出國報告（出國類別：進修）

新型態通訊工具監察之研究

服務機關：臺灣臺北地方法院檢察署

姓名職稱：吳孟竹檢察官

派赴國家：美國康乃爾大學

出國期間：102 年 8 月 13 日至 103 年 8 月 12 日

報告日期：103 年 11 月 10 日

摘要

美國最高法院在 *Katz v. United States* 一案將監聽（Wiretapping）定位為搜索，偵查機關若欲使用通訊監察作為偵查手段，程序上須取得法院核發之令狀外，更必須確認個案中存有足以發動通訊監察之「相當理由」。透過觀察美國最高法院對 GPS 追蹤定位科技、紅外線穿透科技及搜索智慧型手機等高科技電子偵查手段的理解，可發現憲法增修條文第 4 條在科技時代下的全新面貌，最高法院對於侵害人民隱私權的公權力行為，逐漸採取較為嚴格的檢驗標準，不再輕易以「風險承擔」、「第三人原則」等概念免除「令狀原則」的要求，顯示司法部門對於人民隱私的尊重。

我國檢警機關也隨著科技的進步發展出各式各樣的電子偵查手段，例如以M化車定位追蹤嫌犯所在位置，或是對嫌犯持有之智慧型手機進行手機鑑識，以取得手機內儲存的各式資訊。我國雖無類似美國憲法增修條文第4條明文賦予人民「不受不合理搜索、扣押權利」之規定，但釋字第631號解釋指出我國憲法第12條所謂人民享有「秘密通訊之自由」，旨在確保人民就通訊之有無、對象、時間、方式及內容等事項，有不受國家及他人任意侵擾之權利。因此，如果新型態的通訊監察工具已侵害人民秘密通訊之自由，即需檢視該等公權力行為是否具有法律依據？縱有法律授權，仍應檢視該等法律能否通過合憲性檢驗？依*Katz*案，偵查作為是否構成搜索不再單以是否具有「物理侵入」為單一判準。更重要的是，推定同意提供個人資訊的「第三人原則」已趨式微，任何國家未經司法部門授權而取得個人敏感性資訊的行為都有可能是違法搜索甚至違法的通訊監察。科技輔助設備之使用，雖可強化偵查人員感官能力，但也同時增加侵害，判斷該等科技輔助設備之使用是否構成「搜索」或「通訊監察」，可綜合：1. 受觀察處所之性質。2. 用以強化隱私之措施。3. 監察措施對私人財產物理侵入之程度。4. 被觀察對象或活動之性質。5. 該項科技提升人類感官能力之程度。6. 該項監察不必要地蔓延、侵入或引起混亂的程度等因素綜合判斷。

新型態通訊工具監察之研究

*吳孟竹

目次

* 臺灣臺北地方法院檢察署檢察官。

壹、前言

一、問題意識（目的）

2012 年臺灣爆發前行政院秘書長林益世索賄案，該案檢舉人陳啟祥向媒體爆料後即不見蹤跡，負責承辦之最高法院檢察署特別偵查組檢察官以證人身分傳喚陳啟祥後，發現陳啟祥隱匿行蹤，不斷變換居處，拒不到案說明，該案承辦檢察官請求警政署刑事警察局（下稱刑事局）協助，刑事局即出動「M 化定位車」（M 化偵查網路手機定位系統），透過確認對象所在區域，再調整發射器角度後，根據蜂鳴聲頻率精準鎖定所在位置，順利在信義區某國際級酒店內將證人陳啟祥拘提到案 。[1]M 化偵查網路手機定位系統，對於偵辦刑事案件確有相當助益，然此種辦案方式係透過精密儀器結合手機基地台，即時掌握人民當下精確所在位置，與向電信業者調取手機門號通聯記錄及基地臺位置逐步比對之方式顯然不同，幾乎讓受追查之對象無所遁形，對人民隱私權侵害更大。因 M 化定位係利用高科技設備剖析犯罪嫌疑人使用手機所在位置，偵查單位用以掌握人民行蹤時是否需受通訊保障監察法規範？又或者此種偵查作實屬「搜索」之強制處分，必須符合刑事訴訟法之相關規定，實有釐清之必要。

透過安裝全球衛星定位（Global Position Satellite, 以下簡稱 GPS）功能之追蹤器追查犯罪嫌疑人是否構成「搜索」之強制處分？就此問題，美國法院判決前後有許多之意見，可供我國司法實務參考。在 *United States v. Knotts*[2]一案中，美國最高法院認為追蹤器僅係協助警方發現無法以肉眼觀察之目標，以肉眼觀察並無憲法爭議，故警方使用協助肉眼觀察之追蹤器也不會有憲法之爭議，並未侵害個人合理隱私期待，不構成搜索 。在 *United States v. McIver*[3]一案中，警方將 GPS 追蹤器裝置在被告所有之四輪傳動卡車上，法院認為汽車外部為一般人皆可見聞之處，警方將追蹤器裝置在屬於汽車外部之汽車底盤處，被告無法主張具有合理隱私期待，因此警方裝置追蹤器之行為不構成搜索。 [4]然而，美國最高法院於 2012 年在 *United States v. Jones* 一案中，就在汽車裝設 GPS 追蹤器追蹤位置之行為是否構成搜索，作出不同認定，多數意見認為裝設 GPS 追蹤器於汽車底盤處侵害憲法增修條文第 4 條所保護的權利，構成搜索。[5]

在科技日新月異的今日，不論是偵查刑事案件或獲取國家安全情報，均可能會使用異於傳統監聽之新型態通訊監察工具，針對透過智慧型手機應用程式、網路社群軟體所為之通訊，相關偵查或國安機構可能已有進行通訊監察之能力。然而，若欲使用各種新型態通訊監察工具，從執法單位之角度觀之，必須確認使用各種通訊監察方式是否符合刑事訴訟法、通訊保障及法之規範。另外，為因應新型態通訊監察工具之使用可能侵害人民隱私權、秘密通訊自由、言論自由甚至人

---

[1] 蘋果日報，特偵「M 化車」料鎖定陳啟祥，2012 年 6 月 30 日。載於：http://www.appledaily.com.tw/appledaily/article/headline/20120630/34336344/ （最後瀏覽日期：2014 年 5 月 12 日）。

[2] United v. Knotts, 460 U.S. 276 (1983).

[3] United States v. McIver, 186 F.3d 1119 (9th Cir. 1999).

[4] *Id*.

[5] United States v. Jones, 132 S.Ct. 945 (2012).

性尊嚴，有重新檢視我國相關法規之必要，避免在強化偵查、情蒐能力之同時，不當地犧牲人民之隱私權。不論是為偵查重大犯罪或蒐集國安情資，若所使用之偵搜方法已屬「搜索」、「扣押」或「通訊監察」，因涉及人民隱私權或財產權之侵害，執行前務必檢驗該等程序是否合法正當，就實質要件部分，必須確保個案具備「相當理由」及相關法律要件，並取得法院之同意。偵查、國安機構之辦案人員、指揮官、機關首長甚至國家元首，均非令狀原則 [6]所要求之客觀中立之「法官」，除在法律另有規範之情況下，不得單方決定發動搜索、扣押及通訊監察等的措施。縱使形式上取得法院之「搜索票」及「通訊監察書」，作為程序發動者的偵察機關
於該等強制處分之妥適性自具有責無旁貸之責任，千萬不得抱持「法院同意法院負責」之消極心態，畢竟在判決確定前，控方對於證據取得之合法性仍具有舉證責任，因此程序發動之指揮者，仍須再行確認各該個案是否確實具備「相當理由」及「執行之必要性」，並要求辦案人員於執行過程中遵行法定程序，以侵害隱私權最小之方式為之。

二、本文論點及架構（過程）

本文在第貳部分將介紹美國通訊監察相關之法制，包括與憲法增修條文第 4 條相關最高法院判例、電子通訊隱私法等。說明在偵查一般犯罪時，美國通訊監察法制所採取之原則。第參部分，本文將介紹數位時代下各種新型態監察手段，並說明各種監察手段所引發美國憲法增條文第 4 條之相關爭議，及如何適用現行美國聯邦法及我國通訊監察法制。最後，本文於第肆部分將歸納美國通訊監察法制值得我國法制參考之處，提出我國通訊監察法制發展之方向。

貳、美國聯邦通訊監察法制

一、憲法增修條文第 4 條及最高法院實務見解

（一）憲法增修條文第 4 條之重要概念

1.「相當理由」及「令狀原則」

美國憲法增修條文第 4 條 [7]保障人民有免於不合理搜索、扣押之憲法上權利，政府欲對人民的身體、住宅、文件及財產實施扣押，必須基於「相當理由」，並具

[6] 關於令狀原則的進一步說明，詳參王兆鵬，刑事訴訟講義，頁 81-97，2006 年 9 月，臺北，作者自版。

[7] 美國憲法增修條文第 4 條：「人民有保護其身體、住處、文件與財產，免於不合理搜索及扣押之權利，除基於相當理由(probable cause)，經宣誓或代誓宣言，並詳載搜索之地點及欲扣押之人或物外，不得核發令狀」。原文為"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."

體特定欲搜索之標的，向法院聲請令狀，始得為之。增修條文第 4 條共有 2 個條款，第 1 個條款為「合理性條款」（reasonableness clause），因為增修條文規定人民有免於「不合理」搜索及扣押之權利；第 2 個條款為「令狀條款」（warrant clause），因增修條文提及：「除基於相當理由，經宣誓或代誓宣言…，不得核發『令狀』」。又增修條文第 4 條明文禁止不合理之搜索、扣押，但並未明白說明令狀之核發為合法搜索、扣押之要件。

關於上開「合理性條款」與「令狀條款」間的關係，在美國學界及實務界有很大的爭議。大約可區分為兩種見解：[8]第一種見解認為上開兩條款具有緊密相連的關係，「令狀條款」可定義及解釋合理性條款。依此見解，除非無法取得令狀，執行搜索之警察必須取得令狀。[9]美國最高法院在 *Katz v. United States*[10]一案中也提及「未經法官事先授權之司法程序所為之搜索，依增修條文第 4 條下本質上就是不合理的」。[11]相對地，另外一種見解則認為，對令狀原則之偏好是司法所創造的，並非憲法所要求的。令狀原則對於合理性原則並無影響，兩者是各自獨立的。持此種見解者認為作為第一條款之合理性條款適用於所有的搜索及扣押，僅要求在考慮各種因素後認為搜索、扣押是合理的。根據最高法院在 *United States v. Rabinowitz*[12] 一案之見解，判斷警方行為之合適標準應該是搜索本身是否合理，而非警方取得搜索票之過程是否合理。[13]根據此種見解，令狀原則的目的在說明何時不應核發令狀，而非何時應或得核發令狀。[14]令狀原則說明任何未經相當理由、特定描述及其他要件支持即核發之令狀，本質上就是不合理的。[15]

暫不論上開爭議結論為何，不管令狀原則是否為憲法增修條文第 4 條之誡命。至少在法律層次，美國刑事訴訟法制就搜索、扣押、通訊監察等強制處分，原則上還是要求政府需先取得法院核發之令狀， 因此令狀原則還是有值得參考之處。政府動搜索需證明個案中具有相當理由，故也可將「相當理由」稱為發動搜索之實質理由。至於何謂「相當理由」，其實不容易清楚定義，判斷個案是否具有「相當理由」更是一件不容易的事。相當理由的概念係指依警方所認知之事實及情形，或根據警方掌握合理可信賴的資訊，足以使謹慎理性之人相信：（1）在逮捕之情形，已有犯罪發生，且所欲逮捕之人即為從事該犯罪之人。（2）在搜索之情況，欲搜索之處所將發現欲扣押之特定物品。[16]

---

[8] JOSHUA DRESSLER & ALAN C. MICHAELS, UNDERSTANDING CRIMINAL PROCEDURE VOLUME 1 : INVESTIGATION,5TH ED.,157-58,NEW PROVIDENCE, NJ, LEXISNEXIS PRESS(2010).

[9] Maryland v. Dyson, 527 U.S. 465(1999).

[10] Katz v. United States, 389 U.S 347(1967).

[11] *Id.* at 357.

[12] United States v. Rabinowitz, 339 U.S.56（1950）.

[13] *Id.* at 66.

[14] Akhil Reed Amar, *Fourth Amendment First Principle*,107 Harv. L. Rev.757, at 774(1994).

[15] *Id.* at 762.

[16] Joshua Dressler & Alan C. Michaels, *supra* note 16, at 116.

2. 何謂「搜索」？

增修條文第 4 條規範之對象限於政府所為之「搜索」、「扣押」，而不及其他不合理之公權力行為，因此，何種政府行為構成「搜索」就成了重要的前提問題。關於搜索之判斷標準，美國實務早期主要是以「物理侵入」為原則，認為公權力之行為必須在物理上侵入「人體、住宅、文件或財產」等增修條文第 4 條所列之標的，才構成增修條文第 4 條之「搜索」。最高法院在 *Boyd v. United States*[17]一案中認為所有私人財產之侵入，即使只有短短幾分鐘，仍為「不法侵入」。[18]*Boyd* 案建立了以「財產權」解釋增修條文第 4 條之基礎。美國最高法院於 1928 年在 *Olmstead v. United States*[19]一案中更確立「物理侵入原則」為判斷增修條文第 4 條「搜索」之標準。該案中認定政府實施電話監聽並不構成搜索，主要理由係因警方實施監聽所安裝之電話線係在受監聽人住處外，並未對受監聽人之財產有任何物理侵入。[20]根據物理侵入原則，美國最高法院認為使用探照燈並不構成搜索，因為光在本質上無法物理侵入。[21]另外，最高法院也認為攜帶隱藏式發報器或錄音機之臥底警察，經同意進入嫌犯之住宅而取得證明犯罪之證據並不構成搜索，因為受邀請之警察並非侵入者。[22]

以財產權或物理侵入作為搜索判斷標準之取徑強調忠於憲法增修條文第 4 條之文義，但隨著科技的進步，公權力侵害人民隱私不再必然伴隨著財產權的物理侵入，透過高科技的輔助，警方不須依賴傳統的住宅搜索即可窺探市民的隱私，若堅持以「物理侵入」作為搜索判斷之唯一標準，缺乏物理侵入之偵查作為即可脫免於增修條文第 4 條之審查，前開最高法院判決之相關事實即可說明。聰明的警察在最高法院的指導下，自然會選擇不具物理侵入，但與「搜索」具有相當效果之偵蒐作為，例如，*Olmstead* 一案中政府所實施之監聽。直到 1967 年 *Katz v. United States*[23]一案，美國最高法院政府推翻了 *Olmstead* 一案之「物理侵入」原則，認為憲法增修條文第 4 條保護的對象不限於財產權，更包括「合理隱私期待」，*Katz* 案為增修條文第 4 條開啟了嶄新的面貌，使該條「免於不合理搜索」之權利從「財產權保護」擴散到「合理隱私期待之保護」。然而，「合理隱私期待」保障之範圍如何界定？在科技不斷進步之時代，警方行為是否侵害「合理隱私期待」更是一個難題。以下將從介紹包括 *Katz* 案在內之數則美國最高法院判決，藉以說明美國法在 *Katz* 案後對於通訊監察之態度。

---

17 Boyd v. United States, 116 U.S. 616(1886).
18 *Id.* at 627.
19 Olmstead v. United States, 277 U.S. 438(1928).
20 *Id.* at 466.
21 United States v. Lee, 274 U.S. 559(1927).
22 Lee v. United States, 343 U.S. 747(1952).
23 Katz v. United States, 389 U.S 347(1967).

（二）通訊內容之監聽（*Katz v. United States*）

1. 案件事實

Katz 透過電話從 Los Angeles 傳送賭博訊息至 Miami 及 Boston 而被起訴違反聯邦法律，聯邦調查局調查員未取得法院令狀即在 Katz 使用的公共電話亭外裝置電子竊聽竊錄設備。Katz 於審理中主張政府竊聽竊錄所得通話內容因違反憲法增修條文第 4 條而不得做為證據。[24]

2. 多數意見（Stewart 大法官主筆）

多數意見不認為本案應從「憲法保障領域」之角度切入，認為憲法保護的是人而非空間，若個人明知卻對公眾揭露時，縱使是在自己的住所或工作場所，亦非憲法增修條文第 4 條保障的對象。但若個人欲保留隱私時，即使在公眾得出入的場所，亦受憲法保護。在電話亭通話的個人可以主張增修條文第 4 條之所保障的權利。[25]多數意見因而認為法院有責任審查被調查者是否期待其行為保有私密性，未取得司法授權之令狀，本案中在公共電話亭外的監聽是不合法的，因此，對被告不利的通話紀錄應被排除不得作為證據。多數意見之論點一改美國最高法院就增修條文第 4 條採取物理侵入之標準，認為增修條文第 4 條保護的對象包括隱私期待。[26]然多數意見並未直接肯認隱私權為增修條文第 4 條所保障之對象，有關隱私權的內容，應保留給各州去立法。

3. Harlan 大法官協同意見書 [27]

Harlan 大法官進一步說明隱私期待之具體的判斷標準，其主張增修條文第 4 條所保護的隱私期待需具備 2 個要件：第一，個人必須實際顯示其主觀上對隱私的期待；第二，個人所顯示之隱私期待須被社會認為是合理的。因此，個人住家在多數的情況是其所認為私密的地方；但暴露使外人一目瞭然的物體、活動或陳述並不受保護，因為並未顯示主觀之隱私期待。[28]本件重要的事實為，使用電話亭的人已將電話亭的門關上，而且付費使用電話，因此該人被賦予通話不受截取的權力。重點不在於電話亭是公眾得出入之場所，而在於該電話亭在該人使用時短暫地成為私密的，享有不被干擾之自由的期待是合理的。[29]最高法院在 *Silverman v. United States*（365 U.S.505）一案已建立截取私密對話構成搜索或扣押的原則，因此毋須檢驗是否侵入私人財產。[30]*Goldman v. United States*（316 U.S. 129）一案雖認為未以有形物理侵入私人財產之電子監察並不違反憲法增修條文第 4 條。但本案促使我們重新考慮 *Goldman* 案的見解，大法官 Harlan 認為該案的見解應被推翻，因為該案對增修條文第 4 條保護之限制，不僅是不當的物理原則，也是不當的法律，因為不管是以電子或是物理侵入方式，都可侵犯合理隱私期待。[31]

---

[24] *Id.* at 348-49.
[25] *Id.* at 351-52.
[26] *Id.* at 352-54.
[27] 大法官 Harlan 在 *Katz* 案的協同意見書，就增修條文第 4 條所保護之合理隱私期待提出進一步的判斷標準，具體說明合理期待的內涵。
[28] *Id.* at 361.
[29] *Id.*
[30] *Id.* at 361-62.
[31] *Id.* at 362.

4. 大法官 White 之協同意見書

大法官 White 強調多數意見在註腳指出本案之決定並不適用於涉及國家安全案件。大法官 White 認為歷來許多總統均授權執行保護國家安全的監聽，若總統或其首席法律官員檢察總長已考量國家安全的要件，其授權之電子監聽就是合理的，就不需要聲請令狀之程序及法官的判斷。總之，大法官 White 認為國安監聽並無令狀原則之適用。[32]

5. *Katz* 案判決評析

Katz 案在物理侵入原則外另外提出「合理隱私期待原則」，不僅將增修條文第 4 條保護之範圍從具體的之財產概念（物理侵入判斷標準）擴大至抽象的合理隱私期待。透過大法官之詮釋，增修條文第 4 條在科技日新月異之現代社會中應能與時俱進。大法官 Harlan 的協同意見雖具體提出合理隱私期待之判斷標準，但大法官 Harlan 所謂在客觀上合理隱私期待必須為社會所能接受的說法可能會產生認定上的不確定性，因為不可能界定何種隱私期待能被社會認為合理，隱私的價值在每個人心中的重要性絕對不同，若過於強調合理隱私期待需被社會大眾所認可，就等於以社會多數意見決定隱私保護之範圍，可能會產生社會多數壓迫社會少數之結果。

（三）得一方同意之監聽（***United States v. White***[33]）

1. 案件事實

1966 年 White 因違反非法交易毒品之聯邦犯罪而被定罪，政府在調查階段派遣線民與 White 接觸，經線民同意，警方在其身上安裝無線電發報器，當線民與被告對話時，警察即利用無線電發報器所發送之無線電波，同步監聽 White 與線民間的對話內容。[34]其中有 4 段對話是發生在線民住處，該等對話內容全為躲在線民住處儲藏室內的警察及在線民住處外使用無線電接收器之警察所監聽。另外警方也使用無線電設備監聽兩人在被告住處、餐廳及線民車上的對話。[35]政府在審判中未讓線民出庭作證，而以實施監聽之警察的證詞作為證據。[36]

2. 多數意見（大法官 White 主筆）

多數意見認為 *Katz* 案雖然推翻了電子監聽僅於物理侵入憲法保護領域時不被許可之原則。但認為 *Katz* 案不影響與本案事實相似之 *Lee v. United States* 一案之結論。因為該案中線民並未不法侵入被告住處與被告對話，最高法院認為利用線

[32] *Id.* at 363-64.
[33] United States v. White , 401 U.S. 745(1971).
[34] *Id.* at 746-47.
[35] *Id.* at 747.
[36] *Id*.

民執行監聽並未違反增修條文第 4 條。[37]此處應探討的是何種隱私期待在憲法上是合理的？亦即什麼樣的隱私期待在無令狀情況下為增修條文第 4 條保護？如果法律並未保障犯罪者所信任之共犯不會是警方的線民，該線民所記錄或發送的對話內容之後成為證據之情況，法律也不該提供任何保護。[38]不容忽視的是從事犯罪活動必須了解並承擔其同夥向警方告密之風險。假若被告的同伴有可能與警方合作，在被告懷疑其同伴可能裝有竊聽器之情況下，認為記錄被告對話內容與同伴向警方告密之情況顯然不同或者較沒有安全感將是純粹的臆測。[39]從證據之價值來看，多數意見認為，相較於警方線民單方的記憶，電子錄音可重複、可靠地呈現被告所說的話。因為錄音的存在，線民較不會改變心意，威嚇或傷害較不可能隱匿不利的證據，也較不可能透過交互詰問證明證詞有誤。[40]雖然上述考量顯然不利於被告，但被告既無法主張憲法上權利排除線民之證詞，多數意見不願承認被告可對本案中更精確的證詞主張增修條文第 4 條之特權。[41]將警方線民無令狀活動及報告當作增修條文第 4 條之合理調查手段，卻將攜帶錄音及無線電發送設備之相同線民視為不合理及違憲的搜索及扣押，這樣的論述是站不住腳的。[42]最後，最高法院在 *Desist v. United States*, 394 U.S. 244(1969)案認為 *Katz* 案之結論只適用於 *Katz* 案宣判後執行電子監聽的案件，而本案電子監聽執行之時點早於 *Katz* 案宣判的，因此，依循 *Desist* 案之結論，多數意見採用 *Katz* 案作成前 *Lee* 案所形成之判例法，認為本案所實施之電子監察並未侵害被告懷特免於不合理搜索及扣押之權利。[43]

3. 大法官 Douglas 所撰寫之不同意見書

大法官 Douglas 認為電子監察是對人類隱私最嚴重的侵害，當我們盲從地容許權力強大的政府以法治、效率及其他有益的目的為由侵入用以保障人民自由的房屋，制憲者透過增修第 4 條所記載隱私的概念將徹底消失。[44]或許沒有人會在意監聽可能造成的侵害，因為僅有少部分不為人知的被告會成為監聽被害人，但因我們今日所崇尚的科技可以控制每個人，故所有人都可能成為監聽的被害人。[45]雖然司法部主張 *Lee* 案的見解在本案中具有決定性的影響，但大法官 Douglas 根據 *Berger* 案及 *Katz* 案堅持反對，並重申根據增修條文第 4 條，電子監察的使用需經司法審查，否則不受控制的電子監察很可能導致美國成為警察國家。[46]

---

[37] White, *Supra* note 33, at 748-50.
[38] *Id.* at 752.
[39] *Id.*
[40] *Id.* at 753.
[41] *Id.*
[42] *Id.*
[43] *Id.* at 754.
[44] *Id.* at 756.
[45] *Id.* at 757.
[46] *Id.* at 760.

4. 大法官 Harlan 所撰寫之不同意見書

On Lee 一案所涉及之事實與本案十分類似，政府探員在該案中利用裝有發報設備的政府線民與被告進行對話，政府探員便可監察線民與被告間對話內容。被告同意線民進入其洗衣房，兩人在洗衣房內相關對話都被政府探員監聽，之後也成為審判中之證據，政府線民在該案中並未出庭作證。[47]最高法院在 *On Lee* 一案並未探討對話內容可否成增修條文第 4 條扣押標的之問題，認為因為欠缺不法侵入，所以不違反憲法。[48]

多數意見依據 *Lopez*、*Lewis*、*Hoffa* 等案而抵擋新近判決強調令狀程序是隱私保障之趨勢，但在多數意見所援引之該等判決中，受監察者所面臨的危險與本案並不相同，在該等案件中，並無第三人秘密監聽之情形。[49]在 *Lewis* 一案，聯邦探員假裝為購毒者而經同意進入被告住處，並完成毒品交易，根據聯邦探員在審判中之證詞，法院同意毒品交易結果作為證據。[50]主筆的首席大法官 Warren 明確表示該案並不存在第三人監聽之情形。同樣地，*Hoffa*、*Lopez* 案亦未涉及秘密監察之事實。[51]多數意見試圖透過以下推論消弭本案事實與上開案件的重大區別：如果 A 可以將 B 所透露的訊息洩漏給其他人（如同 *Lewis* 及 *Hoffa* 案），或者記下之後再透露給其他人（如同 *Lopez* 案），這和 A 與他人串通，以同時發送 A 與 B 間通話內容有何不同？[52]這樣的論述本質上就是主張第三人監聽與臥底偵查兩者是沒有區別的，此種論述主要係基於 2 個假設。第一，第三人監聽之情形不會造成更多的隱私侵害。第二，鑑於政治部門的價值及目標，在電子化時代下不受控管的一方同意監察是可被容忍的執法技巧。[53]多數意見的分析方式，超出對於搜索的主觀期待或風險承擔。我們的隱私期待及所承擔的風險，很大的程度反應出過去至今的習慣及價值所形成的規則。[54]因為法律的任務就是形成、展現及反映，我們不應如法官般僅列出期待及風險，卻未審酌在今日社會是否適用。因此，值得探討的問題為，在憲法所反應的政府體制下，是否應讓人民在連令狀原則保護都沒有的情況下，承擔受電子監聽、監視之風險。[55]

大法官 Harlan 認為應評估實施特定監察手段可能對個人安全感造成的衝擊與該種執法技巧所帶來之效益。對於侵害更廣泛且嚴重危及增修條文第 4 條最在乎的安全感的監察手段，除了需要執法官員的自制外，至少要取得法院的令狀。[56]大

[47] *Id.* at 773.
[48] *Id.* at 773-74.
[49] *Id.* at 784.
[50] *Id.* at 785.
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] *Id.* at 786.
[55] *Id.*
[56] *Id.*

法官 Harlan 認為第三人竊聽的實行將破壞自由社會所標榜處理人際關係間的自信與安全感，這遠超過 *Lewis* 案與 *Hoffa* 案所維持之一般線民偵查手段對隱私所造成的衝擊。[57]

多數意見認為秘密是由告密者或者錄音設備洩漏並無不同的論點，忽略了第三人監聽及錄音將完整及精確地呈現所有對話內容，完全不會有人類報告所具有之錯誤及疏忽的可能性。[58]本案之議題係介於執法機關與私人之間所實施之電子監聽是否需要搜索令狀程序。多數意見僅從違法者的觀點進行期待與風險間之風險分析，是完全未掌握重點。[59]*On Lee* 案並非僅認為罪犯們必須承擔未知的竊聽者會窺探渠等私密生活的風險，該案也讓所有守法的社會成員承擔該等風險。提出增修條文第 4 條之令狀原則之目的，正是要重新分配多數意見認為 *On Lee* 案所塑造的隱私風險。[60]推翻 *On Lee* 案並不會終結電子監聽，但可防止執法官員從事電子監聽，除非執法官員具備相當理由懷疑特定人參與犯罪行為，並經中立司法官員審查該等事實。[61]增修條文第 4 條雖允許在犯罪調查過程中使用現代科技，但根據增修條文第 4 條最近發展的趨勢，僅由執法官員所控制的電子監察，在我們的社會已無容身之處。[62]

5. 判決評析

White 案雖然在提出「合理隱私期待」概念的 *Katz* 案作成，但多數意見竟依循 *Katz* 案作成前 *On Lee* 案之見解，認為政府派遣裝有無線電發送設備的線民從事電子監聽，因犯罪者須承擔遭同夥出賣之風險，所以警方該等電子監察之執行，並未侵害增修條文第 4 條所保障之權利。誠如大法官 Harlan 之不同意見，使用電子設備從事第三人監聽對隱私之侵害遠超過一般臥底偵查手段所侵害之隱私，將秘密訊息告知信任的友人與告知執行電子監聽設備的意義是完全不同的。人類的記憶、精確性及誠實性有其限制，然透過電子儀器所實施之監聽，可正確無誤地揭露個人隱私，多數意見將臥底偵查或者政府線民與使用電子設備之第三人監聽等同視之略嫌速斷。再者，從合理隱私期待之角度來看，在 *White* 案中，被告應可期待其與政府線民在住宅內之私密對話不會受警察竊聽，尤其在私人住處內，被告更可期待該等對話內容，不會遭電子設備同步發送給執行監聽的警察。在未使用監聽設備之臥底偵查或政府線民偵查之情形，嫌疑人自願與臥底警察或線民進行對話，即需承擔對方事後將對話內容告知警方之風險，因此臥底警察或線民事後告知方該等對話內容，未侵害嫌疑人之合理隱私期待。況且，多數意見所謂犯罪者承擔風險的論述顯然是建立在有罪推定的錯誤前提上，事實上，所有人都

[57] *Id.* at 787.
[58] *Id.*
[59] *Id.* at 789.
[60] *Id.*
[61] *Id.* at 789-90.
[62] *Id.* at 790.

