論著
© 臺大法學論叢 NTU Law Journal
第 53 卷第 3 期/Vol.53, No.3 (09. 2024)

國家植入間諜程式遠端搜索之法制*

溫祖德**

<摘要>

科技進步使得犯罪者利用電腦等科技裝置在暗網中犯罪，同時利用網路科技隱身於虛擬世界，隱藏自己身分及所在位置，造成偵查困境，因此，美國在 2016 年於聯邦刑事訴訟規則增訂遠端搜索，增訂目的在於解決偵查機關不知電腦資訊設備或媒介硬體所在位置，妨礙政府偵查特定目標對象或目標電腦資訊設備之位置，以免聯邦法院產生核發搜索票之困難，因而承認（跨轄區）遠端搜索之需求及對於多個管轄區域內多個電腦設備，進行遠端搜索之法制需要。

為能妥善解決犯罪匿名化、暗網化衍生之偵查困境，參酌先進國家立法趨勢均已承認遠端搜索或線上搜索，本文從美國法觀點，深入分析美國聯邦刑事訴訟規則關於核發遠端搜索令狀，以搜尋電腦資訊設備（含設備所在位置、資訊設備內容性資訊）之法制。藉由分析美國國家植入間諜程式遠端搜索之科技及執法發展、司法實務對於國家植入間諜程式遠端搜索之憲法定位及闡述增訂遠端搜索條款之新法及規範評析。最後，本文本於我國憲法誡命

* 作者衷心感謝匿名審稿委員惠賜之寶貴意見，使作者得以檢視及強化不足之處，作者受益匪淺，惟文責仍由作者自負之。本文為國家科學及技術委員會補助專題研究計畫（計畫編號：MOST 112-2410-H-008-007-）研究成果及研究計畫（計畫編號：MOST 113-2410-H-008 -044 -MY2）研究成果之一部分，本文特在此感謝與支持。

** 中央大學法律及政府研究所專任教授，美國伊利諾大學香檳分校法學博士（J.S.D.）。E-mail: wentzute@cc.ncu.edu.tw

・投稿日：02/13/2023；接受刊登日：12/27/2023。
・責任校對：江昱麟、陳怡君、黃品樺。
・DOI:10.6199/NTULJ.202409_53(3).0005

之法律保留原則，認為應由立法機關明定授權國家植入間諜程式遠端搜索之詳細規範架構，提供未來可能之規範建議，在兼顧人權保障之前提下，同時促進執法利益。

關鍵詞：遠端搜索、暗網犯罪、國家植入間諜程式、令狀特定性要件、殭屍病毒

♦目 次♦

壹、前 言

隨著科技進步，整個世界及社會正處於物聯網模式的生活，在非常有限的成本下，人們有能力透過一個簡單的點擊動作即連結網路任何設備、行動電話、家電用品、穿戴裝置，甚至是飛機引擎。當代犯罪者利用電腦、行動裝置、網路科技，從事買賣毒品、爆炸物品、買賣偽變造護照及兒童色情相關產品照片等各種犯罪行為，犯罪者更利用病毒駭入資訊系統盜取他人財產或個人資料，比比皆是[1]。更甚者，網路犯罪集團經常性控制電腦病毒，遂行

[1] Andy Greenberg, *Security News This Week: Attackers Keep Targeting the US Electric Grids, Plus: Chinese hackers stealing US Covid relief funds, a cyberattack on the Met Opera website, and more*, WIRED (Dec. 10, 2022 9:00 AM), http://www.wired.com/story/attacks-us-electrical-grid-security-roundup/?bxid=611e04ba9530f748ee0a46b2&cndid=66076897&esrc=bouncexmulti_first&mbid=mbid%3DCRMWIR012019%0A%0A&source=EDT_WIR_NEWSLETTER_0_DAILY_ZZ&utm_brand=wired&utm_campaign=aud-dev&utm_content=WIR_Daily_121022&utm_mailing=WIR_Daily_121022&utm_medium=email&utm_source=nl&utm_term=P4; 鏡週刊（12/06/2022），〈中國駭客盜取6.1億元疫情紓困金！ 美特勤局證實：十幾個州受害〉，http://tw.news.yahoo.com/中國駭客盜取6-1億元疫情紓困金-美特勤局證實-十幾個州受害-075702499.html（最後瀏覽日：12/22/2022）；自由時報（12/07/2022），〈竊取個資、竄改給藥資料 衛服部桃園醫院遭中國駭客攻陷〉，https://news.ltn.com.tw/news/life/breakingnews/4147163（最後瀏覽日：12/22/2022）。

發動攻擊並隱藏身分及位置[2]。舉例來說，知名的 DPR（Dread Pirate Roberts），經營全球知名的地下犯罪王國「絲路（Silk Road）」網站，進行不法活動及違禁品的線上交易，使用加密交易流程進行通訊，從事匿名交易而隱身自己之真實所在位置[3]。利用網路科技隱身於虛擬世界，掩飾自己的真實身分，形成虛擬消失之狀態，使偵查機關根本無從尋找犯罪嫌疑人，美國聯邦調查局特別稱之為「走向隱身之中（going dark）」[4]。而真正問題不僅僅在於犯罪者走向隱身之中，更在於這種現象限制了執法者的權限及蒐集有價值證據之本質能力，無論是在組織犯罪、毒品跨國運輸，甚至是跨國破壞電腦設備基礎建設等[5]。然而，網路犯罪跨越了國界，而不受土地管轄權之限制，但執法單位及司法仍然必須依據物理世界的遊戲規則而運作[6]。

面對上述猖獗的網路犯罪及隱身科技，在比較法制上，透過規則之制定，美國司法會議之刑事規則諮詢委員會（the Advisory Committee on Criminal Rules for the Judicial Conference of the United States），決定減輕聯邦偵查官署的負擔，擴張對電子設備之遠端搜索令狀之管轄權範圍，在 2016 年 12 月修訂聯邦刑事訴訟規則，增訂遠端搜索，增訂理由言明增訂目的在於解決偵查機關不知電腦資訊設備或媒介硬體所在位置，而近年來電腦使用者對於其通訊日漸採取匿名模式，妨礙政府偵查特定目標對象或目標電腦資訊設備之

---

[2] Devin M. Adams, *The 2016 Amendments to Criminal Rule 41: National Search Warrants to Seize Cyberspace "Particularly" Speaking*, 51 U. Rich. L. Rev. 727, 730 (2017).

[3] Marc Goodman, Future Crimes: Everything is Connected, Everyone is Vulnerable and What We Can Do About it 194 (2015). 絲路網站大約是在2011年2月開始活躍於網路世界，一直到2013年10月，才由聯邦調查局查獲後停止其在線上之營運。在這一段期間，絲路網站吸引了超越10萬個全球會員，交易超越了100萬筆以上交易，產生超越12億美金的營收。*See also* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 Stan. L. Rev. 1075, 1077 (2017).

[4] *See generally Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 10 (2011).

[5] *Id.*

[6] Adams, *supra* note 2, at 732. 美國聯邦治安法官法第636條(a)，也對治安法官司法權限劃定管轄權界線。

位置，因而使聯邦法院產生依據管轄區域之劃分核發搜索票之困難，有進行（跨轄區）遠端搜索之需求及對於多個管轄區域內多個電腦設備，進行遠端搜索之需[7]。附帶一提的是，本次規則之修訂，聯邦司法部明白表示本草案本意不在於授權治安法官得以核發跨國（國外）搜索之令狀[8]。然而，這次增訂卻意外創造授權執法機關得為植入間諜程式遠端搜索之新型科技偵查之措施。

其實，這不是美國獨步全球之科技偵查執法，於 2017 年德國也修訂刑事訴訟法增訂來源端電信監察及線上搜索之立法，授權偵查機關植入電腦病毒或木馬程式[9]。我國法務部也曾提出科技偵查法草案，在草案明定設備端通訊監察，其立法理由明載「利用網路以通訊軟體或類似技術進行之通訊，多數係採取去中心化之網際協議通話技術，並將訊息切割為資料封包，不經中央伺服器，透過網路自行搜尋最近的路徑，傳送至受話方，屬於通訊參與者之間端點對端點之傳輸。由於傳輸過程使用加密技術，訊號自源頭端即開始編碼，透過網路傳輸到目的端受話方，再解密還原成訊息。目前在科技上，往往無法比照傳統電信監查之方式，在電信服務業者線路上擷取訊息，因為只能取得傳輸過程中的加密之亂碼，無法擷取到有內容意義的訊息，該亂碼通常無法即時或事後解碼，或可解碼但所費成本過高、時間過長。因此，此類通訊監察之實施，必須在通訊尚未加密前之發出端或已解密後之收取端，即記錄未加密或已解密之通訊內容，始有可能進行有效的通訊監察。……爰

---

[7] RICHARD M. THOMPSON II, CONG. RSCH. SERV., R44547, DIGITAL SEARCHES AND SEIZURES: OVERVIEW OF PROPOSED AMENDMENTS TO RULE 41 OF THE RULES OF CRIMINAL PROCEDURE, Summary, 1 (2016).

[8] Letter from Mythili Raman, Acting Assistant Attorney General, to the Hon. Reena Raggi, Chair, Advisory Comm. on the Criminal rules (Sept. 18, 2013) (on file with Advisory Comm. on Criminal Rules, April 2014), https://www.uscourts.gov/sites/default/files/fr_import/CR2014-04.pdf.

[9] 李榮耕（2018），〈初探遠端電腦搜索〉，《東吳法律學報》，29卷3期，頁50-51；王士帆（2019），〈當科技偵查駭入語音助理：刑事訴訟準備好了嗎？〉，《臺北大學法學論叢》，112期，頁196-198；吳俊毅（2020），〈刑事訴訟上的線上搜索（Online-Durchsuchung）與源頭通訊監察（Quelle-TKÜ）：引進的必要性及實踐上的困境〉，《刑事政策與犯罪研究論文集》，23期，頁461-484。

參考德國刑事訴訟法第一百 a 條，於本條規範設備端通訊監察之程序。」[10]。但這是針對網路應用軟體之通訊，於取得法院之令狀後，准許對於加密之通訊內容進行監聽之草案，不過由於社會誤解，對於這部分之草案，一經公告後，來自社會各界質疑聲浪不在少數[11]，很可惜的是，或許出於社會的誤解或擔心隱私權遭受深度侵害，使該部立法草案至今遭到擱置，無法通過。

為能妥善解決當代犯罪走向匿名化而無從找尋犯罪嫌疑人之困境，參酌世界先進國家立法趨勢均已承認遠端搜索或線上搜索，本文認為有必要深入分析美國聯邦刑事訴訟規則關於核發遠端搜索令狀，以搜尋電腦資訊設備內資訊（含設備所在位置）及面對同時搜索未知所在複數電腦設備之管轄權限制鬆綁之法制。以下本文第貳部分，首先深入探討當前之網路科技發展與網路犯罪，藉以分析美國國家植入間諜程式遠端搜索之科技類型，包括國家植入間諜程式遠端搜索可取得資訊、國家植入間諜程式過程分析，及現行美國司法實務對於國家植入間諜程式遠端搜索之憲法定位及對人民基本權干預之分析。第參部分，闡述美國聯邦刑事訴訟規則增訂遠端搜索條款之提案背景、緣由及對於提案面臨之反對意見，進行討論及分析。第肆部分，針對國家遠端搜索之新法說明及本文進行規範評析。第伍部分，針對我國未來若增訂國家植入間諜程式遠端搜索之規範架構，從對於人民基本權之干預侵害、令狀原則（含相當理由）、授權准許遠端搜索之要件、令狀特定性要件、令狀有效執行期間、執行完畢後技術上恢復原狀之規範、通知要件及延期通知之明定、訂定證據排除規範等內容詳盡分析。但本文論述之遠端搜索，依循美

[10] 科技偵查法草案第14條立法理由。

[11] 風傳媒（09/21/2020），〈《科技偵查法》草案嚴重侵犯隱私權 律師提醒有違憲疑慮〉，http://www.storm.mg/article/3041589（最後瀏覽日：01/29/2023）；法操FOLLAW（09/22/2020），〈科技偵查法，是上太空？還是殺豬公？〉，《自由評論網》，http://talk.ltn.com.tw/article/breakingnews/3299617（最後瀏覽日：01/29/2023）；歐陽弘（10/13/2020），〈科技偵查法草案評析：提供於立法院民國109年10月8日公聽會意見與會後補充〉，《群勝國際法律事務所法律專欄》http://www.btlaw.com.tw/h/NewsInfo?key=0227079976&cont=264581（最後瀏覽日：01/29/2023）。

國聯邦刑事訴訟規則之立法意涵不包含跨國境搜索部分，特於此附帶敘明之。

貳、美國國家植入間諜程式遠端搜索科技類型與干預之基本權

一、網路科技發展與暗網生成

隨著科技進步，網路資安是美國科技界面對之首要問題，美國聯邦調查局局長 James B. Comey 曾在眾議院聽證會表示，在執法人員追訴網路威脅過程中，犯罪者逐步隱身於暗處，甚至透過科技加密走向虛擬消失（virtually invisible）之境，增加偵查機關聲請搜索令狀之行政障礙，當然這也加劇追蹤網路威脅之執法者與犯罪者間之實力差距[12]。許多犯罪型態，走向暗網化，形成線上虛擬犯罪集團，而當代最大的威脅係廣為運用之免費加密科技、行動電話應用程式及暗網之虛擬環境。

基於網路運作，一般網路服務提供者（Internet Service Provider，下稱 ISP）得以知悉用戶之基本資料，包括姓名、地址、瀏覽歷史、IP 位置，因之得以確認使用網路之特定電腦使用人，但人民其實期待的是在搜尋網路及交換敏感資訊時，免於受到國家或第三人企業之監視，特定個人在網路世界透過隱身科技想要隱藏自己真實身分者，不只是犯罪或掠奪者，尚包括選民、吹哨者、爭議性文章或評論之作者、新聞記者等，正因此形成暗網（Dark Web），成為論者所稱暗網是個表達、創意、資訊及想法的自由與權力的世界[13]。暗網是全球性私人電腦網路，讓使用者操作匿名交易，保持隱藏自身位置行蹤[14]。就以非常知名之暗網，即為洋蔥網路（Tor Network），原始發

12 *See Oversight of the Federal Bureau of Investigation: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. 3-5 (2016) (Statement of James B. Comey, Director, FBI).

13 JAMIE BARTLETT, THE DARK NET: INSIDE THE DIGITAL UNDERWORLD 237 (2015).

14 Ghappour, *supra* note 3, at 1087.

展於美國海軍，用以保護政府部門之通訊，現在已成為公開資源及由公眾挹注資金之網站[15]。洋蔥網路中介電腦，使用加密的通訊協定，而為使用一般網路瀏覽器所無法接近，取而代之的是，需要特殊的軟體，例如洋蔥瀏覽器（Tor Browser）才能取得進入之權限。適當地使用洋蔥網路讓國家無可能追蹤如下資訊，如在網路上主持隱藏網站之主持人其電腦位置、任何接近（連結）隱藏網站之電腦資訊設備位置或經過網路的路徑、匿名式造訪公開網站之電腦資訊設備位置[16]。

以技術面言之，洋蔥網路保護使用者通訊免於受到政府監視，因為它將通訊之後設資料與通訊內容脫鉤，在到達目的地前，讓通訊路徑以封包方式通過分散於世界各處之網路，由個人自願提供自己資訊設備於匿名網路作為中介電腦（或稱為代理伺服器）使用之。以實際面言之，洋蔥網路可以保護使用者通訊免於受到傳輸分析（traffic analysis），使用者透過洋蔥網路連結到公眾可點選之網站，從外部來看，其網路傳輸源自於代理電腦而不是真實電腦的連結。舉例來說，假若位在西雅圖之犯罪嫌疑人以匿名傳輸方式上網，將透過使用一系列代理伺服器，呈現在目標網頁之最後傳輸位置可能是位在義大利的代理伺服器，而讓外界誤以為是位在義大利的使用者[17]。其次，洋蔥網路可以保護透過該網路之通訊，使主持網站者之內容或服務，不致於曝露自己的伺服器真實所在位置[18]，可謂免於受到傳輸分析之雙重保護。

在暗網中得作為強化隱身於網路世界之科技，包括代理伺服器（anonymizing proxy）、虛擬私人網路（virtual private networks；VPNs）及洋蔥路由器（Tor；the Onion Router）等，均得為使用科技方式隱藏自己電腦設備之位置[19]。當代犯罪因為網路駭客等專業犯罪，改變或使用他人電腦資訊系統內資訊，國家因之也須以非傳統方式偵查犯罪及蒐集證據，舉例來說，利用資訊科技設備犯罪，確認犯罪者電腦資訊設備所在應該是發覺犯罪

---

15 *See generally* KRISTIN FINKLEA, CONG. RSCH. SERV., R44101, DARK WEB 3 (2015).

16 Ghappour, *supra* note 3, at 1087.

17 *Id.* at 1088.

18 *Id.* at 1089.

19 Adams, *supra* note 2, at 734-35.

者身分最重要的偵查階段，然後才得以蒐集證據進而成功刑事訴追[20]。可惜的是，當偵查機關需要偵查犯罪者 IP 位置或確認犯罪者身分，甚至是蒐集取得儲存於電腦資訊設備之內容性資訊、電子郵件通訊內容之媒介，卻因為暗網科技發展，使得欠缺得以偵查目標電腦設備真實位置之能力，偵查機關基本上無能發動傳統蒐集證據之蒐證流程、並扣押電腦，也弱化了今日偵查機關追訴不法活動之能力，造成犯罪者在暗網上進行犯罪及偵查機關科技弱勢之不對稱能力[21]。

二、美國國家植入間諜程式遠端搜索之科技類型

能破解或規避暗網之科技，有賴於網路偵查技術（Network investigative techniques，下稱 NIT 技術），透過發送及植入程式於目標電腦取得進入他人電腦權限[22]，傳播惡意程式（malware）或間諜程式（下統稱間諜程式）[23]，隱密地監督控制他人電腦系統[24]或者透過間諜程式將重要確認資訊發送回到執法者[25]。NIT 技術佈署間諜程式穿梭於虛擬路徑（virtual pathways），像是在網路中連結電腦之橋樑，最終達到目標電腦虛擬 IP 位置而無庸知悉特定物理位置，一旦間諜程式穿透目標電腦，即可將目標電腦轉變為監視設備

---

[20] Michael B. Mukasey, *The Attorney General's Guidelines for Domestic FBI Operations* 7 (2008), http://www.usdoj.gov/ag/readingroom/guidelines.pdf ("In most ordinary criminal investigations, the immediate objectives include … identifying, locating, and apprehending the perpetrators … ").

[21] Ghappour, *supra* note 3, at 1093-95. 因此傳統透過調取令（文書提出命令）由網際網路服務業者提出後設資料（使用者基本資料），已不再能夠作為鎖定、確認偵查目標對象之方式。此時由第三人企業提供之資料，都將無法揭露使用者（犯罪者）之真實身分，*see* Ghappour, *supra* note 3, at 1094 n.91.

[22] Ghappour, *supra* note 3, at 1095.

[23] 惡意或間諜軟體二者均屬於電腦安全社群用以描述能夠私密地從目標電腦內取得進入或蒐集資訊之名詞，*see* Zango, Inc. v Kaspersky Lab, Inc., 568 F.3d 1169, 1171 (9th Cir. 2009).

[24] *Malicious Technology*, BLACK'S LAW DICTIONARY, 1102 (10th ed. 2014).

[25] THOMPSON II, *supra* note 7, at 3.

[26]。現代型目標監視非常可能積極地滲入目標電腦、植入間諜程式而取得控制網路，有論者表示想要監控個人通訊最簡單的方式，不再是截聽傳輸中通訊，而係直接駭入電腦[27]。因此，電腦駭客順勢產生，駭客暗中地（surreptitiously）從事使用或改變他人電腦中資訊，無論是民間或政府駭客，首要任務就是能夠取得進入他人電腦的權限或能力。而能夠進入他人電腦需要的是間諜程式，暗中布建取得控制或監控他人的電腦資訊設備系統。然而更重要的是，在執行間諜程式前，要先能夠將間諜程式傳輸到他人電腦系統中，此即需要利用人性弱點或科技脆弱性來達成。駭客主要使用下述 2 種方式進入他人電腦之中：社交工程技術或水坑攻擊技術。茲分述如下：

（一）社交工程技術（social engineering）

首先，社交工程其實是利用來自於合法商業寄發於電子郵件信箱之反覆自動跳出之廣告（pop-up ad）或附加檔案。此等廣告或附加檔案帶有間諜程式，在相對人點擊廣告後，秘密地部署進入目標對象電腦資訊設備中，所以又稱為網路版特洛伊木馬[28]。國家幹員在此種行動中可以偽裝成為第三人，通常是相對人之朋友，在執法機關的運用上，早在 2001 年，聯邦調查局首次部署間諜程式從事電腦搜索，即「電腦及網路協定位置確認器（Computer and Internet Protocol Address Verifier；CIPAV）」（又稱「魔術燈籠（Magic Lantern）」），係聯邦調查局秘密使用駭入目標對象之電腦，進行有效地搜索未知目標電腦設備[29]。此種技術即為一般人熟知的 NIT 偵查技術，執法機

---

[26] Ghappour, *supra* note 3, at 1096.

