者僅是訊息傳遞媒介[335]，故應認無第三方原則之適用，較為妥適。當然，此情形其實也涉及交付資訊屬於現代生活型態所必需之評估要素，甚至憲法為保護將通訊內容交予第三方傳遞時所呈現之特別脆弱狀態，另列舉出秘密通訊自由之基本權，故可謂此種資訊交付行為，業經整體社會肯認，而仍得主張具可合理期待之隱私。

4.第三方有無接觸資訊內容之技術及可能性

同樣以電子郵件之傳遞為例，由於技術上之因素，當第三方業者協助傳遞電子郵件時，其實可能直接接觸信件內容，而當隨時代進

329 *Smith*, 442 U.S. at 774.

330 Holland, *supra* note 40, at 1571.

331 *Warshak*, 631 F.3d at 285 (citing *Smith*, 442 U.S. at 746-47 (Stewart, J., dissenting)).

332 *Id.* (citing *Jacobsen*, 466 U.S. at 114).

333 我國之通訊保障及監察法亦同，請參見該法第3條及第5條等規定。

334 *Warshak*, 631 F.3d at 285-86.

335 *Id.* at 288.

步，一般人愈知悉此技術上之狀況時，是否影響隱私期待合理性之判定，即非無疑。就此，除有認為雖在傳統郵務通訊中，一般人皆知悉郵務人員可能違規開拆其信件，而得知信件內容，但仍無礙通訊雙方得主張合理隱私期待外[336]；另有論者指出，就技術層面而言，電子郵件更類似於電話通訊，此因，不論提供電子郵件或電話通訊服務之第三方業者，皆須在不影響通訊之前提下接觸通訊內容，方能使通訊者順利收發訊息，而若參酌Katz案之見解，美國聯邦最高法院並未因電話公司在技術上能側聽用戶通訊內容，即認定通訊者無法主張合理隱私期待，故在電子郵件之情形中，亦應如此認定，較為適宜[337]。

其實，如前所述，如回歸本質部分觀察，若認使用電子郵件溝通已為現代生活所必需，亦可認將資訊交予身為傳遞媒介之第三方業者，乃無可避免之事，不論第三方業者有無接觸信件內容之可能性，皆宜排除第三方原則之適用。

5.使用者條款等雙方約定狀況

若個人與第三方間存在相關契約條款，是否影響隱私期待合理性之判定，應依個案狀況而定。首先，再以電子郵件為例，當契約約定第三方業者有權接觸資訊時，有認為契約既已載明，通訊者即不得再主張合理隱私期待[338]，然亦有以縱使飯店員工可進入房間清掃，亦不影響房客之合理隱私期待為據，認為通訊者仍得主張合理隱私期待[339]，只是，當契約條款內容明確記載業者可審視、檢查及監看用戶之電子郵件時，則可能有不同結果[340]。針對上述不同見解，論者指出，在科技時代下，人們大量使用第三方服務，並因而提交相關資訊，若認契約條款可完全決定隱私期待是否合理，將使能否享受憲法或法律上之隱私權，完全取決於私人間之決定，並不合理；且因絕大

336 *Id.* at 287.

337 李榮耕，前揭註4，頁791。

338 Freedman v. America Online, 412 F. Supp. 2d 174, 183 (2009).

339 *Warshak*, 631 F.3d at 287.

340 *Id.* at 286.

多數業者皆為締約上之強者，用戶只能選擇接受契約或不使用服務，故強調雙方契約對於隱私期待合理性之判定，無異使憲法對隱私權之保護形同具文，或等同剝奪人民使用在現代社會中幾乎已無法不使用之新型通訊服務，故應認第三方原則在此情形中無適用餘地，較為適當[341]。而此其實即以是否屬生活所必需而不可避免為論述核心。

其次，當契約約定第三方業者負有保密義務時，除有指出在此種狀況中，若適用第三方原則，將使相關服務之使用者信心受衝擊，並產生遭背叛之感外[342]；Gorsuch大法官在Carpenter案之不同意見書中亦指出，在科技時代下，個人透過網路從事各種活動與交易，網路公司不僅因而保有個人資訊，亦為使用者持有該等資訊，以致縱屬最私密之個人資訊，亦存放在網路公司等第三方業者處，故現代一般人皆合理期待交付於相關業者之資訊應被秘密保存，而當雙方存在保密約定時，更是如此，因此，第三方原則並未提供令人信服之理由，以說