有可能成為第三人電子監聽的受害者。若因臥底偵查合法即認為透過臥底警察或線民協助之電子監聽均不受增修條文第 4 條之審查，無異於開放政府以臥底偵查手段規避增修條文第 4 條。最後，多數意見因本案實施電子監聽之時點早於 *Katz* 案作成之時間點，而認為本案無 *Katz* 案之適用，而直接套用 *On Lee* 案之結論，更顯示多數意見墨守成規的保守態度。

關於得一方同意之通訊監察，我國通訊保障及監察法（下稱通保法）第 29 條規定通訊監察不予處罰之情形，其中第 3 款為：「監察者為通訊之一方或已得通訊之一方事先同意，而非出於不法目的者，不罰。」上開規定是否表示我國偵查機關，只要得通訊一方之同意，即可在不具通訊監察書之情形下，對監察之對象實施通訊監察？就此問題，我國司法實務認為該款規定僅為對當事人之免責之保護措施，就通訊監察之實施，司法警察仍需依通保法之程序取得通訊監察書，若不符此程序即屬違法通訊監察。[63]至於警方未事前徵得一方同意之通訊監察，若符合通保法第 29 條第 3 款之規定，即無證據排除法則之適用。[64]我國司法實務認為警方事先徵得通訊一方同意而進行無令狀通訊監察原則上仍屬違法通訊監察，相較於美國最高法院在 *White* 案之保守態度，我國實務見解已洞悉若開放警方為「線民式」、「臥底式」的通訊監察，將造成警方規避通保法之令狀原則，確屬進步。

然而，關於私人自行從事符合通保法第 29 條第 3 款規定之錄音、錄影等通訊監察，是否一律無證據排除法則之適用？雖然證據排除法則所規範之對象不包括私人，且依通保法第 29 條第 3 款之，監察者為通訊之一方或已得通訊之一方事先同意，且非出於不法目的者，不罰。然而，通保法第 29 條僅為違法通訊監察罪[65]

---

[63] 最高法院 93 年度台上字第 2949 號判決：「…司法警察機關實施通訊監察時，必須合於通訊保障及監察法第 5 條第 1 項所規定之要件，且依法取得檢察官或法官所核發之通訊監察書，始得為之；其有通訊保障及監察法第六條所規定之急迫危險，經檢察官以口頭通知先予執行通訊監察者，亦應於 24 小時內補發通訊監察書，始符合法定程序。倘未依上開程序之通訊監察所取得之證據，即屬違背法定程序取得之證據，其有無證據能力之認定，依刑事訴訟法第 158 條之 4 規定，應審酌人權保障及公共利益之均衡維護，以為判斷。至於**通訊保障及監察法第 29 條第 3 款雖規定，監察他人之通訊，監察者為通訊之一方或已得通訊之一方事先同意，而非出於不法目的者，不罰。乃基於衡平原則，對於當事人之一方，所賦予之保護措施。並非謂司法警察機關於蒐集證據時，得趁此機會，於徵得通訊之一方事先同意，即可實施通訊監察，而無須聲請核發通訊監察書，以規避通訊保障及監察法第 5 條、第 6 條所規定之限制。從而司法警察機關縱徵得通訊之一方事先同意而監察他人通訊，其所取得之證據有無證據能力，仍應依刑事訴訟法第 158 條之 4 規定，審酌人權保障及公共利益之均衡維護，以為判斷。否則，豈不發生得以迂迴方式徵得通訊之一方之同意，即可規避應由檢察官、法官核發通訊監察書之不當結果**。…」。（粗體字強調為本文所加）

[64] 最高法院 92 年度台上字第 2677 號判決、94 年度台上字第 716 號判決均提及：「…刑事訴訟法上「證據排除原則」，係指將具有證據價值，或真實之證據因取得程序之違法，而予以排除之法則。**而私人之錄音、錄影之行為所取得之證據，應受刑法第 315 條之 1 與通訊保障及監察法之規範，私人違反此規範所取得之證據，固應予排除。惟依通訊保障及監察法第 29 條第 3 款之規定「監察者為通訊之一方或已得通訊之一方事先同意，而非出於不法目的者，不罰」，通訊之一方非出於不法目的之錄音，所取得之證據，即無證據排除原則之適用…」**。

[65] 通保法第 24 條：「違法監察他人通訊者，處 5 年以下有期徒刑。（第 1 項）執行或協助執行通

之阻卻違法事由，實施通訊監察者具備該等事由者，因欠缺違法性而不構成違法通訊監察罪。但屬於程序法層次之證據排除法則，與規範成立犯罪與否之實體法規不具有必然之關聯性。例如，臥底警察雖欠缺執行通訊監察之實質理由，亦未取得通訊監察書，但為保障個人自身安危，而裝置連線警方之錄音、錄影設備，該臥底警察與嫌疑人間之對話內容、嫌疑人之行為均為警方所錄音錄影。雖實施通訊監察的臥底警察、指揮辦案之警方因具備通保法第 29 條第 3 款之阻卻違法事由而不構成違法通訊監察罪，但該等錄音錄影仍因違反通保法相關程序而屬違法通訊監察。無法改變違法取證之事實。是最高法院在公權力參與通訊監察之脈絡下將程序法與實體法之規定脫勾處理，認為仍有證據排除法則之適用，是合乎邏輯的。

但為何最高法院在私人自行錄音錄影之情形，就是否排除證據此一重要審判程序事項，竟要取決於實體法上是否具備阻卻違法事由？最高法院或許是因為我國刑事訴訟法第 158 條之 4 規範主體為「刑事訴訟程序之公務員」，而認為在私人取證時即不受證據排除法則之限制。然而，通訊監察此一偵查手段對於隱私權或秘密通訊自由侵害甚鉅，美國也不乏如 *White* 案利用私人實施通訊監察之偵查實務，若僅因我國通保法將「監察者為通訊一方或已得通訊一方之事先同意」明文定為阻卻違法事由，即一律認為未經公權力參與之私人通訊監察無證據排除法則之適用，等同鼓勵政府放任私人實施通訊監察，再坐享其成地等待私人提供所得之證據。蓋私人若具有通保法第 29 條第 3 款之阻卻違法事由，則警方自私人取得之證據即完全不需經證據排除法則之審查，可通行無阻地進入審判程序，作為定罪之證據。若私人監聽不符通保法之規定，警方亦可將該等證據作為「秘密情資」使用，再透過法定程序實施通訊監察，取得相關證據。如此一來，任何人都可能成為政府的線民，憲法所保障之秘密通訊自由、隱私權及人與人間的信任關係，均可能因為私人通訊監察的盛行而被徹底摧毀，最高法院此部分見解，應有檢討之必要。

我國通保法於 103 年 1 月修正新增證據排除相關規定或許可為此問題提供一條新的出路。新修正通保法第 18 條之 1 第 3 項：「違反第 5 條、第 6 條或第 7 條規定進行監聽行為所取得之內容或所衍生之證據，於司法偵查、審判或其他程序中，均不得採為證據或其他用途，並依第 17 條第 2 項規定予以銷燬。」上開規定明示違反通保法之通訊監察程序，應採「絕對證據排除原則」，而非刑事訴訟法第 158 條之 4 所採之「相對證據排除原則」，就涉及通訊監察之違法取證，新修正通保法第 18 條之 1 為「特別規定」，應優先於刑事訴訟法第 158 條之 4「普通規定」之適用。鑑於通訊監察對隱私權及秘密通訊自由侵害甚鉅，若公權力不當適用甚

訊監察之公務員或從業人員，假借職務或業務上之權力、機會或方法，犯前項之罪者，處 6 月以上 5 年以下有期徒刑。（第 2 項）意圖營利而犯前 2 項之罪者，處 1 年以上 7 年以下有期徒刑。（第 3 項）

至可能會危及憲法所保障的言論自由。因此對於通保法第 18 條之 1 第 3 項中「違反第 5 條、第 6 條或第 7 條規定進行監聽行為」[66]應在解釋上擴大違背法定程序之通訊監察行為，包括私人實為國家手足延伸之情形，例如政府未取得無令狀而明示或暗示線民使用錄音錄影設備對監察對象實施通訊監察，或者私人本身為長期提供政府情資之線民。該種情況下，若不排除私人通訊監察所取得之證據資料，便無法達成證據排除法則遏止警方違法取證及維護司法正潔之目的，因此該等情形下，私人自行實施之「通訊監察」，縱使私人本身具有通保法第 29 條第 3 款之阻卻違法事由，所取得之證據應仍有證據排除法則之適用。

（四）向銀行調取個人商業紀錄（*United States v. Miller*[67]）

1. 案件事實

1973 年 1 月 9 日，被告所承租的倉庫失火，消防員和警方發現可製造 7,500 加侖之釀酒廠、175 加侖未徵稅之威士忌酒及相關設備。財政部酒菸暨武器管理局在兩週後向被告有開戶之兩家銀行提示由美國聯邦檢察官辦公室核發，而非法院核發之大陪審團要求提示文件之傳票。要求該兩家銀行負責人提出在被告 Mitch Miller 名下所有各種銀行帳戶資料，例如儲蓄、支票或貸款帳戶。兩家銀行均未知被告有關上開大陪審團傳票事宜，即提出相關文件給政府當局。這些文件包括所有支票、存款憑條、兩份財務報表及三份月報表。之後 Miller 及其他 4 位被告遭大陪審團起訴共謀參與違法商業交易。[68]

2. 訴訟程序

政府在審判中提出上開銀行紀錄欲證明被告等所涉嫌之犯罪行為。被告主張上開銀行紀錄是非法扣押之產物，因取證傳票係由聯邦檢察官而非法院核發而具有瑕疵，而提出排除上開銀行紀錄作為證據之動議。上開動議遭到地方法院否決。上訴法院則撤銷地方法院之判決，認為本案中政府透過先要求第三人團體即銀行複製被告所有個人支票，再以要求銀行同意檢視及複製這些銀行紀錄之不當法律程序，規避增修條文第 4 條保護被告免於不合理搜索與扣押之權利。本案中核發傳票並不符合正當法律程序，而銀行職員自願合作亦無影響，因為不當揭露而權

[66] 新修正通保法第 18 條之 1 第 3 項雖規定證據排除對象為「監聽行為」所取得內容或衍生證據，然參考同條第 2、3 項規範對象均為「通訊監察」，且觀察通保法全部法條文字，除第 13 條第 1 項說明「監聽」為「通訊監察」之其中一種方法外，僅第 5 條第 4 項及第 18 條之 1 第 3 項的法條文字使用「監聽」2 字，其他部分法條文字多使用涵蓋範圍較為廣大的「通訊監察」，而不限於「監聽」，本文認為通訊監察取得證據資料不以監聽為限，第 18 條之 1 第 3 項「監聽行為」等文字宜改為「通訊監察」，在立法修正前，對於監聽之外的違法通訊監察行為，或可類推適用該條證據排除之規定。

[67] United States v. Miller, 425 U.S. 435(1976).

[68] *Id.* at 437-38.

利受威脅的是銀行存戶而非銀行職員。[69]最高法院則撤銷上訴法院之判決，認為本案中並無侵害被告增修條文第 4 條權利之事實，地方法院否決被告排除證據之動議是正確的。[70]

3. 多數意見（由大法官 Powell 主筆）

最高法院認為上訴法院將受傳票要求提出之文件置於受保護之隱私領域是錯誤的。首先，系爭文件並非 Miller 之「私人文件」，而是銀行所有之「商業紀錄」，Miller 無法就該等文件主張所有權或持有權。有關 Miller 銀行帳戶之紀錄，就如同其他在銀行法下規定銀行為交易一方時需要保存各種紀錄一樣。[71]Miller 雖主張銀行法之規定使得本案中之傳票在功能上相當於對銀行存款戶私人文件「搜索」或「扣押」。多數意見認為所謂銀行存款戶享有增修條文第 4 條之利益並不存在。[72]Miller 以 Katz 案之意見為依據強調其對銀行保存之紀錄享有增修條文第 4 條之利益，因為這些個人紀錄僅在限定用途內供銀行使用，因此被告對這些個人紀錄具有「合理隱私期待」。

然而，多數意見認為在 *Katz* 案中法院亦強調個人若明知而暴露於眾即不受增修條文第 4 條所保護。縱使以支票原本或者存款憑條為討論對象，而非本案中政府透過傳票所取得及檢視之縮微膠卷副本（microfilm opies），多數意見亦認為個人對於這些銀行紀錄之內容並不具有合理隱私期待。銀行支票並非秘密通訊而是用於商業交易中可轉讓之文件。本案中取得包括財務報表、存款憑條等文件僅含有自願透露給銀行及其職員供作商業目的使用之資訊。國會在制訂銀行法時認為我們對銀行紀錄所保存之資訊欠缺合理隱私期待。蓋立法目的已明確表示要求保存銀行紀錄，因為這些紀錄對於刑事犯罪、稅務及行政之調查及訴訟程序很有幫助。[73]存款戶將其個人資訊給他人時，他就承擔接受資訊者會將該等資訊透露給政府之風險。最高法院已多次認為增修條文第 4 條並不禁止取得由第三人獲悉後而透露給政府機關之資訊，即使該資訊提供時被認為只供限定目的使用，而且相信第三人並不會洩密。[74]縱使在銀行紀錄必要資訊及遵守傳票之命令時把銀行當作政府人員，本案也沒有對存款戶之增修條文第 4 條權利有何侵害。[75]

多數意見認為銀行法要求所有銀行保存銀行紀錄並非刻意規避增修條文第 4 條權利之新工具，而僅是藉著保存銀行紀錄以備隨時需要之方式促使此種存在已

[69] *Id.* at 438-39.
[70] *Id.* at 440.
[71] *Id.* at 440-41.
[72] *Id.* at441.
[73] *Id.* at 442-43.
[74] *Id.* at 443.
[75] *Id.*

久、合適之執法方式能繼續執行。[76] 最後，多數意見認為使用銀行紀錄現有法律程序相符，而傳統區分搜索令狀及傳票之標準仍受認可。總之，Miller 欠缺增修條文第 4 條之利益而無法質疑傳票之有效性。[77]

4. Brennan 大法官不同意見書

加州最高法院在 *Burrow v. Superior Court* 一案中認為個人對於其在銀行之存款報告及相關紀錄具有合理隱私期待，銀行同意交付該等紀錄給警長及檢察官並不代表被告有效同意。因此警方取得該等紀錄即為非法搜索、扣押之產物。大法官 Brennan 認為上開結論亦適用於本案，特別是加州最高法院所適用之加州憲法規定與聯邦憲法增修條文第 4 條之內容完全相同。[78]此外，大法官 Brennan 亦援用本案上訴法院之見解，認為銀行之客戶可預期所提供給銀行商業目的使用如支票等文件會保有私密性，而這樣的期待是合理的。銀行客戶之合理期待係若非基於正當法律程序之強制要求，渠等所提供的資訊應僅限於銀行內部營業使用。因此銀行客戶對於銀行會保持該等文件之機密性具有合理期待。[79]歸納上開判決意見，Brennan 大法官認為 Miller 對於銀行紀錄具有合理隱私期待，而銀行應警方要求而同意交付該等紀錄並不等同 Miller 有效同意交付，因為所討論的是 Miller 而非銀行之隱私權。[80]

5.大法官 Marshall 不同意見書

最高法院在 *California Bankers Assn. v Shultz*(416.U.S.21)(1974)一案中認為銀行秘密法（Bank Secrecy Act）中要求保存銀行紀錄之規定為合憲。大法官 Marshall 在該案的不同意見即認為在欠缺相當理由及法院令狀之情形，要求銀行保存客戶銀行紀錄是非法扣押。最高法院於 *California Bankers Assn* 案中認為遵守法規要求而保留客戶簽發支票之副本，既非搜索亦非扣押。本案多數意見認為被告對銀行紀錄不具增修條文第 4 條保護之利益，了無新意。因銀行秘密法授權在無法院令狀亦無相當理由之情形下扣押客戶之銀行紀錄，而大法官 Marshall 認為這樣的規定是違憲的。[81]

6. 判決評析

Miller 案本有將 *Katz* 案所建構「合理隱私期待」發展至商業紀錄領域之機會，但多數意見以銀行秘密法立法目的提及保存銀行紀錄有助刑事調查、訴訟為由，

[76] *Id.* at444.
[77] *Id.* at445.
[78] *Id.* at 447-48.
[79] *Id.*at 448-49.
[80] *Id.*at449-50.
[81] *Id.*at 455-56.

認為銀行存款戶對於該等銀行紀錄並無合理隱私期待。此種貌似有理的說法實在禁不起法理之檢驗，分析如下：

第一，限定目的用途供銀行使用與明知而暴露於衆顯然不同。被告以 *Katz* 案為基礎主張本案其與銀行間約定個人銀行紀錄僅供限定用途使用，顯然被告對於該等紀錄主觀上具有隱私期待。而客戶與銀行間約定客戶資訊具有秘密性，這樣被告所主張之隱私期待應屬合理，依 *Katz* 案中 Harlan 大法官所提出判斷「合理隱私期待」之標準檢驗，被告對其個人銀行紀錄應具有合理隱私期待。多數意見摘取 *Katz* 案中「明知而暴露於衆即喪失合理隱私期待」的論述魚目混珠地否定對銀行紀錄之合理隱私期待。被告提供銀行相關個人資訊僅供有限商業目的使用是一種「原則保密，例外使用」之契約條款，多數銀行客戶應能期待銀行僅在交易上有必要時才會使用該等銀行紀錄，這與將個人支票影本張貼在網路上供人觀覽之「暴露於眾」作法顯然無法劃上等號？多數意見再以支票是可流通之交易支付工具為由說明發票人欠缺「合理隱私期待」。問題是，本案偵查機關是從「銀行」而非其他「個人」取得與被告有關之完整銀行紀錄，「銀行」既與銀行存款戶有限定目的使用之約定，被告仍應就銀行所保存之銀行紀錄享有合理隱私期待。

第二，非權利主體無權處分無補正效果。如大法官 Brennan 不同意見書所述，本案牽涉之隱私權享有主體為銀行存款戶，而非保存銀行紀錄之銀行。因此，若正確地將調取、檢視銀行紀錄之行為定性為「搜索」，非隱私權主體之銀行，在未告知銀行存款戶之前，即越俎代庖地將被告之銀行紀錄提供給政府使用，無法被理解為合法的「同意搜索」。

（五）調取電話通聯紀錄（*Smith v. Maryland* [82]）

1. 案件事實

1976 年在美國馬里蘭州巴爾的摩發生一樁搶案，被害人向警方描述嫌犯及其在犯罪現場附近看到疑為嫌犯使用之汽車。搶案發生後，被害人開始接到自稱是搶劫嫌犯所撥打的恐嚇及色情騷擾電話。警方也在被害人住處附近發現符合被害人描述之男子駕駛符合描述之汽車。透過追蹤該車車牌號碼，警方得知該車登記在本案被告 Smith 名下。[83]警方後來請求電話公司在其中央辦公室安裝撥號記錄器（pen register），以記錄 Smith 住處電話所撥出的電話號碼。警方在安裝撥號記錄器前並未取得令狀或法院命令，撥號記錄器顯示 Smith 住處之電話曾撥話至被害人所使用的電話，警方以此及其他證據為基礎取得搜索 Smith 住處之令狀。[84]執行搜索後發現 Smith 住處內之電話簿載有被害人姓名及電話的那頁被折起來，Smith 遭警方逮捕，並於列隊指認（lineup）時為被害人指認為搶劫嫌犯。[85]Smith 遂被以搶劫罪名起訴。Smith 在預審階段主張排除所有由撥號記錄器衍生之證據，

[82] Smith v. Maryland, 442 U.S. 735(1979).
[83] *Id.* at 737.
[84] *Id.*
[85] *Id.*

理由是警方在安裝撥號記錄器前並未取得法院核發之令狀。[86]

2. 多數意見（大法官 Blackmun 主筆）

多數意見認為增修條文第 4 條適用與否，取決於政府是否侵害 *Katz* 案所提出之合理隱私期待。[87]因為撥號記錄器是被安裝在電話公司所有的中央辦公室，被告顯然無法主張其財產遭受侵害或者警方侵入憲法所保護的領域。儘管並無物理侵入，被告另主張州政府侵害其所享有之合法隱私期待。[88]但撥號記錄器與 *Katz* 案中之竊聽設備迥然不同，因撥號記錄器並未取得通訊的內容。該儀器僅僅透露被撥打的電話號碼，既未表明撥話者與接聽者之任何通訊內容、對話者之身分，亦無法表明該通話是否已經完成。[89] 有鑑於撥號記錄器功能有限，被告主張安裝及使用電話號碼記錄器等行為構成「搜索」之論點必須建構在其對所撥打的電話號碼具有合法隱私期待之基礎上。[90]

首先，多數意見就一般人民對其所撥出之電話號碼是否存有隱私期待一事，持懷疑的態度。所有電話使用者均了解必須透露電話號碼給電話公司，電話公司才能透過轉接設備接通電話。所有電話使用者均知道電話公司能將用戶所撥打的電話號碼之紀錄永久保存，以便確認每月的長途電話費用。[91]事實上，撥號記錄器及相類似的設備已被慣常地用於確認電話計費、偵測電話詐欺以及防範違法等用途。[92] 電話用戶基本上了解他們必須透露電話號碼的資訊給電話公司，而電話公司具有記錄這些資訊的設備，而事實上保存這些資訊也符合各種正當合理的商業目的。雖然無法以科學方式測量主觀期待，但若認為電話用戶在此情況下仍期待所撥打的電話號碼具私密性就太不合理了。[93]

被告雖主張其藉著在私人住宅內使用電話的行為，顯示其隱私期待。然而，電話的位置對於本案的分析而言並不重要。雖然被告在家中撥打電話之行為可視為其欲將電話通話內容視為私密的，但其行為無法被視為其欲保持所撥打之電話號碼的私密性。不管在什麼地方，被告若欲成功通話，均必須提供欲撥打之電話號碼給電話公司。 被告以其住宅電話或其他電話通話並無差別。[94] 再者，縱使被告對其所撥打之電號碼話的私密性主觀上具有隱私期待，這樣的期待也無法被社會認為是合理的。 因為最高法院一向認為個人對於其自願提供給第三者的資訊沒有合理隱私期待。[95]例如，在 *Miller* 案中，最高法院認為銀行存款人對於其同意提供給銀行之財務資訊，並沒有合理的隱私期待，因為存款人提供資訊時就已承擔該等資訊會被提供給政府之風險。[96]最高法院不斷主張增修條文第 4 條並未禁止取得已被透露給第三人，並由第三人提供給政府的資訊，即使該等資訊在透露給第三人時被設定為用於有限用途，且資訊提供者認為第三人不會背叛資訊提

---

[86] *Id*.
[87] *Id*. at 740.
[88] *Id*. at 741.
[89] *Id*.
[90] *Id*. at 742.
[91] *Id*.
[92] *Id*.
[93] *Id*. at 743.
[94] *Id*.
[95] *Id*. at 743-44.
[96] *Id*. at 744.

供者。存款人已承擔資訊遭揭露的風險，因此 *Miller* 案認為存款人認為其銀行紀錄具有私密性之隱私期待是不合理的。[97]本案中，因被告自願提供電話號碼給電話公司，並將該等資訊揭露給電話公司商業經營所使用的設備，如此一來，被告已承擔電話公司可能會將其撥打之電話號碼提供給警方的風險。[98]多數意見認為被告很可能對於其所撥打之電話號碼實際上並無隱私期待，縱使有，這樣的隱私期待也不是合理的。因此，本案安裝撥號記錄器之行為並不構成「搜索」，故不需令狀。[99]

3. 大法官 Stewart 不同意見書（大法官 Brennan 加入）

大法官 Stewart 認為從私人電話撥打的電話號碼，仍在增修條文第 4 條及第 14 條的保障範圍內。[100]最高法院在 *Katz* 案中已承認用來進行通秘密通訊的公共電話具有重要的地位，私人電話自然具有更重要的地位。然而，多數意見竟因為撥話者所撥打之電話號碼可能因為收費之目的而被電話公司記錄，而認為從私人電話撥打之電話號碼不受憲法保障。[101]電話通訊內容本身必須以電子傳輸方式傳遞至電話公司之設備，透過使用電話公司的設備，該等通訊內容可能被記錄或被偶然聽到，但我們仍認為即使是公共電話的使用者，都享有其談話內容不會對外播送之權利。[102]大法官 Stewart 認為從私人電話撥打的電話號碼，就如同電話通話內容，均在 *Katz* 案所承認之憲法保障範圍內。電話用戶對於透過撥號記錄器對私人電話監察所取得之資訊內容具有合理隱私期待。該等資訊是透過對在私人住處或其工作場所內之私人行為進行監察所取得的，而這些場所無疑地是受到增修條文第 4 條及第 14 條所保障。再者，無論是否以物理侵入方式取得，該等資訊都為 *Katz* 案所保障之電話資訊所不可或缺的一部分。[103]雖然私人電話所撥打的電話號碼，的確較通話內容本身平凡許多，但並非與內容無關的資訊。多數私人電話用戶的電話號碼可能被列在公開的電話簿中，但我懷疑是否有任何人樂意地將其撥打之長途及市內電話號碼公告週知。並非這些資訊會顯示某人涉及犯罪，而是該等資訊能輕易透露通話對象及地點，進而透露個人生活中最私密的細節。[104]

4. 大法官 Marshall 不同意見書（大法官 Brennan 加入）

多數意見認為當被告提供資訊給第三人時，已經承擔該等資訊會被透露給政府的風險，大法官 Marshall 認為這樣的分析有 2 個誤解。[105]第一，風險承擔理論透露選擇的概念，至少在經第三人同意監察之情形，個人對於要與何人進行秘密通訊一事具有決定權。相對地，在本案中，除非個人已放棄使用個人或工作上之必需品，否則個人不得不接受被監察的風險。在個人實際上沒有其他選擇的情形下，承擔風險是一種懶惰的說法。[106]

---

97 *Id*.
98 *Id*.
99 *Id.* at 745-46.
100 *Id.* at 746.
101 *Id*.
102 *Id.* at 746-47.
103 *Id.* at 747-48.
104 *Id.* at 748.
105 *Id.* at 749.
106 *Id.* at 749-50.

