科技偵查中的合理隱私期待—
以美國 *Chatrie v. United States* 案為借鏡*

陳昱捷**

---

* 2026 年理律文教基金會專題報告。

** 國立政治大學法學院法律學系碩士班公法組碩士生。

目錄

摘要.....II

第一章 緒論.....1

第二章 *Chatrie* 案「合理隱私期待」認定方法的分析.....3

第一節 案件事實與爭點簡述.....3

第二節 多數意見之認定框架.....3

第三節 小結.....6

第三章 我國刑事訴訟法第 153 條之 2 的審查密度缺失.....7

第一節 概論.....7

第二節 需有審查密度的考量.....8

第三節 小結.....9

第四章 結論.....10

摘要

我國於 2024 年增訂刑事訴訟法（下同）第 11 章之 1 特殊強制處分規定，以因應科技化犯罪偵查之需求。惟第 153 條之 2 及第 153 條之 6 所建構之科技偵查審查機制，是否已能充分保障受調查人之隱私權，仍有待檢視。本文以美國聯邦最高法院於 2026 年 6 月作成之 *Chatrie v. United States* 案為觀察核心，梳理該案多數意見援引 *Katz v. United States* 及 *Carpenter v. United States* 先例，就「地理圍欄令狀（geofence warrant）」所取得之「定位歷史紀錄（Location History）」是否構成美國憲法增修條文第 4 條之搜索，所提出之「合理隱私期待」認定方法，具體萃取出資料精確度、回溯性與持續性監控能力，以及資訊之個人屬性等三項判斷因素。本文並以為，該案多數意見於反對「短期監控無隱私期待」之主張時所揭示「搜索是否合法，自其開始之時即已確定」之原則，實為理解隱私權保障的核心，侵害之有無，繫諸行為發生之時點，而非事後程序是否完備。

本文以此為借鏡，檢視第 153 條之 2 及第 153 條之 6 之現行規範，發見後者所設之事後補發許可書機制，僅能填補「事後監督」之要素，對於「事前審查」之欠缺及隱私侵害發生後之具體權利救濟機制，現行法均付之闕如。本文並援引憲法法庭 111 年憲判字第 1 號判決所揭示「事前審查」與「事後監督暨救濟」缺一不可之正當法律程序基準，類推適用於科技偵查脈絡，佐證現行規範審查密度之不足。基於上述觀察，本文於解釋論上提出補充建議。法院於審查科技偵查許可書時，宜將定位資訊之精確度、蒐集頻率及監控回溯期間等要素，納入審查密度分級之判準；第 153 條之 6 之事後補發機制，應輔以明確之權利救濟規定。長遠而言，立法者宜參酌比較法經驗，重新檢討現行條文是否應採更嚴格之事前法官保留原則。

關鍵字：科技偵查、地理圍欄令狀、合理隱私期待、第三方原則、審查密度、隱私權、刑事訴訟法第 153 條之 2 及第 153 條之 6

第一章 緒論

當前社會科技發達，因此所產生的犯罪方式也愈發多樣。我國為了將有效偵查（search）多樣及複雜之犯罪，因此於 2024 年間增訂刑事訴訟法（下同）第 11 章之 1，特殊強制處分之相關規定。然此偵查方式嚴重影響人民受我國憲法第 22 條隱私權之保障——特別是第 153 條之 2 的規定[1]——於立法理由中亦可窺知立法者有思考到此點，是以「上開調查方式因個人對隨身行動通訊設備本有較高之隱私期待，且調查行動通訊設備位置，將可精確定位及追蹤受調查人位置，對隱私權之干預程度較高，於調查過程中亦可能蒐集虛擬基地台內其他非受調查人之設備號碼或卡片號碼以資比對，對非受調查人之資訊自主權亦造成一定程度之干預，應採較嚴格之程序保障。……為保障非受調查人之資訊自主權不受過度干預，爰於第五項定明使用非受調查人個人資料之限制及供比對結束後應即刪除之規定。[2]」

