出國報告（出國類別：研究）

對以具加密功能之通訊軟體之通訊監察之理論與實務

服務機關：臺灣南投地方法院檢察署

姓名職稱：王晴玲　檢察官

派赴國家：美國

派赴地點：哈佛大學

出國期間：民國 **103** 年 **8** 月 **24** 日至 **104** 年 **8** 月 **23** 日

報告日期：民國 **104** 年 **11** 月 **20** 日

中文摘要

通訊監察為偵辦犯罪之重要利器，應用於犯罪調查已行之有年，近年來，對於隱私權保護意識高漲，我國通訊保護及監察法近年因而多次修正，聲請監察票、調取票之要件更趨嚴格。

另一方向，通訊保障及監察法制定之初，網路尚未發展成熟，惟現今許多犯罪手法皆以網路為主要媒介，以傳統電話監聽為我國監聽之主要模式，已不敷目前辦案所需，是以有必要針對網際網路監察方式及法制進行檢討。

再現今網際網路通訊已不再侷限於在住處、辦公處所使用電腦上網，而是使用手機通訊、瀏覽網頁，惟因通訊軟體之特殊性，更增添對於加密通訊軟體實施監聽之困難度。

是以，本文參考各國立法例，及實務作法，進行分析及辨證，並提出加密之通訊軟體之監察方式，及修法建議，並增強科技技術面之實施，以期檢察官在日後偵辦犯罪時能更兼顧隱私權之保障與犯罪調查之衡平。

目錄

第一章　前言

第一節　問題意識

所謂通訊監察，係指司法警察、司法警察官為偵查犯罪而截收受監察對象之通訊內容，其目的有三：一、監控對象之即時動態；二、記錄犯罪通訊內容；三、確定犯罪行為人身分。但通訊監察對人民秘密通訊自由有所侵害，因此如何在打擊犯罪與維護隱私中取得平衡，引起諸多爭議。

通訊監察在動員戡亂時期，其法令依據為戡亂時期郵電抽查條例及動員時期電信監察實施辦法，惟此行政命令業於民國 81 年 7 月 31 日失效。嗣法務部基於偵查犯罪之必要，分別於 81 年 11 月、88 年 2 月，分別制頒「國內犯罪案件通訊監察作業要點」、「檢察機關實施通訊監察應行注意要點」，作為執行通訊監察作業之準據，然上開二要點，僅具行政命令之性質，充其量不過係偵查機關實施監聽時之內部規範，與憲法第 23 條「法律保留原則」之規範要求有間。然有學者自刑事訴訟法之觀點，認此種憲法保障之重要權益侵害或限制的通訊監察行為，應係強制處分[1]之一環，此往偵查實務以行政命令作為實施通訊監察之依據，即是認為現行刑事訴訟法中關於搜索扣押等之規定可作為監聽之法律依據，故不違憲[2]。為杜絕爭議，於 79 年 3 月 17 日立法院司法、國防、交通三委員會聯席會議時，多位立法委員建議應建立通訊監察法規依據，經法務部函報行政院邀集有關機關研商後，認為確有立法之必要性，遂於 79 年 9 月間指示法務部研擬制定草案，以建立制度。繼於 80 年 5 月間成立起草委員會，綜合所得國內外相關理

[1] 參照陳運財著，偵查之基本原則與任意偵查之界限，私立東海大學法學研究第 9 期，84 年 9 月，頁 300 以下。

[2]。行政院於 81 年 1 月 30 日送請立法院審議之「通訊監察法草案」總說明中，首先指出「目前司法實務上雖依據刑事訴訟法有關搜索、扣押之法理，對於重大犯罪，亦運用通訊監察方法，追尋嫌犯處所及蒐集犯罪證據。但我國刑事訴訟法並無明文規定通訊之監察，其監察要件與實施程序等仍難免爭議。」，轉引自陳運財著，監聽之性質及其法律規範－兼評通訊監察法草案之爭議，東海法學研究第 13 期，87 年 12 月，頁 144。

論與實務資料，審慎斟酌人民秘密通訊自由與國家、社會及其他法益間之均衡維護，並針對我國實際需要，擬具「通訊保障及監察法草案」，於 80 年 9 月完成並陳報行政院審查，業經立法院審查三讀通過後，於 88 年 7 月 14 日制訂公布通訊保障及監察法。

前因最高法院檢察署特別偵查組監聽立法委員、立法院總機，而引起立法委員及社會極大關注，立法院乃於 103 年 1 月大幅修正通訊保障及監察法，增加受監察人之程序保障、限縮監聽對象及明定監聽資料發現另涉他案犯罪行為等證據之使用等規定，以極大幅度限縮執機關對於偵查犯罪之功能，對偵查犯罪機關之衝擊不可謂不小。

再者，網際網路無遠弗界的穿透力及提供資訊的流通性，更助長犯罪的便利，網路犯罪匿名性、無地域性及資料混雜等特性，也為執法者刑事偵查的技術及法定程序，帶來新的挑戰，網路科技發展一日千里，使得犯罪偵查困難性勝於以往，因此如何使網路通訊監察法制明確化，降低對於網路發展之阻礙，是一值得研究之課題。

第二節　研究方法

在撰寫本文前，為瞭解對以加密通訊軟體之通訊監察實施方式，先行蒐集網路及書籍、論文相關議題的資料加以研讀、整合。本文係採文獻分析法、比較研究法及系統整理法：

一、文獻分析法：大量蒐集有關實務、學術對於網路通訊監察之方式，及探討美國、日本對於通訊監察之法規制定情況。

二、比較研究法：透過對於上開所蒐集資料之分析，了解目前美國、日本對於網路通訊監察之立法概況，再對比我國刑事訴訟法、通訊保障及監察法關於通訊監察制度有無引進之必要。