第二，更重要的是，若以風險分析來決定隱私期待的合理性，等於容許政府定義增修條文第 4 條的保障範圍。例如，執法官員只要透過宣布政府欲隨機檢查限時郵件或私人電話通話之內容，即可讓社會大眾知悉使用該等通訊可能會承擔的風險。[107]多數意見雖認知到風險承擔理論之分析方式隱含上開意思，但僅願勉強承認在某些情況下，更進一步的探討會比較適當。關於何種為特殊情況，或者本案是否屬於其所稱之特殊情況，多數意見並未為任何解釋。[108]

大法官 Marshall 認為 *Katz* 案所揭示之隱私期待是否合理並非取決於個人於透露資訊給第三人時被推定應承擔的風險，而在於個人於自由開放的社會中被強迫承擔的風險。[109]大法官 Marshall 認為使用撥號記錄器構成廣泛性的侵害，若反對這樣的看法，就是忽略電話通訊在個人及職業關係中所扮演的重要角色。使用電話的隱私，並非僅在於牽涉犯罪行為之通話中具有重要性。[110]不受限制的政府監察無疑地會對毫無涉及不法的人們造成困擾。包括不受歡迎的政治團體成員或者具有秘密消息來源的記者可能會合理地期待自己的聯絡對象不被揭露。允許政府以低於相當理由（probable cause）之門檻取得電話記錄可能會阻礙某些政治結盟，或者作為自由社會指標的新聞工作。[111]如同進入公共電話亭的人被賦予通話不被對外播送的權利，個人應享有其在家中撥打之電話號碼，縱使被紀錄也僅限於電話公司之商業用途之權利。因此，執法人員向電話公司調取電話資訊前應取得法院令狀。[112]

5. *Smith* 案判決評析

Smith 案雖認為安裝及使用撥號記錄器並不在增修條文第 4 條的範疇內，但是美國國會於 1986 年立法限制執法人員使用撥號碼記錄器。911 恐怖攻擊後，國會賦予檢察總長在涉及國際恐怖主義或外國情資的緊急情況時，可不經法院許可即授權使用撥號記錄器。多數意見以「第三人原則」（Third Party Doctrine）為據認為電話用戶對於通話時所提供給電話公司之通話對象之電話號碼並無合理隱私期待。然而第三人原則不僅未考慮到在現代社會許多消費者為了使用已成為生活必需之科技產物，事實上並無選擇「拒絕」之權利， 也沒有正視電話通聯紀錄會透露個人對話對象、所在地理位置、交談時間，若行政部門未經司法審查即可任意取得通聯紀錄，更有可能產生壓制人民言論之「寒蟬效果」。而多數意見將「同意作為商業目的使用」悄悄地偷渡為「同意執法機關刑事調查使用」企圖魚目混珠的論述方式，更顯示 *Smith* 案論據之薄弱。

數位資訊在今日社會已成為生活不可或缺的一部分，以 *Smith* 案之「第三人原則」欲正當化政府侵害人民合理隱私期待之作為是難以令人信服的。我國因立法院長疑似涉及關說引發之監聽爭議事件，而迅速地於 2014 年 1 月修正通訊保障及監察法（下稱通保法），規範檢警於偵辦涉及最重本刑 3 年以上之罪時，若欲調

[107] *Id.* at 750.
[108] *Id*.
[109] *Id*.
[110] *Id.* at 751.
[111] *Id*.
[112] *Id.* at 752.

閱通信紀錄及通信使用者資料，除有急迫情形外，需書面聲請法院核發調取票。[113] 以比較法之角度觀察，調閱通信記錄或通信使用者資料是否相當於美國法上之「搜索」概念？依照美國 *Smith* 案的多數意見，人民因為自願提供個人資訊給電話公司，所以對其所撥打電話號碼並無合理隱私期待，政府使用撥號記錄器取得個人撥號記錄，不構成增修條文第 4 條之「搜索」，此為目前美國最高法院對於此一議題之態度。然而這樣的說法是否禁得起檢驗？特別是在高科技時代下，是否需以更嚴謹的態度去檢驗政府可能侵害人民隱私的行為？首先，個人對所撥打的電話號碼真的不具有隱私期待嗎？試問，有人願意將自己所撥打的所有電話號碼公開給全世界的人知道嗎？電話號碼所能透露的訊息雖不及通話內容般豐富，但若掌握個人電話通話對象、時間，幾乎可窺探個人生活作息、交友狀況甚至興趣偏好。需說明的是，目前電信公司提供司法機關辦案使用的通聯記錄還包括查詢手機門號之基地台位置，所以一旦警方調閱某人長時間的通聯記錄，即可分析其於各時間點在何地點與何人通話？若偵查單位通聯紀錄調閱之範圍不受任何節制，一旦人民成為偵查對象，其生活細節無論與刑事犯罪有關或無關部分，均受偵查單位一一檢視，對人民隱私期待勢必造成侵害。

以物理侵入標準分析，警方從電信公司調取某特定電話用戶之通聯記錄，電信公司係將保存供作內部商業用途使用之通聯紀錄提供警方，因電信公司本有特定儀器能記錄其用戶的通聯紀錄，無須另於該等用戶之住家或其他財產上裝置任何儀器，自然不會有物理侵入該特定對象所有財產之行為，從物理侵入標準來看，似乎並未構成美國法上之「搜索」。

然而，因新型態偵查技巧多無須伴隨物理侵入，在欠缺物理侵入之個案，必須以「合理隱私期待」之標準進一步檢驗，美國憲法增修條文第 4 條保障人民免於不合理搜索、扣押之權利才能獲得妥善保護。人民對其電話通信紀錄（包括通話對象、時間及地點）是否有隱私期待？從主觀角度觀察，個人無論使用市內電話或手機時，並不會自然將其通話對方之電話號碼、身分告知他人知悉。除非通話一方對外透露，或者透過檢視電話顯示之通話紀錄，除電話公司外，幾乎無人能正確判斷通話對象之電話號碼。因此，在一般人民不會主動將對話方號碼告知他人之情形下，應可認為人民對於通話對方之電話號碼主觀上具有隱私期待。從客觀角度分析，集會結社自由、言論自由及秘密通訊之自由已屬民主法治社會之基本價值，通聯紀錄可以顯示人民生活細節及交友情形已如前述。在一般情形下，人民對其通話對象之電話號碼、雙方通話時間及通話時基地台之位置具有之隱私期待應屬合理而被社會所接受。故警方向電信公司調取通信紀錄，確屬侵害人民合理隱私期待之行為，與美國法上「搜索」之概念相當。我國新修正通保法新增檢警調取通信紀錄原則需經法院審核之制度，就保障人民隱私權及秘密通訊之角度觀察，值得肯定。

（六）小結

在分析通聯紀錄、實施通訊監察或者使用 GPS 裝置等科技偵查逐漸普遍的今日，物理侵入之標準能夠提供之幫助已屬有限，故 *Katz* 案建立之「合理隱私期待」標準，已成為偵查作為是否侵害增修條文第 4 條權利之重要關鍵。若過度側重物

[113] 2014 年 1 月修正之通保法第 11 條之 1 第 1 項、第 2 項參照。

理侵入，或者任意以「風險承擔理論」否定合理隱私期待，都無法妥善保障人民隱私。政府在向第三人取得資訊如通聯紀錄、GPS 定位資訊、網路瀏覽歷程、銀行紀錄等個人資訊時，應考量使用者未必自願提供相關資訊，縱將使用服務視為同意提供資訊，也應僅限服務提供者特定商業目的使用。若偵查機關未經法院授權等正當法律程序即逕自取得該等資訊作為犯罪偵查之用，應非使用者所能合理預期，恐已侵害合理隱私期待，而為非法搜索或非法通訊監察。

二、聯邦電子通訊監察法

（一）犯罪控制及街道安全法

美國國會為回應最高法院 1967 年所做之 *Katz* 案及 *Berger v. New York*[114]案判決，在 1968 年制定犯罪控制及街道安全法（Title III of the Omnibus Crime Control and Safe Streets Act of 1968），一般將該法稱為 Title III，犯罪控制及街道安全法於 1986 年被修正為電子通訊隱私法中之監聽法（Wiretap Act）。[115]犯罪控制及街道安全法規範對象除包括聯邦及州的公務員，也及於私人。依該法，若欲執行通訊監察，需由檢察總長向聯邦法官聲請授權截收「有線」及「口頭」通訊之法院命令，若個案中欠缺「相當理由」，法官不得核發命令。[116]值得一提的是，犯罪控制及街道安全法規定對於通訊監察所有的限制均不適用於以國家安全為目的之通訊監察行為，該等規定亦被稱為國家安全例外。美國總統尼克森就常利用國家安全例外對國內異議分子及激進分子進行監察。但美國最高法院在 *United States v. United States District Court*[117]一案反對尼克森政府的作法，表示國家安全例外僅適用於外國威脅，不適用於國內威脅。[118]因此，對於涉及國家安全之國內威脅實施通訊監察時仍需適用上開規定及增修條文第 4 條。

（二）電子通訊隱私法

1986 年美國國會修正監聽法（Wiretap Act）後，因應電腦科技及通訊網路的發展，再加入 2 部新法律，合稱電子通訊隱私法（Electronic Communication Privacy Act,簡稱 ECPA）。此部規範執法機關之聯邦法律總共包含 3 部分：1. 監聽法（The Wiretap Act）。 2. 儲存通訊法（The Stored Communication Act），3. 撥號記錄器法（The Pen register Act）。電子通訊隱私法將所有的通訊分為下列 3 類：（1）有線通訊（wire communication），有線通訊包括所有透過電線（wire）、電纜線（cable）或其他類似媒介進行之人聲傳導。[119]（2）口頭通訊（oral communication），根據美國聯邦法典第 2510 條第 B2 項，口頭通訊指的是發話人顯示主觀上期待該等通

---

114 Berger v. New York, 388, U.S. 41(1967).
115 DANIEL J. SOLOVE, PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW, 315, 4TH ED., NY, WOLTERS KLUWER LAW& BUSINESS PRESS(2011) .
116 *Id*.
117 United States v. United States District Court, 407, U.S.297(1972).
118 *Id*.
119 18 U.S. C § 2510(1).

訊不受截取，而客觀情形亦證明該等期待是合理的，但口頭通訊不包括電子通訊。[120]口頭通訊通常是由竊聽器或其他錄音或傳送裝置截取。[121]（3）電子通訊，依美國聯邦法典第 2510 條第 12 項，電子通訊包括有線通訊及口頭通訊以外之通訊。[122]。未含有人聲的電子郵件就是一種電子通訊。[123]雖然電子通訊受到監聽法及儲存通訊法之保護，但電子通訊受到保護之程度與有線通訊或口頭通訊不同，最明顯的區別就是監聽法下之「電子通訊」並不適用證據排除法則（exclusionary rule），而有線通訊及口頭通訊適用監聽法時受到證據排除法則之保護，適用儲存通訊法時，因該法並無證據排除法則故不受到保護。[124]以下就組成電子通訊隱私法之 3 部法律進行簡要介紹：

1. 監聽法（The Wiretap Act）：18 USC §2510-2522

監聽法被編在電子通訊隱私法 Title I，包括美國聯邦法典第 2510 條至第 2522 條，規範通訊的截取（intercepton）。[125]該法適用於截取隨即消逝之通訊（communication in flight），截取係指取得藉由電子、機械或其他裝置正通訊傳送過程中取得通訊之內容。[126]此法最常規範的活動就是對電話通話的監聽，透過裝置監聽透過電線傳輸之對話內容。由於監聽法只適用在當通訊於傳輸過程中同時被截取之情形，因此一旦通訊結束且被儲存，監聽法就不再適用，而應適用儲存通訊法。[127]聲請截取通訊必須詳述截取如何執行及截取之期間等細節，而監聽法對於核發令狀之標準較憲法增修條文第 4 條更為嚴格，不僅需具備「相當理由」，尚須要求符合「其他替代手段已失敗，不可能成功或可能過於危險」等要件，且只有高階檢察官始能提出聲請，且限於特定重罪，要件相當嚴格，故有稱監聽法之令狀為「超級令狀」（super warrant）。[128]在監聽法下有兩種例外情形：第一種例外，是經通訊一方同意之監聽。因此，個人秘密地就本人與其他人間之電話對話錄音並未違反監聽法。若參與對話，政府探員或臥底可在對方不知情的情況下錄製對話內容。[129]並非所有得通訊一方同意均不會違反監聽法，在截取通訊之目的為從事違反憲法、聯邦法或任何州法之刑事犯罪行為或民事侵權行為時，縱使通訊一方事先同意監聽，仍屬非法監聽。[130]我國通訊監察保障及監察法第 29 條第 3

---

120 18 U.S. C § 2510(2).
121 DANIEL J. SOLOVE, MARC ROTENBERG, PAUL M. SCHWARTZ, PRIVACY, INFORMATION, AND TECHNOLOGY, 86, NY , ASPEN PRESS(2006).
122 18 U.S. C § 2510(12).
123 Solove , *supra* note 121.at 87.
124 *Id*.
125 *Id*.
126 18 U.S.C §2510(4)""“intercept” means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."
127 Solove, *supra* note 129, at 87-8.
128 DANIEL J SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS, 37, IAPP PRESS, NH(2011)
129 Solove, *supra* note 121, at 89.
130 18 U.S. C § 2511(2)(d), “It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such

款[131]亦將得通訊一方同意之監聽列為非法監聽之例外，不予處罰，與美國監聽法之規範類似。

2. 儲存通訊法（The Stored Communication Act）

傳送中之通訊係由監聽法所規範，經儲存之通訊則受到儲存通訊法所規範。儲存通訊法被編在美國聯邦法典第 2701 條至同法第 2011 條。諸如網路服務紀錄、網路通訊及使用者紀錄等資料通常係由電子通訊服務提供者保存。[132]儲存通訊法將故意侵入提供電子通訊之設備等行為列為刑事犯罪，[133]但將提供有線或電子通訊服務之個人或業者，或該等通訊之使用者排除在刑事處罰之適用範圍外。[134]相較前述監聽法（The Wiretap Act），儲存通訊法所規範取得儲存通訊之程序較截取通訊來得寬鬆一些。[135]就包含內容之通訊，若政府欲取得之通訊儲存時間在 180 日以內，必須取得由相當理由支持之法院令狀。[136]若欲取得之通訊儲存超過 180 日，政府必須事先通知使用者，並且取得大陪審團、審判法院所核發之行政傳票（administrative subpoena）或者取得法院命令，此時聲請法院命令不需具「相當理由」，僅需有「特定明確事實顯示具有相信該通訊與刑事調查有關之合理根據」。[137]但若欲取得之通訊儲存超過 180 日，而政府不願事前通知使用者，政府即須取得法院令狀。[138]至於不包括通訊內容之使用者紀錄（例如使用者之身分資料、地址、電話號碼等），電子通訊或遠端運算服務提供者亦不可任意揭露，僅在政府取得法院令狀、法院命令、經使用者同意或者政府提出書面請求協助有關電信詐騙之調查之情況，[139]業者可將該等使用者資料提供給政府。

3. 撥號記錄器法（The Pen Register Act）

該法規範撥號記錄器（pen register）、追蹤電話設備（trap and trace devices），編入美國聯邦法典第 3121 條至同法第 3127 條。撥號記錄器是記錄從特定電話撥打出去之電話號碼之設備；而追蹤電話設備是記錄撥入特定電話之電話號碼之裝置。[140]因此該法主要規範的就是所謂的通聯紀錄。雖然最高法院在 *Smith* 案中認為撥出之電話號碼不受增修條文第 4 條所保護，但 1986 年制訂之撥號記錄器法規定，除非在特定例外情形外，未取得法院命令前，不得安裝或使用撥號記錄器或

---

interception **unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State**".

131 通訊保障及監察法第 29 條第 3 款：「監察他人之通訊，而有下列情形之一者，不罰：三、監察者為通訊之一方或已得通訊之一方事先同意，而非出於不法目的者。」

132 Solove, *supra* note 121.

133 18 U.S. C § 2701(a)(b).

134 18 U.S. C § 2701(c).

135 Solove, *supra* note 121, at 90.

136 18 U.S. C § 2703(a).

137 18 U.S. C § 2701(b).

138 *Id*.

139 18 U.S. C § 2701(c)(B).

140 Solove, *supra* note 121, at 91.

追蹤電話設備。[141]若政府證明透過安裝或使用該等設備可能取得之資訊與進行中之刑事調查有關，法院應核准政府使用該等設備。[142]該法並無證據排除法則之適用，但故意違反此法使用或裝置該等設備者，可處 1 年以下有期徒刑。[143]

參、新型態通訊監察工具

一、新型態通訊監察之類型

（一）追蹤及定位科技

近年來，美國最高法院對於警方使用全球定位系統追蹤、定位嫌犯位置是否構成搜索一事先後有不同之見解，最高法院於 *Knotts* 案及 *Karo* 案中認為在特定容器安裝追蹤器不構成增修條文第 4 條之搜索或扣押。最高法院於 2012 年作成的 *Jones* 案中，一致認定在警方在嫌犯汽車上裝設 GPS 裝置構成搜索。雖然大法官 Scalia 主筆的多數意見僅從物理侵入角度判斷是否侵害增修條文第 4 條之權利。但 2 份協同意見書均提及在數位時代，特別是多數智慧型手機具有全球定位之功能的今日，政府追蹤定位嫌犯不必然伴隨物理侵入。大法官 Alito 認為焦點應回到「合理隱私期待」之概念，認為嫌犯政府全天候長時間監視嫌犯在公開場合之所有行動，即屬侵犯合理隱私期，但若僅是對於嫌犯在公共道路之單程移動進行監視，嫌犯對其於公開場合之移動軌跡即不具合理隱私期待。大法官 Sotomayor 認為在數位時代有重新檢討「第三人原則」之必要，至少政府長時間利用全球定位系統蒐集個人資料構成增修條文第 4 條之侵害。在利用 GPS 進行短時間之監視時，應考量 GPS 能獲取可透露有關個人家庭、政治、專業、信仰及性等連結之豐富資訊。以及政府可輕易取得有關人民之大量資訊，國家與人民間關係變化等因素。

因此，歸納上開意見，政府以追蹤、定位科技監視目標對象，若涉及物理侵入，無庸置疑已構成搜索。若長時間而非單程追蹤、定位目標對象，因侵害「合理隱私期待」，亦構成搜索，須取得法院之搜索票始得為之。檢警機關欲找出特定人所使用之「M 化車」，基本上就是運用「手機定位」之技術，對隱私權侵害之情形類似公權力利用 GPS 追蹤目標對象。因此，若非短時間之單程追蹤（如 1 日以內），而係長時間追蹤定位目標對象，從保障隱私權之角度來看，宜由法院授權後為之，此部分因為與傳統搜索型態不同，可能有待立法部門研擬修法，在修法前，偵查機關應向法院聲請搜索特定「被告」或「犯罪嫌疑人」之搜索票。

（二）網路監察

141 18 U.S. C § 3121(a).
142 18 U.S. C § 3123(a).
143 18 U.S. C § 3121(d).

在網路科技日新月異的今日，平板電腦、智慧型手機充斥著我們的生活，網路世界不僅提供豐富、多元的資訊，也大大改變人與人之間的交往方式。在網路不發達的時代，若欲與遠在國外之親朋好友聯繫，除了使用價格昂貴的國際電話外，就是依賴極為費時的紙本書信往來。慶幸我們所處的時代已不再需要依賴這些成本高、效率低的通訊方式。通過電子郵件的使用，不管距離再遠，兩地是否具有時差，都能即時傳送、接收訊息。使用目前常見的通訊應用程式如 Skype、Line，只要在具有網路的環境下，不僅能通話，更可以透過使用視訊功能面對面交談。更重要的是，使用電子郵件或通訊應用程式與他人聯絡、通話都不需另外收費，十分經濟及便捷。因此，電子郵件及通訊應用程式（APP）已成為今日社會主流的通訊工具。上述新型態通訊方式，的確使人與人之間的溝通更迅速、便利，但同時也提供犯罪者聯繫共犯、逃避檢警偵查的新方式。以我國常見之詐騙、販毒等犯罪集團為例，由於集團成員擔心警方會對其手機進行監聽，常使用各種智慧型手機通訊應用程式作為犯罪聯絡之工具，造成警方通訊監察的困難。

因此，執法機關在偵查犯罪過程中，為蒐集犯罪證據或掌握執行拘提、逮捕之時機，很可能需要對於嫌犯使用之電子郵件、通訊應用程式、對話之內容進行通訊監察。由於所有網路通訊都是透過封包交換過程完成，偵查機關欲對網路通訊內容進行通訊監察，理論上，可向網路通訊服務提供業者或通訊應用程式公司，調取特定使用者之通訊內容。然而，實際上，目前許多提供電子郵件服務之公司或發行通訊應用程式之公司，多為外國公司，故不受我國法律規範，並無配合通訊監察之義務，難以期待該等公司會提供涉及客戶隱私之通訊內容給我國政府。因此，若欲取得此種網路通訊內容，勢必得透過封包監察技術對網路傳輸之封包直接進行監察，以掌握犯罪集團之通訊內容，以下就常見之網路監察類型，進一步介紹分析：

1. 電子郵件監察

關於電子郵件的搜索，美國聯邦第五巡迴上訴法院於 *Steve Jackson Games, Inc.v. United States Secret Service*[144]一案中，美國聯邦特勤局（United States Secret Service）扣押 Steve Jackson Games 公司存有電子布告欄系統（Bulletin Board System）內發送方已寄送但收受方未閱讀的電子郵件之電腦，本案爭點在於扣押存有寄送至電子布告欄系統而未被閱讀之私人電子郵件是否構成監聽法禁止之截取（intercept）?[145]美國聯邦法典以第 2510 條（4）所定義之截取是指「藉由電子、機械或其他設備，擷取人聲或其他包含通訊內容之任何有線、口頭或電子通訊」（18 U.S.C §2510(4)），而國會在立法時在定義「電子通訊」（electronic communication）時使用「轉移」（transfer）一字，並省略在定義「有線通訊」（wire

[144] *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457(5th Cir.1994)
[145] *Id.* at 458, 460.

communication）時所使用之「任何以電子方式儲存之此類通訊」，反應國會在立法過程中並不欲讓截取適用於處於電子儲存狀態之任何通訊。[146]因此，上訴法院維持地方法院之判決，認為特勤局未獲授權故意存取具有電子通訊之設備，並禁止有權使用之上訴人存取以電子儲存型態在系統中之電子通訊之行為，違反的是儲存通訊法中禁止無權取得儲存通訊之規定，而非監聽法中截取通訊之規定。[147]

依 *Steve Jackson Games* 案，政府在收件者未收取電子郵件前擷取儲存在網路服務提供者伺服器中之電子通訊並不構成「截取」電子郵件，是否意謂對電子郵件之監看、監聽完全不受監聽法（wiretap act）所規範？在美國聯邦法中，電子郵件之監察可由監聽法、儲存通訊法及撥號紀錄器法等 3 部聯邦法規共同規範，各法提供不同程度之保護。決定適用何種法規，端視所使用電子郵件之類型、電子郵件如何儲存及政府如何存取使用電子郵件？[148]假設寄件人寄送 1 封電子郵件給收件人，政府在收件人收信前檢視該信件內容，是否有監聽法之適用？電子郵件傳送之方式與電話不同，寄件者寄送電子郵件後，電子郵件會被送至網路服務提供者處，直到收件者下載該封電子郵件。若政府是在郵件從寄件者電腦傳送至網路服務提供者之過程中，或是從網路服務業者傳送至收件者電腦過程中，因為通訊係在傳送過程中，均有監聽法之適用。[149]但若政府是在該封電子郵件停留在網路服務提供者之伺服器等待收件者下載之過程中遭政府擷取，因為該封電子郵件係在被儲存之狀態，所以不受監聽法所規範，而由保護程度較低之儲存通訊法規範之。[150]若政府是從使用者網路電子郵件帳戶擷取電子郵件內容，因為該等電子郵件均是處於「電子儲存」（electronic storage）之狀態，故應適用儲存通訊法。[151]若政府擷取的是關於說明電子郵件收發過程的標頭題（header）資訊，因為不涉及通訊內容，應適用保護程度最低的撥號紀錄器法。[152]

公權力利用監察電子郵件取得他人通訊內容，要如何適用我國法呢？從程序來看，我國通保法規範之通訊範圍非常廣泛，該法所規範之通訊包括：1. 利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信。2. 郵件及書信。3. 言論及談話。[153]我國電信法中所稱之「電信」係利用有線、無線，以光、電磁系統或其他科技產品發送、傳輸或接收符號、信號、文字、影像、聲音或其他性質之訊息。[154]電信設備則指電信所用之機械、器具、

[146] *Id.* at 460-62.
[147] *Id.* at 463-64.
[148] DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY,167-68,NEW HAVEN ,CONN,YALE UNIVERSITY PRESS(2011).
[149] *Id.* at 168.
[150] *Id.*
[151] *Id.* at 168-9.
[152] *Id.* at 170.
[153] 通訊保障及監察法第 3 條第 1 項。
[154] 電信法第 2 條第 1 款。

線路及其他相關設備。[155]因此，電子郵件屬於通保法所定義之第 1 種通訊。無疑也為「郵件」所涵蓋，且只要含有通訊內容也屬於言論。因此，電子郵件之內容資訊原則上符合通保法任一種類型通訊之定義，而我國未就通訊型態進一步制訂類似美國聯邦電子通訊隱私法之規定，所有只要涉及擷取電子郵件內容之資訊，不論擷取電子郵件的時間點係在寄件人傳送至網路服務提供者之過程中，或從儲存在網路服務業者提供者之伺服器等，因所涉及者均屬我國通保法所定義之「通訊」，均適用者我國通保法通訊監察之相關規定。

因此，政府若欲以對特定對象之電子郵件進行監察，必須依通保法所規定之聲請程序向法院聲請核發通訊監察書，[156]取得通訊監察書後始得進行電子郵件之監察。若未具備通保法對通訊監察所要求之要件即對電子郵件，即屬非法通訊監察，除所得之通訊監察資料不得作為證據使用外，依通保法需負民事[157]及刑事責任[158]。

2. 封包監察程式（Packet Sniffer）

所有網路通訊均可劃分成獨立之封包透過網路傳送再於抵達目的地時組合成最初之通訊內容。因此，大部分網路監察都是「封包監察」。[159] 為進行網路監察，必須使用特定裝置「監聽」網路通訊中某特定線路以尋找通訊。透過網路線路之監察，可以檢視在網路中某位置之封包信息流量（packet traffic），任何被設計為從事上開監察措施之裝置或軟體都被稱作封包監察程式。[160] 由於網路是透過由「零」和「一」字元組成之封包在電腦間傳送及接收資訊。「零」及「一」可被組合成人類可讀之文字，但電腦不需透過字元轉化為文字之程序，即可直接執行由「零」、「一」字元組合成之指令。 [161]在物理世界中，必須透過較先進之科技才能進行較具規模及侵入性之搜索。相對地，進行網路監察時，網路科技可藉著調整設定值進行最具侵入性之搜索，與可透過先進之科技將隱私侵害之程度降到最

155 電信法第 2 條第 2 款。

156 我國警察機關發現受監察對象使用電子郵件逃避追查時，也有向法院聲請通訊監察書監察攔截電子郵件通訊內容之情形。

157 通訊保障及監察法第 19 條：「違反本法或其他法律之規定監察他人通訊或洩漏、提供、使用監察通訊所得之資料者，負損害賠償責任。（第 1 項）被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。（第 2 項）前項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。（第 3 項）」

158 通訊保障及監察法第 24 條：「違法監察他人通訊者，處 5 年以下有期徒刑。（第 1 項）執行或協助執行通訊監察之公務員或從業人員，假借職務或業務上之權力、機會或方法，犯前項之罪者，處 6 月以上 5 年以下有期徒刑。（第 2 項）意圖營利而犯前二項之罪者，處 1 年以上 7 年以下有期徒刑。（第 3 項）」

159 Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 Nw. U. L. Rev. 607 , 649(2003)

160 *Id*.