341 李榮耕，前揭註4，頁793-796。另可參見臺灣彰化地方法院105年易字第867號刑事判決：「公訴檢察官雖另謂依中華電信與用戶簽訂之定型化契約『市內網路業務服務契約』第45條之約定（見105偵5369卷第215頁反面），中華電信原則上固對業務上所掌握用戶之相關資料有保密義務，但在有司法機關為偵查犯罪或調查證據所需時，得以提供，而主張系爭列印之簽注單影像資料具證據能力（見本院卷第84頁）。惟揆諸通訊保障及監察法第1條規定『為保障人民秘密通訊自由及隱私權不受非法侵害，並確保國家安全，維護社會秩序，特制定本法。』之立法目的，即在於保障憲法所賦與人民之秘密通訊自由，與確保國家安全、維護社會秩序之權衡兼顧，故如上所述，國家為偵查犯罪目的而取得通訊內容，必須依據通訊保障及監察法之規定，經法官核發通訊監察書，始得為之。另方面，電信業者相較於電信使用人而言，屬支配通訊設備使用之強者，如不接受其定型化契約內容，即無從使用該電信業者之電信服務，處於弱勢之電信使用人顯然無法與其抗衡，也根本無法與之議訂而修改電信業者提供之定型化契約，而只能照單全收；於此情形，若謂憑定型化契約之上開概括約定，即令電信使用人事先概括同意電信業者得單方將通訊內容提供給偵查機關，而無需視具體個案取得電信使用人之同意，亦無須遵守通訊監察之法官保留原則，此舉將使憲法第12條所揭櫫保障之人民有秘密通訊自由成為具文，亦將架空通訊保障及監察法所規定之法官保留原則。是公訴檢察官此部分之主張，有悖於憲法保障秘密通訊自由與通訊保障及監察法規定之法官保留原則，要無可採。」

342 許炳華，前揭註243，頁204。

明科技時代下之個人確實自願承擔個人資訊再被轉移之風險[343]。

針對此種情形，本文認為仍應回歸交付資訊是否屬不可避免進行探討，因如上述論者所述，能否主張可合理期待之隱私權，不應完全取決於私人間之決定，而此種主張，不僅在降低隱私期待之合理性判定時可資適用，在人們試圖利用雙方契約以提高隱私期待之合理性時，亦無不同，否則，無疑將使犯罪者在科技時代下可能利用第三方服務進行犯罪，並隱身於第三方之後[344]。因此，雙方契約內容究竟為何，僅是考量是否適用第三方原則的評估要素之一，並不具決定性。

6. 所交付資訊之數量及性質

關於資訊之性質，可分為單一資訊及集合資訊說明。針對單一資訊，如論者所言，因各種資訊應受保護之程度本不相同，故應視資訊之本質，以決定是否適用第三方原則，不得僅因將資訊交予第三方，即令政府享有不受限制之調取權限[345]，例如，當特定資訊涉及個人醫療狀況或性生活等極度私密之事項時，理論上個人自願交予第三方之機會較低，故較可能認定是因不得已方交付；且縱認屬自願交付，而可適用第三方原則，然若參酌Carpenter案之說明，合理性是否降低至完全無法適用第四修正案之程度，須視個案而定，而因原本之隱私期待合理性較高，故調降後仍得主張合理隱私期待之可能性，也較高。

另就集合資訊，則與Carpenter案所提之深度揭露性及全面觸及性有關。基本上而言，愈私密、愈全面之資訊，個人愈不可能自願向第三方揭露，故愈能推定公開屬不可避免之行為，而可排除第三方原則之適用。例如，美國聯邦最高法院於Carpenter案中指出，Miller案及Smith案之見解並非完全以交付資訊之客觀行為進行考量，而是以所交付之資訊是否具敏感性之本質，判斷可否主張合理隱私期待[346]；另

343 *Carpenter*, 138 S. Ct. at 2262-63 (Gorsuch, J., Dissenting).
344 Kerr, *supra* note 155, at 575-77.
345 SLOBOGIN, *supra* note 156, at 157.
346 *Carpenter*, 138 S. Ct. at 2219-20.