三、系統整理法：先研擬論文大綱，並依現有大綱將蒐集之資料分門別類融會貫

通後，歸納出適合我國未來在修正刑事訴訟法、通訊保障及監察法新的思考方向。

第二章　通訊監察之外國立法例簡介

第一節　日本「犯罪偵查之通信監聽相關法」

早期之日本學說向來認為電話監聽，屬於日本刑事訴訟法第 197 條第 1 項但書規定之強制處分，依該條規定：「為達偵查目的，得進行必要調查，但關於強制處分，除本法有特別規定者外，不得為之。」(即強制處分法定原則)。惟日本刑事訴訟法，有特別規定之強制處分類型僅有搜索、扣押、鑑定及勘驗四者，因而實務上自平成 3 年 5 月 1 日甲府簡易裁判所之裁判官，對覺醒劑販賣案件核發勘驗票，認依勘驗票得對該犯罪案件使用電話之通話內容進行監聽。

惟依強制處分法定原則，通訊監察於刑事訴訟法並無明文可據，實務創造之勘驗說，法理上仍有其問題存在，故為妥適解決多年來實務上對刑事訴訟法規定之通訊監察，確有必要以法律明文規定監聽強制處分之要件、程序，以解決適用上諸多疑義。最後國會終於在平成 11 年 8 月 17 日通過第 137 號之「犯罪偵查之通信傍受相關法」，同時於平成 11 年 12 月以第 160 號法律案修正後，以平 12 政第 390 號政令，公布自平成 12 年 8 月 15 日開始實施。自此，日本監聽之強制處分，乃正式取得法源依據。

第二節　美國網路通訊監察法制介紹

第一項　簡介

美國犯罪調查多與通訊偵查相關，諸如電子郵件、電子通訊以及網路之偵查。早期美國聯邦最高法院認為，憲法第四修正案係為保障人民財產權免受公權力任意侵入之規範，由於通訊監察行為之實施，並未侵入人民之住居所，並無物

理上之侵入，亦即除非有「實體之物質侵入」(Actual Physical Invasion)情形外，言語談話並不包括於該條所保護人民之身體、住宅、文件及其他財物之範圍內[3]。但於 1967 年 Katz V. United States 一案[4]中，聯邦最高法院推翻了 Olmstead 案之「實體之物質侵入」說，認為憲法第四修正案保護之對象乃為「人」，而非「地域」，不僅指出以電子儀器對受監察人加以監聽係屬侵害其隱私權之行為，同時揭示司法機關依一定之適當程序核發監聽令狀(Interception Order)， 授權犯罪偵查機關所為之監聽行為方合憲，因此，美國國會於 1968 年之「犯罪控制及公路安全綜合法」(Omnibus Crime Control and Safe Street Act)第 3 篇中(第 2510 條至 2520 條)制定有關有線通訊及口頭對話監聽制度之規範(Wire Interception and Interception of Oral Communication)，並於 1986 年修正制定為「有線與電子通訊之截取及截取口頭對話法」(Wire and Electronic Communication Interception of Oral Communication)，作為監聽實施之法律規範[5]。

第二項　郵件

一、郵件及包裹資訊之接觸、取得

美國憲法第四修正案對於郵件保護之基本架構在百年前第四修正案解釋文中已明確宣示--Ex Parte Jackson 案[6]。Field 大法官在上開解釋意見書認為，因應郵

---

[3] 參照張銘晃著，論違法監聽資料之證據價值，法學論叢，93 年 7 月，頁 84。美國最早有關通訊監察之判例，係 1928 年 Olmstead V. United State 案，聯邦調查局人員於無令狀之情況下，在住所外之電話線上裝置竊聽器來監聽 Olmstead 與其律師之談話內容。美國聯邦最高法院認為，雖然 Olmstead 與其律師之談話內容被監聽，但並不違反憲法第四修正案之規定，蓋該條僅保障封緘信件(sealed letter)不被非法搜索扣押，電話並非憲法保護之範疇，且截聽電話非屬物理性之侵入，故聯邦調查局人員所為之行為合法。

[4] 轉引自江舜明著，監聽在刑事程序法上之理論與實務，法學論叢第 168 期，頁 101-102。在 Katz v. United States 中，最高法院推翻 Olmstead 案之非法侵入認定標準，並確立合理隱私之期待法則。在 Katz 案中，聯邦調查局官員得知被告經常使用特定之公用電話亭對外聯絡，而在電話亭外裝置竊聽器竊聽被告之通話，最高法院認為公用電話亭雖非被告之財產，且裝置之竊聽器亦無物理之侵入，但仍除依此所獲得之證據。其理由在於被告進入電話亭並關上門時，被告已表現出對其通話內容有合理隱私之期待，而政府之行動侵犯被告於使用電話亭時之正當信賴，已構成憲法第四修正案之搜索扣押，因事未獲得令狀許可，故排除依此所獲得之證據。

[5] 同前揭註。

[6] 96 U.S. 727,24 L.Ed. 877(1987).

件種類的不同，應有不同的處置方式，例如信件以及封緘的包裹應免受檢查，然而像報紙、雜誌以及宣傳小冊子等開放型之郵件，則應受到檢查。信件以及封緘的包裹受到完全的保護，除了外觀以及重量外，不受到檢查及檢驗。這個見解在日後為最高法院在百年後的 United States v. Van Leeuvwen 案[7]以及 United States v. Jacobsen 案[8]再度被引用。

依據上開 Ex Parte Jackson 案以及相關之見解，封緘之信件及包裹的內容，例如第一類郵件(first class mail)[9]及私人包裹，全然受到憲法第四修正案之保護，亦即此類信件的內容對於發信人、收信者有隱私權之合理期待(reasonable expectation of privacy)。發信者和收信者雙方在信件遞送過程中，對於信件之內容有隱私權之合理期待，且不論信件之運輸者是政府機關或是私人公司，例如 UPS 或是 FedEx.，均有隱私權之合理期待。

惟上開原則有二限制:一是信件及包裹之外包裝並無憲法第四修正案之保障，此可參照前述 Ex Parte Jackson 案中提及外觀及重量不在此限可知，在 Katz 案中對於隱私權之合理期待也是基於此一架構。因為信件或包裹之外包裝、體積以及重量是直接曝露在運送者眼前，所以無法援引對於隱私權之合理期待原則。其二，郵政機關檢查郵件並無隱私權之合理期待之適用，Katz 案之隱私權合理期待原則上不適用第四類郵件，亦即郵政機關有權在運送過程中檢查郵件，交寄人對於第四類郵件之內容並無對於隱私權之合理期待。