161 *Id*. at 650.

低。網路科技之特性使得人們有使用篩選程式以降低隱私侵害之需求。[162] 對於現代科技來說，真正的挑戰是設計一個能僅僅篩選及紀錄法院命令所允許調查之封包之篩選程式，而非需蒐集所有資料再交由人類檢視之工具。與物理世界相較，由某位址蒐集所有在網路上之封包訊息流量並不困難，但若欲進行局部範圍之監察，就需要依賴先進之篩選程式。[163]

3. 肉食者（Carnivore）

90 年代中期至晚期，美國聯邦調查局在發現執行封包監察存在篩選資訊不易的問題，便著手設計能有效率地篩選及分析網路通訊之監察工具。雖然系統管理者常使用網路監察工具監督網路訊息流量，但市場上並沒有販售符合聯邦調查局隱私保護需求之網路監察工具。[164]聯邦調查局所需要的是較一般系統管理員所使用之監察工具更能保護網路使用者隱私之網路監察工具。 為確保所使用之監察工具能完全符合法院命令之要求，聯邦調查局認為有自行發展監察工具以符合監察法制相關限制之需求。

在多數情形，聯邦調查局僅以法院命令請求網路服務提供者以其監察工具執行法院命令。雖網路服務提供者使用監察工具能蒐集到較法院命令所要求更多之資料，但網路服務提供者可在提供資料給聯邦調查局前以人工方式過濾並排除敏感性資訊。將監察之責任委由網路服務提供者辦理與政府自己執行監察相較，委由網路服務提供者執行不僅花費成本較少，且不需太多技術支援。故此種間接監察較為執法人員所喜愛。另外網路服務提供者是否值得信任也是一個重要的議題。執行間接監察時，政府需信任配合之網路服務提供者會有效率地執行法院命令，並且將所有取得之證據提交給政府之調查人員。[165] 然而，規模較小之網路服務提供者可能不樂意協助聯邦政府，甚至可能本身就是犯罪嫌疑人之共犯。這意謂政府不能完全依賴間接監察執行法院命令，如果所有間接監察之手段均失效，政府就必須直接使用自身監察工具執行法院命令。 [166]

聯邦調查局將其自行研發之網路監察工具取命為「肉食者」（Carnivore），如此駭人的名稱欲彰顯該是監察工具保護個人隱私之特色。聯邦調查局研發之第一代監察工具蒐集到法院命令許可範圍以外之資訊，因此被命名為「雜食者」。相較於「雜食者」，二代監察工具能精確找出並紀錄欲取得之資訊，因此被命名為「肉食者」，意即該裝置僅「吃」程式設所計要紀錄的「肉」。[167] 聯邦調查局後來又研發名稱為「DCS-1000」之第三代監察工具，以確保能符合法院命令對隱私侵害

[162] *Id.* at 650-51.
[163] *Id.* at 651.
[164] *Id*.
[165] *Id.* at 652-53.
[166] *Id.* at 653.
[167] *Id.*

最小化之要求。如果能依設計目的去執行上揭監察工具，相較於其他市場上可取得之網路監察工具，應更能保障隱私。事實上，「內食者」基本上就是額外具有遵守法院命令功能之網路監察工具，因此亦可稱為「遵守法院命令之網路工具」。[168] 網路服務提供者透過安裝此種工具，不但可將需要掃瞄之網路流量降到最少，也把對隱私之侵害降到最低。[169]

反對愛國者法的論者宣稱該法鼓勵使用「肉食者」這種網路監察工具。然而，「肉食者」僅是某一種可用以執行網路監察之工具，認為上開法律鼓勵使用「肉食者」勝於其他監察工具是沒有道理的。此種論調就像建立新高速公路之法案鼓勵使用「Volvo」廠牌汽車一樣站不住腳。問題不在於是使用何種特定工具執行監察，而在於法律授權政府做何事及政府是否在授權範圍內執行。除非有法律規定之例外情形，政府必須依撥號紀錄器法取得法院命令，始能蒐集「撥話、路由、定址及其他傳遞性之資訊」，需取得監聽命令才能蒐集包含通訊內容之資訊。若政府未取得正確之法院令狀，不管所使用者是否為「肉食者」均屬違法。[170]

4. 按鍵側錄裝置（key logging devices）

由於數位時代人們大量依賴電腦，許多重要資料均存放在電腦檔案中，為了資訊安全之考量，會透過許多密碼來確認使用者是否被授權閱覽資料，除了開機要輸入密碼外，通常會在儲存機密資料之檔案另設密碼驗證程序，使用者必須輸入正確密碼才能檢視特定檔案所儲存之內容。為破解電腦檔案所設之重重密碼，美國偵查實務有透過在目標電腦上安裝「按鍵側錄系統」（key logging system）的案例，安裝案件側錄裝置的目的在側錄該電腦鍵盤之按鍵敲擊紀錄，並透過按鍵敲擊紀錄之分析，以取得相關密碼。

2001 年美國聯邦紐澤西地方法院在 *United States v. Scarfo*[171]一案就涉及聯邦調查局使用按鍵側錄系統取得被告電腦檔案密碼之相關問題。在該案中，聯邦調查局探員執行搜索令狀，搜索被告 Scarfo 位於紐澤西州辦公室，並檢視 Scarfo 個人電腦中之部分檔案，但無法進入某個名稱為「Factors」之加密檔案。[172]聯邦調查局懷疑該檔案含有被告經營非法賭博及高利貸之證據，為了破解該加密檔案之密碼以檢視檔案內容，便依所聲請之搜索令狀，在該電腦及鍵盤上安裝「按鍵側錄系統」。聯邦調查局便依「按鍵側錄系統」所紀錄之按鍵敲擊紀錄取得加密檔案「Factors」之密碼，並取得證明被告涉犯賭博及高利貸罪嫌之證據。聯邦陪審團繼而對被告 Scarfo 等人提出涉嫌賭博及重利等 3 項指控。[173]

---

168 *Id.* at 653-54.
169 *Id.* at 654.
170 *Id.* at 655-56.
171 United States V. Scarfo,180 F.Supp.2d 572(D.N.J.2001)
172 *Id.* at 574.
173 *Id*.

被告 *Scarfo* 案在預審程序提出動議要求檢方出示從其電腦中取得之證據，並主張排除該等證據。[174]審判法院將政府在被告 Scarfo 電腦安裝按鍵側錄系統是否違反監聽法之規定列為重要爭點，特別是按鍵側錄系統是否於使用者藉由該電腦透過數據機連結電話與他人進行溝通之期間維持運作，因欠缺監聽法之令狀而違法截收有線通訊。[175]為了處理上開爭議，審判法院命令政府提出報告解釋按鍵側錄系統如何運作，以及當電腦數據機、網路通訊、電子郵件及其他電腦使用之情形時按鍵側錄系統如何運作。[176]聯邦政府則主張為符合機密資訊程序法之程序，請求法院修正命令之內容。聯邦調查局表示因詳細地揭露按鍵側錄系統如何運作將危及國家安全，因此該等資訊為機密資訊。審判法院在經過秘密及單方地聽證，核准政府不揭露按鍵側錄系統如何運作之請求。政府必須就按鍵側錄系統如何運作提供被告 Scarfo 及其律師一份非機密之摘要。[177]根據政府提供之摘要，被告 Scarfo 主張按鍵側錄系統侵害增修條文第 4 條之權利，因為按鍵側錄系統不僅紀錄密碼，更能蒐集所有按鍵紀錄。[178]

法院認為本案中聯邦調查局係依據法院核發之搜索令狀在被告之電腦上安裝按鍵側錄系統，且核發搜索令狀之法官授權聯邦調查局可以搜索及扣押以任何形式保存之商業紀錄，包括通訊錄、電子儲存裝置、收支帳簿（ledgers）、其他會計紀錄、銀行紀錄及報表、旅行紀錄、往來書信（correspondence）、備忘錄、摘記、行事曆及日記等所有含有共犯、賭客、重利被害人之身分或行蹤而可揭露非法賭博、重利或其他敲詐勒索等犯罪資訊之資料。[179]該令狀已指明聯邦調查局所欲搜尋者均為具備相當理由認為與犯罪有關之證據。最重要的是，法官之命令已詳細記載聯邦調查局所欲尋找之關鍵證據－Scarfo 加密檔案之密碼。[180]因此，雖然按鍵側錄系統的確記錄 Scarfo 電腦鍵盤之敲擊記錄而非僅搜尋密碼，但並未因此如被告所主張使有限的密碼搜索轉變為一般廣泛性的搜索。蓋在許多合法搜索之情形，警方在偶然發現證據前，並不會知道得證明犯罪證據之確切本質為何。[181]知悉被告 Scarfo 的電腦具有數據機而得透過數據機傳送電子通訊，聯邦調查局將按鍵側錄系統設定為無法在該電腦進行電子通訊時接收敲擊鍵盤所進行之電子通訊。因此，當數據機在運作時，按鍵側錄系統不會記錄按鍵敲擊記錄。[182]因為被告 Scarfo 之電腦並未以其他形式儲存數據機所進行之通訊。因此，被告 Scarfo 主張為政府違反監聽法而要求排除證據之動議不被法院認可。[183]

---

174 *Id*.
175 *Id*. at 575.
176 *Id*.
177 *Id*.
178 *Id*. at 576.
179 *Id*. at 578.
180 *Id*.
181 *Id*.
182 *Id*. at 581-82.
183 *Id*. at 582.

根據 Scarfo 一案之見解，似乎只要將按鍵側錄系統設定成在電腦網路連線使用時不會運作即可規避聯邦監聽法之適用。值得探討的是，鍵盤敲擊記錄是否為我國通保法所指之「通訊」？通保法第 3 條第 1 項所定義之通訊有 3 種型態：1、利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信。2、郵件及書信。3、言論及談話。鍵盤敲擊記錄為電腦使用者敲擊電腦鍵盤所產生之紀錄。根據使用電腦之不同脈絡，鍵盤敲擊記錄可能成為通保法所規範之 3 類通訊中之任何一種。故安裝及使用鍵盤側錄系統可能會構成通訊監察。我國通保法第 13 條第 1 項但書已規定「不得於私人住宅裝置竊聽器、錄影設備或其他監察器材」，因此安裝硬體設備之鍵盤紀錄器可能不為我國法所容。

至於從遠端安裝按鍵側錄軟體系統，多半會透過電子郵件夾帶病毒在目標電腦植入具按鍵側錄功能之軟體程式，本文認為在目前所處數位時代，幾乎任何桌上型電腦、筆記型電腦及智慧型手機都具有透過網路進行通訊之功能，故取得具有網路通訊功能之電腦之按鍵敲擊記錄之監察行為原則上構成「通訊監察」，須依通保法之聲請訊監察程序取得通訊監察書後始得為之。關於以遠端安裝側錄系統之駭客手法取得「密碼」或其他重要資訊是否違反我國刑法第 358 條之入侵電腦設備罪，本文認為偵查機關自遠端植入間諜程式以取得他人密碼之行為，形式上固該當入侵電腦設備罪之構成要件。然而，若偵查作為符合我國通保法發動通訊監察之要件，且依合法通訊監察書實施之，即為依通訊監察法相關規定所為之「依法令之行為」，依刑法第 21 條第 1 項，得以阻卻違法，自不成立該條犯罪。[184]

從以上分析，依現行法制，偵查機關仍有使用按鍵側錄系統軟體去取得重要檔案密碼之空間。值得探討的是，使用鍵盤側錄系統可能引起政府監察人民思想之爭議。因為透過監視個人在電腦上輸入之內容，政府將能直接監察思想。按鍵側錄裝置讓政府能記錄個人不欲公開分享、不欲存入硬碟、不欲以任何形式保存供將來參考之思想及意見。因此，政府使用按鍵側錄系統可能產生政府審查人民思想而引發寒蟬效應之疑慮。本文認為，若已可合法搜索、扣押電腦及相關檔案，偵查機關其實可以向法院聲請授權檢視電腦所含特定檔案內容之搜索票，再請求電腦解密專家破解檔案密碼，或命被告輸入正確密碼以檢視檔案內容，毋須為了取得密碼而迂迴地側錄按鍵敲擊情形，大範圍監察使用者按鍵敲擊紀錄，而引發不當侵害基本人權之質疑。

5. 智慧型手機通訊應用程式之監察

在數位時代下，政府偵查犯罪或蒐集外國情資可能需取得含有人聲之「口頭

[184] 就如同未依通保法程序之非法監聽可能觸犯通保法第 24 條之非法監聽罪一樣，大部分依法定程序實施之通訊監察，均可主張符合「依法令之行為」而阻卻違法。

通訊」，例如取得通訊應用程式用戶間之視訊通話內容；或者取得不含人聲之「電子郵件」、透過 Line、Wechat 等通訊應用程式所傳送之「文字訊息」，在美國法下該等偵查行為，視其取得通訊內容之時間點係於「通訊傳輸過程中」或「電子儲存中」，而分別適用聯邦電子隱私法下之「監聽法」或「儲存通訊法」，公權力欲取得該等通訊內容，原則上須依法律程序取得法院令狀。因此，主張基於「第三人原則」政府可不經司法審查直接向通訊業者取得通訊內容或使用者資料之論調顯然與美國聯邦法律之規定不符。蓋判斷是否違反增修條文第 4 條所保障之合理隱私期待時，需考量聯邦法原則上已政府取得各種通訊內容已有不同程度之規範，除非得通訊一方之同意，原則上必須經過司法審查政府始得取得儲存之通訊，與最高法院在電子通訊隱私法制訂前作成 *Smith* 案之時空背景已不相同。姑不論電子通訊隱私法對各種通訊規範之正當化標準不盡相同，既然電子通訊隱私法已要求事前司法審查，人民當然可合理期待政府不會違反電子通訊隱私法直接向業者調取通訊內容或使用者資料。因此，依美國法，政府若未取得法院令狀、法院命令，逕向業者調取該等資料，自屬侵犯合理隱私期待而違反增修憲法條文第 4 條。

在我國法下，由於對室內電話之通訊監察已行之有年，許多犯罪集團以改用通訊應用程式取代電話通話以躲避檢警偵查。因此，若技術上可監聽、監看或調取嫌疑人使用通訊應用程式所進行之通訊內容，很可能獲取更多有價值的證據，[185]對犯罪偵查必有莫大助益。依我國通保法，通訊包括「利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信。」[186]；通訊監察以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法為之。[187]因此，不管檢警直接截收通訊應用程式所傳遞之文字訊息或含有人聲的視訊影像，或從通訊應用程式之發行公司取得該等資料，均屬通訊監察之偵查手段，應適用通保法聲請法院核發通訊監察書之程序。

對於通訊應用程式之監察，黃茂穗氏認為對偵查實務有 5 大挑戰：[188]第一，通訊過程加密，解密不易。多數通訊應用程式均使用加密機制，而多數國外業者不願提供我國政府解密金鑰，故執法機關難以瞭解通訊內容。[189]第二，應用程式倍增。通訊應用程式隨時可在網路上提供使用者免費或付費下載。Apple App Store 及 Google Play 中通訊應用程式之數量已超過 70 萬，累計下載次數更高達數百億次。由於多數通訊應用程式提供者為國外業者，我國政府無法要求配合執行通訊監察，因此應用程式改版時，通訊監察機關即需重新研究，並分析通訊協定及加

185 利如透過通訊應用程式傳遞文字訊息直接進行毒品交易，文字訊息可能包括交易毒品種類、價金、重量、地點等重要資訊。

186 通訊保障及監察法第 3 條第 1 項第 1 款。

187 通訊保障及監察法第 13 條。

188 黃茂穗，從智慧型手機的興起論新世代網際網路通訊監察挑戰與政府因應作為，刑事科學，第 74 期，2013 年 3 月，頁 73-頁 75。

189 同前註，頁 73。

密方式。[190]第三，雲端難以監察。目前國際上尚無雲端監察之標準，或者資料保存之規範，加上多數業者及伺服器均在國外，受限各地法規或業者利益考量，未必願配合我國執法機關協助執行通訊監察或提供資料。[191]第四、接取速度變快，通訊監察資料量龐大。因高速行動上網因逐漸普及，因此通訊監察中心可能接收到大量與犯罪內容無關的資料，造成執行通訊監察之機關難以有效掌握犯罪線索。[192]第五、使用者難以定位追蹤及個化。因智慧型手機多具備 3.5G 與 WiFi 兩種行動上網功能，若採用不同之上網方式，再加上使用不同之通訊應用程式進行犯罪聯繫，將造成偵查單位無法追蹤通訊應用程式所使用之網路，亦難個化智慧型手機使用者之身分。[193]

鑑於監察通訊應用程式不易，在相關通訊監察技術突破前，或許執法機關可透過扣押犯罪嫌疑人所持用之智慧型手機以取得相關證據資料。[194]因為智慧型手機通常會保存使用者使用通訊應用程式所發送之文字訊息、語音留言，該等資料可能包含得證明犯罪之證據。因此，逮捕、拘提被告後執法機關若能立即扣押智慧型手機，並向法院聲請搜索票檢視手機內使用通訊應用程式之相關紀錄，透過檢視通訊應用程式之通訊錄、通訊內容（文字訊息或語音留言），便可確認通訊之相對人，對於通訊監察資料之解譯有極大的幫助。[195]為避免檢視手機引發違法搜索之疑慮，本文建議執行搜索、扣押之執法人員最好能事先即取得法院核准搜索、扣押智慧型手機之搜索票，若未事前取得搜索票，亦可依刑事訴訟法規定先附帶扣押智慧型手機，待取得搜索票後再檢視智慧型手機內之相關資料。[196]

6. 調查 IP 位址及 URLs（網址）資料

---

190 同前註。

191 同前註，頁 74。

192 同前註。

193 同前註，頁 74-頁 75。

194 刑事訴訟法第 133 條：「可為證據或得沒收之物，得扣押之。（第 1 項）對於應扣押物之所有人、持有人或保管人，得命其提出或交付。（第 2 項）」；同法第 137 條：「檢察官、檢察事務官、司法警察官或司法警察執行搜索或扣押時，發現本案應扣押之物為搜索票所未記載者，亦得扣押之。(第 1 項)第 131 條第 3 項之規定，於前項情形準用之。（第 2 項）」

195 若原搜索票內未將智慧型手機內之資料列為應搜索之物，或將智慧型手機列為應扣押之物，執行搜索之人員或可先依刑事訴訟法第 133 條、第 137 條之規定扣押智慧型手機。至於要進一步檢視智慧型手機內通訊應用程式使用之相關記錄，除非符合同法第 131 條之 1 同意搜索之規定，參考美國法增修條文第 4 條之相關實務見解之意見，執法人員應先保管智慧型手機，直到取得法院授權檢視手機內容之搜索票後，始得依搜索票之指示，進一步「搜索」智慧型手機內之資料。

196 關於警方執行逮捕得否附帶搜索受逮捕人之（智慧型）手機，即得否無令狀檢視手機內之資訊，本文撰寫上開意見前，美國最高法院尚未就此議題明確表示意見，本文完稿前，美國最高法院恰於 2014 年 6 月 25 作成 Riley v. California ,573,U.S._(2014)之判決，全體大法官一致認為執行逮捕時僅得附帶扣押受逮捕人持有之手機，不得附帶搜索手機，若欲檢視手機內資訊，必須取得搜索之令狀始得為之，適與本文原來提出之結論相同，關於 Riley 案之事實及意見，將於本文第參、二、（三）部分進行介紹、分析。

查詢犯罪嫌人所使用之 IP 位址或其瀏覽之網址，為政府偵查利用電腦從事犯罪之重要偵查手段。犯罪嫌疑人對於該等資訊是否具有合理隱私期待？該等資料在美國法受保護之程度如何？

美國聯邦第九巡迴上訴法院在 *United States v. Forrester*[197]一案中，政府利用類似撥號紀錄器之設備，監察被告電子郵件之收件人及寄件人帳號、被告在網路上所瀏覽網站之 IP 位址及被告帳戶所接收或寄送之所有資料。[198]上訴法院以 *Smith* 案中最高法院認為個人對於撥出之電話號碼沒有合理隱私期待，所以使用撥號紀錄器並不構成增修條文第 4 條之「搜索」。[199]

該法院基於下述理由認為本案政府對被告所為電子郵件、網路活動之監察與 *Smith* 案中之撥號紀錄器並無不同。[200]第一，電子郵件或網路之使用者，如同電話使用者，必須依賴第三人之設備進行通訊，因此對於傳送或接收訊息之位址，以及所瀏覽網頁之 IP 位址並無合理隱私期待，因為使用者係出於為協助網路服務提供者網路傳送訊息之目的而自願提供該等資訊。[201]第二，電子郵件之收件人及寄件人之帳號及 IP 位址所透露有關內容之資訊未必多於電話號碼所透露之資訊。當政府取得某人之電子郵件收件人及寄件人帳號，或其所瀏覽網站之 IP 位址，政府無法知悉信件的內容或其在網站上所瀏覽之特定網頁，最多只能猜測信件中之內容或者網頁中被瀏覽的部分，這與根據撥話對象之身分而猜測電話談話內容大同小異。如同 IP 位址，某些特定之電話號碼可強烈顯示通話內容。例如，某人撥打化學公司或販售槍枝商店之電話可能是詢問有關化學原料或槍械的資訊。再者，若所撥打的是具有特定用途之電話，如詢問運動比賽比數、樂透結果的電話，或者色情電話。[202]第三，政府監察電子郵件的收發資訊雖然在技術上比較複雜，但與監察實體郵件在概念上並無從區別。電子郵件就如同實體郵件，寄件人讓網路服務提供者知悉收件人電子郵件之位址，以傳送訊息給預定之收件者，而電子郵件也含有僅欲讓收件人閱讀之訊息。[203]第九巡迴上訴法院因此認為法院本案政府所為之電腦監察並不構成增修條文第 4 條之搜索。[204]

美國電子隱私法（ECPA）及憲法增修條文第 4 條均嚴格區分「內容資訊」（content information）及「信封資訊」（envelope information）。Orin S. Kerr 教授認為，在科技上雖有不同，但從實體郵件到電子郵件，內容資訊與信封資訊之主要區別仍然是不變的。在實體郵件之情形，內容資訊指的是妥善存放在信封內之

197 United States v. Forrester, 512 F.3d 500（9th Cir 2008）
198 *Id.* at 505.
199 *Id.* at 509.
200 *Id.* at 510.
201 *Id.*
202 *Id.*
203 *Id.* at 511.
204 *Id.*

信件；信封資訊包括寄件及收件地址、郵票及郵戳、及密封信件之大小及重量。[205]同樣的區別也存在電話對話的情形。內容資訊為通話者間實際談話內容；信封資訊則包括撥打之電話號碼及撥話者本身之電話號碼，通話時間，以及通話長度。[206] Daniel J. Solove 教授則認為適用到 IP 位址及統一資源定位器（URLs）時，　信封資訊與內容資訊間之區別就變得模糊不清了。IP 位址係分配給每一部連結網路之電腦之獨特符號。因此每個網站均有其 IP 位址。透過列出完整的 IP 位址，政府能對個人瞭解不少，因為 IP 位址可以追蹤個人如何瀏覽網頁。政府可以得知個人購物商品之名稱，所感興趣之政治組織、個人之性癖好或性幻想，及健康問題等。[207]

統一資源定位器可透露更多資訊。統一資源定位器是一個能指出特定資訊在網路上所在位置之指針。當我們引用某些網路上之資料，所引註的就是該等資料的網路資源定位器。網路資源定位器可透露人們在網路上所瀏覽之資料，也可以包含某些搜索字詞。因此，內容資訊與信封資訊之區分並非總是很清楚。在許多情況，信封資訊就是內容資訊，信封資訊能透露個人之私生活有時候比內容資訊所透露的來得多。[208]區分內容資訊與信封資訊之困難在於並未與敏感性資訊與無危險性之區別妥善連結。信封資訊可以是非常敏感性的，而內容資訊亦可很沒有危險性。不可否認地，在很多情形，人們並未將兩者相連結。[209]

在我國偵查實務，涉及電腦犯罪之情形，檢警常需調閱目標電腦之使用者名稱、IP 位址及該電腦所瀏覽網站之 IP 位址、統一資源定位器等資料而進行網路監察。對於調閱該等紀錄我國原本並無類似美國撥號紀錄器法之規範，2014 年 1 月通訊保障及監察法修正，新增調取通信紀錄制度。依新修正之通保法，通信紀錄係指電信使用人使用電信服務後，電信系統所產生之發送方、接收方之電信號碼、通信時間、使用長度、位址、服務型態、信箱或位置資訊等紀錄。[210]因此，個人使用電腦連結網路所瀏覽之網站 IP 位址及統一資源定位器等資料均屬通信紀錄，依新修通訊保障及監察法，若欲調閱該等通信紀錄，必須是偵辦最重本刑 3 年以上之罪，有事實足認通信紀錄及通信使用者資料於本案之偵查有必要性及關連性，並由檢察官或警方經檢察官許可後向法院聲請核發調取票。[211]在修法之前，若欲取得 IP 位址及統一資源定位器等資料，實務上作法係由檢警等偵查單位以行政公函請求網路服務提供者提供相關資料，在新法修正後，除非當事人自行提供該等資料，否則原則需持法院核發之調取票為之，對資訊隱私提供進一步之

[205] Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 Nw. U. L. Rev. 607 , 611(2003)
[206] *Id*.
[207] Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 Geo Wash. L. Rev. 1264, at 1287(2004).
[208] *Id.* at 1287-88.
[209] *Id*. at 1288.
[210] 2014 年 1 月修正之通訊保障及監察法第 3 條之 1 第 1 項。
[211] 2014 年 1 月修正之通訊保障及監察法第 11 條之 1 第 1 項、第 2 項。

保障。[212]值得討論的是，如 Solove 教授所言，在網路世界中不易區分內容資訊與信封資訊之差異，通訊保障及監察法新增之通信紀錄同時包含使用電話及網路所產生之相關紀錄，並未因兩者對隱私侵害之程度可能不同而給予不同強度之規範，或許將來適用新法調取網路 IP、統一資源定位器等通信紀錄時，需考量某些網路通信紀錄所透露之個人隱私程度不亞於通訊監察所獲得之通訊內容，在適用上應從嚴認定，以保障人民之隱私權。

（三）雲端運算監察

1. 雲端運算所帶來的隱私疑慮

隨著網路科技不斷發展，網路服務有逐漸朝向「雲端運算」發展之趨勢。「雲端運算」之概念，其實就是指「網路運算」，係將過往由個人本身操作的運算功能，例如資料儲存、硬體維護、安裝運用軟體等功能，透過網路連線，交由遠端之雲端服務業者進行運算。只要是利用網路聯繫多臺電腦進行運算工作，或者透過網路連線取得由遠端主機提供之服務，均可算是一種「雲端運算」。[213]個人使用雲端運算服務，包括在網路上儲存或修改照片、建立地址簿、紀錄行事曆、備份資料等。為企業服務的雲端運算功能，則包括處理顧客關係、儲存資料或以遠端電腦操作應用程式等。**[214]**雲端運算固然可提供個人或企業使用者許多便利性，但因雲端運算係將個人資訊從個人電腦移轉到遠端的伺服器上，對於資訊隱私之保護必然會帶來一定程度的威脅。除了在資料傳輸的過程中，資料可能有洩漏的風險。雲端運算服務提供者所取得使用者的資訊後，亦有可能提供給其他商業組織甚者政府。因此，在雲端運算逐漸普遍的數位時代下，政府可以不需大費周章取得法院核發搜索票到嫌疑人住處執行搜索，只需命令雲端運算服務提供者提出嫌疑人所提出的個人資料，即可輕易取得嫌疑人資料，對於人民隱私甚具威脅。

2. 雲端運算資料是否為增修條文第 4 條保護？

根據美國最高法院判決所衍生之「第三人原則」（Third Party Theory），個人將財務資訊等交易資料提供給銀行，即需承擔銀行可能將該等交易資料提供給警方之風險，因此對於其所提供之交易資料並無「合理隱私期待」，該等資料不受增修條文第 4 條所保護。**[215]**此外，最高法院在 *Smith* 案中認為電話使用者因需將電話號碼之資料交給電話公司才能獲得服務，且知悉電話公司會保存該等資料，因此認為電話使用者對其所撥打之電話號碼並無合理隱私期待。亦不受增修條文

---

[212][212] 關於 2014 年 1 月修正通訊保障及監察法新增調取通信紀錄、通信使用者等規定之介紹及評析，詳後述。

[213] 黃重憲，淺談雲端運算，http://www.cc.ntu.edu.tw/chinese/epaper/0008/20090320_8008.htm（最後造訪日期：2014 年 5 月 24 日）

[214] 劉靜怡，新興科技與犯罪：以美國法制之通訊隱私程序保障為論述中心，刑事政策與犯罪研究論文集〈13〉，頁 201。

[215] United States v Miller, 425 U.S. 435(1976).