美國法上，美國聯邦最高法院（下稱聯邦最高法院）早已透過一系列判決發展出「第三方原則（third-party doctrine）」，作為處理科技偵查中隱私權爭議之既有框架[3]，於該國學說亦有所討論[4]。而在今年（2026 年）6 月，聯邦最高法院針對美國政府依「地理圍欄令狀（geofence warrant）」要求 Google 公司提供特定時空範圍內裝置使

---

[1] 刑事訴訟法第 153 條之 2：為調查犯罪情形或蒐集證據認有必要時，得使用科技方法調查被告或犯罪嫌疑人管領或使用之行動通訊設備之位置、設備號碼或使用之卡片號碼。
對第三人管領或使用之行動通訊設備之位置、設備號碼或使用之卡片號碼實施前項調查，以有相當理由可信與被告、犯罪嫌疑人、證人或應扣押之物或電磁紀錄有所關連時為限。
前二項情形，應由檢察官依職權或由司法警察官報請檢察官許可後，以書面記載第一百五十三條之五第一項各款之事項與實施調查之必要性及其理由向該管法院聲請核發許可書。
前項許可之期間，每次不得逾三十日。有繼續實施之必要者，至遲應於期間屆滿之二日前，由檢察官依職權或由司法警察官報請檢察官許可後，以書面記載具體理由向該管法院聲請核發許可書。
實施第一項、第二項調查時，因技術上無可避免取得非受調查人之個人資料，除為供第一項、第二項之比對目的外，不得使用，且於調查實施結束後應即刪除。

[2] 參刑事訴訟法第 153 條之 2 立法理由，立法院法律系統，https://lis.ly.gov.tw/lglawc/lawsingle?00611B7B8D740000000000000000140000000400FFFFFD00^0455 2113071600^00000000000（最後瀏覽日：2026/8/10）。

[3] Katz v. United States, 389 U.S. 347 (1967); United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979); Carpenter v. United States, 585 U.S. 296 (2018).

[4] Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561-602(2009); Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508-29 (2021).

用者之「定位歷史紀錄（location history）」一案[5]，再次引發對於該國憲法增修條文第4條[6]（*the Fourth Amendment*，下稱增修條文第4條）之討論[7]。

回觀我國，第153條之2之立法理由，雖已意識及行動通訊設備定位所涉隱私權干預之特殊性。惟現行條文對於「較嚴格之程序保障」究竟應如何操作、審查密度應達何種程度，似乎尚缺乏具體判準。反觀聯邦最高法院於 *Chatrie* 案中，就「合理隱私期待（reasonable expectation of privacy）」之認定，提出一套具操作性之判斷方法。本文擬以此為觀察借鏡，檢視第153條之2與關聯較為密切之現行規範審查密度是否足夠，並嘗試提出解釋論上之補充建議。是以，本文首先將關懷美國法上對於「合理隱私期待」的相關論述（第二章）；接著關心我國第第153條之2與相關聯的條文，嘗試解構現行法之規範是否合乎憲法的要求（第三章）；最後將縱觀全文提出本文見解（第四章）。

附有言者，因 *Chatrie* 案於本文寫作時方作成不過兩個月[8]，故本文能參閱該案之文獻有限。是以，本文以下將以本案多數大法官據以作成判決的理由，進行較為詳盡之關懷。

---

[5] Chatrie v. United States, 609 U.S. ___ (2026).

[6] *See* U.S. Const. amend. IV ("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.").

[7] Michael Dorf, *Breaking Down Chatrie v. US, the Supreme Court's Landmark Fourth Amendment Decision*, Dorf on Law (July 6, 2026), https://www.dorfonlaw.org/2026/07/breaking-down-chatrie-v-us-supreme.html(last visited August 10, 2026); Cong. Rsch. Serv., LSB11274, *Geofence Warrants and the Fourth Amendment: The Supreme Court Weighs In (June 30, 2026)*, https://www.congress.gov/crs-product/LSB11274(last visited August 10, 2026).