二、郵件及包裹之扣留

憲法第四修正案允許政府單位在取得搜索票搜索郵件前，短暫扣留郵件，第四修正案允許扣留郵件係指「對於個人財權之持有行為進行有意義之干預」[10]。在運送過程中拖延物品之運送最終會形成對於持有利益有意義之干預，此種干預

[7] 397 U.S. 249, 251, 90 S.Ct. 1029, 25 L.Ed.2d 282(1970).
[8] 466 U.S. 109, 114, 104 S.Ct. 1652, 80 L.Ed2d 65(1984).
[9] 美國普通郵件(general mail)分 4 類:第一類郵件是書信，第二類是報章雜誌，第三類郵件則是書籍、小冊子等，第四類郵件則為商品。
[10] United States v. Jacobsen, 446 U.S. 109, 104 S. Ct. 1652, 80 L.Ed.2d 85(1984)

即為「扣押」(seizure)。

但得扣押標的物多久，方屬合理(reasonable)?Douglas 大法官在 United States v. Van Leeuwen 案[11]之見解可謂最高法院對於此問題最初方針，Van Leeuwen 案中郵政公司職員認為有一郵件很可疑，在取得搜索票進行檢查前，該郵件被扣押達 29 小時，Douglas 大法官認為此案應適用總體情況標準(totality-of-the circumstances test)[12]，當員警在取得搜索票之前對於郵件之扣押均屬合理，在對包裹有合理懷疑時，扣押住包裹遠較讓其流通於運送過程中更加謹慎。

三、郵檢制度(Mail Covers)

另一對於郵件之犯罪偵查需仰賴郵檢制度，郵檢制度規定於美國聯邦法規彙編(Code of Federal Regulations)第 39 篇郵政法規內。郵檢制度係指為取得資訊而對於封緘或未封緘郵件外觀所為非同意下之紀錄，或是依法對於未封緘郵件內容之紀錄，而取得該資訊之目的，係基於 1.保護國家安全；2 追索逃犯；3.搜集犯罪或著手於犯罪之證據；4.搜集違反或是著手違反郵政法規之證據；或 5.協助可沒收的財物之確認。任何執行機關只要釋明郵檢程序有其必要，即可進行檢查。而郵檢並無第四修正案之適用或有聲請搜索票之必要，因為郵件之外觀或是未封緘郵件之內容並無隱私權之合理期待。

第三項　電信監聽及憲法第四修正案

一、搭線監聽(Wiretapping)和竊聽(Eavesdropping)[13]

現今通說均認電話對話內容係受第四修正案所保護，政府執法單位植入竊聽器而聽取對話內容，係構成第四修正案規範之「搜索」(search)。惟最高法院前

[11] 397 U.S. 249, 90 S.Ct. 1029, 25 L.Ed.2d 282(1970)

[12] 係指傳聞證據(hearsay)是證明力是否達有合理根據(probable cause)而得核發搜索票。依此一標準，傳聞證據之證明力應就全體情況來判斷，而非僅考慮其中一因素。

[13] 所謂 wiretapping 搭線監聽係指裝設監聽設備而聽取對話內容；竊聽(Eavesdropping)是為在線民、便衣員警身上掛竊聽設備而聽取對話內容。

於 Olmstead v. United States 案[14]認為搭線監聽並不該當於搜索，因為監聽並不可類比為司法單位實體侵入個人私人領域，例如:家、住處等搜索行為，使用電話不過係以電線之方式將聲音對外發布，因此第四修正案並不保障此種以電線發聲之方式。然而，此見解具有極有爭議性，嗣在 Berger v. New York 案[15]及 Katz v. United States 案[16]間接被最高法院推翻。最高法院在 Berger 案中認為紐約州監聽法係違憲，因為該法未達第四修正案之防衛門檻，而在 Katz 案中，美國聯邦探員將麥克風放在 Katz 非法下賭注時所使用之公用電話亭內，最高法院認為此舉違反第四修正案，在 Katz 案中，正式宣告 Olmstead 案見解不再適用，自此，執行單位對於私人電話之監聽或是竊聽均應屬搜索行為，皆有第四修正案之適用。

二、監聽及竊聽屬搜索原則之例外

如上所述，在 Katz 案中，最高法院確立政府對於私人電話之監聽或竊聽係屬搜索行為，然仍有下列之例外情況:

(一)、經通訊之一方同意監聽者--不論同意之人係在政府請求而自行錄下電話對話或是由執行單位裝置監聽設備而錄下電話對話，均屬之。此種方式之監控並未侵害在對話中之任何一人之隱私權。

(二)、憲法第四修正案係允許政府單位攔截（intercept）以電波方式廣播之電話，亦即法院通說認為攔截無線傳送之電話通話並不違反第四修正案，因為無線電話之通話攔截裝置僅係截取向公眾傳送之電波之訊號，而攔截並未違反任何隱私權之合理期待[17]。

三、撥打之電話號碼以及簡訊

電話聯絡方式有二種:一是以講話方式行之，另一則是在手機鍵盤上鍵入數

[14] 277 U.S. 438, 48 S.Ct. 564, 72 L.Ed. 944, 66 A.I.R. 376(1928).
[15] 388 U.S. 41, 87 S.Ct. 1873, 18 L.Ed.2d. 1040(1967).
[16] 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d. 576(1967).
[17] 例如: Tyler v. Berodt, 877 F.2d. 705, 707(8th Cir. 1989)或 Price v. Turner, 260 F.3d 1144, 1149(9th Cir. 2001).

字或字母、符號等，而電話使用者撥號有二種目的:一是為了接通電話，而撥打電話之門號，係為聯絡電信公司以達到與他人通話之目的；第二，在接通電話後，使用者或許想利用鍵盤傳送訊息，現今最常使用此類的方式，即是簡訊。政府搜集此類之數字或字母，是否有第四修正案之適用?