第 4 條所保護。[216] 依目前美國最高法院實務見解，在判斷政府行為是否構成不合理之搜索時，「第三人原則」還是具有支配性之影響力。因此在政府透過雲端運算服務提供者取得特定人資料之場合，政府可以主張基於「第三人原則」，使用者係自行將個人資料交由雲端服務業者進行運算，應能預見偵查機關可能向雲端服務提供者調取相關資料，因此對於其所提供的資料，自然無合理隱私期待。學者劉靜怡認為在處理第三人從電信服務或雲端服務所合法取得之交易資料時，應思考取得電子郵件、IP 位址等資訊是否等同以撥號記錄器取得資料？以及密碼、未顯示網址或雲端可存取之資料究為可向第三人合法取得之交易資料或內容應受保護之資訊？[217]將電子郵件之信件寄件資訊及收件人郵件等資訊類推為 *Smith* 案中之撥號記錄器的問題在於撥號記錄器僅顯示通話雙方之電話號碼，而電子郵件通常可連結到特定使用者，甚至郵件帳號就是使用者姓名，兩者侵害程度有別。[218]在雲端環境中，交易資料與內容資料間不易區分，例如在搜索引擎鍵入搜索字串，等於開啟與服務者之間的數據交換，使用者將承擔雲端服務者可能揭露該資訊的風險。[219]

3. 本文見解

美國憲法增修條文第 4 條保障人民的文件（papers）免於政府不合理搜索、扣押。過去政府要持搜索票進入嫌疑人住處、辦公場所搜索文件資料，在雲端時代，檢警只需一紙公文即可要求雲端服務業者提供客戶之相關資料，使用者對於提供雲端服務業者的資料是否具有合理隱私期待？因雲端服務所標榜的是更安全、更迅速的資料處理過程，在虛擬的網路世界提供使用者更大的空間去存放更多重要資料。試想，如果內線交易的嫌疑人承租一間私人套房存放商業交易文件，政府須持搜索票搜索該辦公室搜索、扣押相關文件。雲端運算亦同樣重視資料之保密性，只不過實體的文件轉變為電子格式，存放文件的套房還成虛擬網路存放空間。除非使用者欲將文件內容公告周知，否則根據業者與使用者雙方同意遵守之隱私權保障條款，使用者應可合理期待政府不得在欠缺相當理由或未取得法院令狀之情況下搜查其所提供給雲端服務業者之資料。綜上，美國最高法院發展出來之第三人原則在說理上有諸多謬誤，[220]政府不得主張第三人原則，未經法院審查，即向雲端服務業者取得使用者提供之資料。

（四）資料探勘（data mining）

1. 何謂資料探勘？

---

[216] See *Smith v. Maryland*, 442 U.S. 735(1979).
[217] 劉靜怡，註 214 文，頁 215。
[218] 劉靜怡，同前註。
[219] 劉靜怡，註 214 文，頁 216。
[220] 就第三人原則理論的謬誤，以及適用第三人原則造成的危害，本文在【參、三、（二）再思第三人原則】部分會再進一步說明，詳參本文頁 67-68。

美國電視劇「犯罪心理」（Criminal Minds）中聯邦調查局探員透過觀察犯罪動機、手法、嫌犯與被害人間之關係等因素，依犯罪心理學對特定犯罪行為進行嫌犯特寫，研判可能具備某些特質，再將相關變數輸入電腦資料庫以篩選可能的犯罪嫌疑人。劇中聯邦調查局探員總是透過電腦比對出連環殺手的真實身分，而得及時阻止兇嫌繼續犯案。其實利用電腦資料庫比對各種變數進而列出可能嫌犯就是一種資料探勘技術。資料探勘技術其實在現代日常生活中並不陌生，百貨業者透過電腦分析消費者購物紀錄、網路瀏覽記錄等消費行為，並進而分析消費者偏好，再針對個別消費者之偏好以寄送廣告、折價券（coupon）等方式推廣商品以增進營收。

美國國防部在 2002 年開始發展一項名為 TIA（Terrorists Information Awareness）的反恐資料探勘計畫，在此計畫下，美國政府建構一個包括美國人民財務、教育、醫療等各種資料的大型資料庫，藉由分析各種資料以篩選出符合恐怖分子特寫的對象，該計畫負責人認為透過觀察過去恐怖攻擊之行為模式，可將恐怖分子繩之以法。[221]在數位時代下，利用資料探勘技術對於犯罪偵查、反恐等工作勢必可提供幫助。然而，大量蒐集、分析個人資訊可能產生侵害人民隱私的風險，若政府將資料探勘技術用於打擊政治異議分子、審查人民思想等不當用途，將不當扭曲政府與人民間之關係，甚至戕害民主制度之發展。因此如何規範資料探勘技術的使用，值得深思。

2. 學者見解

支持政府使用資料探勘技術的 Richard A. Ponser 法官認為因資料探勘係以機械化方式蒐集、處理個人資料，並使用電腦篩選過濾具有情報價值的個人資料，而電腦並非具有感官能力之人（a computer is not a sentient being），因此大多數個人資料不會由情報員直接閱讀，而對隱私侵害較輕微。[222]Ponser 法官認為資料探勘可能帶來的潛在危險係使用獲取的資訊去威脅、嘲笑批評政府之人及政治對手。[223]

美國知名隱私權學者 Daniel J. Solove 教授認為 Ponser 法官的論點忽略資料探勘實際上可能造成的問題。除了不當揭露獲取資訊的問題外，資料探勘還可能引發不精確、言論自由、公平性、正當法律程序（Due Process）及資訊透明（Transparency）等爭議。[224]恐怖分子未來的行動可能與其過去行為類似，但也有可能不同。若將焦點放在恐怖份子過去的行為模式，可能會忽略未來恐怖份子的

[221] John M. Poindexter, *Finding the face of terror in data*, N.Y. TIMES, Sep.10, 2003, at A25.
[222] Richard A. Ponser, *Our Domestic Intelligence Crisis*, WASH. POST, Dec. 21, 2005, at A31.
[223] RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY, 97,NY,OXFORD UNIVERSITY PRESS(2006).
[224] Solove, *supra* note 148, at 186-194.

特徵及行為。縱使研究過去的行為模式有助於識別恐怖份子，但資料探勘有效的前提是不能有太多的「錯誤特寫結果」（false positive）－符合特寫之人實際上並非恐怖分子。此與商業上預測顧客行為、對準確度要求不高的資料探勘不同。[225]

資料探勘所帶來的另一個威脅是其可能以增修條文第 1 條所保護之活動為基礎而鎖定目標對象，蒐集有關閱讀習慣及言論等資訊可能會造成人們怯於行使言論自由。[226]資料探勘技術可能意味法律應公平地對待不同種族、民族或宗教之人，有些人會主張資料探勘可以消除刻板印象及歧視，因電腦可將人的因素降到最低，防止偏見及種族主義滲入程序中。然而，某些資料探勘技術仍包括人所創造如何識別恐怖份子的特寫（profile），雖表面上係由電腦分析已知恐怖分子的行為模式，但實際上還是隱含人的價值判斷在內。[227]

此外，資料探勘也引發正當法律程序之問題。由資料探勘所篩選而得之人若不同意特寫的結果，因特寫具有秘密性，所以可能無法質疑其結果，也無法主張進行聽證的權利。[228]Solove 教授認為資料探勘技術最不容易處理的是資訊透明的問題，許多資料探勘的計畫都欠缺適度的資訊公開機制。若不需公開說明，非民選的官員可任意進行未經任何審查的資料探勘。若沒有監督機制，政府在何種情況下可蒐集及使用相關資訊就變得不清楚。若政府是以種族、言論等社會認為不宜作為判斷標準的因素為基礎，要如何將這樣的事實公開討論呢？欠缺資訊公開的資料探勘計畫勢必無法在隱私保障與國家安全間取得平衡。[229]Solove 教授贊成政府在對特定威脅掌握資訊的情況下，使用資料探勘技術以發現可能的犯罪者，但反對政府將資料探勘用於一般行為預測。[230]

Cole 教授則認為有關個人生活之私密細節可透過錄影（錄音）、比對（collation）及分析數以百計有關個人消費、旅遊、通訊、聯絡方式及觀看及閱讀習慣之片段資訊被拼湊出來。此種以資料探勘創造「圖象」的方法，使個別來看屬於公開資訊之事物，在其透露通常無法被公權力機關取得之個人行為模式時，已轉變為私密資訊。[231]資料探勘已成為開發個人私生活圖像強有力之工具。是否應允許警察、檢察官及其他政府官員使用此種強有力之工具獲得個案調查所需的資訊？Cole 教授認為在判斷是否侵害增修條文第 4 條之合理隱私期待時，可參考歐洲人權公約之模式，考量政府是否已用盡其他侵害較小手段。[232]

---

225 *Id.* at 188.
226 *Id.* at 189.
227 *Id.* at 190-91.
228 *Id.* at 191-92.
229 *Id.* at 193-94.
230 *Id.* at 195.
231 David Cole, *Preserving privacy in a digital age*, in Surveillance, Counter-Terrorism and Comparative Constitutionalism at 110(Fergal Davis, Nicola MaGarrity and George Williams ed.,2014)
232 *Id.* at 110-11.

3. 本文見解

資料探勘其實一種透過資料分析去篩選目標對象的方式，在犯罪發生後，調查人員其實也是綜合現場跡證、犯案手法、被害人之人際關係、證人證詞等相關因素，加上調查人員之知識、辦案經驗，逐步縮小調查範圍直到偵查結束為止。用於偵查的資料探勘技術其實只是提升偵查效率，加速鎖定目標流程的一種科學化偵查手段。就此而言，似乎並無禁止政府使用資料探勘偵查犯罪、鎖定恐怖分子之正當理由。然而，從基本權保障的角度來看，資料探勘使用功能強大的資料庫分析數據而篩選嫌疑人，由於係透過機械操作，未必會留下資料取得之證據，使得受調查之人難以質疑政府取得個人資料之合法性，可能提高政府以不法取得之資料進行資料探勘之情形。例如，警方非法監聽得知有關犯罪嫌疑人的部分資訊，繼而將非法監聽所得之資料與資料庫內的資料分析比對而特定出犯罪嫌疑人，若資料比對過程沒有資訊透明公開的機制，犯罪嫌疑人是不可能質疑資料探勘結果的。

再者，縱使資料探勘所使用的資料都是合法取得，資料探勘技術畢竟不是一種公眾慣常使用的技術，人民應無法期待政府會結合各種資訊去分析比對個人資料以建構自己可能為犯罪嫌疑人的事實。況且，誠如 Solove 教授所述，資料探勘尚潛藏著資料錯誤、危害言論自由、資訊不透明、不具公平性及欠缺正當法律程序等風險。綜上所述，當政府動用資料探勘技術分析個人資料時，已侵害人民之合理隱私期待，應證明具有「相當理由」相信操作資料探勘技術有助於偵查特定犯罪事實，已無其他侵害較小之偵查手段，且說明所使用者均屬合法取得資料，並取得法院之同意，始得進行資料探勘。此外，為避免事後無法質疑資料探勘過程，聲請書應記載所欲分析之資料種類、設定分析之變數及查詢對象之範圍等資訊以供法院審查，以確保資料探勘程序未不當侵害人民隱私。

二、法院實務見解

（一）追蹤定位科技

1. *United States v. Knotts*[233]

1) 案件事實及訴訟經過

3M 化學公司通知明尼蘇達緝毒組警員其前員工 Armstrong 曾偷取可製造毒品的化學原料，警方發現離開 3M 公司後曾從另一間名為 Hawkins 的化學公司購買相類似的化學原料，警方發現 Armstrong 會將化學原料交給共犯。經 Hawkins 公司之同意，警方在可作為製造毒品之先驅原料之三氯甲烷（choroform）的容器內安裝追蹤器（beeper）。[234]當 Armstrong 購賣三氯甲烷時，Hawkins 公司就將裝有

[233] United States v. Knotts, 460 U.S.276(1983).
[234] *Id*. at 278.

追蹤器的容器交付 Armstrong，警方就透過行動跟監及追蹤器發送的訊號追蹤載有三氯甲烷容器的汽車動向。Armstrong 後來將容器交付給共犯 Petschen，由 Petschen 駕車繼續運送，後來警方因跟丟而停止跟監，追蹤器的訊號也一度斷訊。[235]斷訊 1 小時後，警方透過直昇機上的監視設備，重新取得系爭追蹤器的訊號。穩定的訊號顯示追蹤器在 Knotts 的小木屋內，根據本案資料，警方在發現該小屋後，並未繼續使用追蹤器。[236]

根據使用追蹤器取得之三氯甲烷所在位置，及斷斷續續監視該小屋約 3 天所獲資訊，警方取得搜索令狀。執行搜索過程中，警方發現小屋中有 1 個秘密的實驗室，並在實驗室內發現安非他命甲基安非他命之配方、價值超過 1 萬美金的實驗設備及足以製造 14 磅以上安非他命之化學原料。警方並在小屋外發現用來裝三氯甲烷的 5 加侖容器。[237]Knotts 在一審時提出排除警方無令狀利用追蹤器監視所取得之證據，但為審判法院駁回，並因共同製造管制物質之罪名被定罪，上訴法院認為使用追蹤器監察因侵害被告合理隱私期待而違反增修條文第 4 條，因此撤銷一審有罪判決。[238]

2) 多數意見（大法官 Rehnquist 主筆）

多數意見認為本案中政府透過追蹤器所為之監察，主要是跟蹤汽車在公路及高速公路。最高法院曾不只一次表示人們對在汽車內之隱私期待會逐漸遞減。個人搭乘汽車在公路移動時，對於從某處至另一處的移動軌跡並無合理隱私期待。[239]當 Petschen 在公路上旅行，就已自願地將其在公路上的移動軌跡透露給任何想要瞭解的人。本案被告 Knotts 對於其所擁有的小屋及鄰近建築具有隱私期待，但這樣的隱私期待無法延伸至監視 Petschen 之汽車從離開高速公路至前往 Knotts 之小屋的過程，也不及於三氯甲烷在小屋外開放空間移動的過程。[240]從公開場合肉眼觀察 Petschen 之行車路徑，或者其靠近小屋的過程已能讓警方掌握全部事實。雖然警方在肉眼觀察外，也使用追蹤器追蹤該汽車的位置，但並不會改變本案的情形，憲法增修條文第 4 條並未禁止警方藉由科技強化人類與生俱來的感知能力。[241]

容許無令狀使用追蹤器主要的理由是追蹤器僅為取得原本已公開資訊的有效手段。但人們每日不斷從公開場合移動至私人場所，若未預先取得令狀即追蹤人們在其私人財產內之資訊，警方須承擔此種強化的監視可能偶然不合理地侵入增修條文第 4 條保護的私人領域。[242]本案並無任何資料顯示警方在裝有三氯甲烷的容器抵達 Knotts 之小屋後仍繼續接收或依賴追蹤器所發送的訊息。不可否認，因為警方行動跟監失敗，追蹤器讓警方在本案中得知單憑肉眼觀察無法取得之資訊

235 *Id*.
236 *Id.* at 278-79.
237 *Id.* at 279.
238 *Id*.
239 *Id.* at 281.
240 *Id.* at 281-82.
241 *Id.* at 282.
242 *Id.* at 284.

—三氯甲烷最後停留的位置。本案中使用追蹤器強化監視之科技，如同肉眼監視一般並未引發任何憲法上之爭議。[243]一輛從頭到尾跟蹤 Petschen 的警車也能觀察到其離開高速公路及抵達小屋的行車路徑，及化學容器仍在汽車內之事實，而上開事實及其他資訊，正是警方據以聲請搜索票搜查化學工廠之事實。但並無任何證據顯示本案警方所使用的追蹤器曾透露化學原料在小屋內移動情形或任何無法透過肉眼自小屋外觀察到的資訊。因本案欠缺無物理侵入私人財產之情形，而根據以上分析，多數意見認為，警方監察追蹤器發送之訊號亦未侵害 Knotts 的合理隱私期待，故本案並未構成增修條文第 4 條之搜索或扣押。[244]

2. *United States v. Karo*[245]

1) 案件事實

1980 年 8 月間，藥品管制局（Drug Enforcement Administration,DEA）執法人員 Rottinger 透過線民 Muehlenweg 知悉被告 Karo 及其他兩名被告 Horton、Harley 曾向 Muehlenweg 訂購 50 加侖乙醚（ether）的消息，Muehlenweg 表示乙醚將被用來提煉古柯鹼（cocaine）。政府取得授權在乙醚容器內安裝追蹤器的法院命令，徵得 Muehlenweg 同意後，執法人員將政府所有已安裝追蹤器的容器混入已裝運的化學容器中，並且將所有 10 個容器油漆成相同的外觀。[246] DEA 人員見 Karo 從 Muehlenweg 處取走乙醚後，便透過肉眼監視及追蹤器監察跟蹤 Karo 到其住處。透過使用追蹤器，DEA 人員知悉乙醚仍存放在 Karo 的屋內，但後來追蹤器顯示乙醚已被秘密地搬到 Horton 的房子。DEA 人員從 Horton 住處附近人行道上嗅到乙醚的味道。2 天後，DEA 人員發現乙醚又被移轉到 Horton 父親的住處，隔天，DEA 人員跟著追蹤器的訊號找到 1 個商用倉庫。[247]因為追蹤器並無法精確地讓 DEA 人員知道乙醚放在那個置物櫃內，DEA 人員取得行政傳票而獲知倉庫的紀錄，並得知編號 143 號的置物櫃由 Horton 承租。DEA 人員再用追蹤器確認乙醚存放在編號 143 號的置物櫃同一排的其中一個置物櫃內，並且嗅到編號 143 號置物櫃散發出異味。[248]

經由倉庫經理通知辦案人員才知 Horton 已取走置物櫃內的物品。藉由使用追蹤器，辦案人員發現裝有追蹤器的容器移動到另外 1 個倉庫，於是在該倉庫安裝監視攝影鏡頭監視 Horton 承租之置物櫃，透過監視攝影畫面，辦案人員發現 Rhode 及 1 位不知名的女子將容器該置物櫃移出，並放在 Horton 的卡車上。透過跟監及追蹤器監察，辦案人員得知該卡車曾停留於 Rhode 的住處，Rhode 及不知名的女子將箱子及其他物品放在該卡車上後，又駛往 Horton 等人所承租的房子。辦案人員根據追蹤器所取得之資訊及其他資料取得搜索令狀，搜索後將 Horton 等人逮捕，並扣押古柯鹼及實驗器材。[249]

---

[243] *Id.* at 284-85.
[244] *Id.* at 285.
[245] United States v. Karo ,468 U.S. 705(1984).
[246] *Id.* at 708.
[247] *Id.*
[248] *Id*.
[249] *Id.* at 709-10.

2) 多數意見（大法官 White 主筆）

多數意見認為本案需要處理 Knotts 案所未處理的兩個問題：第一，經原所有人同意後在化學容器內裝置追蹤器，當該容器交付給不知有追蹤器存在的買受人時，是否構成增修條文第 4 條的「搜索」或「扣押」？第二，使用追蹤器取得肉眼監視所無法取得之資訊，是否為增修條文第 4 條所要處理的問題？[250]

很顯然的單純將追蹤器安裝於容器內的行為不會侵害任何人增修條文第 4 條的權利。因為安裝追蹤器時，不論乙醚或 10 個容器，都是在同意安裝追蹤器的 Muehlenweg 持有中。無法想像被告對於容器有何隱私期待。[251]多數意見認為容器的移轉不構成搜索。因為必須合理隱私期待被侵犯才算是搜索。將裝有追蹤器的容器移轉給 Karo 並未侵害任何隱私利益，移轉容器的行為並未透露任何資訊，所以也未透露 Karo 欲保持私密的資訊。精確地說，上開行為創造隱私侵害的可能性，但最高法院從未將隱私侵害的可能性視為增修條文第 4 條的搜索。[252]

多數意見也認為移轉上開容器不構成扣押。因為對財產的扣押係指所有人對財產的持有利益被嚴重干擾。雖然本案的容器被安裝不知名且多餘的外來物體，但並無法說任何人的財產利益被嚴重干擾了，至多只因追蹤器所占據的空間而有科技上的物理侵入。此種微量的物理侵入不足以構成憲法上的侵害。當然，如果只因追蹤器的存在就構成扣押，這將推導出只要有任何物體的存在，不管其內容為何，均違反增修條文第 4 條。[253]

多數意見認為本案所安裝的追蹤器並未侵害 Karo 或其他被告增修條文第 4 條之利益。較有可能發生的是追蹤器監察所伴隨的隱私利益侵害。本案使用追蹤器將乙醚定位在特定的房子內，更將該等資訊用於聲請搜索房屋之令狀。引發利用追蹤器監察肉眼所無法觀察到的私人住處是否侵害增修條文第 4 條在住處享有的隱私利益的問題。[254]本案中，政府未取得令狀即使用電子裝置取得從屋外觀察所無法取得之資訊。追蹤器讓辦案人員知悉特定物品在特定時間在受監察的私人住處內，且為私人所持有。縱使肉眼監視已觀察到追蹤器進入房屋的事實，追蹤器的監察不僅確認警員的觀察，也證實特定物品仍在屋內的事實。本案中，乙醚被送抵系爭房屋後，辦案人員在聲請令狀便使用追蹤器實施監察一段時間。[255]

多數意見不認為本案有不採令狀原則搜索住宅之理由。辦案人員使用追蹤器監察確認在乙醚仍在屋內，且知悉乙醚在令狀聲請過程中，仍持續存於屋內之事

[250] *Id.* at 707.
[251] *Id.* at 711.
[252] *Id.* at 712.
[253] *Id.* at 712-13.
[254] *Id.* at 713-14.
[255] *Id.* at 715.

實。因政府取得該等資訊並未依令狀，所以在審判過程中不得使用該等資訊證明對系爭房屋享有隱私利益的被告犯罪。若可證明聲請令狀宣誓書所包括之該等資訊為形成核發令狀之「相當理由」之重要證據，可能會使搜索令狀無效；但若令狀宣誓書中所提出未受污染的證據已足以建構相當理由，已核發之令狀仍為有效。[256]只要審查含有聲請事實之令狀宣誓書，即可知悉辦案人員縱使不使用追蹤器定位欲搜索的乙醚也可取得令狀。有疑問的是，令狀宣誓書所包含的任何其他資訊是否本身是否也是違反增修條文第 4 條的結果。多數意見認為本案中除了使用追蹤器監察確認乙醚在房屋內之事實應被排除，其他證據並非違法搜索之產物，扣除被排除的證據，依其他資訊仍足以形成核發搜索令狀之「相當理由」，因此在系爭房屋所扣押的證據不應被排除。[257]

3) 部分協同部分不同意見書（大法官 Stevens 撰寫，大法官 Brennan 及 Marshall 加入）

大法官 Stevens 認為追蹤器的安裝構成扣押。財產的所有權人，享有專有使用其財產的排他性權利，可排除包括政府在內之任何人侵害其財產。當政府在私人財產上安裝電子監察儀器，基本上該物已為政府使用，而侵害被告於物品交付時所取得之排他性財產權。[258]透過安裝及使用追蹤器，且將追蹤器藏放在容器中，政府已宣稱了對該財產統治及控制的權力－以其目的使用該財產的權力，而這樣統治及控制的權力基本上就是一種扣押。[259]

3. *United States v. Jones*[260]

本案為美國最高法院首度針對裝置 GPS 設備追蹤是否構成「搜索」乙節表示意見，Knotts 案、Karo 案等判決先例認為警方於特定容器裝置追蹤器（beeper）並不構成搜索或扣押。然而，在 *Jones* 案中，所有參與決定的法官，或有不同的理由，但均一致肯定該案中 GPS 的安裝或使用，構成憲法增修條文第 4 條的「搜索」，警方必須取得令狀後始得為之。不管多數意見或者是協同意見，均再次確認 *Katz* 案中增修條文第 4 條保障範圍及於「合理隱私期待」的原則，協同意見甚至「合理隱私期待」的判斷標準具體適用到 GPS，不僅擴大增修條文第 4 條的射程範圍，也讓偵查單位知悉新型態的偵查手段一旦侵害合理隱私期待，無論是否有物理侵入，均屬「搜索」或「扣押」。本案因涉及新型態的科技偵查手段，對於偵查實務有極高的重要性，值得參考。

1) 案件事實

被告 Jones 為哥倫比亞特區（District of Columbia）某間夜店之負責人，因涉

256 *Id.* at 718-19.
257 *Id.* at 719-21.
258 *Id.* at 729.
259 *Id.* at 730.
260 United States v. Jones, 565 U.S.__, 132 S.Ct.945（2010）

嫌交易麻醉藥品而成為警方調查目標，警方使用各種偵查手段，包括在其所經營之夜店跟監，裝設攝影機拍攝該夜店的大門，以及使用監視記錄器及監聽 Jones 的手機。根據上開偵查手段所得之資訊，美國政府在 2005 年向哥倫比亞特區法院申請核發登記為被告妻子所有之汽車上裝設電子追蹤設備之令狀，法院核發令狀授權警方於 10 天內在哥倫比亞特區範圍內裝設上開電子追蹤設備。[261]警方於法院核發令狀後的第 11 天，在哥倫比亞特區範圍外的馬里蘭州某處公共停車場內將 GPS 儀器安裝於上開汽車之底盤處，接下來的 28 天，警方利用上開儀器追蹤該車的移動軌跡，且期間曾於該車停放在馬里蘭州另一處停車場時，更換儀器的電池。透過電子訊號及衛星系統，GPS 顯示該車的位置，並將該車位置透過手機傳送至政府的資料庫，在 4 週期間內，追蹤器傳送了超過 2,000 頁的資料。美國政府後來對 Jones 提出包括共同運送及持有古柯鹼等多項罪名。Jones 在預審階段提出排除透過 GPS 取得之證據的動議。[262]

2) 多數意見（由大法官 Scailia 主筆）

汽車為憲法增修條文第 4 條所指之「動產」（effect），多數意見認為本案政府將 GPS 儀器安裝在目標汽車上，以及利用 GPS 監視汽車的移動軌跡構成搜索。本案中，政府為了取得資訊的目的，在物理上占據私人財產之行為，在過去會被認為是憲法增修條文第 4 條所指之「搜索」。[263]憲法增修條文第 4 條的文字顯示與財產之緊密關連，因為若非如此，該條文中「個人、房屋、文件及動產」等用語就顯得多餘不必要。在 *Olmstead v. United States*, 277 U.S. 438（1928）一案中，最高法院認為在公共街道透過電話線監聽並不構成增修條文第 4 條所指之「搜索」，因為並未進入被告之房屋或辦公室。最高法院在 *Katz* 案中，認為憲法增修條文第 4 條保護的對象是人而非地方，因此認定透過在公共電話亭裝置竊聽設備違反增修條文第 4 條。[264]

最高法院在後續案件適用 *Katz* 案中大法官 Harlan 協同意見書之分析意見，認為當政府侵害人民合理隱私期待即違反憲法增修條文第 4 條。在本案中，被告之權利並未因 *Katz* 案之出現而有所改變。實際上，必須確認憲法增修條文第 4 條所接受之隱私權被有效保護。增修條文第 4 條被理解為特別著重政府侵害「個人」、「房屋」、「文件」及「財產」等被列舉之領域，而 *Katz* 案並未否定這樣的理解。[265]*Katz* 案並不是主張增修條文第 4 條僅保護人民及私密對話，而有放棄該條文對住家等領域的保護。在 *Katz* 案中，法院雖然建構財產權並非增修條文第 4 條侵害之判斷標準，但並未扼殺過去被認可之財產權保護取徑。如同大法官 Brennan 在 *Knotts* 案中之協同意見，*Katz* 案並未侵蝕政府為達獲取資訊之目的而從事物理侵入憲法保護領域構成憲法增修條文第 4 條之違反的原則，*Katz* 案並未限縮增修條文第 4 條之保護範圍。[266]

在 *Katz* 案後有 2 件追蹤器之案件。在 *Knotts* 案，最高法院認為使用追蹤器定

[261] *Id.* at 948.
[262] *Id.*
[263] *Id.* at 949.
[264] *Id.* at 949-50.
[265] *Id.* at 950.
[266] *Id.* at 951.