[8] *Chatrie* 案之判決作成時間為2026年6月29日。*See*, Supreme Court of the U.S., *Opinions of the Court – 2025*, https://www.supremecourt.gov/opinions/slipopinion/25(last visited August 12, 2026).

第二章 *Chatrie* 案「合理隱私期待」認定方法的分析

在本章中，本文首先將簡述本案的爭點與案件事實，爾後將進一步關心本案多數意見為何會認定「地理圍欄令狀」要屬增修條文第 4 條的搜索；最後將縱觀本章，提出本章之小結。

第一節 案件事實與爭點簡述

本案源於 2019 年維吉尼亞州（Virginia）一起信用合作社（credit union）搶案。警方鎖定案發地點周邊 150 公尺範圍，向 Google 聲請地理圍欄令狀，依三階段程序取得使用者「定位歷史紀錄」[9]。第一階段取得匿名化（anonymized）裝置定位資料[10]；第二階段，就縮小後的名單取得更長時段、範圍不限於圍欄內外之資料[11]；第三階段取得身分辨別資訊[12]。最終 Google 提供三名使用者身分，其中即包含被告 Chatrie[13]。地方法院認定該令狀違反增修條文第 4 條，惟依善意例外原則（good-faith exception）未排除證據[14]；第四巡迴上訴法院就是否構成「搜索」一事以 7 比 7 票數僵持不下，終仍維持原判決[15]。聯邦最高法院僅就「是否構成增修條文第 4 條之搜索」此一爭點准予調卷，未處理善意例外問題[16]。

第二節 多數意見之認定框架

多數意見援引 *Katz v. United States* 建立之標準，即當個人尋求保護某事物之隱私，且該隱私期待係社會所認為合理者，政府之侵入即構成搜索[17]。而進一步以 *Carpenter v. United States* 案（處理基地台位置資訊，下稱 CSLI）作為分析起點，認為 *Carpenter* 案

---

[9] Chatrie v. United States, 609 U.S. ___, 6-8(2026).

[10] *Id.* at 6

[11] *Id.*

[12] *Id.*

[13] *Id.* at 8.

[14] *Id.* at 9.

[15] *Id.* at 9.

[16] *Id.* at 9. "We granted certiorari solely on the question whether the police violated the Fourth Amendment in obtaining Chatrie's location data, thus declining to consider the exclusionary rule issue."

[17] *Id.* at 11; *see* Katz v. United States, 389 U.S. 347, 351 (1967); Carpenter v. United States, 585 U.S. 296, 304 (2018) "When an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' we have held that off[i]cial intrusion into that private sphere generally qualif[i]es as a search and requires a warrant supported by probable cause."

據以認定搜索成立之理由，「同等或更強烈地」適用於定位歷史紀錄[18]，具體說明三項比較因素：資料精確度[19]、回溯性與持續性監控能力[20]、資料之個人特徵[21]。

首先，針對資料精確度，多數意見以為，在 *Carpenter* 案中，CSLI 只能將特定人位置定位在「1/8 到 4 平方英里（sector ranging from one-eighth to four square miles）」的範圍內；而 Google 定位歷史紀錄則能精準將特定人定位在「20 公尺」以內（該值小於 2% 英里）[22]；另外，針對「監視（logged）」頻率，多數意見說明[23]，CSLI 平均每天只記錄 Carpenter 的位置 101 次；而定位歷史紀錄通常每兩分鐘記錄一次，每日平均高達 720 次[24]。最後，多數意見更以「估算手機垂直高度（estimate a phone's elevation）」進行細緻化的考量標準。其謂，不同於 CSLI，定位歷史紀錄還能估算手機垂直高度，精準透露使用者是進入了多層建築物中的何一層[25]。綜上所述，在第一個標準中，可見定位歷史紀錄所能蒐集到的個人資料相較於 CSLI，除了量多外，更能細緻化獲取之資料客體（data object），而明確知悉（或推知）資料主體（data subject）在建築物中的具體位置。

復次，對於回溯性與持續性監控能力之部分，多數意見以為政府不需像 CSLI 一樣提前決定要監視誰，讓警方能夠在事後「回溯性地（retrospectively）」重構任何區域所

---

[18] *Id.* at 16. "Location History provides an even more fine-tuned picture of a person's movements than CSLI."