在 Smith v. Maryland 案[18]，在執法單位要求下，於馬里蘭州巴爾的摩電信公司之中央機房裝設電話紀錄器(pen register)[19]以搜集一件騷擾案(harassment case)之犯罪證據，目的在監控該騷擾之電話是否來自於 Smith 之住處，Blackmun 大法官在理由意見書中指出:使用電話紀錄器取得 Smith 從住處電話撥出之門號並未違背 Smith 對於隱私權之合理期待，因此並不屬於第四修正案所定義搜索之範疇，因為 Smith 在撥號的當下，知悉其所撥出之號碼係向電信公司發送，所以當 Smith 使用電話時，其是自願向電信公司傳遞該門號之資訊並在傳送號碼之過程中自動揭露此一資訊，Smith 在撥打門號時即已知電信公司可能將撥打之門號訊息透露予警方之風險。而電信交換設備等同於早年為用戶接通電話之接線生，倘 Smith 係經由接線生接通電話，其並無法主張對於隱私權有任何之期待，因此最高法院認為即便電信公司使用自動化接線設備，法律見解也無二致。

雖然現今之法院判決就 Smith 案之解釋方向並未區別其不同之處，但基本上就 Smith 案有兩種基本解釋之方向:其一、此案僅係前述通話保障之例外規定之再次闡述，因為電話公司是 Smith 撥打號碼之一方，因此電信公司得同意監控。第二種解釋是:此案擴張解釋認為電話撥出之號碼並不受到第四修正案之保障。

此二者之差別對於監控撥通後傳輸之數字(post cut-through dialed digits)影響甚鉅，這些在撥通後所輸入之數字、符號係對受話者傳送通話內容，而非對於電信公司。是以，法院應持撥通後輸入之數字及簡訊並不適用 Smith 案之見解，而應受 Katz 案之保障之見解，因為電信公司並非撥打者所欲傳送撥通後傳輸數字或簡訊之對象，電信公司記錄此種數字或簡訊與電信公司聽取電話通話內容之情

[18] 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220(1979)
[19] 美國執行單位在電話中置入該裝置以監控撥出之號碼，但不監聽通話內容。

況並無不同，二者均應受第四修正案之保障。

第九巡迴法院在 Quon v. Arch Wireless Operating Co.案[20]認為，簡訊服務之使用者對於儲存在電信公司伺服器內之簡訊有隱私權之合理期待，因為簡訊與信件之性質並無不同。

第四項　網路通訊監察與憲法第四修正案

一、簡介

目前對於憲法第四修正案應如何適用於政府對於網際網路之監聽之法律見解仍無定論，全然依靠類比電信使用方式或是郵政系統方式來解釋，亦即法院多依靠將電腦通訊方式類比成傳統通訊方式來解釋第四修正案之適用。因此，目前多認為網際網路通訊內容(content)係受第四修正案之保護，而與內容無關者，則不受第四修正案之保障。

二、與內容無關之資訊(Non-Content Information)

第九巡迴法院在 United States v. Forrester 案[21]之判決係法院首度討論第四修正案與內容無關之網際網路通訊之關係，Forrester 及其共同被告 Alba 因製造迷幻藥而受調查，調查單位取得電話紀錄令(pen register order)以監控 Alba 住處之個人電腦網路使用量，網際服務提供業者(ISP)Pacbell Internet 公司在調查單位出示電話紀錄令之要求下，於機房置入 mirror port[22]，使調查單位得以知悉 Alba 往來電子郵件住址、Alba 瀏覽網頁之 IP 位址，以及所有從其郵件帳戶寄出、接收之容量訊息。

第九巡迴法庭認為此類之監聽並非第四修正案中所定義之「搜索」，因為此種監聽方式與前述 Smith v. Maryland 案之電話紀錄令相當。政府單位在監聽電子

[20] 29 F.3d. 892(9th Cir. 2008).
[21] 495 F.3d 1041 (9th Cir. 2007).
[22] 是指以旁路模式(mirror)來側錄封包，即複製電腦之所有流量後，轉送至其他電腦之程式。

郵件位址或許在科技運用上有所不同，但概念上與監看實體郵件相差無幾。過去19世紀累積之案例，最高法院向來認為政府不得對於封緘郵件之內容實施無令狀搜索（warrantless search），但得觀察任何郵件外觀之資訊，因為這些外觀資訊係寄件者自願向第三方揭露。電子郵件如同實體郵件一般，具有對第三方－即資訊運送者揭露外寄之位址和僅收件者得閱讀之內容，實體郵件與電子郵件這二種通訊方式，就隱私權而言，係如出一轍，郵件之內容或受第四修正案之保護，惟地址及信件之重量、尺寸，並不在保護之範疇。

三、通訊之內容

雖然電子郵件以及網際網路之使用日趨頻繁，惟美國案例對於第四修正案應如何適用於電子郵件以網際網路之通訊監察著墨不深。如前述之 Quon v. Arch Wireless Operating Co.案[23]，第九巡迴法院認為簡訊服務使用者對於儲存在服務提供業者之伺服器內之簡訊有合理隱私之期待，第九巡迴法院係將簡訊服務與實體信件相類比而得出上述結論。若他法院與第九巡迴法院持相同見解，則私人網際網路通訊內容亦應同受第四修正案之保護。

有鑑於第四修正案應如何適用於電子郵件之見解尚無定論，是以探討反方見解，亦即電子郵件監察不受第四修正案拘束仍有其必要。持反方見解最主要立場在於網際網路服務提供業者（ISPs）性質只是媒介（intermediary），係一能接觸所有傳送內容之媒介。以此推論，電子郵件性質與第三類郵件[24]或是無線電話性質類似，在傳送過程中，業者勢必接觸到通訊之內容。此種見解乍聽似乎合理，但並非無懈可擊，第三類郵件以及無線電話不受第四修正案之保護，是因傳送之內容在運送過程中係有意揭露第三人，惟電子郵件傳送過程中，電子郵件之內容僅係經由網路發送，只經由機器轉送，ISP 業者並無法接觸電子郵件之內容。因此，較佳之類比方式是將私人電子郵件性質類比為傳統電話通信以及第一類信

[23] 29 F.3d 892(9th Cir. 2008).
[24] 即書籍、傳單以及其他不屬於第一、二、四類之郵件。

件。

倘日後法院接受此一見解，即將網際網路通訊內容歸類在第四修正案保護範疇，而與內容無關之通訊，則不在此限，厥應審究者，內容及與內容無關之通訊的界線何在？郵件寄送人對於其電子郵件帳號以其他網際網路通訊之隱私權合理期待之一般規則為何？