位裝有三氯甲烷之容器並不未侵害 Knotts 的合理隱私期待，因為被取得之資訊為載有容器之車輛行駛在公共道路之位置，以及在開放空間卸貨之化學容器所在位置，都可被認為是自願向公眾揭露之資訊。*Knotts* 案中只強調合理隱私期待的判斷標準，因為傳統之判斷標準在該案中並不重要。因為被告持有該容器前，追蹤器已經當時持有者之同意而被放置於容器內，但 *Knotts* 案沒有去探討安裝追蹤器之行為。[267]

Karo 案之爭議在於是否在容器內裝置追蹤器構成搜索或扣押？如同 *Knotts* 案，在 *Karo* 案中追蹤器被裝置於容器時，容器尚在第三人之持有中。政府僅在該容器為被告 Karo 持有前，對該容器有物理接觸，接著轉移並未裝有監視設備之容器給被告，並未侵害 Karo 之隱私。多數意見認為本案中警方安裝 GPS 儀器在被告使用車輛上之行為，已侵害增修條文第 4 條保護之領域，警方進入汽車內部時已構成搜索。[268]

3) 大法官 Sotomayor 之協同意見書

大法官 Sotomayo 認為憲法增修條文第 4 條所不僅關注對財產權之物理侵入，縱使沒有物理侵入，當政府侵害社會所認為合理的主觀隱私期待，就產生憲法增修條文第 4 條之搜索。如多數意見所闡述，*Katz* 案之合理隱私期待之判斷標準擴大了，但並未取代或縮減先前習慣法之物理侵入判斷標準。物理侵入原則適用在多數意見中，反應了不可再縮減的憲法最低要求：當政府為了獲取資訊而物理上侵入個人財產，就是「搜索」。[269]

儘管如此，如大法官 Alito 所述，現在許多偵查手段未必會有物理上之侵害。政府可能藉由受徵召之工廠、私人所有汽車內建 GPS 定位裝置或者具有 GPS 功能之智慧型手機。使用電子或其他不需倚賴物理侵入之新型態偵查手段之個案中，多數意見所採之物理侵入標準並無法提供明確的方向。在單純傳輸電子訊號而無物理侵入之情形，仍應適合 *Katz* 案之分析方式。科技的進步可能使得不具物理上侵入性的偵查作為，因著社會合理隱私期待之演進，而影響判斷標準。在此前提下，大法官 Sotomayor 同意大法官 Alito 之協同意見，最起碼在長時間以 GPS 監察方式調查多數犯罪行為侵害合理隱私期待。[270]

即使在短時間 GPS 監察之情況，某些有關 *Katz* 案所分析之 GPS 特性需要特別關注，GPS 能獲取精確、廣泛的個人公開活動軌跡，這些資訊可透露有關個人家庭、政治、專業、信仰及交往等關係之豐富細節。[271]此外，相較於傳統偵查技巧，利用 GPS 實施偵查成本較底，而且透過刻意秘密進行之方式，GPS 監察能規避濫用執法權限的監督，不僅可以節省警力資源，更可減少來自社會的反對。GPS 監察可以相對低之成本取得有關政府所欲追蹤目標之大量個人資訊，如此一來，可能改變政府與人民間之關係，而對民主社會有害。在評估社會合理隱私期待時應將上述 GPS 偵查之特性一併納入考量。應考量人民是否合理地預期其行動軌跡

[267] *Id.* at 951-52.
[268] *Id.* at 952-53.
[269] *Id.* at 954-55.
[270] *Id.* at 955.
[271] *Id.* at 955.

將被記錄、整合，並供政府檢視其政治、宗教信仰、性習慣，及政府是否透過例行性的監察獲得 GPS 偵查所得到的資訊。[272]大法官 Sotomayor 認為在欠缺任何其他機關監督之下，將如此容易濫用的工具交託給行政部門使用並不妥適，憲法增修條文第 4 條之目的在於抑制警察權的任意行使及避免過於全面的警察監察。[273]

更重要的是，必須重新思考個人在自願透露個人資訊給第三人之情況下即無合理隱私期待之假設前提。這樣的取徑，在人民於日常工作中揭露大量個人資訊給第三人之數位資訊時代並不合適。或許有些人認為以隱私換取便利是值得的，或者接受此類隱私的縮減是不可避免的。人民是否會毫無怨言地同意無令狀揭露渠等過去一個禮拜、一個月甚至一年的網路瀏覽紀錄。無論社會隱私期待之內涵為何，只有在憲法增修條文第 4 條不再將秘密性當作隱私保護之前提，無令狀揭露個人資訊才有可能符合憲法之保障。[274]大法官 Sotomayor 認為並非所有自願提供第三人作有限目的使用的個人資訊，無法僅以此為由即剝奪人民享有憲法增修條文第 4 條之保護。隱私並非只有絕對享有或完全剝奪兩種選項。那些提供部分資訊給銀行或電話公司供有限商業目的使用的人不需假設這些資訊會因其他目的被提供給他人使用。人民欲保留為秘密的事物，即使在某些情況是對外公開的，也應被憲法保障。[275]

4) 大法官 Alito 撰寫之協同意見書（大法官 Ginsburg、Breyer、Kagan 加入）

本件應將憲法增修條文第 4 條－禁止不合理的搜索、扣押－適用於 21 世紀的監察技巧－使用 GPS 裝置長時間監察某輛交通工具的動態。很諷刺的是，法院選擇依據 18 世紀的侵權法決定這個案件。多數意見的決定曲解了憲法增修條文第 4 條的用語，不僅無法對增修條文第 4 條的判例法提供幫助，且顯得非常矯揉造作。[276]憲法增修條文第 4 條係禁止不合理的搜索、扣押，多數意見並未致力於解釋「安裝」或「使用」GPS 裝置是否符合上開用語。安裝 GPS 本身並未構成搜索，因為如果 GPS 未發揮作用，或者執法人員並未使用該儀器，並不會取得任何資訊。多數意見並未主張「使用」GPS 裝置構成搜索。[277]

多數意見所提出物理侵入原則並無法在 *Katz* 案之後的案例找到有力的支持論點。多數意見的論點有以下問題：第一，多數意見的論點過度忽視使用 GPS 進行長時間追蹤此一重要爭點，反將重點放在「安裝」GPS 此一相對不重要的枝微末節。如果長時間監察並未伴隨物理侵入，舉例而言，假設聯邦政府要求或鼓勵汽車製造商在生產汽車時將 GPS 追蹤儀器列為汽車必要配備，依多數意見之理論即無法提供有效保護。[278]第二，多數意見的取徑將導致不合適的結果。假如警方將 GPS 安裝在某汽車上，並使用 GPS 短暫地追蹤該車，依多數意見，應有增修條文第 4 條的適用；但如果警方使用車輛甚至從空中長時間地追蹤相同的車輛，則不受到增修條文第 4 條之限制。本案警方係在被告的妻子將系爭汽車交付給被告使用後才安裝 GPS， 因此多數意見認為有增修條文第 4 條的適用。但如果警方是

[272] *Id.* at 956.
[273] *Id.*
[274] *Id.* at 957.
[275] *Id.*
[276] *Id.* at 957-58.
[277] *Id.* at 958.
[278] *Id.* at 961.

在被告妻子交付上開汽車前安裝 GPS，依多數意見的論點可能會有不同的結果，被告無法主張非法侵入，大概也無法主張增修條文第 4 條的侵害。[279]

第三，依多數意見所述，增修條文第 4 條涵蓋的範圍會因各州是否採取夫妻共同財產制而有所不同。若本件發生在採取夫妻共同財產的州或者是採取統一婚姻法（Uniform Marital Property）的州，不論 GPS 是在汽車移轉前或後安裝，被告均屬系爭汽車之所有人。但若發生在不採夫妻財產制的州，因系爭汽車登記於被告妻子名下，很可能會被認定汽車所有人為被告之妻。[280]第四，多數意見依賴物理侵入標準的取徑，在使用電子監察而非使用物理侵入追蹤的情形，會產生令人困惑的問題。*Katz* 案所提出的合理隱私期待標準可避免上開困難的問題。[281]

科技所產生的劇烈轉變可能會導致公眾的期待不斷的變遷，最終可能促成社會大眾的態度產生重大的變化。現代的科技在提供更高的便利性及安全性的同時也需要以犧牲隱私作為代價，許多人這樣的交易是合理的。即使有些人不喜歡現代科技所帶來隱私減損的結果，但這些人最終可能妥協地認為這是科技發展不可避免的結果。[282]近年來，許多科技裝置可以監察個人的行動，在某些場所，監視攝影已經是無所不在。許多人購買的汽車安裝有允許行控中心追蹤汽車定位之裝置，以便實施道路救援或尋找失竊車輛的服務。更重要的是，現在手機及其他無線裝置可以讓通信業者追蹤並記錄使用者的位置。[283]

具有 GPS 功能的新型態智慧型手機，相較於傳統的電話，可以提供更精確的追蹤。舉例而言，當使用者開啟智慧型手機上的 GPS 功能，該服務提供業者可以透追蹤該手機的定位及移動的速度，在結合上開資訊後回報即時的路況資訊。同樣地，手機定位追蹤服務也提供消費者登錄於該系統的消費資訊。這些科技裝置的使用將繼續形塑一般人民對於他們日常生活的隱私期待。[284]本案中使用的 GPS 裝置讓長時間監察變得相對地容易、便宜，在科技急速變遷的環境下，或許關於隱私議題最好是透過立法途徑來解決。在尚無有關 GPS 追蹤的立法前，本案最好的處理方式是適用增修條文第 4 條的法則去判斷伴隨物理侵入而使用 GPS 進行追蹤是否為一理性之人所不能預期的。在此取徑下，短時間追蹤個人在公共街道的移動應，相對來說，應能符合社會所認知的隱私期待。但使用 GPS 長時間監察以進行大多數犯罪的偵查，應已侵犯社會合理隱私期待。因此本案的長時間監察已構成增修條文第 4 條的搜索。[285]

（二）紅外線穿透科技（*Kyllo v. United States*[286]）

美國最高法院在 *Kyllo* 案首度認為使用熱影像顯示儀構成合理隱私期待之侵犯，並就新型態科技與憲法增修條文第 4 條間之關係做出說明，該案的意見對於

279 *Id*.
280 *Id.* at 961-62.
281 *Id.* at 962.
282 *Id.*
283 *Id.* at 963.
284 *Id.*
285 *Id.* at 964.
286 Kyllo v. United States, 533 U.S. 27 (2001).

理解美國實務對於利用高科技執行搜索、扣押及通訊監察之態度有很大的幫助。

1. 案件事實

美國內政部探員懷疑 Kyllo 在其屋內栽種大麻。因為在室內栽種大麻通常需要高熱度之燈光。為了判斷 Kyllo 屋中所散發出之熱度與使用栽植大麻所使用之燈光相符，內政部探員使用紅外線熱顯像儀對 Kyllo 之房屋掃瞄，熱顯像儀可偵測到肉眼所無法看到之紅外線輻射。熱顯像儀根據不同的溫度將輻射轉換為不同的影像－黑色代表低溫，白色代表高溫，灰色的陰影代表溫度不同。[287]探員使用熱顯像儀從 Kyllo 房屋前後掃描了幾分鐘，掃描結果顯示該屋車庫之屋頂及牆壁之溫度較該屋其他部分及鄰近之房屋之溫度來得高。探員因此認為 Kyllo 使用鹵化燈在室內栽種大麻，法院依據政府提出之線民情資、電費帳單及熱顯像影像核發搜索令狀，探員執行搜索後發現 Kyllo 在室內栽種超過 100 株的大麻，Kyllo 被控違法製造大麻。[288]

2. 多數意見（由大法官 Scalia 主筆）

多數意見認為增修條文第 4 條之核心價值在於堅持個人享有退避到房屋內以免於政府不合理之侵犯之權利。除了少數例外情形外，對房屋進行無令狀搜索通常是不合理且違憲的。[289]藉由增強人類感官能力之科技而取得過去通常需以物理侵入憲法保障領域始得取得之資訊應構成搜索，而判斷標準在於該政府使用之科技是否為「一般公眾使用」(in general public use)。根據這樣的判斷標準，本案政府所使用之熱顯像儀並非一般公眾所使用之工具，因此以熱顯像儀所取得之資訊即為搜索之產物。[290]雖不同意見認為本案所使用之熱顯像儀僅獲得屋內散發出來之熱量，僅屬牆外觀察(off-the-wall observation)，而非牆內監視(through-the-wall surveillance)。多數意見就此反駁，認為不同意見之論述如同認為 *Katz* 案中監聽裝置僅蒐集電話亭外部之音波一般，為對增修條文第 4 條之機械化解釋。[291]

不同意見另認為不得使用熱顯像儀蒐集屋內之私密細節，多數意見認為僅禁止熱顯像儀探測私密細節不僅理論上是錯誤的，實際上更無法適用。監視設備之精密程度與其所觀察內容之私密性並無必然關連，使用本案相對簡陋之熱顯像儀並非總是合法的。例如，本案所使用之熱顯像儀可以揭露屋內之女士每天在何時做蒸汽浴或洗澡，及屋內櫥櫃的燈是否亮著等私密細節。[292]多數意見認為最高法院無法就何種牆內觀察是容許地設定標準，但必須發展一個界定室內活動是否具

[287] *Id.* at 29-30.
[288] *Id.* at 30.
[289] *Id.* at 31.
[290] *Id.* at 34-5.
[291] *Id.* at 35.
[292] *Id.* at 36, 38.

有私密性之體系。為了就搜索住宅劃分明確之界線，使執法人員在執法前知道何種偵查手段為憲法容許，必須說明何種監察手段需要令狀。[293]在本案中，政府使用未為公眾普及使用之熱顯像儀去獲取過去必須透過物理侵入房屋始得獲得之資訊，此種監察手段構成「搜索」，在無令狀之情形下實施此種監察應被推定為不合理之搜索。[294]

3. 不同意見書（大法官 Stevens 撰寫，首席大法官 Rehnquist 及大法官 O'Connor、Kennedy 加入）

不同意見認為對於房屋以目光掃視（plain view）進行搜索、扣押應被推定為合理的。當個人將資訊明知地暴露給公共大眾，即使在其自宅或辦公室內，亦不受增修條文第 4 條之保護。[295]本案所涉及的僅為執法人員使用牆外監視從被告住宅牆外蒐集暴露於公眾之資訊，本案所獲得之測量資料僅顯示不同熱量之散發，概略地顯示房屋之屋頂及外牆的部分範圍較其他部分溫度為高，而紅外線掃描所得之影像，並未揭露被告屋內之活動。[296]

雖然多數意見欲劃出一條明確、固定的界線，但其所提出的新標準非常不確定，因為新標準所賦予的保護在相關科技為「一般公眾所使用」時就消失了。[297]雖然多數意見並未提出判斷一般公眾使用之標準，但令人懷疑本案所使用之熱顯像儀是否滿足一般公眾所使用之標準。撇開明確性不足之問題，多數意見所提出之「一般公眾使用」之判斷標準仍不合理。因按此標準，對於隱私之威脅只會增加不會減少，因為侵入性設備會越來越容易取得。[298]

大法官 Stevens 認為多數意見所提出之新標準適用於任何涉及住宅內部之資訊，這樣的標準同時具有涵蓋過廣及涵蓋不足的問題。[299]用來保障個人隱私不因感官增強設備過度使用而被侵犯的標準不應僅適用於住宅。若科技設備讓使用者能在功能上進入私密領域，例如，*Katz* 案中之公共電話亭或者辦公大樓，該標準如適用於住宅之情形一般適用於該等私密領域。[300]

（三）檢視手機內資訊（***Riley v. California***[301]）

1. 案件事實

---

293 *Id.* at 40.
294 *Id*.
295 *Id.* at 42.
296 *Id.* at 42-3.
297 *Id.* at 47.
298 *Id*.
299 *Id.* at 48.
300 *Id.* at 48-9.
301 Riley v. California, 573 U.S._（2014）

第 1 個案件中，Riley 因為汽車登記標籤過期遭警察攔停，警察在攔停過程中得知 Riley 的駕照已被吊銷。警察於是扣押 Riley 的汽車，根據警局之政策，另一名警員對該車進行清點式搜索（inventory search），發現汽車引擎蓋下藏有 2 把手槍，警方便以持有及藏匿裝有彈藥之槍械之罪名將 Riley 逮捕。[302]警方在執行逮捕過程中附帶對 Riley 搜索，發現與街頭幫派「Bloods」有關的物件，並將從 Riley 長褲口袋中搜到之智慧型手機（smart phone）扣押。執行之員警查看該智慧型手機內之資訊，發現許多文字前都註記「CK」兩字母，警方認為「CK」代表「Crip Killers」，為幫派「Bloods」成員所使用的暗語。[303]逮捕 Riley 後約 2 小時，另一名負責幫派犯罪的警探在警局內進一步檢視上開手機所含的資訊欲尋找證明犯罪的證據。警方在該手機中發現數張 Riley 站在 1 輛被懷疑與數週前所發生之槍擊案有關的照片。[304]Riley 被指控使用半自動槍械攻擊他人及謀殺等罪名。在進入審判前，Riley 提出動議排除所有從其手機中取得之證據，主張警方搜索其手機違反增修條文第 4 條，因為執行搜索前警方並未取得令狀，亦欠缺緊急情況。[305]

第 2 個案件中，警方從事執行例行性跟監時發現 Wurie 在汽車內販賣毒品，警方隨即逮捕 Wurie 帶回警局。在警局內，警方從 Wurie 身上扣押 2 部手機，其中 1 部是以折疊方式打開使用，功能不如智慧型手機的折疊式手機（flip phone），警方從手機螢幕發現該手機不斷收到標記為「我家」之電話號碼所撥入之電話。[306]警方於數分鐘後打開該手機，看到手機桌布為 1 個女人及 1 個小孩之照片。警方便按功能鍵查看手機之通話記錄，並再按功能鍵查詢與「我家」之標示有關之電話號碼。警方透過線上電話簿查到某一間公寓。[307]警方在該間公寓發現信箱上載有 Wurie 的姓名，並從窗外看到屋內有 1 名與 Wurie 手機上照片中女子相像的女子。警方在聲請搜索令狀期間派人看守該間公寓，取得令狀後，警方執行搜索過程發現並扣押了了古柯鹼、大麻、施用毒品器材、槍械、彈藥及現金。[308]Wurie 被指控轉讓古柯鹼、意圖販賣而持有古柯鹼等罪，以及持有槍械及彈藥的重罪。Wurie 提出排除警方搜索其公寓所取得之證據的動議，他主張該等證據為警方對其手機違憲搜索所衍生之證據。[309]

2. 多數意見（首席大法官 Roberts 主筆）

本案所涉及的 2 個事實產生共同的問題：警方可否在無令狀情形下，對逮捕時附帶扣押之手機內的數位資訊進行搜索？[310]如增修條文第 4 條的文字，該條規

302 *Id.* at 1-2.
303 *Id.* at 2.
304 *Id*.
305 *Id.* at 2-3.
306 *Id.* at 3-4.
307 *Id.* at 4.
308 *Id*.
309 *Id*.
310 *Id.* at 1.

定最終的判斷標準在於「合理性」，而合理性通常要求政府取得法院令狀。此種令狀確認支持搜索之推論係經中立且公正的法官審查，而非由從事偵查犯罪的政府官員判斷。在欠缺令狀之情形下，通常僅在符合令狀原則特定例外情形時，無令狀搜索才會被認為是合理的。本案所需考量者為合法逮捕所附隨無令狀搜索之合理性。[311]伴隨合法逮捕所為之無令狀搜索雖一直被認為是令狀原則之例外，但此種無令狀搜索的範圍一直被激烈地論辯，辯論的焦點在警方對於對被告身體或周圍的物件能搜索到什麼程度，有三個相關的判決前例提供標準規範此種搜索。[312]

第一個判決是 *Chimel v. California*, 395 U.S. 752 （1969），該案可說是為無令狀附帶搜索的基礎。警方在屋內逮捕 Chimel 後，又徹底搜索其含有 3 個房間的房屋，包括搜索閣樓及車庫，在某些房間，警方也查看抽屜內的物件。[313]最高法院在 *Chimel* 一案對於如何評估附帶搜索之合理性，提出以下標準：『執行逮捕時，執行逮捕的警員為了除去可能用於反抗逮捕或脫逃的武器，而搜索受逮捕人之身體是合理的。否則，可能危及警員之安全而造成逮捕失敗。此外，為了防止證據被隱匿或破壞，執行逮捕的警員搜索及扣押受逮捕人身上之證據也是完全合理的…，因此，搜索受逮捕人之身體及其能立即控制（immediate control）之範圍—可理解為受逮捕人可取得武器或可被破壞之證據之範圍。』（*Id.* at 762-63）。[314] 警方在 Chimel 住處大規模無令狀搜索並不符合上開令狀原則之例外，因為當時已無保護警員人身安全及證據之需求。[315]

第二，最高法院在 *United States v. Robinson*, 414 U.S.218（1973） 一案中在搜索受逮捕人身體之情形下使用 *Chimel* 案之分析標準。[316]在 *Robinson* 案中，警方以 Robinson 持被撤銷之駕照駕駛為由逮捕 Robinson。該名員警以拍打 Robinson 的身體，感覺到 Robinson 外套口袋內有 1 個無法辨識物體，警方取出該物體，發現是個香菸盒，打開該盒後發現裡面有 14 個海洛英膠囊。[317]最高法院在 *Robinson* 案中認為伴隨合法逮捕之附帶搜索不需要個案判斷其正當性。最高法院進一步闡釋：『伴隨於合法拘捕而搜索受逮捕人之權力，是建立在卸除武器及發現證據之需求，而非取決於事後法院判斷在個別逮捕情況下，是否可能在嫌犯身上發現武器及證據。基於相當理由對嫌犯的拘捕係增修條文第 4 條下合理的權利侵害，既然係合法的權利侵害，附隨於合法逮捕之搜索就不需要另外具備之正當理由。』（*Id.* at 235）[318]因此，最高法院認為對 Robinson 的搜索是合理的，即使當時並無證據滅失或者 Robinson 持有武器的考量。最高法院在 *Robinson* 案並未在搜索 Robinson

311 *Id.* at 5.
312 *Id.* at 5-6.
313 *Id.* at 6.
314 *Id.* at 6-7.
315 *Id.* at 7.
316 *Id*.
317 *Id.*
318 *Id.*

身體及進一步檢視香菸盒之搜索間做出明確區分。[319]

第三個案例，最高法院在 *United States v. Chadwick*, 433 U.S. 1, 15(1977)一案將附帶搜索的範圍限縮在與受逮捕人立即發生關連的個人物品。[320]另外，最高法院在 *Gant* 案就附帶搜索受逮捕人之汽車做出分析，如同 *Robinson* 案一般，最高法院肯認 *Chimel* 案將員警人身安全及證據保存視為附帶搜索基礎之見解，認為 *Chimel* 案授權員警搜索汽車之範圍，僅限在受逮捕人未被制伏之情形，搜索時乘客可觸之置物箱（compartment）。但最高法院在 *Gant* 案補充，當可合理相信與逮捕之犯罪有關之證據可能在汽車中被發現時，本身即屬一種可無令狀搜索汽車置物箱之例外情形。此種例外並不是源自 *Chimel* 案，而是出自汽車搜索之特殊脈絡。[321]

多數意見認為在搜索數位資訊的脈絡下，並沒有類似 *Robinson* 案所歸納危害警員人身安全或證據滅失的風險。雖然 *Robinson* 案認為任何個人保存的隱私利益都因逮捕的發生而逐漸減損。由於手機保存大量的個人資訊，多數意見認為對手機的搜索與 *Robinson* 案所認知的短暫實體搜索並不相同，因此 *Robinson* 案的標準不能適用，因此認為政府在搜索手機內之資料前應先取得令狀。[322]儲存在手機中的數位資料本身並無法當作傷害執法警員的武器或協助受逮捕人脫逃。執法人員仍然自由地從物理層面判斷該手機是否可能被當作武器使用—例如，判斷在手機與外殼間是否藏有刮鬍刀片。然而，一旦警員已取得手機並排除潛在的物理侵害後，儲存於手機內的資料就再也無法危害警員的人身安全。[323]

再者，從避免證據滅失的角度觀察，一旦警方取得手機，被逮捕人本身不再可能自行透過手機刪除得證明被逮捕人犯罪之證據。[324]政府則主張透過遠端清除技術（remote wiping）或資料加密技術（data encryption）等措施可能造成手機內之數位資料滅失。遠端清除係指手機在連接無線網路之狀態收到清除儲存資料的訊號，遠端清除資料可藉由第三人從遠端發送指令或者預先透過程式設計，使手機在進入或離開特定地區時即自動刪除資料（所謂地理圍欄，「geofencing」）。[325]加密技術則是指手機的使用必須通過密碼檢驗程序的安全措施。當使用加密技術的手機上鎖後，複雜的加密技術就保護其內的資料，除非警方知道密碼，否則該手機幾乎牢不可破。[326]

---

319 *Id.* at 7-8.
320 *Id.* at 8.
321 *Id*.
322 *Id.* at 9-10.
323 *Id.* at 10-11.
324 *Id.* at 12.
325 *Id*.
326 *Id.* at 12-13.