[27] BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD, 84-86 (2015). 作者也論述諸多國家之間彼此相互駭入，蒐集取得資訊之例子，比比皆是。

[28] Adams, *supra* note 2, at 737; Rachel Bercovitz, *Law Enforcement Hacking: Defining Jurisdiction*, 121 COLUM. L. REV. 1251, 1260 (2021).

[29] Kevin Poulsen, *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats*, WIRED (July 18, 2007), https://www.wired.com/2007/07/fbi-spyware/; Ted Bridis, *FBI is Building a 'Magic Lantern'*, WASH. POST (Nov. 23, 2001), https://www.washingtonpost.com/archive/politics/2001/11/23/fbi-is-building-a-magic-

關聲請令狀時，命名為 NIT 令狀[30]，做為蒐集包括電腦資訊設備之大數據，像是目標對象電腦之 IP 位置及儲存於電腦之資訊內容，如電子郵件通訊及照片。

真正首次公開報導使用 NIT 偵查技術案件為 2007 年，聯邦調查局為追蹤以暱稱「Myspace」名義對華盛頓某高中發出電子郵件進行炸彈威脅之炸彈客及來源，乃透過虛構電子郵件發送上述 CIPAV 軟體，給該炸彈威脅恐怖分子「Myspace」，進而追查 IP 位置、乙太網路卡位址（MAC address of ethernet）及其他確認資訊[31]。這種軟體所能取得之資訊包括，IP 位置、現在登錄使用者姓名及登錄公司、正在執行程式清單、乙太網路卡位址、操作系統、版本及登記使用者及網路瀏覽器及版本。之後，此軟體將存於目標電腦資訊設備內，持續蒐集、監視目標電腦使用者之登錄紀錄、該設備連結之個別電腦之 IP 位置[32]。

此種技術稱為社交工程技術，秘密佈署間諜程式探知需要的資訊。因此，聯邦調查局使用上述間諜程式技術，在聲請令狀時稱之為請求部署網路偵查技術令狀（下稱 NIT 令狀），此種令狀，授權鎖定（locate）匿名犯罪嫌疑人或行為人，透過寄發電子郵件加以確認位置，偵查機關透過令狀授權得使用有間諜程式之電子郵件確認對象，而令狀記載以通訊寄送給目標對象，啟動電腦回傳特定資訊於偵查機關控制電腦內[33]。換言之，NIT 技術，就是秘

---

lantern/ca972123-83a8-46d8-b95c-c2edafda0fea/.

[30] Third Amended Application for a Search Warrant at 1, *In re* Matter of the Search of Network Investigative Technique (NIT) for E-mail Address Texan.slayer@yahoo.com, No: 12-sw-05685-KMT, (D. Col. Dec. 11, 2012), https://cryptome.org/2013/12/nit-email-search.pdf.

[31] Poulsen, *supra* note 29; 法院在該案核發之搜索票並不准許搜取任何電子訊息之內容，*see* THOMPSON II, *supra* note 7, at 3。

[32] Poulsen, *supra* note 29 (“Under a ruling this month by the 9th U.S. Circuit Court of Appeals, such surveillance -- which does not capture the content of the communications -- can be conducted without a wiretap warrant, because internet users have no "reasonable expectation of privacy" in the data when using the internet.”); SCHNEIER, *supra* note 27, at 87.

[33] ORIN S. KERR, COMPUTER CRIME LAW, 551 (4th ed. 2018). Orin Kerr教授提到NIT本質

密安裝間諜程式於目標電腦資訊設備內蒐集資訊，是一種駭客工具，用以調查犯罪嫌疑人電腦，於使用人下載間諜程式時蒐集使用人之資訊、運作軟體（operating system）及網路內部控制位址[34]。NIT 令狀，於記載時，不會使用「駭客、間諜程式」之文字，而是在令狀聲請過程當中，陳述發送一種足以啟動電腦回傳特定資訊（to cause an activating computer to send certain information to a computer）於聯邦調查局（執法機關）電腦設備之通訊方式[35]。

（二）水坑攻擊技術

其次，偵查機關運用下載程式技術（Drive-By-Downloads；Watering Hole Attacks），由目標對象點擊連結不法網站，僅僅是連結不法網站就足致安裝間諜程式於使用者電腦內，並由不法網站秘密傳輸間諜程式碼於目標對象，強制瀏覽器下載、儲存及秘密地執行惡意應用程式（a malicious application）。傳輸方式為遠端注入間諜程式碼到網站，待目標對象點擊網站後程式碼將秘密地植入特定造訪者（包含所有造訪者），進而搜索目標電腦資訊設備，並造成大量電腦被入侵者侵入，因而命令受侵入電腦回傳資訊給偵查機關[36]。此與前述駭客類型不同之處在於上述係針對特定之電子郵件信箱所發送間

上為電腦病毒，而將感染使用者之設備，例如在一科羅拉多州寄送給該州警方電子郵件中，聲稱要置放阿摩尼亞炸彈之恐怖案件中，要確認之電子郵件信箱為texan.slayer@yahoo.com，所以向法院聲請NIT令狀。

34 Nate Raymond, *U.S. Judge Rules Search Warrant in FBI Child Porn Website Probe Invalid*, REUTERS (Apr. 21, 2016), https://www.reuters.com/article/idUSL2N17O0DE/.

35 Adams, *supra* note 2, at 739.

36 Ellen Nakashima, *This is How the Government is Catching People Who Use Child Porn Sites*, WASH. POST (Jan. 21, 2016), https://www.washingtonpost.com/world/national-security/how-the-government-is-using-malware-to-ensnare-child-porn-users/2016/01/21/fb8ab5f8-bec0-11e5-83d4-42e3bceea902_story.html; Mary-Ann Russon, *FBI Crack Tor and Catch 1,500 Visitors to Biggest Child Pornography Website on the Dark Web*, INT'L BUS. TIMES (Jan. 6, 2016), http://www.ibtimes.co.uk/fbi-crack-tor-catch-1500-visitorsbiggest-child-pornography-website-dark-web-1536417; Adams, *supra* note 2, at 739.

諜程式，而水坑攻擊則是就所有接近（點擊）特定網站之電腦資訊設備為之。通常水坑攻擊針對分享共同興趣之同好者間多人之電腦植入監視軟體，執法者在此等情況可能事前並不知道特定目標的身分，甚至是目標對象[37]。

在 2012 年，聯邦調查局展開暗網「Playpen」兒童色情網站之偵查，基於向法院治安法官聲請之 NIT 令狀，發動魚雷行動（Operation Torpedo），由該 NIT 令狀授權植入程式碼（inserting code）於不法網站，藉由水坑攻擊方式，對於「Playpen」兒童色情網站，植入間諜程式，待會員造訪點擊後，方得搜索任何下載、上傳所在地點（wherever located）之電腦資訊設備，取得網站影像或閱覽私人訊息[38]。最後，聯邦調查局一共從多達 120 個國家取得超過 9000 筆的 IP 位置紀錄，並據而追訴超過 200 多位不法色情網站之造訪者[39]。

三、植入間諜程式遠端搜索得取得之資訊類型

運用 NIT 技術可取得資訊，分為下列幾種，第一、取得目標電腦資訊設備主持者姓名（the target computer's "Host Name"），操作系統、IP 位置資訊[40]，其後，執法機關再從網路服務業者調取用戶資訊，據以聲請搜索票搜索目標電腦資訊設備所在之住宅或商業處所；第二、乙太網路卡位址（"Media Access Control" address；Ethernet card）、運作程式種類、網路瀏覽器及版本、操作系統之登記使用者、登記公司名稱；第三、如果更徹底搜索電腦是必要的，NIT 技術也得以獲得網路活動之紀錄，包括防火牆登錄紀錄（firewall logs）、網路瀏覽歷史及瀏覽追蹤、被列為書籤或我的最愛的網頁、搜索名

---

37 Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End up in Your Computer*, WIRED (Aug. 5, 2014), https://www.wired.com/2014/08/operation-torpedo/.

38 *See* Warrant for Computers that Access the Website "Bulletin Board A" Case No.12-sw-05685-KMT, *supra* note 30, at 3-17.

39 McKenzie Hightower, *The Fourth Amendment and the Dark Web: How to Embrace a Digital Jurisprudence that Protects Individual Liberties*, 109 The GEO. L. J. ONLINE 173, 173-74 (2021).

40 Kurt C. Widenhouse, *Playpen, the NIT, and Rule 41(b): Electronic "Searches" for Those Who Do Not Wish to be Found*, 13 J. Bus. & Tech. L. 143, 143 (2017).

詞及儲存之使用者名稱及密碼、電子郵件內容及聯絡簿及照片等。第四，除上述可取得儲存於目標電腦中任何資料外，遠端搜索亦可用於啟動特定行動電話之麥克風、電腦之麥克風，以錄音方式記錄對話、行動裝置及 GPS 晶片[41]。最後，可以接近使用電腦之照相機，而不觸碰到啟動燈光效果之功能，以免於使用者知悉正在錄影之功能[42]。

四、國家植入間諜程式遠端搜索執法各個階段分析

（一）國家植入間諜程式前之發送階段

國家傳遞發送間諜程式於目標電腦，通常是以釣魚訊息發送給嫌疑人之帳號，引誘嫌疑人點擊連結。此種間諜程式之遞送，又稱為網路釣魚（phishing）。近年來，執法機關另外常使用的是隱藏服務，通常政府已經先確認隱藏服務營運者，經執法後取得扣押該營運者基礎建設之後，由政府接管營運並附加間諜程式[43]。前述水坑攻擊模式，國家則是輸入已先準備之電腦碼於瀏覽網頁中，後引導嫌疑人之網路瀏覽器，造訪國家政府控制或持有之某網站或內容[44]。當在特定誘發情況下，犯罪者與網站互動後，藉由造訪、登入或進入特定網頁之後，間諜程式即可順利傳遞（植入）。這與上述網路釣魚不同，係針對專門部署用以從事特定行為之任何行為人[45]。

使用水坑攻擊成功打擊犯罪的執法案例，主要包括由聯邦調查局於 2012 年內布拉斯加之魚雷行動（Operation Torpedo）、2013 年在馬里蘭地區

---

41 ACLU, *Second ACLU Comment Letter on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media* 4 (Oct. 31, 2014), https://www.aclu.org/sites/default/files/field_document/aclu_comment_on_remote_access_proposal.pdf.

42 Jennifer Valentino-DeVries & Danny Yadron, *FBI Taps Hacker Tactics to Spy on Suspects*, WALL STREET JOURNAL (Aug. 3, 2013, 3:17 PM), https://www.wsj.com/articles/SB10001424127887323997004578641993388259674.

43 Jonathan Mayer, *Government Hacking*, 127 YALE L. J. 570, 583-84 (2018).

44 ACLU, *supra* note 41, at 8.

45 Zach Lerner, *A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure*, 18 Yale J. L. & Tech. 26, 40-42 (2016).

調查之自由主持平臺行動（Freedom Hosting Platform）及 2015 年在維吉尼亞州東部地區之撫平者行動（Operation Pacifier）。無論如何所採取的行動，目的在於將間諜程式著陸於犯罪者之資訊設備上[46]。

（二）利用（Exploitation）

現代科技設計之軟體程式並非全部均具值得信賴性，因此軟體程式通常執行有限的許可行為，例如：僅能在資訊設備上取得特定資料及功能。網路瀏覽器及行動設備特別施加嚴格安全沙盒，而特定軟體只能以特定能力之接近使用，例如：只能取得儲存資料。至於某些極具敏感性的能力，例如：啟動設備網路攝影機、GPS，須視使用者積極同意後才可使用。執法者駭入後，破壞與沙盒有關之安全障礙，才能取得所需要資料及特徵。舉例來說，在「利用」這個階段，在社交工程情況下，當目標對象點擊釣魚郵件之連結，執法者植入一種軟體稱為「外殼代碼（shellcode）」於目標電腦後，繞過或規避任何安全軟體或其他內建之保護，「外殼代碼」就會自動執行。如果是使用水坑攻擊，則當目標對象造訪由國家控制網站時，即發生利用之執行[47]。

（三）執行

一旦執法者規避資訊安全保護，即得執行程式，此時程式有效地轉變成監視工具，讓電腦有能力從事任何可行之任務[48]。如果單純之間諜程式，就像上述魚雷行動，間諜程式僅僅註記執行程式的時間，發送包括電腦資訊設備 IP 所在位置之網路請求[49]。更複雜的間諜程式，可以透過設備運作系統，取得額外的確認資訊，例如，聯邦調查局的自由主持惡意程式（Freedom Hosting malware），蒐集電腦名字及電腦製造商指定之網路卡之獨特的確認

---

[46] Mayer, *supra* note 43, at 586.

[47] Ghappour, *supra* note 3, at 1097（該文特別提到利用的是軟體安全之脆弱性才能使得程式進入該系統）；ACLU, *supra* note 41, at 8.

[48] Ghappour, *supra* note 3, at 1097.

[49] Mayer, *supra* note 43, at 588.

資料[50]。在 2015 年，聯邦調查局之撫平者行動則更進一步，可以取得現在登錄在電腦上之使用者姓名及過去曾否執行過間諜程式軟體[51]。更甚者，部分聯邦調查局的間諜程式則能夠持續隱藏並在嫌疑人電腦設備中持續運作一段時間，同時可以接近檔案、登錄按鍵碼、攔截通訊、追蹤位置並可以打開電腦之攝影機[52]。

（四）回報（回傳資訊）

在嫌疑人電腦設備執行間諜程式後，任何政府控制的伺服器將發生作用而接收回報之資訊，舉例來說，在魚雷行動，聯邦調查局伺服器接受間諜程式回報之專屬網路伺服器之軟體[53]。

（五）小結

綜上，上述 4 個階段為國家間諜程式運作之基礎，各個階段包括發送（植入）、利用、執行、回傳資料，都屬於美國聯邦憲法增修條文（下稱增修條文）第 4 條意義之搜索及扣押，而無庸政府執法者「物理性」侵入憲法保障之財產權範圍內[54]。詳言之，在「利用」階段，植入利用間諜程式後即為「執行」NIT 技術，而該技術最大目的在於檢視、蒐集、翻搜電腦所在 IP 位置及電腦資訊設備內容性資訊，從而，其所檢視的內容，是當事人（使用者）具有合理隱私期待之資訊（特別是電腦資訊設備內容性資訊），因此此一階段之執法行為，即為搜索關於個人具有合理隱私期待之隱私資訊，國家此一階段偵查行為即為憲法意義之搜索行為。最後，執法機關搜索相關電腦

---

50 *Id*.

51 *Id*.

52 *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 755-56 (S.D. Tex. 2013).

53 Mayer, *supra* note 43, at 589.

54 Jeremy A. Moseley, *The Fourth Amendment and Remote Searches: Balancing the Protection of the People with the Remote Investigation of Internet Crimes*, 19 NOTRE DAME J. L. ETHICS & PUB. POL'Y 355, 356 (2005).

資訊設備內容性資訊後，需要複製回傳該等資訊，而複製本身表面上不會影響檔案所有人之財產利益，且不影響檔案之所有或持有權利，因此似乎沒有干涉使用人持有電腦資訊之利益，依據聯邦最高法院在 *United States v. Jacobsen* 案法則[55]，該院向來將扣押解釋為對於個人財產得享有之利益，造成了實質的影響（meaningful interference），而複製行為看似對於他人使用電腦之持有利益，沒有造成實質的影響。但論者認為，複製行為干涉使用人「控制及支配」該等資訊之利益，做為未來偵查或追訴之用，亦為憲法意義之扣押行為[56]。

至於美國司法實務，目前聯邦最高法院對於偵查機關以遠端搜索蒐集取得個人隱私資訊，是否屬於憲法意義之搜索、扣押，並未表示意見，但聯邦下級法院，特別是聯邦巡迴上訴法院就關於基本權干預及是否受憲法誡命及限制，已有較為明確之見解，茲分述如下。

五、國家植入間諜程式遠端搜索涉及之基本權干預及美國司法實務見解

承前所述，國家從事遠端電腦搜索，由國家駭客取得電腦使用者 IP 位置及目標電腦資訊設備之內容性資訊，屬於高科技偵查之強制處分，其對於人民何種基本權利造成干預或侵害。其次，此種新興強制處分，是否屬於美國聯邦憲法增修條文第 4 條之憲法意義之搜索？若此一命題的答案為肯定的話，則遠端搜索偵查行為應受憲法令狀原則之誡命及限制。

因聯邦下級法院判決依據搜索取得資訊之不同，大致區分為電腦內容性資訊、IP 位置資訊，形成不同之見解。此等判決，主要源自於聯邦調查局主導調查之兒童色情網站案例，茲先詳細論述該案事實。於 2014 年 12 月，聯邦調查局查獲以洋蔥伺服器技術在暗網中營運之大型色情網站（Playpen），

---

55 United States v. Jacobsen, 466 U.S. 109, 113 (1984).

56 Andrew Crocker, *With Remote Hacking, the Government's Particularity Problem Isn't Going Away*, JUST SECURITY (June 2, 2016), http://www.justsecurity.org/31365/remote-hacking-governments-particularity-problem-isnt/; 中文文獻部分，相同見解見李榮耕，前揭註9，頁67。

提供匿名服務，該網站連結模式不同於一般網站連結模式透過造訪者 IP 位置連結上網，實經由網站提供之軟體將連結路徑轉至第三人電腦作為節點（nodes），通過一連串節點後，造訪者方能連結到網站上網。於 2015 年，聯邦調查局查獲該網站真正營運者，逮捕犯罪行為人後，改由聯邦調查局接管並取得該色情網站網域之控制權，在維吉尼亞東區，持續運作該網站[57]。但該網站造訪者遍及全國，管轄權的限制造成聯邦調查局取得令狀之能力難以搜尋全國造訪者所在位置。儘管上述限制，聯邦調查局向維吉尼亞州東區聯邦地方法院（下稱維州東區法院）聲請 NIT 令狀，取得由法院授權植入間諜程式於控制網站之 NIT 令狀，對於該暗網兒童色情網站之網路造訪者，藉由將間諜程式植入造訪者電腦資訊設備搜尋 IP 位置，秘密地回報使用者真實 IP 位置及其他確認資訊追查造訪者之身分資訊，以冀望能鎖定造訪者，該次核發令狀，也搜尋到多位所在不同州之被告[58]。因而衍伸諸多刑事追訴之案件。以下依據該案國家執行 NIT 令狀取得之資訊，分別探討司法判決對於國家植入間諜程式遠端搜索造訪者之電腦設備內容（含所在位置），是否屬於憲法意義之搜索及管轄權爭議，茲分別論述如下。

（一）國家駭入取得電腦設備內容（包括使用者 IP 位置）構成憲法意義之搜索

1. 國家駭入取得電腦內容性資訊侵害人民之隱私權

在 2015 年，聯邦調查局執行維州東區法院 NIT 令狀後，查獲在愛荷華州南區被告 Horton 及 Croghan，二人分別因取得持有兒童色情照片被訴，被告二人均主張該令狀違反聯邦刑事訴訟規則第 41 條(b)管轄權規定，聯邦地

---

[57] *In re* Search of Computers that Access upf45jv3bziuctml.onion, No. 1:15-SW-89 (E.D. Va. Feb. 20, 2015), https://ia601805.us.archive.org/8/items/gov.uscourts.vaed.340813/gov.uscourts.vaed.340813.27.3.pdf

[58] United States v. Workman, 863 F.3d 1313, 1315-16 (10th Cir. 2017). 上述治安法官核發令狀，因而找到隱身在科羅拉多州之本案被告Workman，並於執行逮捕令後，正好在其住處逮獲正在下載兒童色情之被告及證據。

方法院因而裁定排除因治安法官核發 NIT 令狀蒐集取得之證據[59]。聯邦地方法院審理時裁准排除證據之主張。上訴後，聯邦第八巡迴上訴法院首先討論的爭點即為國家植入之間諜程式遠端搜索，是否屬於增修條文第 4 條之搜索，對於這個問題，有其他地方法院認為以 NIT 令狀遠端搜索僅僅取得 IP 位置資訊，本於第三人原則，個人對於自願提出之 IP 位置並無合理之隱私期待，無須透過聲請令狀執行此種偵查技術，因為此為被告公開可得之資訊，不受增修條文第 4 條之保護[60]。

但聯邦第八巡迴上訴法院認為本案不同於第三人原則，本案聯邦調查局發送電腦程式碼足以搜索被告二人個別電腦內之資訊，並回傳於聯邦調查局，故聯邦調查局蒐集的資訊，含有特定個人電腦內容性資訊，即便被告對於個人 IP 位置並無合理隱私期待，對於個人電腦內之內容性資訊，非個人自願提供與第三人資訊，仍具有合理隱私期待。依據美國聯邦最高法院見解，國家偵查機關蒐集取得個人資訊時，侵害個人合理隱私期待之隱私權時，基於以隱私權作為增修條文第 4 條之判斷基準，偵查機關之遠端搜索已構成憲法意義之搜索[61]。再者，於 2014 年，聯邦最高法院在 *Riley v. California* 案[62]表示，搜索現代型行動電話，因行動電話巨大儲存能力之本質，本於內部儲存資訊之質與量，即使執行附帶搜索行動電話，對於行動電話負載資訊，已非傳統之物理性之有體物所可比擬，因此不得直接搜查行動電話之儲存資訊，偵查機關仍應先取得令狀，方得蒐集取得行動電話內數位資訊。因此，

---

59 United States v. Croghan, 209 F.Supp.3d 1080, 1090-91 (S.D. Iowa 2016). 該令狀蒐集資訊為computer's Internet Protocol (IP) address, operating system information, operating system username, and its Media Access Control (MAC) address, which is a unique number assigned to each network modem.