四、內容和與內容無關之資訊之界線

通訊中，與內容無關之資訊通常係在信封上足供資料從甲地傳送至乙地之資訊；而內容資訊則是寄件人只限與收件者分享之訊息。因此，就電子郵件而言，郵件之內文以及主旨欄係與內容資訊，而 IP 位址、電子郵件信箱名稱、郵件容量大小則屬與內容無關之資訊[25]。

惟在某些案例上，內容資訊和與內容無關資訊之界線仍很微妙。譬如，A 在電子郵件附檔裡寄送一連串之電子郵件地址，則這些電子郵件地址仍屬內容資訊，而非只是與內容無關之電子郵件信箱住址。其次，有些情況界線更屬模糊，在 Forrester 案，法院在註腳中提及一致資源定址器（Uniform Resource Locator, URL）應被類比為電話號碼，但另一方面，URL 在某些網站，譬如搜尋引擎，會包含使用者鍵入之內容，例如搜尋之字串，因此界線應設在何處，就第四修正案而言仍很模糊。

五、第四修正案對於電子郵件以及網際網路通訊保障之例外

若法院建立起通說認為網際網路通訊中關於內容之資訊受到憲法第四修正案之保障，下一個問題是：這個原則適用之範圍到何處？以郵件以及無線電話通訊為例，原則上係受第四修正案之保障，但仍有一些例外，例如：第三類信件或無線電話通訊時保障受到若干節制，或是政府雇員使用公部門電子郵件信箱之隱

[25] 參照前述 Ferrester 案

私權則應適用政府機關雇員之隱私權[26]，亦即在使用公部門電子郵件前給予通知表示該電子郵件將受到監督，則政府雇員得援引第四修正案主張之隱私權將受到限縮。

現今許多人使用假資料、假姓名申請電子郵件信箱，有些 ISP 業者傾向保障客戶隱私權，但有些則持否定見解，且信件伺服器有些設在美國境內，但更多是設在境外，則在此種情況下，隱私權之合理期待可以擴及何處？這個問題，迄今莫衷一是。

第五項　與網路監聽相關之法制沿革

網際網路監察之相關規定有二，一是如前所述之憲法層級之保障，另一則是州政府與聯邦政府之法規保障，這些法規包括規範監聽、竊聽、調閱 ISP 業者儲存之資料。

第一部關於聯邦監聽法規係 1934 年之通訊法（Communication Act）[27]，該法原則認為除經寄件者授權外，任何人不得攔截通訊資訊，亦不得洩露、公布內容、主旨或通訊內容之含義。在 Nardone v. United States 案[28]，最高法院認為違反該法規所取得之證據應被排除。

在 1960 年代，通訊法已不足以規範電話監聽，國會在參照最高法院在 Berger v. United States 案[29]關於監聽以及 Katz v. United States 案[30]關於竊聽之見解而制定監聽法（Wiretap Act）以規範竊聽—在屋內植入竊聽器以及監聽—攔截私人通話之依據。監聽法一體適用於政府機關與私人，嚴格限制使用裝置攔截口語對話 oral communication（如：在人身上裝置竊聽器以錄取雙方對話）和使用裝置監聽電信通話（wire communication）（如：在電話上植入裝置以監聽在電話間之私人對話）。

---

[26] O’ Connor v. Ortega, 480 U.S. 709, 107 S.Ct. 1492. 94 L.Ed.2d 714(1987)
[27] 47 U.S.C.A. § 605
[28] 302 U.S.379,384,58 S.Ct. 275, 82 L.Ed. 314(1937).
[29] 388 U.S. 41, 87 S. Ct. 1873, 18 L.Ed.2d 1040(1967).
[30] 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d, 576(1967).

州法院及聯邦法院均適用該法，執法單位得依監聽法之規定取得法院命令以進行監聽，只需釋明有合理懷疑及滿足其他要件，即可聲請。監聽之搜索票門檻遠高於其他搜索票之聲請要件，因此監聽票在實務上常被稱為「超級搜索票」（super warrants）。

監聽法有效且廣泛規範政府單位如何取得傳統電信通話資料之程序，然而在 1980 年代關於網際網路之搜索更具急迫性，因此在 1986 年，美國國會通過電子通訊隱私權保護法案（Electronic Communication Privacy Act，簡稱 ECPA）以填補法規對於現代電腦通訊監聽程序之漏洞，ECPA 包括三部分：一、擴張監聽法範圍，適用對象及於電子通訊部分；其二、制定關於取得儲存電子資料之規定，亦即聯邦儲存通訊法（Stored Communications Act.）；三、則是撥號紀錄器法（Pen Register Statute），呼應前述 Smith v. Maryland 案之精神。此三項法規均規定於美國法典第 18 篇。

ECPA 在 1986 年所建立之基本架構迄今仍適用，架構建立在兩種不同之原則上：一、對未來通訊監聽與已發生之通訊監聽之差別以及二、通訊內容與非通訊內容之差別。

對未來之通訊監聽(Prospective surveillance)係指在傳送通訊時，藉由在特定網路端點裝置監聽設備掃瞄通過該端點之方式取得通訊資訊，而對已發生之通訊監聽(Retrospective surveillance)則指讀取儲存在第三方即 ISP 業者的傳送資訊。例如：FBI 傳喚 ISP 業者提供某網路帳戶註冊者之資訊，則屬對已發生之通訊監聽，ISP 在傳送通訊過程中，通常自動產生紀錄，FBI 所欲傳喚命提出者是 ISP 業者儲存於伺服器之資訊。

所謂通訊內容係指從寄件者傳送至收件者訊息之主要內容；而與內容無關之資訊則係寄件者為使訊息能到達收件者所提供之資訊或其他網路自動產生之資訊。

監聽法(Wiretap Act)及撥號紀錄器法(Pen Register Statute)係規範未來發生資訊之監聽，而聯邦儲存通訊法(Stored Communications Act)則針對已發生資訊之監