美國聯邦第六巡迴上訴法院於United States v. Warshak案[347]中，亦以Miller案之銀行往來紀錄、支票及存款單僅涉及財務資訊，而電子郵件則涉及各式私密資訊[348]，可在分析電子郵件後，推知個人最為深層且私密之生活圖像，而認定將電子郵件交予第三方業者，仍得主張合理隱私期待[349]。此外，除由第三方業者處取得個人資料之情形外，論者亦認為當政府自行以科技設備所取得之個人資訊量愈大及愈精確時，愈應適用令狀原則進行管控[350]。據此，不論是偵查機關自行蒐集或向第三方業者調閱，當所取得之個人資訊愈具深度揭露及全面觸及性時，即愈無第三方原則之適用空間。

以前述Gratkowski案為例，針對被告所提比特幣區塊鏈及Coinbase公司所蒐集之個人資訊，應與手機基地臺位置資訊受相同程度保護之抗辯[351]，聯邦第五巡迴上訴法院回應指出，雖區塊鏈上所儲存之資訊基本上皆永久保存，且任何人皆可存取，然其僅記錄比特幣交易雙方之比特幣地址及交易金額等有限資訊，尚未構成普遍或生活日常中不可或缺之部分，加上移轉比特幣須持有者之積極行為，故判定被告對此公開資訊不具合理隱私期待[352]。

7.控制國家濫權之必要性

由上述評估要素之介紹可知，應否適用第三方原則，主要皆環繞在交付資訊是否屬不得已之行為的判定上，然控制國家濫權之要素，主要為政策考量，與個人是否自願承擔風險之判斷較無關連。

至於為何將此要素列入評估範圍，主要是基於使警察權力回復到新技術出現前之平衡狀態，以避免濫權之考量[353]，如Alito大法官於

347 *Warshak*, 631 F.3d at 266.
348 *Id.* at 288.
349 *Id.* at 284.
350 施育傑，前揭註321，頁166。
351 *Gratkowski*, 964 F.3d at 312.
352 *Id*.
353 Orin S. Kerr, An Equilibrium-Adjustment Theory of the Fourth Amendment, 125(2) HARV. L. REV. 476, 482 (2011).

Jones案之協同意見書中所述，在科技時代來臨前，由於以人力進行長期跟監相當困難且所費不貲，而此現實面之執行限制，即成為隱私權最強而有力之保護機制，然在科技時代來臨後，政府可使用GPS等科技設備，在低成本之狀況下，長期監控個人之車輛移動狀況，此非社會所期待發生之事，而為避免警察權力因科技進步而顯著擴張，以保護人民權利，自應給予相關管制[354]。另在Carpenter案之狀況中，由於歷史性基地臺位置資訊將揭露個人圖像，可達幾乎完美監控之程度，若完全適用第三方原則，即可不受令狀原則等事前管控機制之約束，而使國家得以全面監控個人私生活，且因此種監控方式之成本甚為低廉又具效率，難以透過有限之預算，達成控制國家濫權之目的。因此，為避免過度適用第三方原則，可能導致無法有效管控政府濫權監控之結果[355]，當以其他要素進行評估後，仍無法決定應否適用第三方原則，即代表個案中之爭議頗大，此時，本文基於控制國家濫權之考量，較傾向認定不得適用第三方原則。

伍、結　語

在過往，由於個人以有形財產作為屏障，即可相當程度確保其隱私不被侵犯，且在滿足生活所需時，亦無向第三方交付大量資訊之必要，故只要個人向第三方揭露資訊，被認為符合自願性之要件，而可適用第三方原則，較無爭議。然在科技時代下，除有形財產已無法確

354 *Jones*, 565 U.S. at 429-31 (Alito, J., Concurring). 另可參考李榮耕，前揭註29，頁948-950。此外，依論者以問卷方式所進行實證研究結果，絕大多數受訪者亦認為管制GPS之重點，在於警察濫權使用之可能性，Matthew B. Kugler & Lior Strahilevitz, *Surveillance Duration Doesn't Affect Privacy Expectations: An Empirical Test of the Mosaic Theory* (Coase-Sandor Working Paper Series in Law and Economics No. 727, 2015), at 53-55, https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2419&context=law_and_economics (last visited: 2024.08.22).

355 *See* Joseph T. Thai, Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?, 74(4) FORDHAM L. REV. 1731, 1734-36 (2006).