[19] *Id.* at 16-7. "*Carpenter* noted that through CSLI records, police could 'achieve[]near perfect surveillance' of an individual holding a cellphone."

[20] *Id.* at 17-8. "Location History also allows police officers to reconstruct 'retrospective[ly],' and with no real effort, people's comings and goings in any area."; "'he has effectively been tailed every moment of every day.'"

[21] *Id.* at 18. "Indeed, Location History records implicate those privacy interests still more than CSLI data because the former is more the individual's own."

[22] *Id.* at 16. "Here is one way of comparing the two: At any given time, CSLI placed Carpenter within a 'sector ranging from one-eighth to four square miles,' whereas Location History pinpointed Chatrie's location within around twenty meters, which is less than two percent of a mile."

[23] *Id.* at 16-7.

[24] *Id.* at 17. "CSLI logged Carpenter's location an average of101 times a day, whereas Location History commonly records a person's location every two minutes, for a daily average of 720 chartings."

[25] *Id.* at 17. "Unlike CSLI, Location History can estimate a phone's elevation—so, for example, can tell whether someone has gone into a doctor's office on the first floor of a multi-story building, or a private apartment on the tenth. Of course, the accuracy of each of the two techniques may vary in different places and at different times. But across the board Location History is the far more precise measure. When the Carpenter Court said that CSLI provides a 'detailed' and 'encyclopedic' portrait of a person's whereabouts, it did not know what further technology was on the horizon."

有人的來往軌跡[26]。此種僅需「點擊按鈕（click of a button）」即可實現的監控，超越了傳統警力所能達到的極限，構成了對無數人和無數地點「不知疲倦且絕對的監控（tireless and absolute surveillance）」[27]。職是以言，Google 的歷史定位紀錄相較過去 CSLI 的定位模式，歷史定位紀錄幾乎等於可以無時無刻監控資料主體，且幾乎沒有任何技術上阻礙[28]。最後，資料之個人特徵。在多數意見的說明中可知，過去 CSLI 時代大多數手機用戶完全不知道有 CSLI 紀錄的存在，更不會去存取它，此些紀錄純粹係電信商基於業務需求所維護的紀錄；相反地，Google 用戶經常主動使用歷史定位紀錄回顧自己曾到訪的位置，因此歷史定位紀錄成為一種「個人日記（personal journal）」[29]。由是可知，當歷史定位紀錄成為資料主體日常使用或是經常關注的資料後，已大大改往過去 CSLI 紀錄的意義。

最後，針對「第三方原則（third-party doctrine）」，多數意見認為在本案中並無適用餘地[30]。原因也許可從該原則定義進行理解[31]，亦即，自然人若將其個人資料自願交付第三方使用時，就需承擔其個人資料再次被移轉與他人知悉的風險。就本案而言，當用戶使用 Google 任一應用程式時，該應用程式即會跳出是否紀錄檢索歷史；此時通常用戶會選擇同意，原因是此乃使用該應用程式的「代價」，因此被迫選擇同意[32]。前述理解

---

[26] *Id.* at 17. "Location History also allows police officers to reconstruct "retrospective[ly]," and with no real effort, people's comings and goings in any area." "As with CSLI, the Government need not decide in advance the kind of surveillance it should undertake, whether of a person or a site. 'Whoever the suspect turns out to be,' Carpenter said of CSLI, 'he has effectively been tailed every moment of every day.'"

[27] *Id.* at 17-8. "Far less could those officials ever perform the 'tireless and absolute surveillance' of any number of people in any number of places, public and private, that Location History can accomplish."

[28] 就此，蓋過去以 CSLI 進行監控需要被監控人，亦即資料主體攜帶手機（當然還需考量訊號是否優良，否則基地台依然無法收到資料）方可以蒐集到其相關資訊；惟在 Google 歷史定位紀錄時代下，幾乎每個人手機所下載的應用程式都會使用定位，因此方產生幾乎沒有任何技術上的阻礙；另外，當然是資料主體個人是否會注意其自己曾經到訪過的位置。後者正是本案多數意見所說明的。*See id.* at 18.