60 United States v. Horton, 863 F.3d 1041, 1045, 1046 (8th Cir. 2017).

61 Katz v. United States, 389 U.S. 347, 351 (1967); Carpenter v. United States, 138 S.Ct. 2213 (2018). 中文文獻請參考李榮耕（2015），〈科技定位監控與犯罪偵查：兼論美國近年GPS追蹤法制及實務之發展〉，《臺大法學論叢》，44卷3期，頁930-939；溫祖德（2021），〈偵查機關調取歷史性行動電話基地臺位置資訊之合憲性審查：從美國聯邦最高法院判決檢視我國法制〉，《政大法學評論》，167期，頁179-181。

62 Riley v. California, 134 S.Ct. 2473, 2489-91 (2014).

在本案搜索電腦設備前，執法機關應該先取得憲法意義之令狀，因此該院認為執行 NIT 偵查技術也需要事先取得令狀為之[63]。

雖然本案執法機關確實已取得 NIT 令狀，但本案令狀也涉及另一個爭議，該案判決認為，國會立法規範治安法官在任命之轄區內具有司法權，在本案核發 NIT 令狀時，聯邦刑事訴訟規則第 41 條(b)(1)授權治安法官有權核發轄區內搜索、扣押個人或財產權之令狀，但對於管轄區域外之搜索、扣押令狀，則須符合該規則明訂之管轄權轄區之例外規定，如：財產權移動至管轄權範圍外、國內及國際間恐怖犯罪、追蹤設備裝設及財產權位於聯邦轄區外。這些規定並無明示准許某一轄區治安法官得授權搜索轄區外之電腦資訊設備。檢方爭執此一令狀依據聯邦刑事訴訟規則准許裝置追蹤設備之例外規定，主張被告以虛擬方式在維州東區下載兒童色情圖片，因此在維州管轄區域內部署 NIT 偵查技術，以追蹤被告之所在。然而聯邦第八巡迴上訴法院認為真正安裝植入程式地點在被告 2 人位於愛荷華州的住處，法院採取多數法院見解認為聯邦刑事訴訟規則第 41 條追蹤設備之規範定義，並不採取廣義說，運用 NIT 偵查技術之設備不屬於追蹤裝置設備，因此，最終認定本案 NIT 令狀已經超出治安法官之核發管轄權之權限。

2. 國家駭入取得電腦內容性資訊構成美國憲法意義之搜索

本文所探討上述聯邦巡迴上訴法院之案例，為國家偵查犯罪、取得治安法官核發之 NIT 令狀後，植入間諜程式於控制網站，對於在暗網之兒童色情網站造訪者，於下載間諜程式植入造訪者電腦設備搜尋 IP 位置及電腦內容，秘密地回報使用者真實 IP 位置及電腦內容性資訊，追查造訪者之身分資訊，冀望能鎖定造訪者。目前聯邦巡迴上訴法院認為對於個人之行動電話及個人電腦之內容進行搜索，將暴露遠甚於對個人住宅最詳盡之搜索內容[64]，依據合理隱私期待理論，個人對於電腦內容性資訊展現真實主觀的隱私期待；而個人主觀隱私期待為社會承認係合理的[65]，因此，聯邦巡迴上訴法

---

[63] *Horton*, 863 F.3d at 1047.

[64] *Riley*, 134 S. Ct. at 2491.

[65] United States v. Jones, 132 S. Ct. 945, 950 (2012).

院認為以 NIT 偵查技術遠端搜索電腦內容性資訊，屬於美國憲法意義之搜索，應屬無疑。

（二）國家植入間諜程式單純取得 IP 位置不構成憲法意義之搜索

國家對犯罪嫌疑人之電腦植入間諜程式以取得 IP 位置是否構成憲法意義之搜索，則有完全不同於上述聯邦巡迴上訴法院之見解。以下將以聯邦地方法院見解為例，論述分析國家植入兒童色情網站造訪者之間諜程式，藉以搜尋造訪者之電腦資訊設備 IP 位置，是否屬於憲法意義之搜索及管轄權爭議，進行詳盡之說明。

本案事實同樣為聯邦調查局調查以 TOR 方式經營之 Playpen 色情網站，而於 2015 年 2 月 27 日，透過 NIT 偵查技術，查獲被告 Matish 住處電腦 IP 位置，依據該 IP 位置，再核發提出命令（subpoena）網路服務提供業者，調取特定某日期、時間持有該 IP 位置之電腦及確認資訊，憑藉著該等資訊，才另外由治安法官核發搜索令狀，於同年 7 月，至被告住處搜索扣押數臺電腦、硬碟、行動電話等證據，但被告主張授權搜索之令狀欠缺相當理由（包括聯邦調查局有意或輕率地納入錯誤資訊或忽略實質資訊）及欠缺特定性要件，因此令狀是無效令狀，本案搜索是違憲搜索，應排除該次扣押取得之證據及搜索所取得之結果[66]。

不過，聯邦地方法院在 Matish 案認為本案透過 NIT 偵查技術搜索取得被告 IP 位置，對於 IP 位置，個人並無合理之隱私期待，從而國家取得被告 IP 位置並非代表著憲法意義之搜索。聯邦地方法院之理由，主要引用聯邦第九巡迴上訴法院在 Forrester 案見解[67]，在 Forrester 案，「聯邦第九巡迴上訴

---

66 United States v. Matish, 193 F. Supp. 3d 585, 622 (E.D. Va. 2016).

67 United States v. Forrester, 512 F.3d 500 (9th Cir 2008). 在該案，「被告Forrester及Alba以共謀製造毒品罪定罪，偵查機關運用電腦監控科技，包括發話撥號記錄器及追蹤技術以追查監控被告於網際網路活動，該網路監察工具是透過被告之網路服務業者（ISP）裝設發話撥號記錄器於被告之帳戶，偵查機關方得以取得被告於電子郵件寄、收件人地址、造訪之網頁IP位址等。被告Alba因為曾寄送數則電郵

法院認為個人對於電子郵件寄、收件人地址、造訪之網頁 IP 地址並沒有合理隱私期待，其所取得之資訊為路徑資訊（routing information），非內容資訊，與使用發話撥號記錄器之設備取得通聯記錄，均不構成美國聯邦憲法第四增修條文之搜索」[68]。該案最主要理由是「電子郵件之寄、收件者之帳號資訊及 IP 位址構成位置資訊（addressing information），因之，揭露之資訊未甚於電話號碼之資訊，當偵查機關取得個人所撥打之電話號碼，足以決定該電話號碼所對應之個人或法人等，並無法得知真正通話內容。同樣地，當偵查機關取得個人電子郵件往來之地址或其造訪網站之 IP 位址，偵查機關仍無法取得信件內容或在網站上瀏覽之特定網頁內容」[69]。從而，在 Matish 案，網路使用者應該知悉位置資訊提供給網路服務業者運用，做為指引路徑資訊之特別目的，第九巡迴上訴法院在 Forrester 案業已表示 IP 位置，毋寧是網路使用者自願傳輸給第三人做為引導伺服器之用[70]。這種情形即使針對本案使用 TOR 路由器隱藏自己 IP 位置，也同樣欠缺合理之隱私期待。因為即使使用者對 IP 位置資訊保有主觀的隱私期待，然而依據 TOR 路由器運作模式，此一隱私期待卻非客觀合理的。TOR 使用者，連結網路時，必須揭露 IP 位置資訊給 TOR 節點的營運者，以至於其通訊連結可以達到最終目標點（目的地），在這樣系統運作下，個人必須揭露 IP 位置資訊給完全陌生之人，因之，法院結論認為 TOR 使用者在使用 TOR 網路時，對於自己 IP 位置清楚地欠缺合理之隱私期待[71]。

信件給共同被告Forrester並且上網瀏覽數個製造毒品之網站乃被認定共謀犯罪，其乃以偵查機關違法監控其網路活動違反憲法第四修正案而提起上訴。」事實部分，參閱熊誦梅、溫祖德（2018），〈從馬賽克理論（Mosaic Theory）談通訊使用者資料之法官保留：評智慧財產法院106年度刑智上易字第65號刑事判決〉，《法令月刊》，69卷9期，頁40。

68 熊誦梅、溫祖德，前揭註67，頁40-42。

69 熊誦梅、溫祖德，前揭註67，頁41-42。

70 *Matish*, 193 F. Supp. 3d at 616; *Forrester*, 512 F.3d at 500.

71 *Matish*, 193 F. Supp. 3d at 616.

是而，本案聯邦地方法院及目前聯邦巡迴上訴法院均認為網路使用者，對於個人 IP 位置並無合理之隱私期待，因之，難以主張以植入間諜程式方式取得 IP 位置，構成憲法意義之搜索，縱然欠缺令狀為之，亦非違憲。

六、分析與討論

（一）植入間諜程式搜索取得電腦內容性資訊

偵查機關植入間諜程式遠端搜索究竟是否屬於美國憲法意義之搜索，造成增修條文第 4 條之判斷難題。此種駭客方式取得相對人之電腦資訊設備內資訊，與一般搜索一樣，都是從相對人物理性設備內搜索取得資訊。除此以外，也跟強制網路服務提供者提供資訊共享相同的特徵，也就是對相對人之財產毫無物理性的接觸（或侵入）[72]。從而，國家植入間諜程式涉及發送、利用（植入）、執行、回傳資料，在相對人之電腦設備，植入間諜程式、執行、搜索複製內容後回傳內容性資訊，才構成增修條文第 4 條之搜索、扣押（可見前述四、（五）小結）。更重要的是，儲存於電腦中資訊包含著巨量資訊及個人資訊之敏感內容，2014 年 *Riley v. California* 一案，對於國家執行逮捕，「附帶搜索」行動電話時，在欠缺對於行動電話之搜索令狀而搜索、翻閱蒐集行動電話內儲存資訊時，聯邦最高法院明確表示當執法機關附帶搜索行動電話時，若將行動電話當成是封閉容器，逕行點擊嫌疑人之行動電話內，翻閱蒐集儲存資訊，由於當代行動電話，扮演人類生活重要特徵，行動電話與一般物理性有體物重大差異性質在於，當代行動電話涉及隱私利益遠甚於搜索一包香菸、皮夾及皮包等所牽涉之隱私利益，聯邦最高法院在該案分析行動電話與其他物理性有體物在質與量、負載資訊內容及與一般容器均具有差異性。因此，「附帶搜索」行動電話時，即不再可以適用容器理論，不得將行動電話等資訊載體類比為封閉容器，而得以直接搜索查看其資訊載

[72] Mayer, *supra* note 43, at 594.

體內之資訊[73]，此時對於資訊載體之翻閱蒐集已經另外構成憲法意義之搜索，受到憲法令狀原則之誡命及適用[74]。

在 Riley 案，聯邦最高法院還特別針對當代資訊載體內儲存資訊進行質與量及負載內容分析，首先，聯邦最高法院認為行動電話本身事實上已成為迷你型電腦設備而又同時作為電話使用，並包括眾多功能，如相機、錄影音設備、名片盒、日記等，其中最顯著特徵即為其巨大容量，在行動電話問世前，過去許多人並無法攜帶所有歷來收受的信件，所有照片及所有讀過的文章或書籍，若想要隨身攜帶上述資訊的話，他們必須拖曳著一卡車的文件等，而對這些文件資料的搜索即須有搜索票，方得為之，因此對行動電話隱私之侵害即非等同物理性地受限於其物體之本質[75]。再者，就行動電話負載資訊而言，聯邦最高法院認為「個人從一般到親密生活之各個層面以數位記錄於行動電話內，若容許警方基於例行性基礎得檢視行動電話之生活親密紀錄，即不同於在一般案件容許警方得搜索個人物件之情形，……網路歷史搜尋紀錄可在連結上網之行動電話資訊內取得之，且足以揭露個人之隱私及興趣，甚至個人在網路所逛到之網站，歷史定位紀錄資訊亦成為標準的智慧型行動電話之特徵，且足以重建每個時段個人所在位置，不僅是所在城市，甚至包括所在特定大樓內，當收集或檢視積累的數位資訊即構成搜索。[76]」所以，行動電話負載內容不僅包括以往應在住處方能取得以數位模式儲存的敏感資訊，甚至含括許多無法從住家取得之隱私資訊[77]。最後，法院復就其儲存容量之差異性闡述分析，由於行動電話記憶體使其得以攜帶龐大資訊內容，因此可預見與一般物理性有體物容量之差異性與日俱增[78]。

---

[73] 李榮耕，前揭註9，頁63。

[74] *Riley*, 134 S. Ct. at 2488-95; 溫祖德（2015），〈行動電話內數位資訊與附帶搜索：以美國聯邦最高法院見解之變遷為主〉，《月旦法學雜誌》，239期，頁207-209。

[75] *Riley*, 134 S. Ct. at 2488-95.

[76] *Id*. 聯邦最高法院亦點到在許多行動電話程式軟體或是「apps」提供一系列工具來管理個人生活細節所有詳盡的資訊。

[77] *Id*.

[78] *Id*.

綜上所述，聯邦最高法院認為，自本質上而論，行動電話負載之功能及角色，已非傳統手機之單純功能，其實際上已經等同於隨身攜帶之小型個人手提電腦及資料庫，而非傳統手機或一般物理性有體物可資比擬，自其負載資訊而言，直接涉及個人隱私及個人在網路所有搜尋或所到之處，其記憶體均足以揭露個人隱私及事務，此已非一般單純物理性有體物可資比擬，其內容揭露遠比一般物件之揭露更具有侵害性，而可直接侵犯個人隱私。另外，就儲存容量之特性闡述之，其容量除包括現在資訊，同時包括以往歷史資訊等具有綜合性資訊，自非傳統物理性紀錄或紙本書本日記紀錄可比[79]。以今日來說，毫無疑問的，不僅是行動電話負載資訊質、量及功能，任何電腦等資訊設備之本質及功能（包含負載資訊），遠甚於上述行動電話含載之資訊，國家植入間諜程式進行遠端搜索個人之資訊設備，可說是嚴重侵害個人之生活私密領域及個人資料自主權利。因此，國家以間諜程式駭入人民電腦資訊設備，無論是翻閱、搜找電腦內檔案、內容性資訊，從目標對象電腦回報之資訊可能包括傳輸通訊內容或檔案等，均屬於個人極私密之私生活領域及個人資料自主領域之隱私資訊，屬於個人具有合理隱私期待之資訊，可認為國家駭入行為屬於憲法意義之搜索。

本文另從國家取得儲存於第三人企業之通訊內容，是否受到增修條文第4條隱私權之保護，聯邦巡迴上訴法院已有不少判決，其中指標性判決以聯邦第六巡迴上訴法院曾在 *United States v. Warshak* 案[80]，因為被告經營宣稱有增強性能力的藥品，透過電視等媒體散佈不實廣告，觸犯郵件詐欺等法。偵查中，偵查機關請求調取電子郵件服務提供業者（下稱第三人企業）保存之被告所有電子郵件。被告主張偵查機關電子郵件之調取，實構成憲法意義之搜索及扣押。針對這一個爭點，聯邦第六巡迴上訴法院表示即使由第三人企業，持有保存當事人間已結束通訊之通訊內容，當事人對於電子郵件之通

[79] 溫祖德，前揭註74，頁207-209。

[80] United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010). 關於此案之中文文獻，可參閱李榮耕（2022），〈犯罪偵查中通訊內容的調取〉，《臺大法學論叢》，51卷3期，頁781-788。

訊內容仍保有主觀上之隱私期待，而電子郵件包含著個人生活的全貌、資訊等最為深層及隱密之事項，因此，電子郵件是個人日常生活中重要且必要的工具，如此才能保護個人之間通訊，若由偵查機關向第三人企業取得該等已結束通訊之電子郵件信箱內之通訊內容，該院認為係相當於虛擬之旅館房間或個人住宅，因此，電子郵件之調取，像是對於通訊內容之監察，仍屬憲法意義之搜索，應受增修條文第 4 條之誡命，才能命令第三人企業交付使用者之電子郵件內容[81]。而若將 Riley 案、Warshak 案見解適用於本文所指之國家遠端搜索行為，乃是以更具侵入性方式（駭入），獲取相同資訊，則隱私權受到侵害之本質及程度，有過之而無不及，理當受到相同程度之保護，否則二相比較之下，如果以駭入方式取得資訊反而受到較少之隱私權保護，將造成荒謬之結果[82]。

（二）植入間諜程式蒐集取得 IP 位置資訊

當執法機關植入間諜程式傳送回報之資訊不包括任何內容性資訊時，例如聯邦調查局常用之駭入方式為確認 TOR 使用者身分，亦即主要回報資訊是犯罪嫌疑人 IP 位置，依據以往之聯邦法院見解，個人 IP 位置其實屬於不受憲法保護之非內容性資訊，因此有部分聯邦地方法院認為植入間諜程式遠端搜索方式取得 IP 位置資訊，不受到增修條文第 4 條之保障。而現行美國聯邦巡迴上訴法院在 Forrester 案見解，也認為個人對於造訪之網頁 IP 地址並沒有合理隱私期待，其所取得之資訊非內容性資訊，不構成增修條文第 4 條之搜索。

至於有美國學者之見解，主張 NIT 偵查技術，包括虛擬性侵入電腦資訊設備、植入程式碼而佔據儲存空間，藉此也取得扣押電腦之控制權，而強迫電腦回報確認資訊，因而使偵查機關取得 IP 位置資訊，此已屬於憲法意義之搜索、扣押[83]，固有其論據。不過，本文認為上述學者見解尚待斟酌，

---

81 *Warshak*, 631 F.3d at 284-86.

82 Mayer, *supra* note 43, at 595.

83 Adams, *supra* note 2, at 758-59. 該學者認為「增修條文第4條保護財產權及隱私權，

其在論證上，將植入程式與安裝 GPS 相類比，顯然誤會植入安裝程式，在物理上並未物理性佔據電腦之有形體空間，所以將之類比 Jones 案事實，顯然是無法相類比之案例。況且，因為 IP 位置資訊非屬內容性資訊，依據美國聯邦巡迴上訴法院 Forrester 案見解，也認為個人對於造訪網頁 IP 地址並沒有合理隱私期待，其所取得之資訊非內容性資訊，因此不構成增修條文第 4 條之搜索。

（三）管轄權爭議

上述聯邦調查局執行魚雷行動及撫平者行動，法院暗示搜索地點即可能是目標資訊設備或相關伺服器而由偵查者執行搜索。無論是撫平者行動或魚雷行動，偵查機關僅取得一張 NIT 令狀即對於「所有」連結暗網之資訊設備植入間諜程式。但這些設備其實位於全美各地，因之，被告紛紛提出抗辯主張核發 NIT 搜索令狀之治安法官欠缺管轄權，該等令狀授權搜索的電腦資訊設備其實是司法轄區外之資訊設備，違反治安法官法及聯邦刑事訴訟規則第 41 條(b)規定，搜索令狀構成無效令狀而應排除取得之證據[84]。

當為了蒐集資訊目的，植入間諜程式於電腦資訊設備，NIT程式碼也就物理性佔據私人財產權內，這跟2012年Jones案一樣，聯邦最高法院在該案也認為為了蒐集資訊目的，安裝GPS定位追蹤器於汽車車體，構成憲法意義之搜索。植入NIT程式碼是將間諜程式寫入網頁及傳輸於使用者電腦，NIT程式佔有電腦之物理性空間，屬於憲法保障之財產範圍，並進一步作為蒐集證據資訊所用，所以執行NIT偵查技術，構成憲法意義之搜索。」

[84] 此部分另可見聯邦第三巡迴上訴法院在United States v. Werdene一案，本案NIT令狀在2015年2月20日核發，聯邦刑事訴訟規則第41條(b)(6)於2016年12月1日修訂，本判決所提到之第41條(b)，均為舊法。在該案聯邦調查局執行維州東區法院NIT令狀後，在賓州查獲被告Werdene，並因其持有兒童色情照片違反聯邦法律而遭訴。被告主張令狀核發違反聯邦刑事訴訟規則第41條(b)管轄權要件，因此主張應該排除搜索、扣押之證據及因部署NIT技術揭露之資訊，聯邦地方法院駁回證據排除之聲請，但不認為上述NIT偵查技術構成增修條文第4條之搜索，因為被告對於IP位置，欠缺合理隱私期待，因此NIT偵查行為沒有涉及違憲，而僅為技術上違反，被告上訴主張聯邦地方法院錯誤認定此偵查技術不構成增修條文第4條之搜索。United States v. Werdene, 883 F.3d 204, 206-07, 209 (3d Cir. 2018).