實用以維持個人資訊之私密性外，向第三方業者提交個人資訊，往往是從事現代生活所不得不之選擇，故能否再一味適用以自願揭露為前提之第三方原則，即生重大爭議。

針對此項爭議，本文認為以第三方原則之實質內涵為風險分配而論，應有其論理上之正當性，故尚無全面廢棄之必要，重點仍在如何判斷提交資訊予第三方是否出於自由且自願。另就如何分配風險而言，誠如論者所述，人們應承擔之風險，應由法律定義[356]，如此，方有較為客觀之判準可供人民及偵查機關遵循，也較易判斷個人在將相關資訊交予第三方後，是否將被降低隱私期待之合理性，並須自行承擔資訊遭外洩之風險。只是，雖以法律明定為最佳選項，然法律畢竟難以全面規範，故除如刑事訴訟法第182條等可作為第三方原則適用界限之規定外，在具體個案中應否適用第三方原則，仍宜有較為具體之評估要素。對此，本文先由美國法上搜索概念之演進出發，帶出合理隱私期待之判斷標準，並說明第三方原則對於隱私期待合理性判斷之影響，最後提出在科技時代下可用以評估是否適用第三方原則的七項要素，以期作為實務運作之參考。

最後須說明者是，在美國法之運作上，縱於評估後決定適用第三方原則以削弱隱私期待之合理性，然是否調降至不受第四修正案保護之程度，仍應視個案狀況，無法一概而論；且縱調降至不受第四修正案保護之程度，亦非謂完全不受保護，只是不受令狀條款及合理條款之約制。因此，我國在操作第三方原則時，亦可參酌此作法，視資訊之性質建立層級化之管控，以期兼顧人權保障及偵查公益所需。

356 Stephen E. Henderson, The Timely Demise of the Fourth Amendment Third Party Doctrine, 96 IOWA L. REV. BULL. 39, 46 (2011).

參考文獻

一、中　文

㈠專　書

・溫祖德，GPS定位追蹤監視之立法論，載台灣2019年聯合國反貪腐公約專題學術研討會實錄論文集，法務部廉政署，2019年11月，頁224-253。

Tzu-Te Wen, Legislative Discussion on GPS Tracking Surveillance, in: *Proceedings of the 2019 Taiwan United Nations Anti-Corruption Convention Symposium*, Agency Against Corruption, Ministry of Justice, pp. 224-253 (2019).

㈡期刊論文

1. 王兆鵬，重新定義高科技時代下的搜索，月旦法學雜誌，第93期，2003年2月，頁166-182。

Jaw-Perng Wang, Redefining Searches in the High-Tech Era, *The Taiwan Law Review*, 93, 166-182 (2003).

2. 王郁霖，智慧聯網時代下數位監聽與第三方保密義務之衝突——以包裹式授權契約為中心，月旦刑事法評論，第10期，2018年9月，頁77-101。

Yu-Lin Wang, Conflicts Between Digital Surveillance and Third-Party Confidentiality in the Smart Network Era—Focusing on Blanket License Agreement, *Criminal Law Review*, 10, 77-101 (2018).

3. 李榮耕，你好，我不好——得一方同意的通訊監察及近年最高法院相關判決簡評，月旦法學雜誌，第174期，2009年11月，頁181-192。

Rong-Geng Li, You're Okay But I'm Not—A Brief Review of Communication Surveillance with One-Party Consent and Recent Supreme Court Decisions, *The Taiwan Law Review*, 174, 181-192 (2009).

4. 李榮耕，論偵查機關對通信紀錄的調取，政大法學評論，第115

期，2010年6月，頁115-147。

Rong-Geng Li, The Law Enforcement's Acquisition of Call Detail Records, *Chengchi Law Review*, 115, 115-147 (2010).

5. 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，國立臺灣大學法學論叢，第44卷第3期，2015年9月，頁871-969。

Rong-Geng Li , GPS Surveillance and Criminal Investigation: A Lesson from United States v. Jones, *National Taiwan University Law Journal*, 44(3), 871-969 (2015).

6. 李榮耕，犯罪偵查中通訊內容的調取，國立臺灣大學法學論叢，第51卷第3期，2022年9月，頁757-831。

Rong-Geng Li, The Obtainment of Communications During Criminal Investigation, *National Taiwan University Law Journal*, 51(3), 757-831 (2022).