聽。在未來發生資訊之監聽中，監聽法處理內容資訊之監聽，而撥號紀錄器法規範取得與內容無關之資訊。基本架構整理如下表格所示:

	未來發生資訊之監聽 (Prospective)	已發生資訊之監聽 (Retrospective)
內容(Contents)	監聽法 (Wiretap Act)	聯邦儲存通訊法(Stored Communications Act)
非內容(Non-Contents)	撥號紀錄器法 (Pen Register Statute)	聯邦儲存通訊法

第六項　監聽法（Wiretap Act）

一、有線(Wire)、口語(Oral)及電子(Electronic)通訊

監聽法主要保護對象為參與通訊雙方之通訊隱私權，該法原則禁止非通話當事人之第三方使用電子儀器或其他裝置攔截通訊資訊，惟法規有特別規定則不在此限。監聽法保障三種通訊方式:有線通訊、口語通訊以及電子通訊，一般而言，有線通訊係指撥打電話；口語通訊則是雙方間私人對話；電子通訊則指藉由電腦科技傳送之通訊。

(一)、有線通訊

監聽法定義有線通訊如下[31]:任何全部或一部經由電線(wire)、電纜(cable)或其他相類之設備進行聲音傳輸，經由提供服務或設備之人協助、運作而連接傳送方與接收方，以進行州際間或國外通訊或是影響州際間或國外交易之通訊。聲音傳

[31] 18 U.S.C.A.§ 2050(1) any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.

輸是包括人類聲音在從發送點至接收點間任何點之傳輸，因此有線通訊必然包括人類聲音。雖然有線通訊在傳送過程中需全部或一部藉由電線、電纜或其他相類之設備，以電話通訊在某一點是需藉助電線來達成傳輸目的，縱然該部分是在機房內交換。雖然廣播傳送人聲在傳送或接收時需使用電線，然並不該當上述要件，因為傳輸過程中之任一點並未全部或一部藉由電線[32]。錄影監聽（video surveillance）如無人聲，則不成立有線通訊，因為欠缺「人聲」此一要件[33]。

（二）、口語通訊

監聽法定義口語通訊如下[34]：任何人類所發出之聲音，其在發聲時並未預期對話將遭攔截，且此預期在該情況下係屬合理。此迂迴之定義不免讓人產生疑問：政府使用監控裝置在這種狀況下是否侵害第四修正案所保障之隱私權合理期待？

在住處、私人辦公室或是飯店房內置入隱藏型麥克風以搜集私人對話，這種對話構成口語通訊，但另一方面，如果臥底人員或是線民穿戴監聽設備，或是對話之參與者，或在對話時，突然刻意出現在現場，則將對話錄下，並未違反對隱私權合理期待，且無口語通訊被攔截之情事。

（三）、電子通訊

監聽法定義電子通訊如下[35]：任何所有種類之符號、信號、書寫、圖像、聲音、數據或信息傳輸全部或一部藉由影響州際或國外交易之電線、廣播、電磁、光電、光學系統，惟下列項目不在此限：1.任何有線或口語通訊；2.任何經由語

---

[32] United States v. Rose, 669 F.2d. 23(1st Cir. 1982); United States v. Hall, 488 F.2d 193(9th Cir. 1973)

[33] United States v. Torres, 751 F.2d. 875, 885-86(7th Cir. 1974)

[34] 18 U.S.C.A.§ 2050(2) any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication.

[35] 18 U.S.C.A.§ 2050(12) any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—(A)any wire or oral communication;(B)any communication made through a tone-only paging device;(C) any communication from a tracking device (as defined insection 3117 of this title); or(D)electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

音呼叫器所發出之通訊；3.任何從追蹤裝置所發出之通訊；4.金融機構在基金之電子儲存及傳送通訊系統內儲存之電子資金傳輸資訊。

對於電子通訊定義範圍極其廣泛，實務上幾近囊括所有使用電腦之通訊方式，連非人聲之通訊，如電子郵件或是其他電腦網路傳輸均在定義內。如同有線通訊一般，電子通訊需為資訊之轉換，較獨特的是，轉換、傳送之過程中全部或一部需藉由電線、廣播或光學等物質，因此電子通訊必然包含始點端與終點端，在電話轉換資訊中，很容易解釋始點端與終點端，即電話筒與電話筒間，依靠電話線來轉換[36]。惟在電子傳訊中之始點端與終點端則較難界定。在 United States v. Scarfo 案[37]，調查員在取得搜索票後在被告電腦秘密裝置鍵盤側錄器（Key Logger System ,KLS），為了規避監聽法，KLS 設計成僅在電腦未連網時，記錄鍵盤之敲擊，地院判決認為 KLS 並未取得任何電子通訊，因為係在未連網時取得鍵盤敲擊之紀錄，電腦未連網時，自然無法產生電子通訊，在監聽法下定義之通訊，是州際間網路間之資訊轉換，單獨電腦在未連網情況下，並不具轉化之能力。

二、攔截（interception）

原則上，監聽法禁止任何故意攔截通訊[38]，所謂攔截係指使用任何電子、機械或其他裝置取得聲音或其他電線、電子或口語通訊之內容[39]。何謂「取得」（acquisition）、「內容」（contents）以及「使用電子、機械或其他裝置」（electronic, mechanical, or other device）？

（一）、取得

雖法條中並未明確說明「取得」有「時間」（temporal）之限制，法院解釋取

[36] Goldman v. United States, 316 U.S. 129. 133-134, 62 S.Ct. 993,86 L.Ed. 1322(1942)，此判決解釋 U.S.C.A47 編第 605 條，雖然 Goldman 案之憲法理論為 Katz 所推翻，但判決之法條適用並未被推翻，其原則迄今仍適用。

[37] 180 F. Supp.2d 572 (D.N.J. 2001).