上訴後，聯邦第三巡迴上訴法院認為本案涉及違反刑事訴訟規則第41條(b)及增修

事實上，令狀要件之誡命，包含管轄權之問題，有關於此，涉及到二套法律來源明定管轄區域內治安法官得核發搜索令狀，包括治安法官法及聯邦刑事訴訟規則第 41 條(b)規定。其中治安法官法第 636 條規定，治安法官權力及權力行使受地理上（管轄區域）之限制[85]，聯邦刑事訴訟規則第 41 條(b)則明定上述治安法官其中之一項權力，除有規則第 41 條(b)列舉 4 種例外情況外，治安法官核發搜索財產權令狀之權限限於治安法官之司法轄區內[86]。因此，在增訂聯邦刑事訴訟規則第 41 條(b)(6)遠端搜索之前，治安法官核發 NIT 令狀，確實在地方法院間引發多種不同見解，有法院認為在增修條文第 4 條之傳統架構下，實際搜索之處為 NIT 偵查技術植入之每一部正在運作之電腦資訊設備之所在位置[87]。但多數法院認為 NIT 令狀搜索地點在於政府伺服器及偵查官員所在之位置[88]。

換言之，也有法院實務見解認為 NIT 令狀搜索實際執行處所很可能是植入間諜程式之個別電腦資訊設備實際所在之位置，因此屬於在治安法官之司法轄區外，依據（舊）聯邦刑事訴訟規則第 41 條規定，限制僅有管轄權

條文第4條2個層次問題。首先，依據聯邦治安法官法第636條(a)：聯邦治安法官行使由刑事訴訟規則賦予之權利及義務，限於3種類型管轄區域內：（1）指派任職治安法官之轄區內；（2）法院得發生功能之其他所在；（3）法律授權之其他地方。因此，聯邦治安法官法創造治安法官權力之管轄權限制，因為該法明示獨立限制治安法官權力效力之所在。當第636條(a)明定治安法官之土地管轄權力之效力，聯邦刑事訴訟規則第41條(b)則定義權力之內容。聯邦刑事訴訟規則第41條(b)明定治安法官得核發搜索票搜索、扣押位於管轄區域內之個人及財產。該規則明訂4種管轄權限制之例外。……。很顯然地，本案核發NIT令狀並不符合此等例外，故聯邦刑事訴訟規則並無明示准許轄區內治安法官授權搜索不同轄區之電腦資訊設備。*See Werdene*, 883 F.3d at 210 (“While § 636(a) defines the geographic scope of a magistrate judge’s powers, the Rules of Criminal Procedure—including Rule 41(b)—define what those powers are.”).

85 28 U.S.C. § 636(a).

86 FED. R. CRIM. P. 41(b)(1).

87 United States v. Austin, 230 F. Supp. 3d 828, 832 (M.D. Tenn. 2017).

88 *See* United States v. Jones, 230 F. Supp. 3d 819, 825 (S.D. Ohio 2017), *aff’d*, No. 18-3743, 2019 WL 3764628 (6th Cir. June 27, 2019); United States v. Matish, 193 F. Supp. 3d 585 (E.D. Va. 2016); United States v. Darby, 190 F. Supp. 3d 520, 536 (E.D. Va. 2016), *aff’d per curiam*, 721 F. App’x 304 (4th Cir. 2018).

區域內之治安法官得核發令狀，因之，在舊聯邦刑事訴訟規則適用之下，可能導致治安法官基於目標對象之資訊設備所在位置不明或超出管轄區域而駁回令狀之聲請。也正因為存在著此一治安法官核發 NIT 令狀之管轄權爭議，因而有倡議聯邦刑事訴訟規則增訂遠端搜索及增加管轄權例外條款之規範，茲詳述如下。

參、美國國家植入間諜程式遠端搜索之增訂提案及立法

一、遠端搜索之提案緣由

依據聯邦刑事訴訟規則土地管轄權之劃分，作為限制土地管轄內之搜索，聯邦刑事訴訟規則第 41 條(b)明定治安法官得核發搜索票搜索、扣押位於管轄區域內之個人及財產。治安法官對於管轄區域外搜索令狀之聲請，得裁定駁回之，除非符合下列幾種例外情形，該規則明訂 4 種管轄權限制之例外：（1）執行令狀前，財產權可能移動離開於管轄區域外（規則第 41 條(b)(2)）；（2）為進行反恐犯罪之偵查（規則第 41 條(b)(3)）；（3）於治安法官管轄域內裝置追蹤設備而得以追蹤財產於管轄區域外之移動（規則第 41 條(b)(4)）；及（4）搜索扣押已發生有關犯罪活動之任何地區或對管轄區域外之財產權而非屬美國任何一州或地區者（規則第 41 條(b)(5)）。

但此限制增加國家偵查凡與電子資訊相關犯罪之難題，偵查面臨之狀況即為土地管轄權之限制，當遠端搜索取得電腦儲存資訊或發送監控程式於電腦資訊設備。特別是，搜索令狀需要清楚描述搜索之電腦資訊設備，但是搜索目標電腦資訊設備之所在地其實是不為人知的，主要是網路犯罪者目前都使用複雜的匿名科技，例如，發送詐欺通訊或共享兒童色情之濫用者現在使用代理伺服器，足以隱藏真正的 IP 位置，所以通訊的本身透過代理伺服器，

通訊收到方接收到的也只是代理伺服器的位置，而非原始的真實 IP 位置，所以執法機關無法確認真正的原始電腦實際位置及司法轄區。

審酌上述聯邦巡迴上訴法院對於管轄權之判斷，在在顯示治安法官核發令狀應受管轄權之限制，然而對偵查網路世界之犯罪而言，受限於管轄權限制，治安法官大抵上不被認為可以核發跨越管轄權之 NIT 令狀。而真正促成增訂聯邦刑事訴訟規則第 41 條(b)(6)之規定，其實是源自於發生在德州南區之案例，因檢方聲請令狀遭治安法官駁回，聯邦司法部因而倡議提出增訂聯邦刑事訴訟規則第 41 條(b)(6)之例外規定。茲詳述該案如下。

在 2013 年，某「不確定犯罪嫌疑人」未經同意取得登入 John Doe 電子郵件帳號，進入 Doe 銀行帳戶內詐取財物並將存款轉出國外。該案由德州聯邦偵查機關聲請對於「位置及犯罪嫌疑人均不詳」目標電腦，植入間諜程式搜索資訊（data extraction software），該軟體將有能力搜索電腦硬碟、取得記憶體及其他儲存媒介、啟動電腦內建照相機（取得已經拍攝之相片）、產生調整後帶有經度及緯度之電腦位置及傳輸汲取之資訊給執法人員[89]。但本案德州地方法院治安法官基於下列二點理由，依據聯邦刑事訴訟規則第 41 條規定駁回令狀聲請，表示：1、不符增修條文第 4 條之管轄權要件，裁定理由認為該搜索並非在管轄權區域內，雖然聯邦刑事訴訟規則第 41 條授權可以核發管轄區域外令狀，而有 4 種例外情況，但並不包括本案之遠端搜索對象身分及目標電腦之位置自始即無法特定[90]；2、違反增修條文第 4 條之特定性要件，特別是增修條文第 4 條指的是令狀核發要件，不得未特定描述搜索之地點及扣押之人或物，且聲請機關並未釋明如何發現目標電腦，如何搜索以免偵查機關不法取得其他非犯罪使用者之隱私資訊，而波及其他無辜者，因此違反特定描述搜索之地點或扣押之人或物，而駁回該聲請[91]。治

---

[89] *See In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013); CYRUS FARIVAR, HABEAS DATA: PRIVACY VS. THE RISE OF SURVEILLANCE TECH 216-17 (2018).

[90] *See In re* Warrant to Search a Target Computer at Premise Unknown, 958 F. Supp. 2d 757 (S.D. Tex. 2013)

[91] *See In re* Warrant to Search a Target Computer at Premise Unknown, 958 F. Supp. 2d

安法官也特別解釋，當目標位置不特定時，很有可能鎖定的是無辜者之電腦之風險[92]。

此外，治安法官也認為基於電腦搜索之科技進步，有相當充足理由修訂聯邦刑事訴訟規則之管轄權要件[93]。因上述裁定結果及建議，於 2013 年 9 月，聯邦司法部基於重大公益偵查及追訴使用匿名科技之犯罪者，欠缺遠端搜索犯罪者電腦資訊設備之能力，將無法鎖定犯罪者，因此提出聲請修訂聯邦刑事訴訟規則，建請美國司法會議之刑事規則諮詢委員會，除去妨礙執法機關偵查橫跨多個管轄區之網路犯罪（multi-district internet crimes）之障礙。增訂聯邦刑事訴訟規則第 41 條特別回應偵查機關面臨 2 種限制情形：當令狀應充足地描述應受搜索之目標電腦資訊設備，但並無法查知該電腦資訊設備位置之管轄區域及當偵查需要執法機關協調搜索數個管轄區域內之數個電腦[94]。

因此，當不知所在電腦資訊設備位置，使得偵查者發送電子郵件，遠端植入軟體於電腦資訊設備，接收電子郵件、確認真實 IP 位置或設備端中之確認資訊。聯邦司法部也提供數個宣誓證言證明此種情況之真實性。而在實務上，雖然有部分法官核准此等令狀之核發，仍然有法官基於土地管轄權之理由，以搜索資訊設備之電腦所在不明，駁回遠端搜索令狀之聲請，該法官並提出建議修訂土地管轄權之限制，來因應科技進步之趨勢[95]。再者，在數個地區，使用多臺電腦作為犯罪計畫之一部分，因為日漸增加的線上犯罪包括以殭屍病毒秘密地感染攻擊數臺電腦，而此為犯罪個體或犯罪團體基於遠端命令進行整體電腦損害之命令及控制，包括對於政府及商業、家用電腦之

757-59 (S.D. Tex. 2013); FARIVAR, *supra* note 89, at 217.

92 *See In re* Warrant to Search a Target Computer at Premise Unknown, 958 F. Supp. 2d 759 (S.D. Tex. 2013).

93 FARIVAR, *supra* note 89, at 218.

94 THOMPSON II, *supra* note 7, at 4; Raman, *supra* note 8, at 64.

95 Sara Sun Beale & Nancy King, *Rule 41 Memo to Members of Criminal Rules Advisory Committee*, Advisory Committee on Criminal Rules (Mar. 16-17, 2015).

破壞。此外，殭屍病毒並竊取個人及財務資訊、操作大規模之服務攻擊之否定或拒絕，而散布侵害主控電腦使用者隱私之間諜軟體[96]。

本次增訂修法之提案委員會及聯邦司法部宣稱增訂規則第 41 條(b)(6)之部分，使檢察官得以訴追使用匿名化科技犯罪者，也解決對於源自於多個管轄區域之多部電腦資訊設備發動之殭屍病毒攻擊[97]。而諮詢委員會也特別表明草案僅有針對現行管轄權限制部分進行修訂，偵查機關聲請遠端搜索時仍需滿足憲法令狀要件[98]。增訂後，犯罪活動可能發生所在任何地區之治安法官有權核發符合新法所定要件之令狀，2016 年 4 月，聯邦最高法院將增訂之規則提交國會，最終國會根據規則生效法（Rules Enabling Act），使該規則於同年 12 月 1 日生效[99]。值得注意的是，這不代表該規則已通過憲法審查，其合憲性與否，依據修法諮詢委員會之註釋，仍留待法院或聯邦最高法院解決[100]。不過可以確定的是，聯邦刑事訴訟規則既已經通過此一規則，治安法官即得依授權核發遠端搜索之令狀。

二、對於提案之反對意見

對於上述提案，科技業巨擘企業如谷歌等及美國有力之民權組織（American Civil Liberty Union，下稱 ACLU）均表達高度關切，認為草案擴張國家偵查權限，如同草案全面性變革立法，嚴重涉及侵害個人隱私，應該屬於國會立法之範疇，一如以往幾部關於隱私權之立法，如國外情報監聽法、1968 年之綜合犯罪控制與安全街道法案（包含聯邦監聽法）、聯邦儲存中通訊法或愛國者法案等[101]。大部分反對本草案意見均認為草案條文將削弱或

---

96 *Id*. at 2-3.

97 Raman, *supra* note 8, at 179-235.

98 *Id*. at 155.

99 Adams, *supra* note 2, at 741.

100 Legal Information Institute (LII), FED. R. CRIM. P. 41 Committee's Note on Rules 2016 Amendments, https://www.law.cornell.edu/rules/frcrmp/rule_41 ("The amendment does not address constitutional questions.").

101 Beale & King, *supra* note 95, at 3.

放寬增修條文第 4 條對於個人隱私之保障，授權由已發生犯罪行為相關轄區之法院得核發令狀[102]。外界對於本草案之反對意見，主要分述如下：

1. 令狀核發違反特定性要件

增修條文第 4 條明定「人民對個人人身、住宅、文書或物件享有受保護之權利，不受不合理搜索及扣押，並不得違反之；令狀核發，非基於相當理由，並經宣誓或代誓宣言及明載特定之搜索地點及扣押之人或物外，不得為之」。乃憲法禁止國家不合理搜索及扣押行為，同時宣示令狀記載應符合特定性原則，為美國憲法誡命及要求。早在草擬憲法該條時期，制憲者即意在禁止核發概括令狀（general warrant），概括令狀僅僅特定一個犯罪，而關於何犯罪嫌疑人應遭逮捕及應該搜索之地點均保留裁量權給執法官員[103]。而最高法院解釋特定性要件，依據 *Dalia v. United States*[104]案，要求令狀應具備下列三個要件，以免造成無效的概括令狀原則，第一、令狀應由中立、無特定利害關係之治安法官核發；第二、聲請令狀者應向治安法官展現其相當理由相信搜索之證據得以協助特定犯罪嫌疑人之特定犯罪之逮捕或定罪；第三、令狀必須特定描述應扣押之物件及應搜索之地點[105]。這個要件也是制憲者設計避免作為非常廣泛而探索性的搜索（exploratory searches）[106]。

但是如果犯罪者使用匿名科技方式，因為無法具體明載特定之搜索地點（財產）或扣押之人或物在特定司法轄區內，將可規避遠端搜索令狀之核發

---

102 *Id*. at 4.

103 Steagald v. United States, 451 U.S. 204, 220 (1981).

104 Dalia v. United States, 441 U.S. 238, 255-56 (1979).

105 *Id*. (quoting Stanford v. Texas, 379 U.S. 476, 485 (1965)) (“Nothing in the language of the Constitution or in this Court's decisions interpreting that language suggests that, in addition to these requirements, search warrants also must include a specification of the precise manner in which they are to be executed. On the contrary, it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant -- subject to the general Fourth Amendment protection "against unreasonable searches and seizures.”) *see Dalia*, 441 U.S. at 256-57.

106 Maryland v. Garrison, 480 U.S. 79, 84 (1987).

[107]。然而，植入間諜程式進行遠端搜索之草案條文，並未明載令狀如何記載特定性所要求之遠端搜索電子儲存媒介或扣押、複製電子儲存資訊。美國知名的民權團體 ACLU 即提出二次評論意見，表示水坑技術（watering hole）攻擊，利用網站發送間諜程式植入到造訪者電腦，政府終將搜索原本無法特別特定或描述之私人電腦，同時擴及於欠缺相當理由之對象[108]。另外，對於未知犯罪嫌疑人之不特定人數，該如何符合增修條文第 4 條特定性要件，且增訂條文將提供執法機關規避增修條文第 4 條之機制，導致規避其他法律監督規則，甚至當對特定目標（收件人）將電子郵件附載連結，轉發於無辜第三人（且為偵查機關欠缺相當理由之人）[109]，都屬侵害人民權利之執法。對於草案第 41 條(b)(6)(B)有關殭屍病毒之部分，民權團體也表示修正草案將使執法機關「一票搜索多機」，形成一紙令狀搜索多臺電腦，也就造成沒有辦法描述搜索特定之電腦，或者對於使用者釋明相當理由[110]。此也違反聯邦巡迴上訴法院曾經表示搜索多個地點之搜索令狀，治安法官應謹慎分別地評估個別地點，必須包含足夠之相當理由以證明對每一個人或地點核發之理由[111]。

知名的谷歌企業對於草案表示谷歌的任務在於組織全球性資訊並使資訊在世界各地接近使用，所以其有重大利益保護使用者及確保基礎架構之資訊安全，因之，認為該草案造成一系列重大憲法上、法律上及政治上關切，而最妥適及必要的授權條款，應該是國會制定法律[112]。谷歌企業另認為條文中並未限制或特定搜索如何進行，同時當進入媒介物或資訊位置時，精確的

---

107 Beale & King, *supra* note 95, at 5.

108 ACLU, *supra* note 41, at 21-22.

109 *Id*.

110 *Id*.

111 Greenstreet v. County of San Bernardino, 41 F.3d 1306, 1309 (9th Cir. 1994).

112 Richard Salgado, *Google Inc. Comments on the Proposed Amendment to Federal Rule of Criminal Procedure 41*, Google Inc. (Feb. 13, 2015), http://s3.amazonaws.com/s3.documentcloud.org/documents/1672788/13feb2015-google-inc-comments-on-the-proposed.pdf.

搜索物件或扣押對象得以搜索並不特定。當偵查機關聲請搜索之位置、搜索方式或範圍不能特定時，即不符合特定性要件[113]。

2. 令狀核發應限於重大犯罪要件

刑事辯護人國家協會（National Association of Criminal Defense Lawyers）特別表示網路搜索應該限於重大犯罪始能為之，而不該適用於所有一般犯罪類型之犯罪[114]。

3. 遠端搜索應仿照聯邦監聽法由國會立法為之

谷歌表示此等重大立法，應該要仿照聯邦監聽法之規範，因為使用科技偵查技術之能力而進行如此侵入性的搜索，以往例如國外情報監聽法，依據美國法典第 1804 條，明定執法機關具有監視及蒐集國外情報資訊之能力；又例如 1968 年之綜合犯罪控制與安全街道法案（包含聯邦監聽法），於美國法典第 2518 條明定執法機關得以法律上截聽有線、口頭及電子通訊之資訊；此外，依據聯邦儲存中通訊法之規定，第 2701 條明定偵查機關有權力去合法接近取得電子儲存之通訊；最後是如愛國者法案，依據美國法典第 1842 條規定，偵查機關得以合法攔截現時電話之後設資料[115]。於通過此等法案，國會才能夠以公開辯論方式衡量各式憲法上價值問題決定立法。所以，谷歌主張是立法機關，而非以制定聯邦刑事訴訟規則方式，才足以衡酌平衡偵查機關之需求，同時考量重要憲法上及政策上之考量[116]。

---

113 *Id*.

114 Peter Goldberger, *Comments of the National Association of Criminal Defense Lawyers on the Proposed Amendment to Rule 41*, National Association of Criminal Defense Lawyers (Feb. 17, 2015), at 2-3, 5, http://www.nacdl.org/getattachment/8c63efe9-7282-4e2f-a5c7-ad17a0212f30/nacdl-comment-crimr41.pdf.

115 Salgado, *supra* note 112, at 5.

116 *Id.* at 6.

4. 應遵守最後手段性原則及最小侵害性原則

偵查機關應被要求符合最後手段性原則，也就是說遠端搜索應以原則上不能以其他偵查方法蒐集取得資料時或已經用盡其他偵查手段時，方得為之[117]。其次，使用截聽非必要性的通訊內容，必須採取最小侵害原則（minimized）[118]。最後，有論者認為缺乏透明性及最小性原則，將使法官無法適當地評估使用遠端搜索技術之潛在使用[119]。換句話說，令狀聲請時，應該要載明有必要使用遠端搜索之科技手段，若非不能以其他偵查方法蒐集取得資料時，難謂有核發遠端搜索令狀之必要，聲請機關必須明載釋明最後手段性，治安法官方能審查是否具有核發之必要性。

5. 暗中植入搜索涉及侵入性、毀損性之本質

多數評論強調遠端搜索之危險，可能造成不可預測、全面而廣泛且嚴重地損害。而且損害所及之資訊設備，不是只有設備本身、對於資訊及系統本身也都將造成損害[120]。民主科技中心表示執行遠端搜索令狀之結果，將變得非常困難去預測，也可能變得非常嚴重，侵入性行為可能涉及設備、資訊及依賴系統之損害，這不僅僅造成立即之損害，也因為系統中逐漸增加之脆弱性而造成更進一步之損害[121]。同樣地，ACLU 也表示遠端搜索足以弱化設備，並且曝露資訊設備於損害之中，而且國家未必具有科技優越性之紀錄，承認遠端搜索將造成國家對於一般通用軟體及硬體（common software and hardware）科技脆弱性之濫用，反而不是主動去通知此等科技製造商對於科技脆弱性部分之修正或改變[122]。

---

117 *Id.* at 9; 18 U.S.C. § 2518.