7. 林利芝，從美國最高法院United States v. Jones案分析美國政府運用GPS定位追蹤器探知個人位置資訊之適法性，月旦法學雜誌，第272期，2018年1月，頁177-188。

Li-Chih Lin, Analyzing the Legality of U.S. Government's Use of GPS Tracking Devices to Obtain Personal Location Information from the United States v. Jones Case, *The Taiwan Law Review*, 272, 177-188 (2018).

8. 林其樺，數位時代個人隱私界線怎麼畫？——從美國Carpenter v. United States案淺介行動電話定位資訊之隱私合理期待，科技法律透析，第30卷第11期，2018年11月，頁11-15。

Chi Hua Lin, Drawing the Line of Personal Privacy in the Digital Age—An Introduction to the Reasonable Expectation of Privacy in Mobile Phone Location Information from Carpenter v. United States, *Science and Technology Law Review*, 30(11), 11-15 (2018).

9. 林鈺雄，干預保留與門檻理論——司法警察（官）一般調查權限之理論檢討，政大法學評論，第96期，2007年4月，頁189-232。

Yu-Hsiung Lin, The Doorsill Theory—A Study on the Investigative Authority of the Police, *Chengchi Law Review*, 96, 189-232 (2007).

10. 林鈺雄，科技偵查概論——干預屬性及授權基礎（上），月旦法學教室，第220期，2021年2月，頁46-57。

Yu-Hsiung Lin, Introduction to Technological Investigation—Intervention Attributes and Authorization Basis (Part 1), *Taiwan Jurist*, 220, 46-57 (2021).

11. 林鈺雄，科技偵查概論——干預屬性及授權基礎（下），月旦法學教室，第221期，2021年3月，頁42-52。

Yu-Hsiung Lin, Introduction to Technological Investigation—Intervention Attributes and Authorization Basis (Part 2), *Taiwan Jurist*, 221, 42-52 (2021).

12. 金孟華，GPS跟監之程序適法性——從美國United States v. Jones案談起，裁判時報，第68期，2018年2月，頁24-35。

Mong-Hwa Chin, Procedural Legitimacy of GPS Tracking—Starting from the United States v. Jones Case, *Court Case Times*, 68, 24-35 (2018).

13. 施育傑，科技時代的偵查干預處分——兼論我國法方向，月旦法學雜誌，第306期，2020年11月，頁154-174。

Yu-Chieh Shih, Investigative Interventions in the Age of Technology—Discussing the Direction of Taiwan's Legal System, *The Taiwan Law Review*, 306, 154-174 (2020).

14. 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，第48卷第2期，2018年6月，頁267-332。

Chen-Hung Chang, New Development Regarding Search Warrants Under the Fourth Amendment of the U.S. Constitution: Jones, Jardines & Grady, *EurAmerica: A Journal of European and American Studies*, 48(2), 267-332 (2018).

15. 張陳弘，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，2018年12月，頁82-112。

Chen-Hung Chang, The Application of the Reasonable Expectation of Privacy Test in Taiwan—My Expectation? Reasonable in Your View?

Whose Privacy?, *The Law Monthly*, 69(2), 82-112 (2018).

16. 許炳華，大數據時代下隱私權之保護——可能之影響暨對策，興大法學，第20期，2016年11月，頁129-191。

Pin-Hua Hsu, The Protection of Right to Privacy in Big Data Era—Possible Impacts and Countermeasures, *Chung-Hsing University Law Review*, 20, 129-191 (2016).

17. 許炳華，穿戴式科技發展下隱私權保護之探討，財產法暨經濟法，第63期，2021年3月，頁157-217。

Pin-Hua Hsu, The Study on Protection of Privacy Rights Under Development of Wearable Technology, *Property and Economic Law Journal*, 63, 157-217 (2021).

18. 許華孚，錄影監視系統在控制犯罪運用的省思，犯罪學期刊，第12卷第1期，2009年6月，頁1-40。

Hua-Fu Hsu, A Reflection of the Use of Closed-Circuit Television on Crime Control, *Journal of Criminology*, 12(1), 1-40 (2009).

19. 許福生，我國運用監視錄影系統法制規範之回顧與展望，中央警察大學學報，第46期，2009年6月，頁13-62。

Fu-Seng Hsu, A Review and Prospect of Taiwan's Legislation on the Use of Surveillance Systems, *Journal of Central Police University*, 46, 13-62 (2009).