[29] *Id.* at 18. "But Google users, too, regularly employ Location History—for example, 'to remind themselves of a restaurant they ate at two weeks ago, the time they were last at a friend's home, the sites they saw on vacation, or the distance they walked on a particular day.'" "The records thus serve as a personal journal of a user's movements, which that user consults (and even can edit) for his own purposes."

[30] *Id.* at 26.

[31] *See*, United States v. Miller, 425 U.S. 435, 441-43(1976); Smith v. Maryland, 442 U.S. 735, 741-46 (1979); 劉耀明，科技時代下之第三方原則－以刑事偵查程序為核心，興大法學，2025 年 5 月，第 37 期，頁 206-207。

[32] Chatrie v. United States, 609 U.S. ___, 27(2026).

同時也是本案多數意見，以為本案不適用第三方原則原因的其中一項[33]。多數意見的第二個主要原因是認為，本案與過去第三方原則所處理的如 *Miller* 案銀行紀錄、*Smith* 案電話紀錄等，性質上具有很大程度的不同[34]。歷史定位紀錄比起過去的 CSLI 紀錄，能更加詳細（完美）且具回溯性重建用戶的歷史位置[35]；且定位紀錄的產生並非使用者發自內心的自願分享給第三方[36]。因此，從上述論述中可以發見為何在本案多數意見選擇不適用第三方原則，而是適用合理隱私期待的概念進行裁判。

第三節 小結

於本章之說明，可知在 *Chatrie* 案中，多數意見所關心者，已不僅止於傳統「公開或隱蔽」二分下資料主體所處位置之定性[37]，而是進一步將此一問題，收攝進資料本身之精確度、回溯性與資料之個人特徵等實質判準之中，據以重新評價「合理隱私期待」是否成立；另將視角轉向第三方資料公司所得利用的資訊提供予政府，是否構成增修條文第 4 條的「搜索」，進而侵害資料主體的隱私權。是多數意見提出從過去 *Katz* 案所建立的合理隱私期待之概念下，並以 *Carpenter* 案中所確立的標準，再次重述先前標準，並提出三項重要因素構成本案判決的核心。

---

[33] *Id.* at 26-7.

[34] *Id.* at 25.

[35] *Id.* at 25-6.

[36] *Id.* at 26.

[37] *See*, Katz v. United States, 389 U.S. 347, 351-52 (1967).

第三章 我國刑事訴訟法第 153 條之 2 的審查密度缺失

在本章中，本文首先探究第 153 條之 2 與第 153 條之 6 規定。原因是，兩條規範雖放在不同法文內，惟對於犯罪嫌疑人（或被告）之隱私權保障係需置於同一線段上觀察。因此第一節本文概述前述二條文之規範與相關見解後；第二節進一步關懷現行法下，第 153 條之 2 究竟為何要有詳盡的審查密度，方為合乎我國憲法之要求，最後為本章之小結。

第一節 概論

按第 153 條之 2 第 1 項規定，為調查犯罪情形或蒐集證據認有必要時，得使用科技方法調查被告或犯罪嫌疑人管領或使用之行動通訊設備之位置、設備號碼或使用之卡片號碼（本文以下概稱科技偵查）。由是可知，本條規範新增目的是因應日益猖獗的新型犯罪所有[38]（或有謂此規範為「M 化車條款」[39]）。然有時因時間考量，避免犯罪嫌疑人湮滅證據或藏匿，故增訂 153 條之 6 規定，於實施第 153 條之 1 之調查已逾連續 24 小時或已累計逾 2 日、實施第 153 條之 2、第 153 條之 3 之調查，檢察官、檢察事務官、司法警察官或司法警察有相當理由認為情況急迫，而有立即實施之必要者，得逕行實施，並應於實施後 3 日內依各該條規定以書面聲請該管法院補發許可書。立法理由謂：「為因應偵查犯罪之時效性及緊急狀況等急迫情形，……於第一項定明檢察官、檢察事務官、司法警察官或司法警察有相當理由認為情況急迫，而認有立即實施之必要者，可逕行實施調查。」