118 *Id.* at 9; 18 U.S.C. § 2518.

119 Laura Donohue, Remarks at Panel on the Legal and Policy Implications of Hacking by Law Enforcement, at 21: 40 (Mar. 4, 2014), https://vimeo.com/88165230.

120 Beale & King, *supra* note 95, at 16; Salgado, *supra* note 112, at 9.

121 *Id*.

122 Beale & King, *supra* note 95, at 16.

綜上所述，對於新增遠端搜索之反對評論者認為遠端搜索議題，極具敏感性，應該透過正式國會的立法程序，而非透過聯邦執法機關之法規則造法程序，既然國會尚未通過授權可以跨越管轄區域或同時授權多個管轄區域之電腦搜索，包括隱藏電腦位置或偵查美國法典第 1030 條(a)(5)案件，因此聯邦刑事訴訟規則等於擴張治安法官之權限，而非如以往須由國會立法方得以完成之立法行為，從而，此等修法建議應該是以國會立法處理而非司法規則造法而為之[123]。直言之，聯邦刑事訴訟規則草案形式上增加治安法官核發搜索令狀之例外規定，但實際上該規則第 41 條(b)(6)條文內容又增加遠端搜索（remote access to search）之法條文字，而此一法文增訂之遠端搜索內容即等同於實質增訂新類型科技偵查處分。復以，承如本文貳、六分析與討論，此種新興科技偵查，足以造成嚴重侵害人民隱私權之本質及其干預手段足以蒐集巨量資訊之性質，在侵害手段及蒐集資訊二方面言之，遠甚於傳統監聽之強制處分。質此，確實誠如上述各種反對或質疑聲浪，應該以國會詳盡立法為之，方屬妥適。

肆、美國國家遠端搜索之新法分析

一、聯邦刑事訴訟規則以管轄權為由增訂之遠端搜索

正因為駭客等犯罪者得以隱身於網路後，使得偵查機關本質能力與法規上蒐集證據之權限產生不小差距。再者，網路犯罪常跨越邊境，甚至及於無管轄權之域外，而執法者卻仍須遵循物理世界之規範，否則無法蒐集取得證據，如此一來造成利用網路犯罪者與執法能力間之差距。以現行聯邦執法言之，依據原本聯邦刑事訴訟規則第 41 條之規範，原則上搜索票由被搜索人

[123] CENTER FOR DEMOCRACY & TECHNOLOGY, WRITTEN STATEMENT OF THE CENTER FOR DEMOCRACY & TECHNOLOGY BEFORE THE JUDICIAL CONFERENCE ADVISORY COMMITTEE ON CRIMINAL RULES (Oct. 24, 2014), http://cdt.org/wp-content/uploads/2014/10/CDT-Rule41-Written-Statement-final-20141024.pdf.

或財產所在之管轄區域內，或犯罪行為發生地之治安法官，核發搜索令狀，治安法官不得核發管轄區域外遠端搜索令狀，除聯邦刑事訴訟規則第 41 條(b)(1)至(5)臚列 4 種例外情形外，搜索令狀效力僅及於治安法官管轄區域內[124]。上述例外，沒有放寬監視網路數位犯罪之管轄權要件，反而更凸顯創造管轄權例外之需要[125]。透過美國司法會議之刑事規則諮詢委員會在 2016 年，於聯邦刑事訴訟規則增訂第 41 條(b)(6)，以便從事發掘並偵查網路犯罪集團[126]，放寬對於聯邦偵查機關之限制，擴大對於匿名電腦攻擊者之電子設備遠端搜索之搜索令狀之管轄權範圍[127]。

本次增訂刪除部分管轄權限制，容許遠端搜索電子儲存資訊，澄清跨管轄區域遠端搜索之合法性。但基於遠端搜索令狀涉及增修條文第 4 條搜索未知電腦設備及其所在位置之情形，因此，提出之增訂案，主要是用以解決下列 2 個問題：一、對未知電子資訊設備所在地之位置資訊取得；二、在多個管轄區域內，取得多個電腦資訊設備之資訊爭議[128]。以下針對聯邦刑事訴訟規則增訂第 41 條(b)(6)規定詳盡論述修法增訂目的、運作及內容。

二、聯邦刑事訴訟規則增訂之規範內容

首先，該條規定具有下列 2 種情形之一時，在任何發生犯罪活動之有關轄區內，該管治安法官，有權核發令狀，授權使用遠端搜索（remote access to search）電子儲存媒介或扣押、複製在管轄區域內、外之電子儲存資訊。

---

124 *See* FED. R. CRIM. P. 41(b)(1)-(5). 4種例外。

125 Lerner, *supra* note 45, at 29.

126 關於網路駭客及駭客激進主義分子的新聞，佔據各大新聞媒體，例如，癱瘓1500臺五角大廈電腦、駭入JPMorgan公司8300萬客戶個資、甚至操縱股價、滲入投票人系統及對於醫療系統進行勒索。*See Whacking Hackers*, NEWSWEEK (Oct. 9, 2007, 11:18 AM), https://www.newsweek.com/whacking-hackers-103531; Pete Brush, *Israeli Suspects in Giant JPMorgan Hack Deny Charges in NY*, LAW 360, (June 9, 2016, 07:03 PM), https://www.law360.com/articles/805660/israeli-suspects-in-giant-jpmorgan-hack-deny-charges-in-ny.

127 Lerner, *supra* note 45, at 5.

128 THOMPSON II, *supra* note 7, at 5.

第一種情形，（A）當電子媒介或資訊所在位置，遭以科技方式隱藏（隱匿）之；或第二種情形，（B）正在偵查電腦犯罪（18 U.S.C. § 1030(a)(5)）中，對於位於 5 個或以上不同轄區內，在未經授權下，對受保護電腦進行損害[129]。因之，其適用 2 種情形，一為當犯罪人使用科技方式隱藏自己電腦資訊設備之位置；二為涉及電腦駭客之犯罪，而電腦位於 5 個或以上司法轄區內，對該等電腦資訊設備進行攻擊損害。

（一）授權要件

1. 使用科技方式隱藏自己電腦設備之位置

第一部分適用之情況在當檢察官得以描述搜索之電腦資訊設備，卻不知道電腦資訊設備所在位置，司法部表示政府面對之難題是在網路世界犯罪者，絕大多數正在使用匿名軟體，而無法查知所在位置時，犯罪者得以隱藏自己的 IP 位置，如前述德州南區地方法院裁定反而係增訂聯邦刑事訴訟規則第 41 條(b)(6)規範之催化劑，因此增訂條文如下：在任何發生犯罪活動之有關轄區內，有權限之治安法官，得核發遠端搜索令狀搜索電子儲存媒介及扣押令狀或複製電子儲存資訊，而無論是位於轄區內或轄區外者，只要該電子媒介或資訊所在之地點業經科技方式加以隱藏。因此本款之增訂同時解決以任何種類科技隱藏電腦儲存資訊設備位置之所在（亦即電子儲存資訊媒介設備所在位置）。至於涉及增修條文第 4 條之問題，則交由判例法持續發展解決之。

本條檢察官應該要證明二要件，一為犯罪活動已經發生；二為電子媒介或資訊所在之地點業經使用科技方式加以隱藏[130]。因此，此增訂條文所明文的遠端搜索，是原本現行規則所未授權之偵查行為。特別需要解釋的是，電子儲存媒介或資訊所在之地點業經使用科技方式加以隱藏自己電腦資訊設備之位置，以目前科技言之，有 3 種方式屬於容易取得之強化隱私科技之方式，包括代理伺服器、虛擬隱私網路（Virtual Private Networks；VPNs）及

---

[129] *See* FED. R. CRIM. P. 41(b)(6).

[130] THOMPSON II, *supra* note 7, at 5-6.

加密匿名瀏覽器（TOR），使用此 3 種方式中任何 1 種於電子資訊設備，均足以滿足上述要件「使用科技方式隱藏自己電腦設備之位置」[131]。茲分述如下：

首先，代理伺服器，是政府機關、私人機構及學校廣泛使用之設備，其作為資訊發送端與接收端中介點之電腦服務，使用者造訪之網站及網路服務提供業者，只能被以代理伺服器之資訊呈現於外界。第二、虛擬隱私網路，具有能夠在自己的設備內發送及接收資料的能力之科技設備之集合，若為敏感性資料，也可以因為加密而受到更高程度之保護免除外界察覺，使資料能在次級傳輸網路之間安全傳輸，縱使以駭客方式想要探索內容也只能看到加密資料[132]。第三，洋蔥伺服器，通常是暗網中透過洋蔥式迴路（the onion router）才能夠接近使用之網路世界，破解洋蔥伺服器之隱蔽能力需要非常大量之時間及高級科技才能突破，使之居於聯邦執法機構執法之災難根源[133]。透過洋蔥伺服器，在 2015 年，每天約有 200 萬人上線使用，使之居於匿名性科技使用之首選，該平臺避免秘密監視者得以確認上網人及使用人、造訪之網站。此外該平臺上面之資訊，屬於重度點對點加密，只能在每個節點解開，並隨即往目的地傳輸，被加密的資訊只能從一個端點到另個端點被看到而已[134]。此外，洋蔥伺服器不僅可以使得造訪者以匿名方式在網路上閱覽資訊，也可以使主持者隱匿閱覽內容，形成暗網（dark website）[135]。

綜上所述，透過上述隱身自己的科技，使得執法機關在偵查使用者身分及使用者位置困難重重，更遑論法律規定搜索時需由土地管轄權之治安法官

---

131 Adams, *supra* note 2, at 734.

132 Paul Ferguson & Geoff Huston, *What Is a VPN?*, http://www.potaroo.net/papers/1998-3-vpn/vpn.pdf.

133 直到2012年聯邦執法機構才破解洋蔥伺服器之運作；Kevin Poulsen, *The FBI Used the Web's Favorite Hacking Tool to Unmask Tor User*, WIRED (Dec. 16, 2014, 7:00 AM), http://www.wired.com/2014/12/fbi-metasploit-tor/.

134 Adams, *supra* note 2, at 735-36.

135 *Id.* at 736. 在隱藏式服務下，個人可以經營自己的政治理念部落格，或提供販賣武器、非法毒品或兒童色情的市場。

核發搜索令狀方得以核發搜索令狀之限制，而這也成為增訂治安法官核發令狀管轄權例外條款最主要之原因。

2. 針對電腦犯罪行為，對於 5 個或以上轄區之電腦資訊設備進行攻擊損害

第二部分增訂目的在於電腦犯罪行為，特別是美國法典第 1030 條(a)(5)之犯罪，攻擊多數管轄地區之多臺電腦資訊設備，在偵查此種犯罪之本質，為減輕需向多個管轄法院聲請多張令狀之程序（負擔），授權容許單一法官監督此種偵查行為及令狀聲請。在違反電腦詐欺與濫用法犯罪（Computer Fraud and Abuse Act；CFAA），特別是透過殭屍病毒攻擊電腦之犯罪[136]，以惡意病毒感染電腦網絡，同時藉由一個控制機制或主人同時下達指令，而傳送病毒給他人或創造虛假網路交通或植入間諜程式藉以蒐集個人資訊，一個殭屍病毒得以同時命令超過 1200 萬隻殭屍病毒，進行大規模之拒絕服務之攻擊、搜取個人及財務資料及散佈惡意軟體藉以侵入個人電腦之使用者隱私，對公眾足以造成重大威脅[137]。

聯邦調查局可以從受感染電腦之病毒獲得資訊或傳佈資訊，警告使用者殭屍病毒、提供指令以決定渠等設備是否受到感染，甚至發送癱瘓（disabling）殭屍病毒指令，徹底移除殭屍病毒[138]。因此執法機關認為遠端搜索對於通知被害人、確認其他被害人及鎖定犯罪行為人，干擾指令及控制殭屍病毒功能具有重要性。正因如此，增訂聯邦刑事訴訟規則第 41 條，使政府機關得以尋求一個管轄區域之法院授權，而同時偵查橫跨數個管轄區域之電腦犯罪活動。因之，在違反美國法典第 1030 條(a)(5)之犯罪，偵查攻擊受保護電腦資訊之媒介，在未經授權下，對位於 5 個或更多之管轄區域內之電腦資訊設備進行攻擊，則有授權使用遠端搜索之需要。

---

136 Lerner, *supra* note 45, at 30, 31-32.

137 *Id.*; Raman, *supra* note 8, at 172.

138 Kim Zetter, *With Court Order, FBI Hijacks 'Coreflood' Botnet, Sends Kill Signal*, WIRED (Apr. 13, 2011, 6:17 PM), https://www.wired.com/2011/04/coreflood/.

（二）增訂合理努力之通知要件規範

依據聯邦刑事訴訟規則第 41 條(f)(1)(C)明定一般搜索之通知要件，執行令狀執法人員應給予令狀複本及因搜索而扣押財產之收據[139]。新增遠端搜索規範修正第 41 條(f)(1)(C)通知要件，意在確保偵查機關「應盡合理努力」送達遠端搜索令狀複本於受搜索人（the person whose property was searched）、受扣押人或資訊被扣押或複製者（whose information was seized or copied）[140]。該條並特別論及送達方式應合理計算以通知相對人（reasonably calculated to reach that person）。此外，通知得以任何方式完成之，包括電子方式及上述合理計算送達該人之方式為之[141]。另外，也需要製給收據給資訊遭扣押或複製或財產遭受搜索或持有被扣押或複製資訊之人[142]。

（三）延期通知規範

基於偵查機關之請求，治安法官或基於同規則第 41 條(b)授權，州法院之記錄處法官得延後本規則要求之通知，只要該延後通知是法律明定者[143]。

（四）小結

綜合上述，遠端搜索之規定，聯邦刑事訴訟規則通過增訂的條文，其實僅區區二條之規定，一條是針對得以發動遠端搜索之授權要件，另一條則是

---

139 *See* FED. R. CRIM. P. 41(f)(1)(C).

140 Committee Notes on Rules-2016 Amendment.

141 *See* FED. R. CRIM. P. 41(f)(1)(C) (“For a warrant to use remote access to search electronic storage media and seize or copy electronically stored information, the officer must make reasonable efforts to serve a copy of the warrant and receipt on the person whose property was searched or who possessed the information that was seized or copied. Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person.”).

142 Committee Notes on Rules-2016 Amendment.

143 *See* FED. R. CRIM. P. 41(f)(3).

增訂應盡合理努力之通知要件規範，嚴格言之，依據增訂理由所示，前者，是針對管轄權增訂例外規定，授權治安法官得對於管轄區域外之電腦儲存資訊設備核發搜索及扣押令狀並複製電腦儲存資訊。另外，該條文確實針對 2 種情況，明定核發遠端搜索之令狀，因此實質上等於在同條 41(b)(1)-(5)承認之搜索類型（一般搜索、核發令狀後財產權移出於管轄區外、針對國內、國際反恐犯罪之犯罪行為之搜索令狀、安裝追蹤器追蹤令狀）外，增加承認新型科技強制處分。就增訂之法律規則之評析，本文分析如後。

其次，由於增訂條文，並沒有另外針對遠端搜索令狀之相當理由、搜索令狀之特定性要件記載、令狀執行期間、令狀之繳回、蒐集資料之保存及銷毀等另行規範，顯然訂定聯邦刑事訴訟規則委員會將遠端搜索令狀之其他要件，比照適用同條關於搜索令狀之其他要件。因此，本文鑒於增訂規範內容僅及於以上論述之部分，且就核發搜索令狀之其他要件，國內學界之研究文獻，已有詳盡之論述，爰不再贅述之。以下，將針對新訂之遠端搜索進行分析與討論。

三、國家遠端搜索之規範評析

雖然聯邦司法部以推動聯邦最高法院修訂聯邦刑事訴訟規則方式，來因應高科技犯罪之新興犯罪手段及擴充國家偵查工具，但正如同大法官 Alito 在 Jones 案所述，因應科技巨變，關心隱私權最好的解決方式可能是立法權[144]。聯邦最高法院已曾在 *City of Ontario. Cal. v. Quon*[145]案則表示在新興科技處於社會的角色變得清楚以前，司法權冒著錯誤的風險，過於詳盡闡述增修條文第 4 條對於新興科技的啟示。而新興科技偵查手段應該由國會衡量憲法及政策上相互競爭的利益，進行造法形塑國家得以發動遠端搜索之要件、配套措施及法律監督等事項。喬治歐維爾於 1984 年的知名著作 dystopia，描述著從未停止監控的老大哥（國家），有學者即比喻本次聯邦刑事訴訟規則之增訂將使小說的描述成真，特別是遠端搜索使得國家得透過一張令狀即

144 *Jones*, 132 S. Ct., at 964.

145 City of Ontario. Cal. v. Quon, 560 U.S. 746, 759 (2010).

授權執法人員可以遠端搜索、同時搜索、扣押及複製來自於多個管轄區內無限數量之未知電腦資訊設備內資訊。本次增訂毫無限制之管轄權條款，也因而引發究竟增修條文第 4 條之令狀要件如何適用於如此全面性的搜索[146]。以下針對增訂之遠端搜索，將造成重大憲法及法規範上之關切，分下列數點進行分析、檢討，也唯有先進行檢討之後，於建構我國法規範，才能夠訂定更完善之立法規範。

（一）植入間諜程式得構成不合理之搜索

聯邦最高法院曾在多數案件表示在實體世界的搜索，不得以太過侵入性、毀滅性及危險性，否則難被認定為增修條文第 4 條之合理性。在 *United States v. Ramirez* 案即指出，增修條文第 4 條之合理性之一般標準取決於令狀執行之方法。在執行搜索程序中，過度及不必要之毀損財產權，得認違反增修條文第 4 條，縱使以合法方式進入財產權，且搜索取得之證據並不受證據排除之[147]。在過往案例，聯邦最高法院曾表示以外科手術方式從犯罪嫌疑人身體取出證據，或者是以閃爆彈方式欲進入人民住宅搜索（並且深知此種方式將很可能引燃火災），均屬於增修條文第 4 條之不合理搜索[148]。同樣地，在網路世界裡，植入間諜程式也帶來相同地關切，當國家植入間諜程式時，國家也難以控制誰得以對於傳輸過程中程式碼擷取之、植入軟體是否能夠正確無誤地植入目標電腦資訊設備、是否會遭其他人複製或重複使用及軟體是否在網路上散播病毒及對無辜之人及商業造成損害[149]。上述考量，確實可以預見，而可能是遠端搜索之自然結果。

---

146 Adams, *supra* note 2, at 727.

147 United States v. Ramirez, 523 U.S. 65, 71 (1998).

148 Winston v. Lee, 470 U.S. 753, 759, 766-67 (1985); Estate of Bing *ex rel.* Bing v. City of Whitehall, Ohio, 456 F.3d 555, 570 (6th Cir. 2006).

149 ACLU, *supra* note 41, at 17. 事實上，美國及以色列曾經對伊朗之核子增生機構（nuclear enrichment facilities）發動網路攻擊軟體（Stuxnet），該病毒軟體快速地散佈到整個電腦系統，甚至主要的美國大企業，例如雪佛龍（Chevron）發現該病毒軟體感染其公司的網路脈絡。*See also* Rachael King, *Stuxnet Infected Chevron's IT Network*, WALL STREET JOURNAL (Nov. 8, 2012, 3:11 PM),

更廣泛地說，使用間諜程式比起其他種類搜索或蒐集資訊更具侵入性，因為運用之後帶來之附帶損害及結果，具有本質上不可預測及無可回復之損害，秘密植入可能造成原本無法預測之後果。更甚者，間諜程式可能造成電腦系統許多無法預見的失靈，導致跟國家搜索完全無關之財產權損失，無論出於設計不良（poor design）或與目標電腦之其他軟體之相容性反應，因而造成運作系統之資料損失或汙染（corruption of the operating system）[150]。

（二）植入間諜程式監視可能進行監聽，非得以搜索令狀授權為之

根據遠端搜索執行方式及蒐集資訊，遠端搜索可能涉及原本應該受到更嚴格審查程序及要件限制之監聽強制處分。舉例來說，若國家植入間諜程式目的在於啟動目標電腦通訊設備（如麥克風），蒐集當事人之通訊內容（包括電子或有線或網路電話），則國家之偵查手段應受到聯邦監聽法規範（Title III, Wiretap Act）[151]。依據美國聯邦監聽法規定，當國家即時監聽有線、言詞或電子通訊時，適用聯邦監聽法規範，因此當電子監聽出現，需要賦予特別的保障，包括聲請機關應特定監視對象或監聽號碼、聲請機關已經使用其他偵查手段而無效（最後手段性原則）、法院應限制監聽期間及禁止無關聯性通訊內容之最小侵害原則[152]。再者，針對監聽令狀之聲請，每一個案向法院聲請監聽令狀前，聯邦司法部刑事執法辦公室（DOJ's Office of Enforcement Operations）會審查每一個案監聽令狀之聲請，確保聲請合於法規要求及聯邦司法部政策[153]。

同樣地，使用間諜程式進行監聽（包括網路監聽），開啟目標電腦之麥克風或來電或撥出電子或有線通訊而監聽內容，也受到相同限制。換言之，當政府之遠端監視是以間諜程式開啟目標電腦之網路監視、網路監聽，毫無

---

http://www.wsj.com/articles/BL-CIOB-1156.