關於遠端清除技術，政府考量的主要是不在逮捕現場的第三人。而資料加密技術的主張又更偏離主題了，因為政府所著眼的是一般手機之安全性功能，而非被告或其同夥在逮捕時隱匿或破壞證據之企圖。[327]警方不太可能剛好在受密碼保護手機未上鎖情形取得資料，因為多數手機只要藉著碰觸按鍵就能上鎖，或系統設定在短暫時間沒有使用後即自動上鎖。[328]關於遠端清除技術的威脅，警方可透過中斷該手機的連結網路功能之方式預防之，多數意見認為至少有二種簡單的方法。[329]第一，警方可以將手機關機或拆除電池。第二，若擔心資料加密或其他潛在的問題，警方可以將手機保持開機裝態並置入可隔絕無線電波的封閉空間，例如，用鋁箔製成的「法拉第袋」（Faraday bags）。事實上，許多執法機關已鼓勵使用這種裝置。[330]

縱使執法人員在特定個案中有具體的理由擔心證據滅失的潛在風險，仍有許多處理的方式。若情況顯示被告之手機可能立刻被遠端清除資料，警方可依「緊急情況」之立即無令狀搜索手機。[331]又或者警方剛好在未上鎖狀態扣押手機，警方可解除該手機自動上鎖的功能以防止該手機上鎖及相關資料被加密。[332]上開預防性措施可從最高法院在 *Illinois v. McArthur*, 531 U.S. 326 （2001）一案所提出之原則中推導出來，該案授權警方在等待取得令狀期間可以採取合理方式保全現場。[333]

附帶搜索此令狀原則之例外並非僅強調逮捕過程中可能危及的政府利益，也同時著眼於受逮捕人被警方拘捕過程中逐漸遞減的隱私利益。[334]但受逮捕人隱私利益遞減的事實並不代表完全沒有增修條文第 4 條之適用。並非僅因逮捕特定人而容許各種搜索，當與隱私相關的考量顯得重要時，儘管受逮捕人的隱私期待不斷遞減，搜索仍需要令狀。[335]

美國政府主張搜索手機內資料與搜索類似的物件實際並無法區別。多數意見批評這種說法就像是說騎馬與飛行到月球實際上並無區別一般荒謬。[336]現代手機所涉及之隱私考量遠超過搜索香菸盒、皮夾、手提包。主張檢視受逮捕人口袋相對於逮捕本身而言並未造成另外的隱私侵害或許在搜索物體時言之成理，但欲將此種論述適用到數位資料的脈絡就需另尋基礎。[337]從質或量來看，手機與其他可

---

[327] *Id.* at 13.
[328] *Id.*
[329] *Id.* at 14.
[330] *Id.*
[331] *Id.* at 15.
[332] *Id.*
[333] *Id.*
[334] *Id.*
[335] *Id.* at 16.
[336] *Id.* at 17.
[337] *Id.*

能為受逮捕人所持有的物件均有不同。許多手機實際上為具有通話功能的微型電腦，這些裝置可能具有照相機、影片播放器、通訊錄（rolodexes）、日曆、錄音機、圖書館、日記、相簿、電視、地圖或報紙等功能。[338]

現代手機最顯著的一個特徵就是強大的儲存能力，在手機問世之前，對於個人的搜索因限於物理實體部分，一般認為只構成有限的隱私侵害。但涉及到搜索手機時，對隱私的侵害就不限於物理層面。目前最暢銷的智慧型手機一般具有 16G 的儲存容量（可擴充到 64G），16G 的容量代表數百萬頁的文字、數千張的照片或數百部影片。即使售價低於 20 美元之最基本手機也具有相片、圖片訊息、文字簡訊、網路瀏覽計錄、行事曆、電話簿等功能。[339]手機強大的儲存功能使其隱私息息相關。第一，手機能將諸如地址、便條、處方、銀行交易明細、影片等各種不同的資訊結合而透露更多訊息。[340]第二，手機的儲存功能使得單一種類的資訊可能透露的訊息亦較過去來得多。個人的私生活可被數以千張標記日期、地點及描述的照片重新建構出來。第三，手機所含的資料可被回溯至購買時，或甚至更早。最後，手機有實體記錄不具有的普及性特徵。[341]

除了儲存的資料量較實體紀錄為多，某些資料就品質而言也與實體紀錄非常不同。例如，可上網的手機內所存留網路搜尋或瀏覽紀錄可透露個人的喜好或關注的事物。[342]手機內的位置資訊更可顯示個人曾去過的地方。顯示位置資訊歷程已為許多智慧型手機基本的特徵，該等功能可重新建構某人各時刻的移動軌跡，位置資訊不僅能顯示某人在某個城鎮，更可精確地顯示某人在特定建築物內。就如大法官 Sotomayor 在 *Jones* 案之協同意見書所述：「GPS 之監察可取得能顯示大量有關家庭、政治、專業、宗教及交往關係細節之個人在公開場合之移動軌跡。」[343]

裝置在手機內的應用程式軟體（或可稱作「apps」）可提供許多管理個人生活不同層面的工具。根據調查，使用者平均在智慧型手機內安裝 33 個 apps ，該等 apps 已足以透露使用者的生活片段。[344]過去司法實務認為搜索個人口袋與徹底搜索個人住家是完全不同的兩回事，然而，如果在口袋裡搜到的是 1 部手機，上述看法就不再適用了。[345]實際上，政府透過搜索手機所得到的資訊基本上遠較對房屋徹底搜索所得到的資訊還多。手機不僅以數位形式保存許多過去可在住處搜索到的敏感性紀錄，手機更包含大量不會在住處發現的私密資訊。[346]

---

338 *Id.*
339 *Id.* at 17-8.
340 *Id.* at 18.
341 *Id.* at 18-9.
342 *Id.* at 19.
343 *Id.* at 19-20.
344 *Id.* at 20.
345 *Id.*
346 *Id.* at 20-21.

進一步說明此處所牽涉到隱私利益，使用者在手機瀏覽的資訊實際上可能未儲存在手機裝置內。因此，將手機視為容器而主張可在附帶搜索時搜索其內容的說法可能有些牽強。此種對比於使用者透過輕敲螢幕而取得存在他處之資訊的脈絡下就完全無法適用了。[347]上開情形就是近來許多手機利用雲端計算所發揮的功能。雲端計算是指與網路連結的裝置可以顯示儲存在遠端伺服器的資料，而非顯示儲存在裝置內的資料。手機的使用者通常不清楚特定資訊儲存在手機內或雲端，一般來說兩者區別不大。[348]若允許警方附帶搜索儲存在雲端的資料，此種搜索就好像在嫌犯口袋內找到鑰匙，而主張警方可以持該鑰匙開門進入嫌犯的住處。當警方搜索手機內的資料時，一般不知道在逮捕時所檢視的資訊是儲存在手機內或是從雲端取得之資訊。[349]就此問題，政府所提出的解決方案並不明確。政府主張警方可在搜索前切斷該手機與網路的連結—此與多數意見在探討遠端清除技術之威脅時所提出之因應之道完全相同，或者政府主張由執法人員發展出處理雲端計算所引發相關問題的協定。搜索範圍可延伸至文件、財產等受逮捕人鄰近的物體以外的可能性，使此處的隱私利益遠超過 *Robinson* 案中的利益。[350]

政府欲將 *Gant* 案的標準引入，主張在執法人員合理相信手機內含有與逮捕之犯罪有關之證據時，即可對受逮捕人之手機進行無令狀搜索。[351]無論如何，*Gant* 案的標準適用在搜索手機之情形時，實際上等於沒有任何限制。在搜索汽車的情形，*Gant* 案通常保護的是過去犯罪之證據；然而，在搜索手機的脈絡，無論犯罪何時發生，都可合理地預期在手機中發現證明犯罪的證據。因此將 Gant 案的標準適用到搜索手機，實際上將給予警方不受節制的裁量權去隨意搜索私人財產。[352]政府雖提出將搜索手機的範圍限於警方合理地相信該等資訊與犯罪、受逮捕人的身分或警方的人身安全有關的標準，但多數意見認為在這樣的標準下實際上還是涵蓋了大量的資訊，而警方不可能總是能在事前知道會發現什麼樣的資訊。[353]

此外，多數意見也反駁政府以 *Smith* 案為依據，認為警方總是能搜索電話通話紀錄的主張。*Smith* 案認為使用撥號紀錄器去辨識特定電話用戶撥出的電話號碼並不需要令狀。[354]在 *Smith* 案中，法院認為使用撥號紀錄器完全不構成增修條文第 4 條之「搜索」。然而，本案中警方已對 Wurie 的手機進行搜索。再者，電話通話紀錄一般包括的資訊並非僅有電話號碼，也包括個人可能添加用以識別的資訊，例如在本案 Wurie 的事實中標記「我家」之訊息。[355]

---

347 *Id.* at 21.
348 *Id.*
349 *Id.*
350 *Id.* at 22.
351 *Id.*
352 *Id.* at 23.
353 *Id.* at 24.
354 *Id.*
355 *Id.*

多數意見並非認為手機內資訊可豁免於搜索，而是認為搜索手機通常需要事先取得令狀，即使在附隨於逮捕之附帶搜索情形也不例外。[356]即使附帶搜索此一令狀原則之例外並不適用於搜索手機，其他需經個案判斷的例外仍有可能正當化對特定手機的無令狀搜索。其中為人所熟知的緊急例外即可作為執法人員執行無令狀搜索的依據。[357] 手機並非僅是提供便利的科技產物。因其所包含及可能透露的資訊，手機涉及許多人們生活的隱私。現代科技雖讓人們能隨時持有此類資訊，但並不會因此使得這些資訊不受憲法隱私保障。多數意見認為警方搜索逮捕所附帶扣押之手機前，必須做一件很簡單的事—取得令狀。[358]

3. 部分協同意見書（大法官 Alito）

大法官 Alito 贊同對儲存在手機內之資料或透過手機可取得的資料執行合法之附帶搜索前原則上需取得令狀之結論。但特別說明以下二點：[359]第一，大法官 Alito 不認為附帶搜索的主要理由是基於保護員警安全及避免證據滅失的需求。首先，附帶搜索原則至少在增修條文第 4 條採行前 1 個 世紀前就已出現了。最高法院於 1914 年在 ***Weeks v . United States*** 案中認為增修條條文第 4 條並不影響附帶搜索之原則。***Weeks*** 案或其他習慣法的法源亦未表示附帶搜索主要基於保護警員安全或避免證據滅失的需求。[360]相對地，觀察 ***Weeks*** 案出現前的相關討論，附帶搜索主要是基於取得證據的需求。早期實務認為附帶搜索的基礎是源自國家具有控訴犯罪或合理相信為犯罪之人，並由正當法律程序決定有罪與否之利益，***Weeks*** 案援引的 2 個文獻也支持相同的看法。[361]最後，大法官 Alito 認為警員安全及證據保全需求的理由無法妥適解釋附帶搜索的範圍。根據最高法院長期以來的看法，在受逮捕人身上發現之書寫文件，可被執法人員檢視並作為審判中證據。然而，一旦這些文件不在受逮捕人身上，受逮捕人破壞這些文件的風險就不存在，讓這些文件處於不被檢視的狀態也不會危及逮捕警員的安全。[362]無令狀附帶搜索的主要理由為保護警員安危及證據保全的論述是源自 ***Chimel*** 案。但大法官 Alito 認為 ***Chimel*** 案的論據是很有問題的，因此讓該種論述影響本案就是一個錯誤。[363]

雖然如此，大法官 Alito 認為不應將數位時代前所採用的原則機械化地適用至搜索手機的情形。現在使用的許多手機具有儲存或取得大量資訊的功能，因這些資訊具有高度私密性，人們不會隨時攜帶記載該等資訊的紙本。[364]多數意見的

---

356 *Id.* at 25.
357 *Id.* at 26.
358 *Id.* at 28.
359 *Riley v. California*, 573 U.S._(2014), Alito,J,concurring, at 1.
360 *Id.* at 1-2.
361 *Id.* at 2.
362 *Id.* at 3-4.
363 *Id.* at 4.
364 *Id*.

看法傾向保護關於手機及其內資訊所涉及隱私利益，但這樣的看法將導致法律不安定的結果。例如，多數意見的見解傾向保護數位資訊甚於以紙本形式呈現的相同資訊。假設有 2 個嫌犯同時被逮捕，第 1 號嫌犯的口袋內有記載可證明犯罪之電話紀錄的電話費帳單，且有可證明其犯罪之照片存放在口袋內的皮夾內。第 2 號嫌犯的口袋則有 1 部手機，該電話內的電話紀錄及數張照片也可證明犯罪。根據判例法，警方可以扣押並檢視第 1 號嫌犯口袋內的電話費帳單及照片而不需取得令狀。但依多數意見的見解，警方不得無令狀搜索儲存在手機內的資訊。[365]雖然多數意見的取徑可能導致不安定的結果，但至少就附帶搜索手機一事提供執法人員清楚的原則，我們還需要時間讓法院從相關案件發展出更細緻的原則。[366]

第二點，若國會或州議會評估執法需求及手機使用人之利益後，根據資訊的型態或其他因素而做出合理的區別，大法官 Alito 將重新考慮本案所涉及的問題。[367]對電子監察的規範即是一個很好的例子。最高法院在 *Katz* 案宣示縱使沒有物理侵入，電子監察仍構成「搜索」後，美國國會即制定犯罪控制及街道安全法作為回應，自此之後，聯邦法規授權實施電子監察，但採行複雜的限制，因此主要規範電子監察的是聯邦法規而非 *Katz* 案的決定。[368]基於手機在現代生活中所扮演的角色，搜索手機，因涉及敏感資訊的隱私利益，大法官 Alito 認為法院的角色並不適合瞭解及判斷此一爭議，具有民意基礎的立法部門，較法院更適合判斷就本案所涉及之問題。[369]

（四）判決評析

在 *Katz* 案確立了「合理隱私期待」 亦為增修條文第 4 條所保護之對象後，*Knotts*、*Karo* 案仍僵化地以財產權的角度判斷合理隱私期待的侵害，造成「合理隱私期待」之概念無法發揮作用。[370]其實是否享有「合理隱私期待」與財產權之歸屬並無必然關係，就如同 *Katz* 案中保護公共電話亭內之私密通話不被刺探，Katz 並非公共電話亭之所有人，然一旦 Katz 透過付費、關門等舉動顯示主觀合理期待，任何人不得任意刺探其私密通話的內容。[371]Knotts 案及 Karo 案均表示政府在徵得所有人同意於化學容器交付買受人前安裝追蹤器於內並未侵害買受人之合理隱私期待。依此邏輯，警方在房東出租套房前，只要徵得房東同意，即可在出租套房裝置針孔攝影器監視房客之私密活動，也不會侵害房客的合理隱私期待。藉由上開案例即知該等論述之荒謬，顯然最高法院並未重視「合理隱私期待」之概念，仍僵化地詮釋合理隱私期待之範圍。

---

365 *Id.* at 4-5.
366 *Id.* at 5.
367 *Id.*
368 *Id.* at 5-6.
369 *Id.* at 6.
370 兩案均認為無令狀使用追蹤器在開放空間監察化學容器的移動軌跡並未侵害合理隱私期待，只有使用追蹤器獲知屋內資訊時才侵害合理隱私期待。
371 Katz v. United States, 389 U.S. 347, 352(1967).

在 *Jones* 案中，多數意見推翻 *Knott* 案及 *Karo* 案認為裝置使用追蹤器並未違反增修條文第 4 條之結論，強調物理侵入原則是最低限度之保障，「合理隱私期待」是較高標準之保障。[372]在該案明顯已有物理侵入之情形 ，多數意見雖未進一步從「合理隱私期待」面向探討「安裝」及「使用」GPS 可能對人民隱私造成之侵害，但協同意見已強調此議題的重要性。大法官 Sotomayor 對於所謂提供第三人資訊即喪失資訊隱私權之風險承擔理論提出強烈質疑，Alito 大法官更提出智慧型手機具有 GPS 功能，使用該等電話資料長時間使用追蹤監察個人已屬侵害合理隱私期待，將 *Katz* 案合理隱私期待的概念適用於數位時代下的科技監察，反映最高法院與時俱進的態度，本文贊同。

延續 Jones 案協同意見對於高科技監察的關注，最高法院在 *Riley* 案中詳盡地詮釋增修條文第 4 條在數位時代所扮演的角色。認為搜索手機內含資訊與附帶搜索保護警員安全及證據的目的並不相符，且清楚地意識到手機所包含的數位資訊與一般附帶搜索所取得的資料，不管在質或量上都有很大的差異。因此認為無令狀附帶搜索的範圍不及於（智慧型）手機。Colb 教授認為 *Riley* 案的決定有極大的重要性，相較於最高法院在 *Jones* 案中保守地從物理侵入角度認定 GPS 的安裝構成「搜索」，最高法院在 *Riley* 案不僅採取合理隱私期待的判斷標準，認為警方檢視手機之資訊構成「搜索」，更援引大法官 Sotomayor 在 *Jones* 案的協同意見說明現代手機之 GPS 功能可透露大量個人隱私，承認科技進步所伴隨的隱私侵害更甚過往。更重要的是，最高法院承認搜索手機對隱私的侵害，實際上超過搜索住宅，打破最高法院將住處視為隱私核心的迷思。[373]

本文認為 *Riley* 案為逮捕時如何搜索、扣押手機此一爭議性問題提供明確的標準—「僅得附帶扣押手機，無令狀不得搜索手機」。雖然這樣的原則側重受逮捕人隱私利益的保護，但實際上也減少執法之不確定性。從執法者的立場來看，因取得手機內大量的資訊可大大提升定罪的機率，警方自然有藉由附帶搜索取得更得資訊的誘因。然而，手機內包含許多與犯罪無關的個人隱私資訊，若在未經法院審核之情況下，概括容許警方藉由附帶搜索手機全面檢視個人生活全貌，無異於賦予警方不受節制的監視權力，與保全的執法利益相較，附帶搜索手機所犧牲的隱私利益更為巨大。*Riley* 案明白地將手機排除於附帶搜索範圍之外，警方為避免搜索手機所獲取之資訊因違法取證而被排除，勢必較過往勤於聲請令狀，不僅可減少因違法搜索造成證據排除的結果，藉由法院審查可否搜索手機內數位資訊，也可減少政府不當侵害人民隱私的情形。

附帶搜索為令狀原則之例外，本來就只有在保護員警安全及證據完整性之特別情形始有適用的餘地。數位時代所誕生的智慧型手機，因具有儲存及取得大量

---

[372] United States v. Jones, 132. S.Ct. 945(2010).

[373] Sherry F. Colb, *The Supreme Court Decides Riley v. California and Update the Fourth Amendment*, , available at : http://verdict.justia.com/2014/07/01/supreme-court-decides-riley-v-california-updates-fourth-amendment (latest vist: 2014.11.7)

資訊的能力，並可顯示使用者精確位置資訊、搜尋或瀏覽紀錄等敏感性資訊，誠如多數意見在 *Riley* 案所述，對該等科技產物搜索，可能較搜索住宅更具侵入性。*Riley* 案將手機排除在無令狀附帶搜索範圍之外，依此邏輯，警方在執行逮捕時在嫌犯身上或立即可控制範圍內所發現之智慧型手機或具有相類似功能之筆記型電腦、平板電腦等電子裝置，應先行扣押，待取得授權搜索該特定電子裝置之搜索票後始得檢視內容。除此之外，多數意見表示電話通話記錄可能顯示電話號碼以外之資訊，檢視手機內的通話記錄較 *Smith* 案中使用撥號記錄器取得電話號碼對隱私侵害更大。雖然沒有直接說明，但多數意見強調電話通話記錄可能透露識別身分之私密資訊，且多數意見論述過程完全未提及 *White* 案或 *Smith* 案所建立的「第三人原則」[374]，*Riley* 案暗示個人對電話通話紀錄具有合理隱私期待，也算是最高法院對於 Smith 案的修正。

至於大法官 Alito 在部分協同意見書主張關於新型態科技的規範，法院應尊重具有民意基礎的立法部門決定的說法，實際上就是 Kerr 教授所謂司法部門在涉及新型態科技的事項應順從立法部門判斷的理論。[375]這樣的論調乍聽之下貌似有理，但出自職司違憲審查的大法官口中，恐怕會讓人覺得是在迴避問題。Solove 教授指出這種論調具有以下謬誤：第一，聯邦法規對於資訊隱私的保護不如增修條文第 4 條來得全面。第二， 聯邦法規並未比增修條文第 4 條來得清楚。第三，立法部門並未較法院更能妥適處理科技變遷所帶來的問題。[376]本文也認為在權力分立之架構下，解釋憲法及審查立法為司法部門重要職責，縱使因科技進步、社會變遷而產生制憲者所未思考到的問題，若涉及合憲性的爭議，具有釋憲權限的司法部門仍應考量憲法原意、時代背景，就涉及爭議的立法或行政作為進行違憲審查。大法官 Alito 的主張等於賦予立法部門在涉及科技的特定事項具有違憲審查的豁免權，若果如此，政府只要透過立法，就可以藉此漏洞肆無忌憚地侵害人民基本權利。尊重立法的論調顯然違反違憲審查制度的精神。

最高法院在 *Kyllo* 案中認為政府使用熱顯像儀探查住宅內之溫度構成「搜索」，顯然跳脫物理侵入之觀點，而採取 *Katz* 案中合理隱私期待判斷標準之取徑，認為利用科技設備取得本需透過物理侵入始得獲取之資訊即屬侵犯合理隱私期待，應有增修條文第 4 條之適用。從合理隱私期待標準之適用來看，*Kyllo* 案固然值得讚許。但誠如大法官 Stevens 之不同意見，多數意見以增強人類感官能力之科技設備是否為「一般公眾使用」作為其是否侵害合理隱私期待之標準甚為不當，因是否侵害合理隱私期待與該項科技是否被普遍使用並無必然關連，「一般公眾使用」之標準不當地限制憲法增修條文第 4 條保障之範圍，更造成是否違憲取決於科技產品普遍性之荒謬結論。例如，當將來熱顯像儀已可輕易取得或者具相同功

---

[374] 手機用戶均知悉電信公司會取得通話紀錄，也應知道政府可從電信公司取得通話紀錄，依第三人原則，該等用戶對於個人電話理應欠缺「合理隱私期待」，政府取得該等資料，應不構成搜索。

[375] Orin. Kerr, *The Fourth Amendment and New Technologies: Constitution Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 806(2004).

[376] Solove, *supr*a note 156, at 165-67.

能之應用程式已可輕易透過智慧型手機免費或付費下載，依「一般公眾使用」之標準，政府使用熱顯像儀或具相同功能之智慧型手機應用程式掃描住宅就不構成「搜索」。

多數意見就何謂「一般公眾使用」亦未明白解釋，究竟是指公眾可輕易取得該項科技產物，[377]或指社會大眾已普遍如警方般使用該項科技，[378]法院究應如何適用此項「一般公眾使用」之標準，多數意見仍未明白說明。[379]Christopher Slobogin 教授觀察判例法歸納出 3 種「一般公眾使用」之定義：第 1 種定義，係指社會大眾均能取得該項科技產物。第 2 種定義稍微嚴格一些，係指社會大眾對於特定科技使用之頻率。第 3 種採最嚴格的定義，一般公眾將特定科技運用於特定目的。多數的科技設備，即使可被社會大眾取得，但大部分的民眾並不會如警方一般地使用該項科技設備。[380]因此，若將最狹義的定義運用於 *Kyllo* 案，需判斷政府使用熱顯像儀掃描 Kyllo 住宅外部時社會大眾是否普遍使用熱顯像儀去探測他人房屋內部之溫度分布情形。

本文推測，*Kyllo* 案多數意見提出「一般公眾使用」原則可能係欲詮釋「明知暴露」之概念，因為若某項科技已為社會大眾普遍使用，縱使該個人主觀上對其個人資訊具有隱私期待，個人若不特別採取防護措施，但因其明知暴露其資訊於公眾，其隱私期待也難被社會認為是合理的。就如同社會大眾慣於使用臉書（Facebook）、推特（Twitter）等社群網路去搜尋甚至是窺探他人之資訊，若嫌犯將其犯罪相關資訊不設限地張貼在其臉書上，使任何人都能觀覽該資訊，縱使警方從臉書上搜尋而獲知其犯罪行動，亦難認警方侵犯其合理隱私期待。當然社會是否普遍使用該項科技對於判斷嫌犯之客觀合理隱私期待有一定之影響，但是公眾是否普遍使用不必然與「明知暴露」有關連性，重點應在個案之脈絡下，個人是否欲保持其行為之私密性，而不欲他人知悉該等私密活動之內容，並採取適當的保護措施。因此，本文認為在公權力使用科技設備監察之情況下，無需考量該項科技是否為一般公眾普遍使用，直接判斷受監察人主觀上之合理隱私期待是否為社會所接受即可。若有明知暴露的情形，就可以推定欠缺客觀合理隱私期待而不受增修條文第 4 條之保護。若真的要適用 *Kyllo* 案中之「一般公眾使用」原則來限制合理隱私期待之範圍，亦應採取 Slobogin 教授所歸納之最狹義之定義，僅於一般社會公眾已普遍運用某項科技於特定目的，而認為受監察人之主觀隱私期待客觀上不為社會所接受，因此不受憲法增修條文第 4 條所保護。至於科技設備之精密性亦與合理隱私期待之判斷無直接關連，利用簡陋之器材或單憑人類感官能力也可能侵犯合理隱私期待。例如，使用反光鏡片窺探裙底風光，並不會因為反光鏡片非精密設備，而認未侵犯合理隱私期待。

三、數位時代下之隱私保障（心得及建議）

（一）物理侵入已非重點

[377] 例如任何人均得以便宜的價格在超市、賣場或從購物網站上購得熱顯像儀。

[378] 例如社會多數擁有熱顯像儀之人都習慣用該儀器掃描他人住宅外部，以獲知屋內溫度分布情形等資訊。

[379] CHRISTOPHER SLOBOGIN, PRIVACY AT RISK, THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT, 56-7, CHICAGO, UNIVERSITY OF CHICAGO PRESS (2007).

[380] *Id*. at 56-8.

美國最高法院於 1928 年在 *Olmstead v. United States*[381]一案中以物理侵入作為判斷竊聽是否違反增修條文第 4 條之標準，因此，若未涉及物理侵入，縱使以竊聽他人電話通訊內容，亦非增修條文第 4 條所保護之範疇。在 *Katz* 案中政府依循最高法院物理侵入原則之標準，以收聽及錄音設備在公共電話亭外截取公共電話通話內容獲知 Katz 涉及賭博罪之訊息。出乎意料之外，最高法院在 *Katz* 案推翻了「物理侵入」之判決先例，另外創設以「合理隱私期待」作為增修條文第 4 條之判斷標準。*Katz* 案中大法官 Harlan 的協同意見進一步說明「合理隱私期待」需具備之兩要件：第一，個人必須實際顯示其主觀上對隱私的期待；第二，個人所顯示之隱私期待須被社會認為是合理的。[382]

按理說，合理隱私期待原則應取代物理侵入作為增修條文第 4 條判斷之重點。然而，美國最高法院並未完全放棄物理侵入原則，甚至在適用增修條文第 4 條時還是著重財產權歸屬之判斷，例如在 *Karo* 案中，最高法院強調政府在特定容器裝置追蹤器之時點係在所有權移轉給被告之前，因而認該等行為不構成增修條文第 4 條之扣押；在 *Knotts* 案中，最高法院強調個人對其所有之財產具有合理隱私期待；甚至最高法院在 2010 年作成之 *Jones* 案，雖然認定警方使用全球定位系統（GPS）追蹤汽車移動軌跡構成增修條文第 4 條之搜索，但由大法官 Scalia 所主筆之多數意見，仍是以物理侵入原則為基調。

然而在數位時代下，公權力對人民隱私之窺探不再需要仰賴物理侵入即可達成，例如在電信機房對於特定手機門號上線監聽、透過手機定位得知特定手機持有人所在位置、透過紅外線熱顯示儀得知嫌犯是否在室內栽植大麻。若拘泥於物理侵入，可能會導致對合理隱私期待的狹隘解釋，甚至認為合理隱私期待僅為財產權之附帶利益。我們應思考的是，40 多年前的 *Katz* 案已意識到個人在公共場所仍得享有秘密通訊之合理隱私期待。誠如 *Katz* 案多數意見所述，增修條文第 4 條所保障的是個人，而非地方。判斷新型態監察手段是否侵害增修條文第 4 條所保障之權利時，直接判斷是否侵害合理隱私期待即可，毋須迂迴地先判斷是否有物理侵入。

（二）再思第三人原則

Solove 教授認為最高法院將「第三人原則」與「風險承擔原則」（assumption of risk doctrine）劃上等號其實是一種錯誤的推論。該推論過程如下：若你承擔了朋友會背叛你的風險，同樣地你也承擔了擁有資訊的第三人會背叛你的風險。[383]但問題是此兩種情況並不具可相提並論性，因為「朋友」通常是自願地洩漏秘密，而銀行或電話公司等「第三人」實際上欲保護客戶資訊之秘密性，但很多時候遭

[381] Olmstead v. United States, 277 U.S. 438(1928).
[382] Katz v. United States, 389 U.S. 347, 361(1967).
[383] Solove, *supra* note 148, at 108.