惟此可值得關懷的問題係：若已實施科技偵查，後因法官不為許可書之補發或裁定（參第第 153 條之 6 第 2 項第 2 款），但當事人之隱私已受侵害，業已遭不可恢復的侵擾，本條項的規定意義何在[40]，本文以為似僅有畫蛇添足之美意[41]。此一問題意識，恰

---

[38] 參林俊益，刑事訴訟法概論（上冊），新學林，2024 年 9 月，頁 441-443；林鈺雄，科技偵查之立法沿革與新法簡介，月旦法學雜誌，2025 年 4 月，第 359 期，頁 6-7。

[39] 林鈺雄，科技偵查之立法沿革與新法簡介，月旦法學雜誌，2025 年 4 月，第 359 期，頁 15。

[40] *See* Chatrie v. United States, 609 U.S. ___, 8-9(2026). Similar procedural contradictions can also be found in U.S. law. In the *Chatrie* case, the district court found that the geofencing warrant "clearly violated" the rights guaranteed by the Fourth Amendment to the U.S. Constitution; however, it did not exclude the evidence on the grounds of the good-faith exception, demonstrating that even if a court finds a warrant unconstitutional, the fact that privacy has already been infringed cannot be remedied through subsequent legal proceedings.

[41] 本文所關懷的主題（issue）是置於我國憲法第 22 條保障「隱私權」架構下進行的討論，故視角必然置於隱私此一旦侵害即無法治癒的觀點。因此縱然未來實務上偵查機關向法院聲請補發許可書，而法院不予補發，該證據雖無證據能力，但犯罪嫌疑人（或被告）之隱私權受到侵害乃不爭的事實。

與本文第二章所梳理之 *Chatrie* 案論證邏輯相互呼應。該案多數意見明白指出，搜索是否成立，不因政府事後選擇性揭露之時間長短、或搜索所得結果為何而受影響[42]。換言之，侵害發生之時點才是隱私權評價之關鍵，而非事後程序是否完備。是從此處往下關心，第 153 條之 2 第 1 項規定於審查密度上，是否已具備足以在偵查之始即攔阻過度侵害之機制，即有進一步檢視之必要。

第二節　需有審查密度的考量

從上述的說明可以知悉，本文一再強調與關心的問題是：隱私權是一遭受侵害事後即無法恢復的權利。因此第 153 條之 6 的補發許可書制度是否合乎我國憲法第 23 條所為的要求，即有進一步思量的空間。此一考量亦非本文所獨創，觀我國憲法法庭 111 年憲判字第 1 號判決（下稱 111 年憲判字第 1 號判決）大法官所示，「系爭規定一（編按：指中華民國 102 年 1 月 30 日修正公布之道路交通管理處罰條例第 35 條第 5 項規定）僅規定汽車駕駛人肇事拒絕接受或肇事無法實施吐氣酒測者，交通勤務警察或交通稽查人員即應將其強制移由受委託醫療機構實施血液之採樣及測試檢定，不分情況是否急迫，事前既未經法官或檢察官之審查或同意程序，事後亦未有任何陳報該管檢察官或法院之監督查核程序；且對受強制實施血液酒精濃度測試檢定者，亦未提供任何權利救濟機制。」該判決雖處理身體權干預之情形，與本文所探討之資訊隱私權干預，於權利性質上尚有不同；惟其所揭櫫「事前審查」與「事後監督暨救濟」三者缺一不可的正當法律程序要求，在類推適用之法理解釋範圍內，對於檢視第 153 條之 6 事後補發許可書制度是否合乎憲法第 23 條比例原則之要求，仍具有參考價值。是第 153 條之 6 之補發許可書制度，是否已足以於「事前」階段，即對科技偵查之發動構成實質有效之審查密度，即非無疑。