150 ACLU, *supra* note 41, at 18.

151 ACLU, *supra* note 41, at 19.

152 18 U.S.C. § 2518(1)-(5).

153 H.R. REP. No. 112-546, at 10 (2012).

疑問地，則須受到更高程度之限制及聯邦法律之限制（例如，聯邦監聽法）。復以，本文前述之遠端搜索足以造成目標電腦無可預測及無法回復之損害，得以構成不合理之搜索，如果要降低或減少不可預測之損害，需要顯著之技術專業，國家發展或部署之遠端搜索程式之管制方式也應該被管制，此應由立法進行造法，包括規制及限制非常具有爭議性的搜索技巧[154]，而以目前先採取刑事訴訟規則第 41 條之增訂，同樣地也將促使違反聯邦監聽法之可能性而已。

（三）遠端搜索違反增修條文第 4 條令狀特定性要件

遠端搜索將容許執法機關持單一令狀遠端搜索不特定多數人之電腦，而此一令狀卻無需要特定描述搜索目標電腦及證明對於所有電腦之所有人或使用者具有相當理由。以往依據聯邦最高法院建構增修條文第 4 條之法論理，令狀未明確記載特定搜索處所及特定扣押物為無效令狀[155]，特別是在物理性侵入搜索（physical searches）理論，原則上是對一個住宅或建築物之搜索令狀，若該住宅或建築物內若有多個獨立財產權，則一般搜索原則應特定個別之財產權為搜索客體，才能符合令狀之特定性要件[156]。同樣地，在相當於物理財產權之數位財產權概念之下，也應適用相同原則。而授權不特定目標電腦資訊設備及不特定對象之遠端搜索，違反令狀特定性要件，首先，國家在特定網站或伺服器安裝間諜程式，散佈植入任何造訪者電腦間諜程式，因而終將可能搜索執法機關無法特定確認或描述之電腦資訊設備及對欠缺相當理由之目標電腦資訊設備進行搜索。

再者，此等網站也可能由媒體、研究者、政策制定者及律師成員造訪，用以報導、研究，此等以合法目的或根本非執法機關目標對象，與恐攻、網路罪犯及販毒者造訪此等不法網站之目的不同，若果真授權安裝間諜程式，

---

154 ACLU, *supra* note 41, at 20.

155 Groh v. Ramirez, 540 U.S. 551, 557 (2004).

156 Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A general Approach*, 62 STAN. L. REV. 1005, 1045 n.173 (2010).

毫無疑問地，將會使搜索及於無辜第三人之電腦[157]。質是，偵查機關可能會搜索無犯罪嫌疑之人、特別是具有充足理由造訪該網站及毫無相當理由可信為從事犯罪之人[158]。因此，遠端搜索之令狀，記載無法明確，不但違反令狀特定性要件，更將可能導致侵及無辜之第三人。

（四）遠端搜索可能違反增修條文第 4 條令狀應具備相當理由之要件

依據增修條文第 4 條之誡命，令狀之核發應本於相當理由為之。一般言之，聲請令狀，應由偵查機關釋明具有相當理由之事實，足使法院相信在搜索地點將得以發現犯罪證據為審查基礎[159]。然而，對於單一犯罪嫌疑人或位置能夠證明具有相當理由，不代表該相當理由得以證明對於其他地點或處所亦具有相當理由，而可以搜索任何其他地點。若政府間諜程式針對具體對象發送時，當犯罪嫌疑人點擊程式連結時，將下載植入犯罪嫌疑人電腦內，同時回傳犯罪嫌疑人位置及 IP 資訊給與執法者，但若犯罪嫌疑人將程式轉發或貼於自己社群媒體上或以其他方式散佈給其他並未具備相當理由之對象，將引發搜索無辜第三人之疑慮，侵害無辜者基本權[160]。其實，在本文前述已有實例顯示，聯邦調查局的間諜程式傳播而感染民間企業之資訊設備，同樣地，也可能發生任何網路使用者在搜索過程當中，點擊此等虛偽的網頁，將觸發搜索造訪者之電腦，因此造成一旦釋放此等間諜程式，政府也難控制可能造成之損害程度[161]。換言之，搜索令狀不該授權可以預見干預無辜人民之基本權，而造成附帶損害之情形，搜索令狀對於造成損害之對象，當屬欠缺

---

157 Brian Krebs, *Cards Stolen in Target Breach Flood Underground Markets*, KREBS ON SECURITY (Dec. 20, 2013, 10:06 AM), https://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/. 作者論述由記者經常性造訪網路犯罪網域才能揭露目標電腦資訊業遭駭客破壞之資訊。

158 ACLU, *supra* note 41, at 22.

159 RONALD JAY ALLEN ET AL., COMPREHENSIVE CRIMINAL PROCEDURE 417, 433 (2d ed. 2016); KERR, *supra* note 33, at 530.

160 ACLU, *supra* note 41, at 22.

161 *Id*.

相當理由。而對於不可能在令狀上載明特定描述搜索之地點及特定應扣押之數位檔案，雖然個別治安法官審查令狀時，或許得以解決上述問題，但是上述間諜程式所帶來之令狀問題將遍及所有遠端搜索令狀之聲請，論者因而認為此應由國會解決特定性要件及缺乏相當理由之疑慮[162]。

（五）新增遠端搜索弱化通知要件（notice requirement）

依據聯邦刑事訴訟規則第 41 條(f)(1)(C)所定一般搜索之通知要件，執行令狀執法人員應給予令狀複本及因搜索而扣押財產之收據[163]。新增遠端搜索規範修正第 41 條(f)(1)(C)通知要件，偵查機關應盡合理努力送達令狀複本於受搜索人或資訊被扣押或複製者[164]，並特別論及送達方式應合理計算方式以通知相對人。修訂理由業已慮及搜索通知無法送達或通知之情形，但事實上，偵查機關聲請以遠端搜索方式蒐集證據之情形，均屬於通知有困難之情形。舉例來說，偵查機關為尋求特定網路使用者之身分及位置，很有可能是從某個大都會區的咖啡店，使用者從該店之網路 IP 位置連結上網，因之，偵查機關得以合理送達通知方式為何，其實並不明確[165]。

而令狀之通知要件，在聯邦法院見解認為不能通知者，將使人產生強烈質疑令狀的憲法妥適性，如同聯邦第九巡迴上訴法院所表示「若未能緊接著秘密侵入後、合理而簡要期間內明示通知，則令狀執行具有憲法上瑕疵。……本院採取之立場因為秘密搜索及扣押無體物正好命中增修條文第 4 條保障利益之核心。單單就陌生人得進入並檢視我們的隱私中心——住宅，即已喚起我們對自由權之熱望。增修條文第 4 條之法源要求秘密進入應被嚴密的

---

162 *Id.* at 23.

163 *See* FED. R. CRIM. P. 41(f)(1)(C).

164 *See* FED. R. CRIM. P.41(f)(1)(C) ("For a warrant to use remote access to search electronic storage media and seize or copy electronically stored information, the officer must make reasonable efforts to serve a copy of the warrant and receipt on the person whose property was searched or who possessed the information that was seized or copied. Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person.").

165 ACLU, *supra* note 41, at 23.

限制（closely circumscribed）。[166]」同樣地，遠端搜索係以隱密地侵入個人電腦資訊設備之儲存資料庫內，其中包括類似於個人之數位日記、聯絡簿、信件及照片集，因而侵害之嚴重程度不會低於個人生活隱私住宅之程度。毫無疑問地，電腦資訊設備得以儲存巨量資訊，包含巨量之隱私資訊，因之遠端搜索涉及重大程度之侵入性，在本質上與搜索其他容器物並無不同[167]。事實上，從聯邦最高法院在 Riley 案說理也同樣地清楚得知，自本質上而論，行動電話負載之功能及角色，實際上已經等同於小型個人手提電腦資料庫，而當代任何電腦資訊設備之本質及功能，更遠甚於上述行動電話含載資訊之質與量（含功能），國家植入間諜程式進行遠端搜索個人之資訊設備，當然是嚴重侵害（干預）個人生活私密領域及個人資料自主權利，因之，更應該踐行即時通知要件。

再者，增訂條文授權偵查機關通知並製給收據予財產權受搜索之個人「或」遭受扣押或複製之資訊持有之個人。嚴格言之，此為二個受通知對象，可以是不同之個人，故通知時是否對二人均進行通知。舉例言之，偵查機關進行遠端搜索，而該電腦資訊設備雖然由個人（或可能是企業體）具有所有權，實際上卻由他人（或消費者）使用（並由該人擁有電腦檔案），因此，若解釋得僅通知電腦資訊設備之所有權人，但反而不對於電腦檔案遭扣押或複製之所有人進行通知，以致於並未賦予真正的遠端搜索之目標對象得以聲明異議或挑戰合憲性之機會[168]，亦屬不妥。但亦有認為增訂條文認為若要通知每一個遭受扣押或複製資訊持有之個人，對政府言之，負擔過重，因此僅須擇一通知即可[169]。

---

166 United States v. Freitas, 800 F.2d 1451, 1456 (9th Cir. 1986); United States v. Villegas, 899 F.2d 1324, 1337 (2d Cir. 1990).

167 United States v. Payton, 573 F.3d 859, 861-62 (9th Cir. 2009).

168 ACLU, *supra* note 41, at 24.

169 *See* FED. R. CRIM. P. 41(f)(1)(C); THOMPSON II, *supra* note 7, at 10.

（六）延期通知要件（delay notice）

另外，「延期通知」之規範，聯邦刑事訴訟規則第 41 條(f)(3)規定，依據檢察官之聲請，治安法官或州法院紀錄法官，在法律授權下，得依據本規則規定，延期通知[170]。然而延期通知應僅在法官審查後，准許短暫延期，但基於遠端搜索侵害人民基本權之深度、廣度及密集程度，若法制上果真准許遠端搜索，延期通知必須在個案中個別審查，且通知應在遠端侵入後之合理時間內為之[171]。由於延期通知之規定，可以預先阻止遠端搜索之目標對象得以提出憲法爭點，而縱使事後在刑事訴追程序中，被告得透過證據排除聲請法院審查該證據之證據能力，檢察官也多得以執法機關出於善意相信令狀之有效性執行遠端搜索，而法院也經常性以善意例外裁定駁回排除證據能力之聲請[172]。因此，承前所述，主要目的在於通知應在搜索、扣押後盡速為之，除避免令狀執行具有憲法上瑕疵之外，亦使得當事人得即時於受搜索、扣押財產權或資訊後知悉之，並得以在日後刑事程序爭執其證據能力，故仍有其實益，從而，縱使准許延期，仍宜盡速為之。

（七）小結

原本聯邦刑事訴訟規則規定應限制於規範程序面事項，而不得剝奪、擴大或增修任何實質權利，雖然關於憲法爭議，刑事訴訟規則提案委員會認為可由未來案例法逐案解決，但社會各界即認為此次增訂規則，將擴大政府實質權利，增加新類型的搜索，也就是當國家想要搜索電腦資訊設備位置之所在「無法查知」時，也就無法向一個特定之管轄法院聲請令狀，此已有德州南區聯邦地方法院駁回令狀聲請之前例在先，事實上，在此等情況，偵查機關欠缺實質權力進行遠端搜索，針對這個理由，聯邦刑事訴訟規則之增訂案

---

170 *See* FED. R. CRIM. P. 41(f)(3) ("(3) *Delayed Notice.* Upon the government's request, a magistrate judge—or if authorized by Rule 41(b), a judge of a state court of record—may delay any notice required by this rule if the delay is authorized by statute.").

171 ACLU, *supra* note 41, at 24-25.

172 United States v. Leon, 468 U.S. 897 (1984).

當然幾近確定肯認國家使用遠端駭客技術或全新的間諜程式，使得表面上看起來僅是程序上改變，實質上則是創造新的權力[173]。

此增訂規則在增訂草案之初，即引起廣大注意及民權團體之關切，主要產生的疑慮是，網路安全性與政府濫用網路及軟體之弱點，都是外界所高度關切的問題。再者，就規則本身，也產生不小的憲法疑慮，例如：特定性要件限制、相當理由及通知要件之疑慮。更重要的是，上述憲法的疑慮，很難被法院逐一審查，治安法官並不適合審查高難度之科技問題，對於技術面陌生及完整評估聲請遠端搜索之核發與否，需要對於儲存資料、網路結構及網路安全之技術專業，縱使表面上符合相當理由之要件，很可能未能通過特定性及合理性審查[174]。而且治安法官之裁定多半不公開[175]，無法得知，更難以期待治安法官可以解決上述規則所產生之憲法疑慮。且真正關於遠端搜索之本質，偵查機關於聲請時並未完全敘述執法機關的遠端搜索之本質，無論是提出的聲請書範例或真正提出於法院之聲請書，以至於未告知治安法官「駭入執法」之本質，並告知公開濫用軟體上未知的安全漏洞，而創造顯著的網路安全之間接損害（對目標電腦及其他人），同時也違反增修條文第 4 條之特定性要件及合理性要件[176]。因此，當偵查機關聲請法院核發令狀時，應向治安法官提供完整正確資訊，使治安法官能真正立於審查者角色，了解遠端搜索干預基本權之嚴重程度、全面性監視之性質及可能造成之損害或於侵害之後能夠回復原狀之程度等，再行審酌核發遠端搜索之令狀。

---

173 ACLU, *supra* note 41, at 16.

174 ACLU, *supra* note 41, at 26.

175 關於遠端搜索之聲請，美國各管轄區治安法官裁判已公開上網的裁定僅有數個，上述德州南區聯邦地方法院治安法官之裁定，即屬少數中之一。

176 Donohue, *supra* note 119, at 21: 45-22:17 (Remarks at Panel).

伍、我國未來國家植入間諜程式遠端搜索之規範架構之討論

一、國家植入間諜程式遠端搜索侵害之基本權及法律保留原則

由於國家植入間諜程式進行遠端搜索取得之資訊，包括使用者 IP 位置資訊、乙太網路卡位址、運作程式種類、網路瀏覽器及版本、操作系統之登記使用者、登記公司名稱、甚至防火牆登錄紀錄、網路瀏覽歷史及瀏覽追蹤、列為書籤或我的最愛之網頁、搜尋字詞及儲存之使用者名稱及密碼、電子郵件內容及聯絡簿及電腦資訊設備內所有之內容性資訊。從而，所能取得之資訊不僅一般個人資料而已，電腦資訊設備內所有檔案、訊息等個人生活私密領域之隱私資訊，均可為間諜程式「一網打盡」蒐集取得之。直言之，國家可以完整監視一個人網路、電腦資訊設備活動及生活之全貌，即可以得知完整的個人生活私密領域，如同國家全面而無間斷監視。承前所述，在 *Riley v. California* 案，聯邦最高法院將與電腦相同之現代行動電話在現代人類生活扮演持續性及普遍性的角色，定論為現代人類生活重要特徵，分析行動電話與其他物理性有體物在質與量、負載資訊內容及與一般容器均具有差異性。聯邦最高法院認為，自本質上而論，行動電話負載之功能及角色，實際上已經等同於隨身攜帶小型個人手提電腦及資料庫，而非傳統手機或一般物理性有體物可資比擬[177]。從而，毫無疑問的，當代任何電腦等資訊設備之本質及功能，遠甚於上述行動電話含載資訊之質與量（含功能），國家植入間諜程式進行遠端搜索個人之資訊設備，可說是重度侵害（干預）個人之生活私密領域及個人資料自主權利。

依據憲法法庭 111 年憲判字第 16 號「維護人性尊嚴與尊重人格自由發展，為自由民主憲政秩序之核心價值，基於人性尊嚴與個人主體性之維護及人格發展之完整，隱私權乃為保障個人生活私密領域免於他人侵擾及個人資

[177] 溫祖德，前揭註74，頁207-209。

料之自主控制，所不可或缺之基本權利；其中之個人自主控制個人資料之資訊隱私權，係為保障人民就是否揭露其個人資料及揭露之對象、範圍、時間、方式等，享有自主決定權，並保障人民對其個人資料之使用，有知悉、控制權及資料記載錯誤之更正權（司法院釋字第 603 號解釋參照）。」其實依據歷來司法院解釋，大法官對於人民隱私權保護之範疇，在司法院釋字第 585、603、631 號解釋均指出「維護人性尊嚴與尊重人格自由發展，乃自由民主憲政秩序之核心價值。隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域（空間）免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第 22 條所保障（本院釋字第 585 號解釋參照）。」換句話說，大法官建立二個隱私權保護之領域，一為私密領域而保障個人生活秘密空間，另一為個人資訊秘密自主領域[178]。其中對於個人生活私密空間之保障，即認為住宅與私人居住空間均屬於隱私權保障之範圍，足以排除政府之任意侵犯[179]。從而人民享有居住生活安寧及財產權空間（住居所空間）之保障，不受國家不合理之搜索、扣押，亦可認為從我國憲法第 22 條推導肯認對人民隱私權之保障，其保障範圍及於個人生活所附著之住宅、隱密處所等其他個人生活秘密領域。

而身處現今科技網路世代，不僅僅是物理世界上個人生活不可分之住宅屬於個人私密領域而已，以虛擬世界言之，以個人電腦資訊設備為核心而展開之網路活動、電腦內相關活動，電腦儲存之資訊，甚至已結束所儲存通訊內容，係相當於虛擬之個人住宅內之私密活動，已見前述美國聯邦巡迴上訴法院見解所為之解釋，是而本文探討之植入間諜程式遠端搜索之科技將得以全面監視相對人之資訊設備內容性資訊及全面線上網路活動，也等同對於個人生活私密領域、甚至可能擴及住宅內私密領域活動進行全面監視。

---

[178] 葉俊榮（2016），〈探尋隱私權的空間意涵：大法官對基本權利的脈絡論證〉，《中研院法學期刊》，18期，頁9。

[179] 葉俊榮，前揭註178，頁10。

其次，從司法院釋字第 631 號解釋針對通訊監察指出「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。此項秘密通訊自由乃憲法保障隱私權之具體態樣之一，為維護人性尊嚴、個人主體性及人格發展之完整，並為保障個人生活私密領域免於國家、他人侵擾及維護個人資料之自主控制，所不可或缺之基本權利（本院釋字第 603 號解釋參照），憲法第 12 條特予明定。國家若採取限制手段，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，方符憲法保障人民基本權利之意旨。」同樣地，本文探討之間諜程式遠端搜索對於個人運用自己之電腦資訊設備從事網路線上活動及個人電腦內活動，均屬於個人生活私密領域內之網路及電腦私人活動，若有科技偵查行為限制干預個人生活私密領域之隱私權，同時干預個人資料自主領域之資料自主權，必須要符合法律保留原則，除有法律依據外，限制要件也需具體、明確，並不得逾越必要之範圍，合先敘明。

二、遠端搜索令狀應採令狀原則及應以相當理由標準審查

由於透過線上虛擬進行遠端搜索電腦資訊設備與一般物理性進入住宅等隱私處所內搜索，雖然是不同的搜索客體，但基於本文前述美國聯邦最高法院在 Riley 案分析可知，當代電腦等資訊設備負載的資訊，在質與量上遠遠超過於住處等隱私處所可以蒐得之資訊。復以，遠端搜索可執行的方式，甚至是全面監視，其侵害個人隱私基本權之程度甚深，自不待言。準此，偵查機關受到之誡命與限制，與一般搜索令狀相較，不該更少，反而應該受到更多之限制。首先，基本上，植入間諜程式遠端搜索，仍應遵循令狀原則，乃為基本要求及誡命。而其核發，須由中立之第三者法官進行審查，此亦為我國搜索法制、甚至是通訊保障及監察法所遵循之原則。

其次，於具備相當理由時，法院方得以核發令狀。一般言之，聲請令狀，應由偵查機關釋明具有相當理由之事實，足使法院相信在搜索地點將得以發

現犯罪證據為審查依據[180]。如何判斷相當理由，依美國聯邦最高法院在 *Illinois v. Gates* 一案表示相當理由所指的是具備公平合理性，而足認犯罪證據或違禁物將得以在特定處所搜得或發覺之謂[181]。但相當理由是一個抽象浮動且彈性之概念，並沒有特定原則足以決定相當理由存在與否，而是在聲請機關之宣示誓詞足為建構相信根據綜合全般證據情況下，以實際且通常方法下，將得以發現證據之公平可能性[182]。舉例來說，對某個不法網站之會員或連結犯罪活動之線上群體，是否即可推論具有相當理由搜索該網站成員住處以取得相關犯罪證據，學者 Orin Kerr 認為法院可以評估下列諸點作為參考依據，被告是否為真正控制該會員帳號或以之為加入該線上犯罪活動之帳號、被告是否可能登入帳號之目的為獲取犯罪證據之用、被告獲取犯罪證據之可能性或者是將該證據儲存於電腦之中及該犯罪證據是否現在正存在於被告住處[183]。

在撫平者行動中之 *United States v. Allain* 一案，被告 Allain 因為登入兒童色情網站而以 NIT 偵查技術植入間諜程式並進行遠端搜索，被告抗辯該令狀欠缺相當理由，且不符令狀特定性要件，但地方法院並不採取該辯詞，表示 NIT 令狀授權植入間諜程式於任何登入 Playpen 色情網站之電腦資訊設備，而令狀聲請須具備之相當理由是任何人登入該色情網站之目的在於觀覽、散佈兒童色情圖片。在本案中登入上述色情網站本身不是犯罪，只要令狀之聲請及宣誓誓詞足以建立公平可能性（fair probability）認為任何人登入上述網站意在觀覽或分享兒童色情圖片即可，被告辯稱登入該色情網站不代表已經建構犯罪之相當理由或透過間諜程式已經搜索取得犯罪證據，NIT 科技偵查技術根本無法區分偶然的瀏覽者或者是毫無疑問地積極搜尋兒童色情圖片之人，但本案法院認為雖然可能有的造訪者登入上述色情網站，但目的不在取得兒童色情圖片，而相當理由不需要達到特定性，令狀聲請及宣誓

---

[180] ALLEN ET AL., *supra* note 159, at 417, 433;KERR, *supra* note 33, at 530.