20. 陳聰富，自甘冒險與運動傷害，臺北大學法學論叢，第73期，2010年3月，頁141-184。

Tsung-Fu Chen, The Assumption of Risk and Sports Injury, *Taipei University Law Review*, 73, 141-184 (2010).

21. 黃清德，警察機關要求私人提供資料協助追蹤監視的法律問題——以調閱電信資料及監視錄影資料為例，真理財經法學，第16期，2016年3月，頁1-48。

Ching-The Huang, A Study of Legal Issues on Police Requested Private to Provide Information to Help Track Monitoring, *Aletheia University Journal of Financial and Economic Law*, 16, 1-48 (2016).

22. 黃楷中、呂明龍、沈芳伃，找到你／妳了——淺論GPS偵查犯罪之合法性，司法新聲，第131期，2019年7月，頁66-100。

Kai-Chung Huang, Ming-Long Lu & Fang-Yu Shen, Found You—A Brief Discussion on the Legality of GPS Criminal Investigation, *Judicial Aspiration*, 131, 66-100 (2019).

23.溫祖德，與談意見：以科技偵查跨境取得證據之研究——以美國法為中心（發言紀錄），檢察新論，第27期，2020年2月，頁208-211。

Tzu-Te Wen, Opinions in Discussion: A Study on Cross-Border Evidence Acquisition Through Technological Investigation—Focusing on U.S. Law (Speech Record), *Taiwan Prosecutor Review*, 27, 208-211 (2020).

24.溫祖德，調取歷史性行動電話基地台位置資訊之令狀原則——自美國Carpenter案之觀察，月旦法學雜誌，第297期，2020年2月，頁130-147。

Tzu-Te Wen, Warrant Requirement for Access Historical Cell Site Location Information—Observations from the Carpenter v. United States, *The Taiwan Law Review*, 297, 130-147 (2020).

25.溫祖德，偵查機關調取歷史性行動電話基地臺位置資訊之合憲性審查——從美國聯邦最高法院判決檢視我國法制，政大法學評論，第167期，2021年12月，頁171-256。

Tzu-Te Wen, Historical Cell Site Location Information and Privacy—An Examination of the Taiwanese Current Norm, *Chengchi Law Review*, 167, 171-256 (2021).

26.劉定基，從美國法的觀點評司法院大法官釋字第六八九號解釋——以新聞自由、言論自由、隱私權的保障與衝突為中心，興大法學，第11期，2012年5月，頁195-236。

Ting-Chi Liu, Rethinking Judicial Yuan Interpretation No. 689—Focusing on the Protection of Freedom of the Press, Freedom of Speech, and the Right to Privacy and Their Potential Conflicts, *Chung-Hsing University Law Review*, 11, 195-236 (2012).

27.劉芳伶，從跨巨庫觀點論刑事訴訟法新設「科技設備監控處分」之定性與規制——以「GPS科技之利用」為檢討中心，月旦法學雜誌，第306期，2020年11月，頁111-138。

Fang-Ling Liu, Discussing the New "Technological Equipment Surveillance Injunction" in the Criminal Procedure Law from the Perspective of Cross-Massive Databases—Focusing on the Use of GPS Technology, *The Taiwan Law Review*, 306, 111-138 (2020).

28. 劉耀明，通訊監察之層級化事前管控機制，刑事法雜誌，第60卷第6期，2016年12月，頁25-60。

Yao-Ming Liu, Hierarchical Advance Control Mechanism of Communication Surveillance, *Criminal Law Journal*, 60(6), 25-60 (2016).

29. 蔡彩貞，定位科技在刑事司法程序之運用與人權保障——以利用GPS追蹤為中心，裁判時報，第65期，2017年11月，頁62-78。

Tsai-Chen Tsai, Pinpointing the Role of Technology in Criminal Judicial Procedures and Human Rights Protection—From the Perspective of GPS Tracking, *Court Case Times*, 65, 62-78 (2017).

30. 蔡達智，衛星監控資訊作為法庭證據之實證研究——以高等以上法院裁判為中心，科技法學評論，第5卷第1期，2008年4月，頁61-101。

Ta-Chih Tsai, Satellite Surveillance Information as Evidence in the Higher Court of Taiwan, *Technology Law Review*, 5(1), 61-101 (2008).