[38] 18 U.S.C.A.§2511(1)

[39] 18 U.S.C.A.§2510(4) 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

得仍需與轉換同時發生[40]，是以監聽法所謂的取得，只在搜集資訊係在未來監聽、現在進行式之通訊，且搜集資訊需即時、且在傳輸中。多數電子通訊均在一瞬間儲存、轉換資料，倘若監聽裝置紀錄通訊之時間點，在通訊抵達接收方後之剎那，則取得資訊究屬與轉換同時或是在轉換已完成之後？

監聽法較諸憲法第四修正案規定之搜索票標準之保障更加提升，監聽法係受前述之 Berger v. New York 案啟發，最高法院在 Berger 案中表示第四修正案當在監聽連續性（series）或是持續進行中活動，而非一次性之侵入時，更應審慎以對，亦即依照最高法院對於 Berger 案之看法，規範繼續性或是進行中監聽應有特別隱私權之保護。

有鑑於監聽法與第四修正案之緊密關係[41]，對於攔截的定義應反映最高法院在 Berger 案界定出之區別，取得是對於部分連續性或是進行中之監聽之攔截，例如對於未來通訊監聽。確切之界線或許難以界定，惟本質問題仍在於分析此種監聽之方式是否與繼續中監聽有功能性相類似，或只是一次性，有限性接近通訊。

（二）、內容

監聽法僅適用於「內容」之取得，所謂內容係指使用任何有線、口語或電子通訊所傳送關於主要內容、主旨或是意義之資訊[42]。在個人對個人對話，「內容」係指從一方傳送至另一方之訊息；或是在電話通訊中，雙方之對話；亦或是在電子郵件中所傳達之訊息。

電子郵件之主旨欄也是屬於「內容」之一部分，電子郵件之附件，例如夾帶之文件，亦是欲傳送之訊息之一部分，附件縱然為圖片檔，也包括在內。所有通訊內容，與前述實體封緘郵件，在信封內所傳送之內容之概念相類似。

惟內容資訊並不包括與有線或電子通訊性質或傳送有關之撥號（dialing）、

[40] 例如：Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d. 457(5th Cir.1994)，縱使通訊資訊尚未被接收方接收，讀取已儲存之通訊資料並非攔截；United States v. Steiger, 318 F.3d. 1039(11th Cir.2003).

[41] United States v. Baranek, 903 F.2d.1068, 1072(6th Cir. 1990)

[42] 18 U.S.C.A.§2510(8) when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication

路由（routing）、信號(signal)資訊[43]。此種類包括所撥打之門號號碼、通話之長度、IP 位址、電子郵件住址，以及其他關於傳送之相類資訊，這些資訊如同包裹外包裝—其上載有寄件、收件住址、包裹重量、信封上之郵戳，這些資料是關於通訊之解釋資料(metadata)，並非傳收雙方間主要通訊目的。

內容資訊和與內容無關之資訊二者之界線在人對電腦之通訊案例變得越來越模糊，當一個人寄送通訊資料予他人，通訊之內容即是訊息本身，但當一個人寄送訊息予機器，「內容」之定義變得不明。然而，兩法院之判決已認定在 URL 輸入之搜索字串應構成通訊之「內容」[44]。

（三）、使用任何電子、機械或其他裝置

「攔截」必然包括透過電子、機械或其他裝置之使用而取得資訊，此等裝置係指任何得使用於攔截有線、口語或電子通訊之裝置或設備，但下列兩類裝置不在此限：1.任何電話或電報器具、設備或場所或任何零件及其有線或電子通訊服務提供者供應註冊者或使用者商務之過程，以及為註冊者或是使用使在商務過程中所使用。或是 2.為一般運輸業者在商務過程中使用之通訊或調查、執行者在執行職務中。而上述第二種豁免包括助聽器或矯正聽力至幾近正常之水準之其他相類裝置。

三、取得及執行監聽令之概述

攔截令(interception order)之核發要件係法官認對於某人正在、已經、將要犯罪之情況有合理根據(probable cause)[45]、與此犯罪行為相關之特定通訊能為此攔截令所取得、無其他一般調查之方法或其他調查方式過於危險者、以及將攔截資訊正被使用、即將被使用之場所與此犯行之關係或是與通訊相關之人[46]。

---

[43] 18 U.S.C.A.§3127(3)-(4)

[44] 在 Pharmartrak, Inc.329 F 3d. 9, 18(1st Cir. 2003)，法院認為監聽法對於內容之定義應包含個人可識別之資訊，例如姓名、出生年月日以及醫療狀況。在 Application, 396 F. Supp, 2d, at 49 建議在 URL 的搜索字串是內容，因其揭露使用者所欲搜尋資訊之主要內容以及意義。

[46] 18 U.S.C.A.§2518(3) Upon such application the judge may enter an ex parte order, as requested or as

攔截令需載明通訊受攔截之特定人身分、通訊之性質、場所以及授權攔截之核准、通訊之種類、涉犯之罪名、執行攔截之機關、核准之人、執行攔截之期間、或是當特定通訊被截聽後，該攔截是否主動終止[47]。不得核准超越攔截目的之期間或是逾 30 日，期間屆至前得聲請延長之，惟目的僅限於取得原先核准之標的。

有下列情況時，特別指派之執法人員得在未取得法院攔截令時執行攔截:1.有立即死亡或重傷害、有危國家安全之共犯或組織犯罪之共犯需使用通訊等緊急狀況；和 2.有相當理由認為攔截令將會核發。

---

modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that—(a)there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated insection 2516 of this chapter;(b)there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;(c)normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;(d)except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

[47] 18 U.S.C.A.§2518(4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify—(a)the identity of the person, if known, whose communications are to be intercepted;
(b)the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;(c)a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;
(d)the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and(e)the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.
An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance. Pursuant tosection 2522 of this chapter,an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

四、聲請程序

與一般搜索票得由任何執行人員聲請不同，依據本法所聲請之監聽票需由高階執行人員始得聲請。在聯邦體系，僅司法部長(Attorney General)、副司法部長(Deputy Attorney General)、次長(Associate Attorney General)或助理司法部長(Assistant Attorney General)或副助理司法部長(Deputy Assistant Attorney General)、或經司法部長特別指派之刑事司(criminal division)代理助理司法部長(Acting Assistant Attorney General)得聲請通訊搜索票[48]。

在 1986 年國會為增加對於電子通訊之保障，因而擴張不限司法部高層始得聲請監聽搜索票原則，在第 2516 條第 3 款增加任何檢察官均得聲請電子通訊搜索票，且得搜索之罪名亦不限於第 2516 條第 1 款，任何涉及聯邦重罪均得為電子通訊搜索聲請之罪名。

五、聲請內容

所有聲請書均應附上書面宣誓(oath)或確認書(affirmation)[49]，並應包括以下之內容[50]:釋明聲請人之聲請權限(敘明其擔任之職位係有權聲請)、調查或執法官員之身分及有權聲請、完全且詳盡說明何以聲請人認為搜索票應予核發之事實與情況:如某罪已經、正在或即將觸犯和通訊被攔截之機構和單位。另一要件係需說明何種通訊將遭攔截.