[181] Illinois v. Gates, 462 U.S. 213, 238-39 (1983).

[182] KERR, *supra* note 33, at 530.

[183] *Id.* at 539.

誓詞已建立公平可能性認為任何人登入上述網站將瀏覽或分享兒童色情照片，而在被告電腦中出現該色情網站的首頁，也僅是治安法官認為具有相當理由審酌因素之一，即使單純持有網頁也不會建立相當理由，而係在全般情況下（the totality of the circumstances）充足展現需要證明之程度（the requisite level of proof）判斷之[184]。最後，法院表示審酌全般情況，包括 Playpen 色情網站之網頁及內容、該兒童色情網站其實是一個洋蔥網路上的隱藏服務網站及其註冊的條件，造訪者必須連結到洋蔥伺服器，才能夠上網，且即使連結上網後，也必須知道該兒童色情網站之地址，才得以連結登入網站，換言之，造訪者必須採取「多階段的積極手段」，使得極度不太可能是在不了解其內容及意義的情況下，由造訪者「意外地」登入網站，本於該網站之秘密本質及在洋蔥網路中能夠尋得該網站的挑戰性，就足以指示凡登入該色情網站之人「很可能知曉」網站的目的及帶有瀏覽兒童色情的動機來登入網站[185]。從而，治安法官具有基礎去認定核發遠端搜索令狀係本於相當理由足以相信登入該兒童色情網站之電腦資訊設備存有犯罪活動證據之結論[186]。

因此，植入間諜程式遠端搜索之相當理由，所需要建立的是在案件之全般情況（脈絡）下，經由令狀聲請之誓詞及證據，建立公平可能性認為犯罪證據足以在登入色情網站之電腦設備蒐集取得之，足已建構相當理由。事實上，在更新的一則聯邦第四巡迴上訴法院判決中，也採取相同的見解，表示從聲請令狀宣誓誓詞內足以展現合理的推論（reasonable inference），知道某網站含有兒童色情圖片，仍使用 IP 位置進行點擊某兒童色情網站，因而係相當合理（fairly probable）認為在該 IP 位置的住家（處）可以搜索發現犯罪證據[187]。

---

184 United States v. Allain, 213 F. Supp. 3d 236, 244-45 (D. Mass. 2016).

185 *See Allain*, 213 F. Supp. 3d at 241, 245.

186 *Allain*, 213 F. Supp. 3d at 245.

187 United States v. Bosyk, 933 F.3d 319 (4th Cir. 2019).

三、授權准予遠端搜索要件

美國聯邦刑事訴訟規則遠端搜索規範授權偵查機關植入間諜程式，使用遠端搜索（remote access to search）電子儲存媒介（電腦儲存資訊設備）或扣押、複製在管轄區域內、外之電子儲存資訊。必須限於下列 2 種情形，第一種情形，當電子儲存媒介或資訊所在位置，遭以科技方式隱藏（隱匿）之，也就是授權發動遠端搜索之要件，係當犯罪嫌疑人於網路世界中以各種科技手段隱藏自身所在位置或隱藏資訊科技設備位置，以至於無法偵查犯罪嫌疑人之身分，也無法蒐集取得犯罪嫌疑人利用網路犯罪之相關犯罪證據，因此有必要授權使用植入間諜程式遠端搜索之科技偵查手段之必要。第二種情形，限於偵查機關正在偵查電腦犯罪（18 U.S.C. § 1030(a)(5)）中，對於位於 5 個或以上不同地區內，未經授權之情況下，對於受保護電腦之資訊設備進行攻擊損害。舉例來說，使用殭屍病毒，在未經授權情況下攻擊受保護之電腦資訊設備，且這些資訊設備分別位於 5 個或 5 個以上之轄區內。

由於美國法植入間諜程式遠端搜索，除上述要件以外，美國法沒有其他限制要件，本文認為在干預條件之限制上過於簡略，由於遠端搜索之偵查手段可以取得之資訊，具有全面觸及性及深度揭露性，植入間諜程式後，資訊蒐集也具有自動性持續不斷蒐集回傳資訊，從 *United States v. Carpenter* 案見解來說，具有上述 3 種內涵之資訊，已經近乎國家對於個人之完美監視，對於個人隱私權將造成廣泛而全面性之侵害，個人對於此等監視之下從事之活動全部，當然具有合理之隱私期待[188]。復以，另一方面，其侵入蒐集取得之資訊之手段又係以秘密方式為之，其植入間諜程式後，在相對人電腦資訊設備上，得以從事偵查之措置，也不限於搜索電腦資訊設備內容性資訊而已，如果沒有以法律限制的話，甚至可以包括開啟麥克風、進行網路上通訊監察、開啟攝影機等，以此種方式所造成之隱私權侵害，遠遠甚過一般搜索，更甚過傳統電話監聽（此部分詳後述，應以法律禁止使用此等手段取得資訊），其授權干預之要件，當然應該採取最高規格之限制，以兼顧平衡人權保障與

[188] 溫祖德，前揭註61，頁215-217。

科技偵查之界線。因此，本文參酌前述美國學者評論或民間團體之建議，認為應具備如下要件，方得核發遠端搜索令狀，茲分述如下。

（一）限於重大犯罪

首先，雖然美國法制並未就遠端搜索明訂偵查機關得以從事之遠端搜索限於重大犯罪，然而考量所使用之科技手段及可取得之資訊，係全面性且深入到個人生活私密之各個層面，審酌通訊保障及監察法設有重罪原則，遠端搜索之手段有過之而無不及通訊監察，其立法也宜採取重罪原則，限制僅有在重罪之偵查，方有必要進行之。在發動使用之犯罪類型，仍應限於重大犯罪，就此，可以仿照通訊保障及監察法之重罪原則為基礎，方得授權發動如此嚴重侵害基本權之科技偵查強制處分。

（二）限於最後手段性原則

承前所述，由於植入間諜程式遠端搜索，係針對現代型手機或其他電腦資訊設備，如個人電腦、手提電腦等為之，以現代人言之，個人幾乎不可能放棄涵蓋個人所有資訊之上述設備[189]，此即所謂「機不離身」。因此，針對具有資訊深度揭露性、全面觸及性的監視或資訊蒐集，縱使不是監聽，也應該是在偵查機關已經使用其他偵查手段不能或難以確認被告之所在位置或使用者真實身分後，方得以向法院聲請採取遠端搜索令狀為之[190]。再者，植入間諜程式遠端搜索，通常屬於秘密地植入（covert-entry）目標對象之電腦資訊設備，因此聯邦法院曾經在要件上明定要求秘密型搜索，偵查機關須於具備合理必要性（reasonable necessity）方得進行此種秘密型搜索，亦屬合理之法制設計[191]。亦即，應在「不能或難以其他方法蒐集或調查證據時」，才有合理之必要性使用遠端搜索。

---

189 林鈺雄（2022），《刑事訴訟法上冊》，11版，頁468，自刊。

190 Crocker, *supra* note 56.

191 United States v. Villegas, 899 F.2d 1324, 1337 (2d Cir. 1990).

（三）最小侵害性原則及限制蒐集資訊之偵查手段

不少論者認為植入間諜程式遠端搜索，其對於隱私資訊之蒐集、對於個人之監視，近乎完美監視，因此，遠端搜索之侵入性絕不下於通訊監察[192]。一般言之，如果是以遠端搜索方式，蒐集相對人之電腦儲存資訊設備內容性資訊、IP 位置及確認特定目標使用者之資訊，此尚屬於美國聯邦刑事訴訟規則新增規範授權偵查機關可以取得之資訊，如果遠端搜索已經取得本案犯罪之相關證據而達成確認犯罪嫌疑人或蒐集、保全證據之目的，執法機關即無再翻搜、查閱與本案無關聯性之電腦資訊設備內容之其他資訊。若此，本文認為也應參酌通訊保障及監察法之最小侵害性原則規範，遠端搜索「不得逾越所欲達成目的之必要程度，且應以侵害最少之適當方法為之」（通訊保障及監察法第 2 條第 2 項）。正如同司法院釋字第 631 號解釋明示「……倘確有核發通訊監察書之必要時，亦應謹守最小侵害原則」，而這也是憲法比例原則之體現。

因此，本於最小侵害性原則，也應該明文限制偵查機關遠端搜索得以蒐集資訊之偵查手段，參酌美國聯邦刑事訴訟規則之遠端搜索規範，原本授權使用遠端搜索電子儲存媒介（電腦儲存資訊設備）或扣押、複製在管轄區域內、外之電子儲存資訊為限。既然如此，若以遠端搜索科技，直接開啟相對人電腦資訊設備之麥克風、智慧音箱，蒐集正在進行中之網路通訊內容，已超過搜索電腦儲存資訊設備內容性資訊，而涉及網路上正在進行中之通訊監察，其所侵害（干預）基本權，即已超過上述之隱私權，而包括個人通訊隱私及秘密通訊自由，甚至構成住宅內之監視、監聽。即有論者主張根據所使用之遠端搜索之手段及蒐集之資訊，如果是涉及網路上正在進行之通訊監察，則此等遠端搜索僅得依據聯邦監聽法之監聽令狀而為之，若僅依據聯邦刑事訴訟規則之授權為之，將構成不法監聽[193]。也就是說，不能將遠端搜索變相成為進行網路通訊監察，甚至是住宅內監視、監聽，更可能造成對人民

---

[192] Crocker, *supra* note 56.

[193] ACLU, *supra* note 41, at 18.

實體上個人生活私密領域及私人活動進行全面監視，除另以法律明文授權以符合法律保留原則外，若以遠端搜索進行此等科技偵查行為，應嚴格明文禁止之。因此，本文認為應該嚴格禁止遠端搜索所得以從事之科技偵查手段及得以蒐集取得之資訊。

職是，在最小侵害原則下，本文認為亦得參酌我國通訊保障及監察法第 13 條第 1 項但書明文「通訊監察以截收、監聽……或其他類似之必要方法為之。但不得於私人住宅裝置竊聽器、錄影設備或其他監察器材。」既然該但書規定，已有與本文主張相類似之立法，即明文禁止在住宅內監聽、錄影或監察。因此，對於植入間諜程式遠端搜索，亦同樣應明定禁止類似於他人住宅內進行監聽（包含網路通訊監察）、監視之行為。此時亦不能基於遠端搜索令狀為之，此應屬於通訊監察範圍，若本於遠端搜索令狀為之，則已超出令狀核准之授權而已涉及人民之秘密通訊自由（通訊隱私權）之基本權干預，需另外依法律授權明文規定，方得為之。

四、遠端搜索令狀之特定性要件

美國聯邦刑事訴訟規則遠端搜索規範授權偵查機關植入間諜程式，使用遠端搜索電子儲存媒介或扣押、複製在管轄區域內、外之電子儲存資訊，其增訂目的之一，即在於當電子儲存媒介或資訊所在位置，遭科技方式隱藏之，因之，於網路世界中以科技手段隱藏自身所在位置或隱藏資訊儲存科技設備位置，以至於無法偵查犯罪嫌疑人之身分或所在位置。然而，此將違反搜索票應明確記載應搜索處所及應扣押物原則。同樣地，增修條文第 4 條明定搜索票必須要明確記載搜索處所及扣押之物，又稱為特定明確性原則，此為憲法誡命要件，且依據美國聯邦最高法院判決，當搜索令狀欠缺特定明確描述應搜索處所或扣押之物，將構成無效令狀[194]，從而在遠端搜索令狀，也無法規避此憲法誡命，為解決此一特定性要件，可能得要透過實務上聲請機關記載方式個案決定之。

---

[194] Groh v. Ramirez, 540 U.S. at 557.

既然遠端搜索之令狀記載特定性可能產生問題，當犯罪嫌疑人於網路世界中以各種科技手段隱藏自身所在位置（或隱藏資訊設備位置），以至於無法偵查犯罪嫌疑人身分，既然無法在遠端搜索前先查得犯罪嫌疑人之真實身分，又如何在聲請搜索令狀時，即可以明確記載搜索處所、搜索及扣押之物。學者有表示「由於一般搜索電腦案件中，令狀上會記載特定的電腦（特定型號或序號），或是某處所內的電腦」[195]，確實是特定方式之一，可為參考。從而，本文認為在特定性要件要求下，執法機關在聲請遠端搜索令狀時，因應特定性記載要求，特別要注意釋明讓法官得以記載符合特定性之要件。舉例來說，以本文前述 Playpen 系列案件中，部分法院認為令狀已經描述特定受搜索之地點，亦即登入該兒童色情網站之電腦資訊設備位置，也就存在著公平可能性，而認定任何「接近（登入）」該網站之人具有瀏覽及交換（交易）兒童色情圖片之意圖，即符合特定性要件之誡命[196]，也就是說，以犯罪嫌疑人之「登入位置」之記載，即符合特定性要件。

但也有少數法院認為特定性要件之要求，不是僅僅描述一個地點（位置）即已足夠，而必須是特定哪一個電腦資訊設備將被搜索[197]。這一說比上述多數聯邦地方法院採取之見解嚴格，也屬於比較少數之見解。本文認為特定性要件之記載，雖應記載將要搜索之特定處所或搜索、扣押物件，但是針對在數位世界之特定性要件之誡命，特別像是在暗網之案例類型當中，吾等可以區分內在及外在 2 個角度觀之，從外在角度觀之，比較像是從功能性角度來看，分析在電腦網路世界之線路或迴路如何傳輸、穿越網路世界來解讀這一個位置，但是若從內在角度來看，比較像是傳統增修條文第 4 條之特定性要

---

195 李榮耕，前揭註9，頁75。

196 *See* United States v. Darby, 190 F. Supp. 3d 520, 533 (E.D. Va. 2016); *Matish*, 193 F. Supp. 3d 585, 608-09; United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263 at *5 (W.D. Wash. Jan. 28, 2016). 事實上，還有更多之聯邦地方法院判決採取此說，本文僅臚列有限之判決供參。

197 採取此一見解之判決代表為United States v. Carlson, Criminal No. 16-317 (JRT/FLN) (D. Minn. Mar. 23, 2017), https://www.govinfo.gov/content/pkg/USCOURTS-mnd-0_16-cr-00317/pdf/USCOURTS-mnd-0_16-cr-00317-0.pdf.

件，不分數位世界與否，誡命一定要記載精確的位置、電子郵件位置等。因此，以上述多數法院見解，遠端搜索令狀所記載的數位世界位置，從外在角度觀之，犯罪行為人真正「登入」兒童色情網站過程的位置即可[198]。換言之，從網路功能角度分析，匿名科技的運作機制，就是一個「登入暗網」之過程，因此准許以這一個登入過程之位置替代真實位置紀錄[199]。尤其是在尚未取得遠端搜索令狀之前，執法機關可能尚難取得特定目標電腦設備之型號、序號或電腦設備內乙太網路卡、操作登記者等更具體之資料，因之，本文認為多數法院見解從一個網路數位世界功能性角度（或外在角度）觀察，以匿名科技來說，登入暗網（或兒童色情網站）之位置，即已經符合現代數位世界所定位之位置，而足以符合特定性之誡命，本文因而也採取聯邦法院之多數說之見解。

五、令狀有效執行期間

依照我國刑事訴訟法明定搜索票應有有效期間，逾期不得執行搜索及搜索後應將搜索票交還之意旨。此一記載一方面在於防範執法機關刻意保存搜索票而遲不執行之缺點[200]，另一方面，搜索根據之相當理由，也可能隨時間經過而消逝，為免過於侵害人權，確保相當理由之存在，搜索當應於一定期間內執行，方屬妥適[201]。但在植入間諜程式遠端搜索之情形，因執行之階段，於植入後須利用並執行該程式，從電腦資訊設備內進行搜索後，再回報執法機關蒐集取得之資訊，此種執行方式，可能需要一段時日，並且需等候犯罪嫌疑人登入連結暗網特定網站，此時才啟動下載於特定犯罪嫌疑人之電腦資訊設備之過程，進而蒐集所欲蒐集之資訊，因此遠端搜索令狀須載明植入後執行期間，無法如傳統搜索票係屬短期、一次性的執行，而須具有一段持續性期間之規範。此外，由於植入間諜程式之後，若無法於期滿自動刪除，將

198 Hightower, *supra* note 39, at 188-89.
199 *Id*.
200 林鈺雄，前揭註189，頁446。
201 李榮耕，前揭註9，頁76。

無法阻止間諜程式繼續傳輸資訊回報偵查機關之執行，因此，除遠端搜索令狀須有一定植入期間及執行期間之規範外，也需要有執行期滿後自動消滅之規定，此部分詳如下述。

六、執行完畢技術上恢復原狀之規範

承上所述，遠端搜索令狀須有一定植入及執行期間之限制。但因間諜程式需要於執行完畢後，自動刪除間諜程式，如果沒有刪除此程式，間諜程式將持續傳輸資訊回報偵查機關，恐有造成人民隱私權永無止境之侵害疑慮。況間諜程式比起其他傳統搜索之形式更具全面侵入性及揭露性之本質，而在執行結果上所造成之損害，本質上具有不可預測性及也常是無法回復性，甚至是造成資料之損害或整個運作系統之癱瘓[202]。故有需要設計間諜程式於執行完畢後，自動刪除植入之間諜程式[203]，而在法律規範上，亦有法律明文此部分之需要，不但符合前述最小侵害原則之外，更避免造成人民隱私權永無止境之侵害。換言之，站在保障個人隱私權之角度，執法機關有義務要恢復受執行之相對人之電腦資訊設備之原狀，亦即執行結束之後，需將該等程式設計成自動刪除之規定，除可免於繼續侵害受執行相對人之隱私權外，亦有論者提到，假若以社交工程技術植入間諜程式方式，若由受執行相對人將特定連結轉傳他人，或貼在社群媒體上，也將造成非偵查機關偵查對象遭受國家駭客之攻擊，導致對無關之第三人進行遠端搜索[204]，為免於使無干之第三人之電腦資訊設備處於科技上脆弱而易受攻擊之狀態，當然應課以偵查機關於執行遠端搜索結束後移除或刪除該間諜程式之需要。

七、通知要件及延期通知之明定

美國聯邦刑事訴訟規則第 41 條(f)(1)(C)規定，執行搜索執法機關通常必須提供令狀之複本，並製給收據給被搜索人及受搜索處所扣押取得之物件

---

202 ACLU, *supra* note 41, at 17-18.

203 王士帆，前揭註9，頁205。

204 ACLU, *supra* note 41, at 22.

[205]。但因為植入間諜程式遠端搜索屬於秘密地植入目標對象之電腦資訊設備，本質上更不可能在植入時，立即提供令狀給相對人，因此，美國法在通知要件上，放寬此部分要件，明定要求偵查機關「盡合理努力」提供令狀之複本，且送達方式應以合理計算方式通知相對人，包括以電子通知之方式為之。而令狀之通知要件，依本文前述聯邦第九巡迴上訴法院即表示欠缺通知者，將使人產生強烈質疑令狀的憲法妥適性，「若未能緊接著秘密侵入後、合理而簡要期間內明示通知，則令狀執行具有憲法上瑕疵[206]」最後，美國聯邦刑事訴訟規則增訂之條文授權偵查機關通知並製給收據予財產權受搜索之個人「或」持有資訊遭受扣押或複製之個人。

本文認為基於植入間諜程式遠端搜索屬於秘密植入而搜取電腦資訊設備資訊，為保障受搜索人之受通知權，借鑑上述外國立法例，偵查機關應「盡合理努力」提供令狀之複本，且送達方式應合理計算方式通知相對人，包括以電子通知之方式為之。至於通知對象，可以採取比美國法更周全之方式，也就是對財產權受搜索之個人「及」資訊遭受扣押或複製之個人，均應通知之，也才能妥適保障無辜受干預第三人之受通知權，並給予事後救濟之機會，而非任由執法機關僅在財產權受搜索個人「或」持有資訊遭受扣押或複製之個人間自行選擇通知之。

至於「延期通知」之規範，依據美國立法例，基於偵查需要，依據檢察官之聲請，在法律授權下，治安法官等得依據規則規定，准許延期通知[207]。事實上，在我國通訊保障及監察法亦有在具體理由足認確有妨礙監察目的之虞或不能陳報時，得暫時不予通知之規定，但法律亦明定不通知之原因消滅後，應陳報法院補行通知之規定（通訊保障及監察法第 15 條）。故本文認為，基於遠端搜索之執法本質，延期通知應在法官審查後，准許短暫延期（例如：1 個月內），但基於遠端搜索侵害人民基本權之深度、廣度及密集程度，

---

[205] FED. R. CRIM. P. 41(f)(1)(C).