反觀第 153 條之 6 之規定，於情況急迫時固然設有「應於實施後 3 日內以書面聲請該管法院補發許可書」之事後審查機制，形式上似已兼顧前揭三項要素中之部分。惟細究其規範內容可知，該機制僅係「事後」之許可補發而非「事前」之審查同意；縱法院嗣後拒絕補發許可書，科技偵查所生的隱私侵害既已發生，實難謂已受到與 111 年憲判字第 1 號判決所要求相當之正當法律程序保障。換言之，若將 111 年憲判字第 1 號判決之審查基準類推適用於本文所探討的科技偵查脈絡下，第 153 條之 6 之補發許可書制度，充其量僅是填補「事後監督」此一要素，至於「事前審查」之欠缺，以及隱私侵害

---

[42] *See* Chatrie v. United States, 609 U.S. ___, 23(2026).

發生後，受犯罪嫌疑人（或被告）所得主張之具體「權利救濟」機制為何，現行法尚付之闕如，此即本文所稱審查密度足之考量之所在。

第三節 小結

綜上所述，本章結合第 153 條之 2 及第 153 條之 6 兩條文綜合觀察，可以發見，雖然可以有效解決法無明文而得到的證據無證據能力此一缺陷[43]，然對於犯罪嫌疑人（或被告）之自身權利——隱私權——可謂毫無保障，是否合乎我國憲法的意旨，在本章所關心的脈絡下，可得到否定的結論。因此，本文以為尚需有進一步之權利救濟措施才是免強合乎憲法所為之要求。

---

[43] 林俊益，刑事訴訟法概論（上冊），新學林，2024 年 9 月，頁 442。

第四章 結論

本文以美國聯邦最高法院於 2026 年 6 月作成之 *Chatrie v. United States* 案為觀察核心，梳理該案多數意見於「合理隱私期待」之認定上，如何援引 *Katz* 案所建立之標準，並以 *Carpenter* 案為分析基礎，具體提出資料精確度、回溯性與持續性監控能力、資訊之個人屬性等三項判斷因素，重新界定政府取得行動裝置定位歷史紀錄是否構成增修條文第 4 條之搜索。本文進一步指出，*Chatrie* 案多數意見於駁斥美國政府「短期監控無隱私期待」之主張時，所揭示「搜索是否合法，自其開始之時即已確定」之原則，實為理解隱私權保障的核心關鍵，侵害之有無，繫諸行為發生之時點，而非事後程序是否完備。

以此為觀察借鏡，本文檢視我國刑事訴訟法第 153 條之 2 及第 153 條之 6 之規範內容，發見現行法雖於立法理由中已意識及行動通訊設備定位所涉隱私權干預之特殊性，並宣示應採「較嚴格之程序保障」；惟第 153 條之 6 所設之事後補發許可書機制，充其量僅填補「事後監督」此一環節，對於「事前審查」之欠缺、以及隱私侵害發生後，犯罪嫌疑人所得主張之具體權利救濟機制現行法均付之闕如。本文並援引憲法法庭 111 年憲判字第 1 號判決所揭示「事前審查」與「事後監督暨救濟」三者缺一不可之正當法律程序基準，類推適用於本文所探討之科技偵查脈絡，益徵第 153 條之 6 現行規範之審查密度尚有未足。

基於上述觀察，本文於解釋論上嘗試提出以下補充建議。首先，法院於審查第 153 條之 2 所核發之許可書時，宜將定位資訊之精確度、蒐集頻率及監控回溯期間等要素，納入審查密度分級之具體判準，而非僅形式審查有無「相當理由」。復次，第 153 條之 6 之事後補發許可書機制，於現行條文架構下應輔以明確之權利救濟規定，使犯罪嫌疑人或被告於隱私權遭受侵害後，至少享有請求確認違法訴訟之相關程序保障，以緩和事前審查欠缺所生之保障落差。最後，長遠而言，立法者宜參酌比較法上之經驗，就科技偵查是否應採行更嚴格之事前法官保留原則，重新檢討現行條文之妥適性。