政府強迫提供資訊。[384]第三人原則無法清楚說明機密性及承諾這兩個概念。當銀行、醫療機構、會計師或任何公司組織承諾履行保密義務，客戶可以合理期待對方會信守承諾，違反保密義務可能會帶來民事責任。然而，根據第三人原則，甚至書面契約也無法說明客戶具有合理隱私期待。承諾及契約為現代市民社會的基礎，若人們無法依賴承諾及契約，商業及貿易將被迫停止。然而，談到隱私，最高法院卻認為承諾跟契約一點都不重要。[385]

第三人原則另一個問題在於最高法院無法說明其適用範圍。例如，第三人原則是否適用於醫療記錄？最高法院是否會認為因病患提供醫療資訊給醫師所以對個人醫療紀錄不具合理隱私期待？[386] 美國知名刑事訴訟法學者 Orin Kerr 教授支持「第三人原則」，Kerr 教授認為在資訊時代，罪犯可以使用電腦等現代科技以強化其犯罪及隱匿之能力，第三人原則正好可以平衡罪犯與警方之間之關係。[387]然而，Kerr 的論點忽略科技雖然有助於罪犯，但同樣提供政府更多更強的能力，「第三人原則」給予政府權力取得無辜人民之個人資料。縱使精通電腦的罪犯利用科技隱匿其犯罪行為，並不意謂我們需放棄所有增修條文第 4 條之保護。[388]

1967 年美國最高法院在 *Katz* 案中提出「合理隱私期待」之概念，揚棄根深蒂固的「物理侵入原則」，肯認不具物理侵入電子監聽侵害合理隱私期待，構成增修條文第 4 條之「搜索」，為增修條文第 4 條開啟嶄新的一頁。然而，最高法院在 *Miller* 案及 *Smith* 案中所發展出之「第三人原則」，不當地限制合理隱私期待的範圍，錯誤地引用「風險承擔原則」的概念，造成人民一旦提供個人資訊即喪失合理隱私期待的荒謬結果。鑑於尊重判決先例原則，第三人原則在實務上限制增修條文第 4 條保障隱私之功能，使得最高法院很長一段時間在涉及搜索、扣押的案件中保守地詮釋增修條文第 4 條。此外，第三人原則也提供政府規避令狀原則絕佳的理由。由於向銀行、電話公司等第三人取得資料都不會侵害合理隱私期待，政府可在不具相當理由之情況獲取該等資料，這可能也是造成布希政府以反恐為名建立大型資料庫蒐集、分析電話資料的其中一個原因。總此以言，第三人原則概念的提出就是一個錯誤，這樣的錯誤還持續地危害美國人民的隱私，在史諾登事件爆發後，更清楚顯示第三人原則的荒謬。綜此以言，理據錯誤的第三人原則破壞合理隱私期待之概念，更造成侵害人民隱私的結果，在數位時代的今日，應沒有再適用的餘地。Sotomayor 大法官在 *Jones* 案的協同意見已倡議重新檢討第三人原則，期盼美國最高法院在不久的將來揚棄第三人原則，如同其在 *Katz* 案中推翻物理侵入原則一般，讓人民合理隱私期待能獲得真正的保障。

---

384 *Id.*
385 *Id.* at 108-9.
386 *Id.* at 109.
387 Orin S Kerr, *The Case for Third- Party Doctrine*, 107 MICH. L. REV. 561, 573-77(2009).
388 Solove, *supra* note 156, at 109.

（三）數位時代下之合理隱私期待

科技不斷發展，不僅強化犯罪者隱匿不法行為之能力，同時也提升執法機關偵查犯罪之能力，追蹤器、GPS、紅外線熱顯像儀、網路監察、資料探勘等科技之運用，讓警方不需透過傳統的人力跟監、物理侵入等方式，亦得迅速掌握嫌犯行蹤及犯罪事證，但也對隱私造成極大的威脅。 雖然美國最高法院在 *Katz* 案建構合理隱私期待之標準，但由於「風險承擔原則」、「第三人原則」、「肉眼例外原則」等概念的不當適用，造成許多侵害人民隱私之公權力運用，可免於增修條文第 4 條之司法審查。司法實務所創造隱私保障之諸多例外，反而侵蝕增修條文第 4 條所要保障之隱私，進而正當化政府監察人民之種種行為。諷刺的是，美國政府在 911 事件發生後所實施無令狀電子監聽、建置大型電話資料庫、蒐集交易資料、資料探勘等監察措施，讓一向重視隱私之美國人在政府之監視下無所遁形，繼 2005 年紐約時報披露布希政府秘密進行無令狀監聽計畫，前美國安局雇員史諾登於 2013 年更揭露美國政府透過電信公司大規模個人電話資料，顯示美國政府透過科技輔助設備更變本加厲地侵害個人隱私。

在科技輔助設備推陳出新之時代中，判斷公權力利用科技輔助設備之行為是否構成「搜索」顯較已往來得困難與複雜，Slobogin 教授認為美國最高法院在判斷警方運用科技之行為是否構成搜索時，並不是僅以該項科技是否為公眾普遍使用為唯一考量，除 *Kyllo* 案所提及之「公眾普遍使用原則」外，法院還會考量：1. 受觀察處所之性質。2. 用以強化隱私之措施。3. 監察措施對私人財產物理侵入之程度。4. 被觀察對象或活動之性質。5. 該項科技提升人類感官能力之程度。6. 該項監察不必要地蔓延、侵入或引起混亂的程度（例如，因為警方未能採取將侵害最小化之手段）等因素而為綜合判斷。[389]我國憲法雖無類似美國憲法增修條文第 4 條之規定，但刑事訴訟法、通訊保障及監察法中有關搜索、扣押及通訊監察之程序規定，基本上是參考美國刑事訴訟法制採用「相當理由」作為發動強制處分之實質理由，許多程序規定更是參考美國憲法增修條文第 4 條相關判例法，因此美國判例法判斷警方運用科技輔助設備是否構成搜索所考量之因素亦值得我國司法實務參考。本文認為我國法院在判斷公權力使用科技輔助設備是否構成「搜索」或「通訊監察」，可採用美國法之「合理隱私期待」為判斷標準，並綜合考量上開因素，以準確界定科技時代下合理隱私期待之範圍。

四、簡評 2014 年通訊保障及監察法新增之通信紀錄調取制度

（一）「通信記錄」與「通信使用者資料」受同等保護？

2014 年 1 月修正之通保法將通信紀錄及通信使用者資料納入規範，依該法第 3 條之 1，「通信紀錄」係指電信使用人使用電信服務後，電信系統所產生之發送

[389] Slobogin , *supra* note 379, at 59.

方、接收方之電信號碼、通信時間、使用長度、位址、服務型態、信箱或位置資訊等紀錄;「通信使用者資料」係指電信使用者姓名或名稱、身分證明文件字號、地址、電信號碼及申請各項電信服務所填列之資料。[390]本次修法新增調取通信紀錄需經法院核發調取票[391]、警方聲請調取通信紀錄應經檢察官許可等制度。[392]對於偵查實務影響甚鉅,因為偵查機關除偵辦最輕本刑 10 年以上重罪及強盜、搶奪等罪外,或有急迫情形不及事先聲請外,均需經法院同意後始得調取通信資料。對於重視偵辦時效性的偵查機關而言,的確可能影響偵辦案件的速度。法務部也就通保法有關通信紀錄制度的新增表示意見。偵辦最重本刑有期徒刑 3 年以下之許多犯罪[393],縱使當事人向檢察官聲請調取通信記錄,亦受限於新法之規定,無法調取通信紀錄,無法落實真實發現,而對當事人不公平,可能對社會治安產生衝擊。[394]但就通信紀錄中之通信號碼、位址、位置資訊等資料可能透露使用者之交往關係、生活細節,通信使用者資料可能洩漏個人資料,偵查機關調取該等資料故能蒐集到豐富的資訊,但鑑於偵查機關之主要任務在於打擊犯罪,若由立於公正中立地位之法院審核調取通信資料、通信使用者資料與偵辦犯罪之關連性及調取之必要性,應較能保障人民隱私,亦符正當法律程序。因此本次修法,引進由法院核發調取票之「令狀原則」,值得肯定。

有疑問的是,新修正通訊保障及監察法第 11 條之 1 第 1 項就「通信紀錄」與「通訊使用者資料」提供相等程度之隱私保障。因此,檢察官在偵辦最重本刑 3 年以上之罪時,不論是欲調取「通信記錄」或「通訊使用者資料」,均須向法院聲請。新法第 3 條之 1 所定義之「通信記錄」包括電信號碼、通信時間、使用長度、位址、服務型態、信箱或位址資訊等,依美國撥號紀錄器法,政府取得該等資訊需證明該等資訊與進行中之刑事調查有關,並經法院核准,始得取得該等資訊。至於「通訊使用者資料」係指電信使用者姓名或名稱、身分證明文件字號、地址、電信號碼及申請各項電信服務所填列之資料,性質上類似我國個人資料保障法中

---

390 通訊保障及監察法第 3 條之 1:「本法所稱通信紀錄者,謂電信使用人使用電信服務後,電信系統所產生之發送方、接收方之電信號碼、通信時間、使用長度、位址、服務型態、信箱或位置資訊等紀錄。(第 1 項)本法所稱之通訊使用者資料,謂電信使用者姓名或名稱、身分證明文件字號、地址、電信號碼及申請各項電信服務所填列之資料。(第 2 項)」

391 2014 年 1 月修正之通訊保障及監察法第 11 條之 1 第 1 項:「檢察官偵查最重本刑 3 年以上有期徒刑之罪,有事實足認通信紀錄及通信使用者資料於本案之偵查有必要性及關連性時,除有急迫情形不及事先聲請者外,應以書面聲請該管法院核發調取票。聲請書之應記載事項,準用前條第一項之規定。」

392 2014 年 1 月修正之通訊保障及監察法第 11 條之 1 第 2 項:「司法警察官因調查犯罪嫌疑人犯罪情形及蒐集證據,認有調取通信紀錄之必要時,得依前項規定,報請檢察官許可後,向該管法院聲請核發調取票。」

393 例如最重本刑為 1 年之刑法第 306 條第 1 項之侵入住居罪、最重本刑為 2 年之刑法第 307 條之非法搜索罪、最重本刑為罰金之刑法第 337 條侵占遺失物罪、最重本刑為 1 年之刑法第 344 條重利罪。這些犯罪如果被告否認犯行,並提出不在場證明,若無法調取通信記錄中之位置資訊此類客觀證據以供查證,偵辦之難度將大大提高。

394 打擊犯罪之手被束縛,法務部新聞稿,2014 年 1 月 14 日。

所規範之「個人資料」，[395]我國個人資料保護法未規定公務機關蒐集、處理、使用該等個人資料需經法院審核，只要公務機關蒐集、處理該等個人資料在法定職務範圍內即可，[396]毋庸另行取得法院令狀。美國規範個人資料之聯邦隱私法（Privacy Act）亦規定聯邦政府官員在提出書面聲請主張該紀錄為其履行職務所需。[397]此次通訊保障監察法將規範偵查機關調取屬於「個人資料」之通訊使用者資料需依令狀原則，此種規範保護程度更甚於我國個人資料保護法及美國聯邦隱私法，然而取得個人資料保護法中認為應予較高程度保障有關醫療、基因、性生活、健康檢查及犯罪前科之敏感性個人資料均無須法院事先審核，何以獨厚通訊使用者之資料？如此一來，偵查機關為聯繫開庭事宜而查詢證人、被告之電話號碼亦須由檢察官向法院聲請通信使用者調取票，對於偵查職務之執行，帶來很大的困擾。況且，新法第 11 條之 1 第 2 項僅要求司法警察官調取「通信紀錄」時，需取得檢察官許可後向法院聲請核發調取票，就警方蒐集「通訊使用者」資料部分因通訊保障及監察法並無規範，即回到個人資料保護法直接向電信公司申請即可。此造成檢察官調取通信使用者資料需向法院聲請，警方調取相同的資料，卻不需向法院聲請之奇怪現象。如此一來，第 11 條之 1 第 1 項有關「通訊使用者資料」規範形同虛設，蓋檢察官在我國屬於具有指揮監督權之偵查主體，若欲取得不包含通信紀錄的通訊使用者資料，檢察官可指揮承辦之員警以警方名義向電信公司調取，何需費工地向法院聲請核准調取票呢？此外，新法在第 11 條之 1 第 4 項規定檢察官、司法警察官在偵辦最輕本刑 10 年以上有期徒刑之罪、強盜、搶奪、詐欺、恐嚇、擄人勒贖，及違反人口販運防制法、槍砲彈藥刀械管制條例、懲治走私條例、毒品危害防制條例、組織犯罪條例等罪時，得由檢察官依職權或警方經檢察官同意後，調取「通信紀錄」，並未包含「通信使用者資料」[398]，綜上，比對新法第 11 條之 1 第 1 項（檢察官向法院聲請調取通信紀錄、通信使用者資料）、第 2 項（警方經檢察官許可後向法院聲請調取通信紀錄）及第 4 項（特定重罪由檢察官決定是否調取通信紀錄），僅第 1 項包括通信使用者資料，或許為立法協商過程中誤植「通信使用者資料」一詞。再者，就通信紀錄與通信使用者資料之性質來看，通信使用者資料為使用者個人資料，公務機關在執行法定職務之必要範圍內，通常可依個人資料保護法之規定，蒐集、處理及利用該等資料。通信紀錄則可透露使用者交往關係、生活細節及所在位置等重要資訊，兩者隱私保障之強度自應有所不同。單獨將檢察官調取通信使用者資料列入通訊保障及監察法

[395] 個人資料保護法第 2 條第 1 款：「指自然人之姓名、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、病歷、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。」

[396] 個人資料保護法第 15 條第 1 款：「公務機關對個人資料之蒐集或處理，除第 6 條第 1 項所規定資料外，應有特定目的，並符合下列情形之一者：一、執行法定職務必要範圍內。」。

[397] 18 U.S.C§522a(b) (1)No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties

[398] 2014 年 1 月修正之通訊保障及監察法第 11 條之 1 第 4 項。

規範，對於警方調取通信使用者資料反未設限，不僅與該條檢察官對於警方聲請調取通信紀錄有審核之權之思維背道而馳，實際上因警方可自行蒐集通訊使用者資料，無法發揮規範之作用。因此，是否有必要將「通信使用者資料」一併納入通訊保障及監察法規範，值得深思。

（二）「重罪原則」是否合適？

此次通訊保障監察法之修正，最重要的莫過於納入調取通信紀錄之程序規定，並引進由法院審核聲請之「令狀原則」。值得一提的是新法第 11 條之 1 第 1 項及第 4 項採取「重罪原則」，限制偵辦特定刑度以上或法律列舉之犯罪始得調取通信紀錄。乍看之下，對於人民隱私權之保障固然大大提升，但重罪原則通常係在某種強制處分對基本權侵害特別嚴重的情形，為了限制該強制處分之使用，而限制偵查機關在偵辦特定重罪時，始能運用。然而，限制偵查機關在重罪或特定犯罪始得使用某種強制處分，等於限制偵查機關偵辦其他犯罪之偵查手段。公權力對基本權干預強弱之規範，較常見是規範不同程度證明事實之舉證責任。例如，傳喚被告需具有「犯罪嫌疑及傳喚之必要性」，實施搜索需具備「相當理由」，檢察官起訴被告需「足認被告有犯罪嫌疑」，需檢察官「證明被告犯罪」，法院始得為有罪判決。是以，立法部門在規範基本權干預行為之要件時，應審慎考量該等強制處分對於基本權之侵害性，而對國家賦予不同程度舉證責任之要求，重罪原則之正當化基礎較為薄弱，應審慎為之。

我國法就強制處分適用重罪原則之情形，並不常見。首先，通訊保障及監察法規定實施通訊監察需符合重罪原則。通訊保障及監察法第 5 條 [399]就限定僅在最輕本刑 3 年以上有期徒刑之重罪，或其他列舉之犯罪，始能由檢察官職權聲請或

[399] 通訊保障及監察法第 5 條：「有事實足認被告或犯罪嫌疑人有下列各款罪嫌之一，並危害國家安全、經濟秩序或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者，得發通訊監察書。1. 最輕本刑為 3 年以上有期徒刑之罪。2. 刑法第 100 條第 2 項之預備內亂罪、第 101 條第 2 項之預備暴動內亂罪或第 106 條第 3 項、第 109 條第 1 項、第 3 項、第 4 項、第 121 條第 1 項、第 122 條第 3 項、第 131 條第 1 項、第 142 條、第 143 條第 1 項、第 144 條、第 145 條、第 201 條之 1、第 256 條第 1 項、第 3 項、第 257 條第 1 項、第 4 項、第 298 條第 2 項、第 300 條、第 339 條、第 339 條之 3 或第 346 條之罪。3. 貪污治罪條例第 11 條第 1 項、第 4 項關於違背職務行為之行賄罪。4、懲治走私條例第 2 條第 1 項、第 2 項或第 3 條之罪。5. 藥事法第 82 條第 1 項、第 4 項或第 83 條第 1 項、第 4 項之罪。6. 證券交易法第 173 條第 1 項之罪。7. 期貨交易法第 112 條或第 113 條第 1 項、第 2 項之罪。8. 槍砲彈藥刀械管制條例第 12 條第 1 項、第 2 項、第 4 項、第 5 項或第 13 條第 2 項、第 4 項、第 5 項之罪。9. 公職人員選舉罷免法第 102 條第 1 項第 1 款之罪。10. 農會法第 47 條之 1 或第 47 條之 2 之罪。11. 漁會法第 50 條之 1 或第 50 條之 2 之罪。12. 兒童及少年性交易防制條例第 23 條第 1 項、第 3 項、第 4 項、第 5 項之罪。13. 洗錢防制法第 11 條第 1 項至第 3 項之罪。14. 組織犯罪防制條例第 3 條第 1 項後段、第 2 項後段、第 6 條或第 11 條第 3 項之罪。15. 陸海空軍刑法第 14 條第 2 項、第 17 條第 3 項、第 18 條第 3 項、第 19 條第 3 項、第 20 條第 5 項、第 22 條第 4 項、第 23 條第 3 項、第 24 條第 2 項、第 4 項、第 58 條第 5 項、第 63 條第 1 項之罪。16. 營業秘密法第 13 條之 2 第 1 項、第 2 項之罪。17. 森林法第 52 條第 1 項、第 2 項之罪。18. 廢棄物清理法第 46 條之罪。

依司法警察機關聲請向法院聲請核發通訊監察書，為適用重罪原則之適例。除了實施通訊監察及 103 年 1 月修正通訊保障及監察法修法新增之調取通信紀錄及通信使用者資料外，難見我國刑事訴訟法制有其他重罪原則之情形。唯一比較接近的是我國刑事訴訟法有關羈押之規定，然與通訊保障監察法中限制特定重罪始得實施通訊監察或調取通信紀錄之規範方式不同，刑事訴訟法第 101 條[400]僅將特定重罪列為羈押理由之一，並未將符合特定重罪列為羈押之前提要件。[401]因此，縱使被告所涉犯並非死刑、無期徒刑或最輕本刑為 5 年以上有期徒刑之罪，但個案若具有逃亡或勾串共犯證人等其他羈押理由，且具有羈押之必要性，法院仍可羈押被告。值得探討的是，大法官釋字第 665 號理由書表示，若將重罪當作許可羈押之唯一要件，不論是否犯罪嫌疑重大，亦不考量有無逃亡或滅證之虞而有羈押之必要，或有無不得羈押之情形，則該款規定即有牴觸無罪推定原則、武器平等原則或過度限制刑事被告之充分防禦權而違反比例原則之虞。[402]

觀諸通訊監察與調取通信紀錄，前者是涉及通訊內容之監聽、監看，至於後者是則是與通訊內容無關之電信號碼、通信時間等資料，雖然兩者與秘密通訊之自由均有關連，但對隱私侵害之強弱迥然有別。通訊監察所得之通訊內容為內容資訊，通信紀錄或通訊使用者資料則屬不涉及內容之信封資訊，[403]前述美國電子隱私保障法也將對涉及通訊內容之監聽、儲存通訊給予較強之保障，規範通信紀錄之撥號紀錄器法，因規範對象不涉及通訊內容本質，對隱私侵害程度最低，政府僅需證明與進行中之犯罪調查有關即可。再者，依目前美國最高法院實務意見，電話使用者對於撥出的電話號碼並無合理隱私期待，[404]該等資料甚至不受美國憲法增修條文第 4 條所保障。本文雖不認同 *Smith* 案以第三人原則作為使用者對撥打之電話號碼無合理隱私期待之論述，但不可否認的是，相較於涉及通訊內容之監聽，通信紀錄因無法顯示通訊內容，也無法確認實際通訊使用者，對於隱私侵害之程度，自不該與通訊監察一般相提並論。我國通訊保障及監察法新增通信紀錄調取制度，採取令狀原則，固值肯定。但就調取通信紀錄適用重罪原則，似乎過度限制調取通信紀錄之範圍，且侵害基本權程度顯然強於調取通信紀錄如搜索、羈押等強制處分，亦未適用重罪原則，新法就調取通信紀錄卻採重罪原則，顯然輕重失衡。

---

400 刑事訴訟法第 101 條：「被告經法官訊問後，認為犯罪嫌疑重大，而有左列情形之一，非予羈押，顯難進行追訴、審判或執行者，得羈押之：1. 逃亡或有事實足認為有逃亡之虞者。2. 有事實足認為有湮滅、偽造、變造證據或勾串共犯或證人之虞者。3. 所犯為死刑、無期徒刑或最輕本刑為 5 年以上有期徒刑之罪者（第 1 項）。法官為前項之訊問時，檢察官得到場陳述聲請羈押之理由及提出必要之證據（第 2 項）。第 1 項各款所依據之事實，應告知被告及其辯護人，並記載於筆錄（第 3 項）。」

401 關於重罪羈押作為羈押理由是否侵害憲法保障之身體自由及訴訟權，請參照大法官釋字第 665 號解釋。

402 大法官釋字第 665 號解釋理由書。

403 關於內容資訊與信封資訊之區分，See Kerr, *Supra* note 159.

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

（三）半套式法官保留：急迫例外及特定重罪例外

新修正之通訊保障及監察法就通信紀錄之調取雖引進法官保留原則，但亦有規定不需適用令狀原則之例外情形。該法第 11 條之 1 第 1 項[405]規定「急迫情形不及事先聲請」，檢察官得不經法院核發調取票即調取通信紀錄，但在急迫原因消滅後，應向法院補行聲請調取票。[406]另外，在同條第 4 項更直接規定檢警在偵辦最輕本刑 10 年以上有期徒刑之罪、強盜、搶奪、詐欺、恐嚇、擄人勒贖，及違反人口販運防制法、槍砲彈藥刀械管制條例、懲治走私條例、毒品危害防制條例、組織犯罪條例等罪時，可以不需向法院聲請調取票，由檢察官決定是否調取通信紀錄。

首先，在急迫情形例外之情況，新法並未明確說明需具備何種事由，且需具備急迫情形即可不需事先書面向法院聲請。但因事後還是要向法院補行聲請調取票，由法院審查調取通信紀錄及通信使用者資料之合法性， 若檢察官調取通信紀錄之程序事後被法院認定不合法，該等通信紀錄自不得作為定罪之證據使用。比較令人訝異的是，新法規定檢警在偵辦最輕本刑 10 年以上重罪或其他列舉之犯罪，可直接跳過法院決定之令狀原則，直接由檢察官決定是否調取通信紀錄。何以在特定重罪之情形就沒有適用令狀原則之必要？偵辦重大犯罪不是更應符合正當法律程序嗎？難道罪名的輕重或涉及的犯罪種類，會影響強制處分決定作成之正當性？新法就最重本刑 3 年以上有期徒刑之罪要求令狀原則，未經法官同意，原則不得調取通信紀錄。然而，在最輕本刑 10 年以上之重罪及其他犯罪之情形，卻說不需法院審核，檢察官決定即可。依此立法之邏輯，重罪原則可以凌駕在令狀原則之上，適用重罪原則是為保障人民基本權而對公權力之特別限制，新法在第 11 條之 1 第 4 項卻規定特定重罪可免除令狀原則之正當法律程序，反而對公權力侵害基本權大開綠燈。

本文認為，鑑於我國憲法秘密通訊自由之保障亦包括通信紀錄所涵蓋之資料，調取通信紀錄應採行法院審核之令狀原則較能保障人民秘密通訊之自由，並符合正當法律程序。然而，重罪原則僅在公權力侵害基本權特別嚴重之情形才需例外適用。而調取通信紀錄相較於搜索、扣押、通訊監察、羈押被告，顯為侵害程度較低之偵查手段。不論何種犯罪，調取通信紀錄都可能是必要、有關連的證據調查方法，也是一種講求客觀證據之科學辦案方法，就所有犯罪調取通信紀錄之聲請，統一由法院審核是否符合法定要件即可，重罪原則之規定，反而是畫蛇添足之舉，更破壞了令狀原則之精神。

[405] 2014 年 1 月修正通訊保障及監察法第 11 條之 1 第 1 項。
[406] 2014 年 1 月修正通訊保障及監察法第 11 條之 1 第 5 項。

肆、結論（心得及建議）

美國在經歷 911 事件後，為了有效打擊恐怖主義，採行電子郵件監察、電話監聽、建立大型資料庫、資料探勘等各種新型態監察手段。科技的發展固然提升政府蒐集反恐情資、偵查犯罪的能力，但也提升公權力不當侵害個人隱私的風險。美國政府無令狀實施通訊監察、大量蒐集電話資料即為適例。美國最高法院在 40 多年前就在 *Katz* 案宣示電子監聽侵害合理隱私期待，構成為憲法增修條文第 4 條之「搜索」。隨著科技不斷進步，各種新型態監察手段不斷推陳出新，如何詮釋增修條文第 4 條的「搜索」成為執法部門及法院的挑戰。*Kyllo* 案中將警方使用熱顯像儀探測住宅內部溫度分布情形的偵查作為，*Jones* 案中將政府安裝及使用 GPS 長時間追蹤汽車在開放空間的移動軌跡的監察行為，以及 *Riley* 案中警方逮捕嫌犯後檢視智慧型手機內的舉動，最高法院都認為構成增修條文第 4 條之「搜索」，必須具「相當理由」並取得法院核發之搜索令狀後始得為之。

美國最高法院與時俱進將增修條文第4條的保障範圍延伸到各種新型態通訊監察工具，該國聯邦法規也對通訊監察、儲存中資料及通信紀錄等各種監察手段提供更進一步的規範。我國雖無類似美國憲法增修條文第4條之規定。但大法官釋字第631號釋記載：「憲法第12條規定：『人民有秘密通訊之自由。』旨在確保人民就通訊之有無、對象、時間、方式及內容等事項，有不受國家及他人任意侵擾之權利。國家採取限制手段時，除應有法律依據外，限制之要件應具體、明確，不得逾越必要之範圍，所踐行之程序並應合理、正當，方符憲法保護人民秘密通訊自由之意旨。因此公權力實施通訊監察、調取通信紀錄等監察手段時均應遵行通保法之程序，始與憲法此保障秘密通訊之精神相符。

不論監察的對象為電話、電子郵件、通訊應用程式之視訊通話、鍵盤敲擊紀錄，偵查機關在執行前均須精準定性偵查手段究為「通訊監察」或為「調取通信紀錄」，並檢驗個案證據是否達通保法規定之門檻，取得法院核發之「通訊監察書」或「通信紀錄調取票」後，再予執行，如此一來，不僅妥適保障人民秘密通訊自由及隱私權，也強調執法機關專業、謹慎的態度。美國憲法增修條文第 4條在刑事訴訟程序中扮演重要角色，從該規定所延伸出的法院實務判決、聯邦通訊監察法制均值得我國參考。我國通保法於2014年1月新增檢警調取通信紀錄應經法院核發調取票之制度，採行令狀原則，與美國撥號紀錄器法規範應經法院命令之規定類似，也反應我國政府保障人民秘密通訊自由及隱私權的態度。然而，合理隱私期待的概念會隨著社會變遷、科技進步而不斷調整，法律制度更不可能臻於完美，最後總需要在自由及安全間進行利益衡量。以美國最高法院能隨著時代進步將增修條文第4條的保護延伸到GPS、搜索智慧型手機為借鏡，我國司法實務應將憲法保障之秘密通訊自由及隱私權落實到各種通訊監察之脈絡下。