㈢網頁文獻

・行政院網站，科技偵查及保障法草案，https://www.ey.gov.tw/File/5B7977D4D8ABA5DC?A=C，造訪日期：2024年8月22日。

Executive Yuan, Draft Act on Technology Investigation and Protection, https://www.ey.gov.tw/File/5B7977D4D8ABA5DC?A=C (last visited 2024.8.22).

二、英　文

㈠專　書

1. SLOBOGIN, CHRISTOPHER, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2008).

2. SOLOVE, DANIEL J., UNDERSTANDING PRIVACY (2010).

㈡期刊論文

1. Arango, Steven, Cloudy with a Chance of Government Intrusion: The Third-Party Doctrine in the 21st Century, 69(4) CATH. U. L. REV. 723 (2020).
2. Arcila Jr., Fabio, GPS Tracking out of Fourth Amendment Dead Ends: United States v. Jones and the Katz Conundrum, 91(1) N.C. L. REV. 1 (2012).
3. Brenner, Susan W. & Clarke, Leo L., Fourth Amendment for Shared Privacy Rights in Stored Transactional Data, 14(1) J.L. & POL'Y 211 (2006).
4. Brotherton, Elspeth A., Big Brother Gets a Makeover: Behavioral Targeting and the Third-Party Doctrine, 61(3) EMORSY L.J. 555 (2012).

5. Brownstein, Charlie, Confronting Carpenter Rethinking the Third-Party Doctrine and Location Information, 92(1) FORDHAM L. REV. 183 (2023).
6. Chambers, Jillian, Carpenter, the Fourth Amendment, and Third-Party Workarounds, 53(1) CONN. L. REV. 183 (2021).
7. Epstein, Richard A., Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations, 24(3) BERKELEY TECH. L.J. 1199 (2009).
8. Gatewood, Jace C., District of Columbia Jones and the Mosaic Theory—In Search of a Public Right of Privacy: The Equilibrium Effect of the Mosaic Theory, 92(3) NEB. L. REV. 504 (2014).
9. Gentithes, Michael, App Permissions and the Third-Party Doctrine, 59(1) WASHBURN L.J. 35 (2020).
10. Henderson, Stephen E., Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too, 34(4) PEPP. L. REV. 975 (2007).
11. Henderson, Stephen E., The Timely Demise of the Fourth Amendment

Third Party Doctrine, 96 IOWA L. REV. BULL. 39 (2011).
12. Henderson, Stephen E., After United States v. Jones, After the Fourth Amendment Third Party Doctrine, 14(2) N.C. J.L. & TECH. 431 (2013).
13. Henderson, Stephen E., Carpenter v. United States and the Fourth Amendment: The Best Way Forward, 26(2) WM. & MARY BILL RTS. J. 495 (2017).
14. Holland, H. Brian, A Third-Party Doctrine for Digital Metadata, 41(4) CARDOZO L. REV. 1549 (2020).
15. Issacharoff, Lucas & Wirsha, Kyle, Restoring Reason to the Third Party Doctrine, 100(3) MINN. L. REV. 985 (2016).
16. Jacobi, Tonja & Stonecipher, Dustin, A Solution for the Third-Party Doctrine in a Time of Data Sharing, Contract Tracing, and Mass Surveillance, 97(2) NOTRE DAME L. REV. 823 (2022).
17. Kerr, Orin S., Four Models of Fourth Amendment Protection, 60(2) STAN. L. REV. 503 (2007).
18. Kerr, Orin S., The Case for the Third-Party Doctrine, 107(4) MICH. L. REV. 561 (2009).
19. Kerr, Orin S., An Equilibrium-Adjustment Theory of the Fourth Amendment, 125(2) HARV. L. REV. 476 (2011).
20. Kerr, Orin S., The Mosaic Theory of the Fourth Amendment, 111(3) MICH. L. REV. 311 (2012).
21. Kerr, Orin S., Katz Has Only One Step: The Irrelevance of Subjective Expectations, 82(1) U. CHI. L. REV. 113 (2015).
22. Martino, Tricia A., Fear of Change: Carpenter v. United States and Third-Party Doctrine, 58(2) DUQ. L. REV. 353 (2020).
23. Murphy, Erin, The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr, 24(3) BERKELEY TECH. L.J. 1239 (2009).
24. Ohm, Paul, The Many Revolutions of Carpenter, 32(2) HARV. J.L. & TECH. 357 (2019).
25. Ormerod, Peter C. & Trautman, Lawrence J., A Descriptive Analysis of

the Fourth Amendment and the Third-Party Doctrine in the Digital Age, 28(2) ALB. L.J. SCI. & TECH. 73 (2018).