[206] *Freitas*, 800 F.2d at 1456.

[207] FED. R. CRIM. P. 41(f)(1)(C).

通知必須貫徹執行之，而在個案中個別由法官審查後，在執行後之合理時間內為之，方屬妥適。

八、證據排除之規範

證據排除法則是現代防止或嚇阻偵查機關違法取證等目的，必須搭配之立法，除了維護人權保障、維持司法廉潔及抑制違法偵查外，同時也決定了違法蒐集證據之證據能力問題[208]。同樣地，在美國聯邦刑事訴訟規則第 41 條(h)統一在搜索篇內（含各種搜索），明定「在審判中，被告得聲請排除證據」，禁止檢察官於審判中，提出直接或間接違反憲法取得之證據（例如，違反令狀原則）[209]。一般言之，違反該規則第 41 條之規定，不至於造成絕對之證據排除，除非是達到憲法之違反，否則若僅僅是違反規則，且該規則規範內容沒有明示要求證據排除之規定（例如，聯邦監聽法之規定），則聯邦法院多半採取不排除證據[210]。從而，針對本文探討之植入間諜程式遠端搜索，聯邦刑事訴訟規則並無明文採取特定之立場。

不過，鑒於遠端搜索科技偵查侵害人民基本權之深度、廣度及全面監視性，其侵害程度甚於一般搜索之強制處分，或許比較接近監聽之性質，本文建議可以比照我國通訊保障及監察法之規範，當偵查機關違反特定條文，如聲請遠端搜索之令狀規定等，因此蒐集取得之資訊或衍生性證據之行為，均不得採為證據（通訊保障及監察法第 18 條之 1 第 3 項參照）。至於我國刑事訴訟法雖採取由法院審酌人權保障與公共利益之均衡維護之權衡法則（刑事訴訟法第 158 條之 4 參照），但參酌遠端搜索於前述嚴重侵害隱私之本質，似不宜由法院以權衡法則權衡之，以免讓法院個案權衡審酌，而造成無法嚇阻偵查機關違法使用之情形，造成嚴重侵害人民隱私權之結果。

---

[208] 林鈺雄（2022），《刑事訴訟法下冊》，11版，頁6-12，自刊；黃朝義（2021），《刑事訴訟法》，6版，頁604-608，新學林。

[209] STEPHEN A. SALTZBURG, DAVID A. SCHLUETER & JONATHAN K. GITLEN, FEDERAL CRIMINAL PROCEDURE LITIGATION MANUAL 357 (2018).

[210] *Id*.

九、事中監督及報告義務

遠端搜索雖然是以令狀授權為之，但因為是秘密植入間諜程式而執行，且執行可能會延續一段時間，其執法過程是否符合法律規範，則需要外部監督才能使執法機關恪遵相關執法規定。因此，無論是在執行中或執行完畢均應對之進行監督。首先，事中監督，即為在執行過程中所為之監督，由執行機關報告檢察官、核發遠端搜索令狀之法官，目前執行階段及結果，例如，已植入、等候造訪者（犯罪嫌疑人）點擊造訪網站或已下載間諜程式或已經取得部分回傳資料或犯罪證據，此等說明將促使執行機關積極遵法及即時回報，讓法院及檢察官隨時追蹤執行狀況。若經由報告，發現有不應繼續執行之狀況，例如，植入對象錯誤而侵害到無辜之第三人，則可決定有無繼續進行遠端搜索之必要，如有應停止執行時，應撤銷核發之遠端搜索令狀。

其次，執行機關於執行遠端搜索後，應按月向檢察官、核發遠端搜索令狀之法官報告執行情形，檢察官及核發遠端搜索令狀之法官亦得隨時命令執行機關提出報告書。

十、蒐集所得資料之處理及銷毀之規定

最後，針對遠端搜索蒐集取得之資料，如果是 IP 位置資訊，可能僅是用以調查並確認犯罪行為人所在位置，進而發動下一步之偵查，但如果蒐集取得之資料是電腦資訊設備內之內容性資訊，可說是與個人隱私極度相關之資訊，除係供作個案案件證據之用或繼續作為偵辦他案之用以外，應完整外加封緘保存之，並於保存一定年限之後即予銷毀。如果所得資料全部與本案毫無相關者，亦應准許執法機關於執法後，經判斷認為與本案毫無相關者，報請檢察官或核發遠端搜索令狀之法官准予銷毀之。

陸、結 論

科技進步使得犯罪者利用電腦、行動裝置等進行暗網中犯罪，同時利用網路科技隱身於虛擬世界，掩飾自己真實身分，形成虛擬消失之狀態，隱藏自己身分及所在位置，造成偵查機關根本無從確認犯罪嫌疑人，因此，美國司法會議之刑事規則諮詢委員會，在 2016 年修訂聯邦刑事訴訟規則增訂遠端搜索，言明增訂目的在於解決偵查機關不知電腦資訊設備或媒介硬體所在位置，妨礙政府偵查特定目標對象或目標電腦資訊設備之位置，以免聯邦法院依據管轄區域之劃分產生核發搜索票之困難，並承認有進行（跨轄區）遠端搜索之需求及對於多個管轄區域內多個電腦設備，進行遠端搜索之法制需要。

本文認為為能妥善解決當代犯罪走向匿名化、暗網化而衍生找尋犯罪嫌疑人之困境，參酌世界先進國家立法趨勢均已承認遠端搜索或線上搜索，乃從美國法之觀點，深入分析美國聯邦刑事訴訟規則關於核發遠端搜索令狀，以搜尋電腦儲存資訊設備（含電腦儲存資訊設備所在位置、資訊設備內容性資訊）等之管轄權限制鬆綁之法制。藉由分析美國國家植入間諜程式遠端搜索之科技演進及執法、司法實務對於國家植入間諜程式遠端搜索之基本權干預及憲法定位及分析，闡述增訂遠端搜索條款之提案背景、緣由，進行討論及分析，並論述國家遠端搜索之新法及規範評析。最後，由於科技偵查之演進往往與隱私權之保護處於對立之立場，延伸監視力量可觸及之處，特別是因為遠端搜索秘密蒐集取得如此大量個人生活私密領域內之資訊，尤其是個人運用電腦資訊設備從事之網路線上活動或電腦內資訊，干預個人生活私密領域之隱私權及個人資料自主領域之資料自主權，必然引起憲法上關切，故本文也認為本於我國憲法誡命之法律保留原則，由立法機關明定授權國家植入間諜程式遠端搜索之詳細規範架構，並提供立法之詳盡建議，做為未來可能之規範藍本，而在兼顧人權保障之前提下，同時促進執法利益。

參考文獻

一、中文部分

王士帆（2019），〈當科技偵查駭入語音助理：刑事訴訟準備好了嗎？〉，《臺北大學法學論叢》，112 期，頁 191-242。

吳俊毅（2020），〈刑事訴訟上的線上搜索（Online-Durchsuchung）與源頭通訊監察（Quelle-TKÜ）：引進的必要性及實踐上的困境〉，《刑事政策與犯罪研究論文集》，23 期，頁 461-484。https://doi.org/10.6482/ECPCR.202010.0014

李榮耕（2015），〈科技定位監控與犯罪偵查：兼論美國近年 GPS 追蹤法制及實務之發展〉，《臺大法學論叢》，44 卷 3 期，頁 871-969。https://doi.org/10.6199/NTULJ.2015.44.03.04

--------（2018），〈初探遠端電腦搜索〉，《東吳法律學報》，29 卷 3 期，頁 49-87。

--------（2022），〈犯罪偵查中通訊內容的調取〉，《臺大法學論叢》，51 卷 3 期，頁 757-831。https://doi.org/10.6199/NTULJ.202209_51(3).0004

林鈺雄（2022），《刑事訴訟法上冊》，11 版，自刊。

--------（2022），《刑事訴訟法下冊》，11 版，自刊。

法操 FOLLAW（2020），《科技偵查法，是上太空？還是殺豬公？》載於：http://talk.ltn.com.tw/article/breakingnews/3299617。

黃朝義（2021），《刑事訴訟法》，6 版，新學林。

溫祖德（2015），〈行動電話內數位資訊與附帶搜索：以美國聯邦最高法院見解之變遷為主〉，《月旦法學雜誌》，239 期，頁 198-220。

--------（2021），〈偵查機關調取歷史性行動電話基地臺位置資訊之合憲性審查：從美國聯邦最高法院判決檢視我國法制〉，《政大法學評論》，167 期，頁 171-256。

葉俊榮（2016），〈探尋隱私權的空間意涵：大法官對基本權利的脈絡論證〉，《中研院法學期刊》，18 期，頁 1-40。

熊誦梅、溫祖德（2018），〈從馬賽克理論（Mosaic Theory）談通訊使用者資料之法官保留：評智慧財產法院 106 年度刑智上易字第 65 號刑事判決〉，《法令月刊》，69 卷 9 期，頁 34-51。https://doi.org/10.6509/TLM.201809_69(9).0003

歐陽弘（2020），《科技偵查法草案評析：提供於立法院民國 109 年 10 月 8 日公聽會意見與會後補充》，載於：http://www.btlaw.com.tw/h/NewsInfo?key=0227079976&cont=264581。

二、英文部分

ACLU (2014, October 31). *Second ACLU Comment Letter on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media*. https://www.aclu.org/sites/default/files/field_document/aclu_comment_on_remote_access_proposal.pdf

Adams, D. M. (2017). The 2016 Amendments to Criminal Rule 41: National Search Warrants to Seize Cyberspace "Particularly" Speaking. *University Richmond Law Review*, *51*(3), 727-772.

Allen, R. J., Stuntz, W. J., Hoffmann, J. L., Livingston, D. A., Leipold, A. D., & Meares, T. L. (2016) (2nd. ed.). *Comprehensive Criminal Procedure*. Wolters Kluwer.

Bartlett, J. (2015). *The Dark Net: Inside the Digital Underworld*. Melville House.

Beale, S. S., & King, N. (2015). *Rule 41 Memo to Members of Criminal Rules Advisory Committee*. Advisory Committee on Criminal Rules. https://www.uscourts.gov/sites/default/files/fr_import/CR2015-05.pdf

Bercovitz, R. (2021). Law Enforcement Hacking: Defining Jurisdiction. *Columbia Law Review*, *121*(4), 1251-1288.

Bridis, T. (2001, November 23). FBI is Building a 'Magic Lantern'. *The Washington Post*. https://www.washingtonpost.com/archive/politics/2001/11/23/fbi-is-building-a-magic-lantern/ca972123-83a8-46d8-b95c-c2edafda0fea/

Brush, P. (2016, June 9). *Israeli Suspects in Giant JPMorgan Hack Deny Charges in NY*. Law 360. https://www.law360.com/articles/805660/israeli-suspects-in-giant-jpmorgan-hack-deny-charges-in-ny

Center for Democracy & Technology (2014, October 24). *Written Statement of The Center for Democracy & Technology Before the Judicial Conference.* Advisory Committee on Rules. http://cdt.org/wp-content/uploads/2014/10/CDT-Rule41-Written-Statement-final-20141024.pdf

Crocker, A. (2016, June 2). *With Remote Hacking, the Government's Particularity Problem Isn't Going Away*. Just security. http://www.justsecurity.org/31365/remote-hacking-governments-particularity-problem-isnt/

Donohue, L. (2014, March 4). *Remarks at Panel on the Legal and Policy Implications of Hacking by Law Enforcement*. Yale Law School. https://vimeo.com/88165230

Farivar, C. (2018). *Habeas Data: Privacy vs. the Rise of Surveillance Tech*. Melville House.

Ferguson, P., & Huston, G. (1998). *What Is a VPN?*. http://www.potaroo.net/papers/1998-3-vpn/vpn.pdf

Finklea, K. (2015). *Dark Web*. Congressional Research Service.

Ghappour, A. (2017). Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web. *Stanford Law Review*, *69*, 1075-1136. https://doi.org/10.2139/ssrn.2742706

Goldberger, P. (2015, February 17). *Comments of the National Association of Criminal Defense Lawyers on the Proposed Amendment to Rule 41*. National Association of Criminal Defense Lawyers. http://www.nacdl.org/getattachment/8c63efe9-7282-4e2f-a5c7-ad17a0212f30/nacdl-comment-crimr41.pdf

Goodman, M. (2015). *Future Crimes: Everything is Connected, Everyone is Vulnerable and What We Can Do About it*. Doubleday.

Greenberg, A. (2022, December 10). *Security News This Week: Attackers Keep Targeting the US Electric Grids, Plus: Chinese hackers stealing US Covid relief funds, a cyberattack on the Met Opera website, and more*. WIRED. http://www.wired.com/story/attacks-us-electrical-grid-security-roundup/?bxid=611e04ba9530f748ee0a46b2&cndid=66076897&esrc=bouncexmulti_first&mbid=mbid%3DCRMWIR012019%0A%0A&source=EDT_WIR_NEWSLETTER_0_DAILY_ZZ&utm_brand=wired&utm_campaign=aud-dev&utm_content=WIR_Daily_121022&utm_mailing=WIR_Daily_121022&utm_medium=email&utm_source=nl&utm_term=P4

Hightower, M. (2021). The Fourth Amendment and the Dark Web: How to Embrace a Digital Jurisprudence that Protects Individual Liberties. *The Georgetown Law Journal Online*, *109*, 173-198.

House Judiciary Committee. (2011). *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*. https://www.govinfo.gov/content/pkg/CHRG-112hhrg64581/pdf/CHRG-112hhrg64581.pdf

-------- (2016). *Oversight of the Federal Bureau of Investigation: Hearing Before the H. Comm. on the Judiciary*. https://www.congress.gov/114/chrg/CHRG-114hhrg22125/CHRG-114hhrg22125.pdf

House of Representatives. (2012). *H.R.* (Rep. No. 112-546). http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt546/pdf/CRPT-112hrpt546.pdf

Kerr, O. S. (2010). Applying the Fourth Amendment to the Internet: A general Approach. *Stanford Law Review*, *62*(4), 1005-1049.

-------- (2018). *Computer Crime Law* (4th ed.). West Academic Publishing.

King, R. (2012, November 8). Stuxnet Infected Chevron's IT Network. *The Wall Street Journal.* http://www.wsj.com/articles/BL-CIOB-1156

Krebs, B. (2013, December 20). *Cards Stolen in Target Breach Flood Underground Markets*. Krebs on Security. https://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/

Lerner, Z. (2016). A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure. *Yale Journal Law & Technology*, *18*, 26-69.

Mayer, J. (2018). Government Hacking. *The Yale Law Journal*, *127*(3), 570-662.

Moseley, J. A. (2005). The Fourth Amendment and Remote Searches: Balancing the Protection of the People with the Remote Investigation of Internet Crimes, *Notre Dame Journal of Law, Ethics & Public Policy*, *19*(1), 355-378.

Mukasey, M. B. (2008). *The Attorney General's Guidelines for Domestic FBI Operations*. http://www.usdoj.gov/ag/readingroom/guidelines.pdf

Nakashima, E. (2016, January 21). This is How the Government is Catching People Who Use Child Porn Sites. *The Washington Post.* https://www.washingtonpost.com/world/national-security/how-the-government-is-using-malware-to-ensnare-child-porn-users/2016/01/21/fb8ab5f8-bec0-11e5-83d4-42e3bceea902_story.html

Newsweek. (2007, October 9). *Whacking Hackers*. https://www.newsweek.com/whacking-hackers-103531

Poulsen, K. (2007, July 18). FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats. *WIRED.* https://www.wired.com/2007/07/fbi-spyware/

-------- (2014, August 5). Visit the Wrong Website, and the FBI Could End up in Your Computer. *WIRED*. https://www.wired.com/2014/08/operation-torpedo/

-------- (2014, December 16). The FBI Used the Web's Favorite Hacking Tool to Unmask Tor User. *WIRED.* https://www.wired.com/2014/12/fbi-metasploit-tor/

Raman, M. (2014). *Letter from Mythili Raman, Acting Assistant Attorney Gen., to the Hon. Reena Raggi, Chair, Advisory Comm. on the Criminal rules (Sept. 18, 2013)*. Advisory Comm. on Criminal Rules April 2014. https://www.uscourts.gov/sites/default/files/fr_import/CR2014-04.pdf

Raymond, N. (2016, April 21). *U.S. Judge Rules Search Warrant in FBI Child Porn Website Probe Invalid.* Reuters. https://www.reuters.com/article/idUSL2N17O0DE/

Russon, M.-A. (2016, January 6). FBI Crack Tor and Catch 1,500 Visitors to Biggest Child Pornography Website on the Dark Web. *International Business Times UK.* http://www.ibtimes.co.uk/fbi-crack-tor-catch-1500-visitorsbiggest-child-pornography-website-dark-web-1536417

Salgado, R. (2015, February 13). *Google Inc. Comments on the Proposed Amendment to Federal Rule of Criminal Procedure 41*. Google Inc. http://s3.amazonaws.com/s3.documentcloud.org/documents/1672788/13feb2015-google-inc-comments-on-the-proposed.pdf

Saltzburg, S. A., Schlueter, D. A., & Gitlen, J. K. (2018). *Federal Criminal Procedure Litigation Manual*. Juris Publishing, Inc.

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.

Thompson II, R. M. (2016). *Digital Searches and Seizures: Overview of Proposed Amendment to Rule 41 of the Rules of Criminal Procedure* (CRS Report No. R44547). Congressional Research Service.

Valentino-DeVries, J., & Yadron, D. (2013, August 3). FBI Taps Hacker Tactics to Spy on Suspects. *The Wall Street Journal.* https://www.wsj.com/articles/SB10001424127887323997004578641993388259674

Widenhouse, K. C. (2017). Playpen, The NIT, and Rule 41(b): Electronic "Searches" for Those Who Do Not Wish to be Found. *Journal of Business & Technology Law*, *13*(1), 143-169.

Zetter, K. (2011, April 13). With court Order, FBI Hijacks 'Coreflood' Botnet, Sends Kill Signal. *WIRED*. https://www.wired.com/2011/04/coreflood/

The Norm of Government Remote Access to Search: A Normative Perspective of Taiwanese law

Tzu-Te Wen[*]

Abstract

Computer technology today provides criminals with the ability to cloak themselves in the dark web, where, with their true identities and locations concealed, they are more emboldened and freer to commit their crimes. This new trend, referred to as “Going Dark”, impedes government efforts to track criminals, identify their true locations, and collect evidence of their criminal activity. Thus, in 2016, the United States Federal Rules of Criminal Procedure were amended to allow law enforcement to remotely access and search a target's computer or electronic storage media where the media or information has been concealed through technological means. This new amendment allows the government to "hack" into the suspect's electronic devices in order to determine identity and location, as well as to search the content of the devices.

This article will analyze this "remote access to search" amendment to the Federal Rules of Criminal Procedure. Additionally, we will seek to illustrate the constitutionality of remote access to search from a U.S. Constitutional perspective. The United States federal courts’ prevailing opinions hold that the "remote access to search" qualifies as a constitutional search, and is thus confined by the requirements of the United States Fourth Amendment. As a result, the remote access to search amendment could be a legislative model for Taiwanese criminal procedure, as we are facing the same types of problems during our investigations. Eventually, this article could help to provide a basic structure for new law, including warrant requirements, particularity requirements, minimization principle, the requirement to have exhausted all other investigative techniques,

[*] Professor, Institute of Law and Government, National Central University
E-mail: wentzute@cc.ncu.edu.tw

warrant execution period, reasonable efforts to give notice requirement, receipt for information seized or copied, delayed notice, the ex post judicial review, the exclusionary rule of evidence if the application procedure violated the warrant requirements, that both serve the needed public interest and protect the rights of our citizens.

Keywords: Remote access to search, darknet, government hacking, particularity of a warrant, botnet malware