26. Park, Eunice, Objects, Places and Cyber-Spaces Post-Carpenter. Extending the Third-Party Doctrine Beyond CSLI: A Consideration of IoT and DNA, 21 YALE J.L. & TECH. 1 (2019).

27. Penn, Daniel, The Fifth Circuit, Fourth Amendment, and the Third-Party Doctrine: Two Takeaways from the Court's First Ruling on Bitcoin Privacy, 24(1) SMU SCI. & TECH. L. REV. 125 (2021).

28. Pozen, David E., The Mosaic Theory, National Security, and the Freedom of Information Act, 115(3) YALE L.J. 628 (2005).

29. Price, Michael W., Rethinking Privacy: Fourth Amendment Papers and the Third-Party Doctrine, 8(2) J. NAT'L SEC. L. & POL'Y 247 (2016).

30. Richards, Neil, The Third Party Doctrine and the Future of the Cloud, 94(6) WASH. U. L. REV. 1441 (2017).

31. Slobogin, Christopher & Schumacher, Joseph E., Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society", 42(4) DUKE L.J. 727 (1993).

32. Thai, Joseph T., Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?, 74(4) FORDHAM L. REV. 1731 (2006).

33. Winner, Kristi, From Historical Cell-Site Location Information to IMSI-Catchers: Why TriggerFish Devices Do Not Trigger Fourth Amendment Protection, 68(1) CASE W. RES. L. REV. 243 (2017).

34. Wold, Ash, Katz in the Digital Age: Why the Katz Subjective Prong Must Be Restrenghtened, 52(1) SW. L. REV. 174 (2023).

㈢網頁文獻

1. Bonvillian, Crystal, *Did Alexa Witness Double Murder? Judge Orders Amazon to Turn over Device's Audio* (Nov. 15, 2018), DAYTON DAILY NEWS, https://www.daytondailynews.com/news/national/did-alexa-witness-double-murder-judge-orders-amazon-turn-over-device-audio/Th2auhV32yPAYro08Y7J0L/ (last visited: 2024.08.22).

2. Kaminski, Margot E., *Carpenter v. United States: Big Data Is Different* (July 2, 2018), THE GEO. WASH. L. REV., https://www.gwlr.org/carpenter-v-united-states-big-data-is-different (last visited: 2024.08.22).
3. Kugler, Matthew B. & Strahilevitz, Lior, *Surveillance Duration Doesn't Affect Privacy Expectations: An Empirical Test of the Mosaic Theory* (Coase-Sandor Working Paper Series in Law and Economics No. 727, 2015), https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2419&context=law_and_economics (last visited: 2024.08.22).
4. Ngov, Eang L., *More Than Friends: Recognizing Dichotomous Relationships in the Third Party Doctrine* (2023), https://ssrn.com/abstract=4357446 or http://dx.doi.org/10.2139/ssrn.4357446 (last visited: 2024.08.22).

The Third-Party Doctrine in the Age of Technology: Centering on Criminal Investigation Process

Yao-Ming Liu*

Abstract

The third-party doctrine holds that when people voluntarily hand over their effects or information to a third party, they should bear the risk of the third party transferring the effects or information to others, including the state, and can no longer claim a reasonable expectation of privacy in respect of such effects or information. However, in the age of technology, it is normal for people to hand over their personal information to a third party while using information appliances. If the third-party doctrine is fully implemented, protecting people's privacy rights may be insufficient. After analysis, this paper holds that because the essence of the third-party doctrine lies in risk allocation, it has legitimacy and is still necessary to exist. This paper also proposes seven evaluation factors to determine whether the third-party doctrine should be applied to investigation measures in the age of technology.

Keywords: The Third Party Doctrine, The Assumption of Risk Rule, Privacy, Reasonable Expectation of Privacy, Warrant Requirement, Surveillance Society

* Assistant Professor, Department of Criminal Investigation, Central Police University; Ph.D. in Law, National Taipei University.

Received: October 27, 2023; accepted: January 14, 2025