再者，法條規定聲請書需說明為何其他調查方式無法蒐證，或使用其他蒐證方式將有危險。此要件設計目的在於避免電子監聽成為「標準」的初步犯罪調查程序[51]，或是若使用其他傳統蒐證方法將使偵查中之案件曝光[52]。

監聽法規定聲請書需載明監聽之期間，或在已取得欲攔截之通訊，依監聽

[48] 18 U.S.C.A.§2516(1)　而特別指定係依工作頭銜而非現今任該職位之人之姓名，參見 United States v. Bynum, 763 F.2d 474(1st Cir. 1985)、或 United States v. Nnfro, 64 F.3d 98 (2nd Cir.1995)認經指定後，該指定適用於日後擔任該職位之任何人。

[49] 用以擔保其證詞為真實之陳述

[50] 18 U.S.C.A.§2518

[51] United States v. Giordano, 416 U.S. 505, 94 S.Ct. 1820, 40 L.Ed.2d 341(1974).

[52] United States v. Kahn, 415 U.S. 143, 94 S.Ct. 977, 39 L.Ed.2d. 255(1974)

方式之性質能否自動終止，以及在合理根據下，額外同種類之通訊自此後會產生之情況。

六、聲請之審查

在法官依據監聽法核發竊聽令前，法官需審核以下之要件:

1.有人正在、已經或即將觸犯 2516 條之罪名之合理根據；

2.有相當理由認經由攔截通訊，得取得與犯罪相關之證據；

3.經進行一般調查程序卻未能達到調查目的，或是合理相信其他調查程序即使進行或未能取得證據或過於危險；

4.在機動式監聽(roving wiretap)[53]之例外情況下，將被攔截之有線或口語通訊之相關人。

七、監聽票之內容

監聽法規定搜索票應詳列以下之內容以符合憲法第四修正案之特別要件，最重要者為：1.倘知悉受監聽人姓名，則攔截令應列受監聽人之姓名；2.受監聽通訊之性質以及監聽之處所、設施；3.受監聽通訊種類之詳述，以及所涉犯之罪名。

攔截令亦應包括執行監聽票之方式，包含：核准執行之期限，及註明核准攔截通訊應在實際可能時立刻執行[54]，此點亦反映出執行監聽票不僅在合理根據

[53] 在美國，機動監聽係指對特定監聽對象之監聽方式，例如，監聽對象以丟棄手機、或離開竊聽地等方式逃避監聽，通常需再聲請另一通訊搜索票，惟此一監聽方式，係針對受監聽人，縱於使用其他通訊設備，仍得依同一搜索票進行監聽。

[54] 18 U.S.C.A.§2518(5) No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not

之證據失效前儘速執行之需求，且點出此種搜索票與一般傳統搜索票不同之處，因為竊聽裝置植入通常不如一般搜索票容易執行。搜索票標註出攔截通訊核准之時間不得長於授權目的之時間[55]，或是長於 30 日[56]。

八、攔截侵害最小原則（Minimization）

監聽法規定執行攔截搜索票應該侵害最小之方式行之，不得逸脫授權攔截之範圍[57]，侵害最小化原則係來自於最高法院於 Berger v. New York 案[58]之判決，判決理由宣示紐約監聽法規部分無效，因該法在全然未考慮對話是否與調查中之犯罪相關，即允許裝置之設備攔截所有經過監聽設備覆蓋區域之人之合部對話。

依監聽票所得攔截之內容應限於取得核准罪名相關之證據，因為只要通訊係與核准搜索之罪名相關，如在某種程序上可提供與犯罪調查有關之證據之資訊，即不受攔截侵害最小化原則所限制，不以包括能證明通訊發送人直接有罪之證據為限。法院對攔截侵害最小化原則下一註解：認為侵害最小化原則係在政府在達到合法監聽目的下，能將監聽範圍縮減至最小之可行性而執行[59]。

九、監聽後通知

在提出核准聲請令之合理時間內，法官應通知受監聽人，惟不得逾 90 日，通知內容應包括：1.聲請或是核准攔截之事實；2.侵入（entry）日期以及核准、駁回攔截之期間；3.在核准期間內，有線、口語或是電子通訊是否被攔截。應受

---

otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

[55] 18 U.S.C.A.§2518(4)(e)

[56] 18 U.S.C.A.§2518(5)

[57] 18 U.S.C.A.§2518(5)

[58] 288 U.S. 41, 87 S. Ct. 1873, 18 L. Ed.2d 1040(1967).

[59] United States v. Turner, 528 F.2d 143 (9th Cir. 1975).

通知人係在攔截令或是聲請上列名之人，或是經法官認為應通知與列名之人通訊之人。

十、封存（sealing）

任何有線、口語或電子通訊攔截之內容如有可能，應儲存於磁帶（tape）或電子或其他相類之裝置，以保存記錄內容免受編輯或其他方式篡改。在核准期限或是延長期限到期，應製作成記錄供法官參閱，以及在法官之命令下封存。最高法院認為封存係為確保電子監聽取得之證據之可靠性及完整性，政府無法進行竄改、修改或是編輯已錄製之對話[60]。

十一、證據排除規定

監聽法明文有線、口語通訊之非法監聽所取得之證據應予排除，但電子通訊不包括在內[61]。美國法典 2518 條 10 項 a 款[62]:任何受害者基於以下理由，得依據本章之規定，提出異議，請求排除任何有線或口語通訊截收取得之內容，或因此內容衍生之其他證據:

1.通訊係非法截收；

2.自形式以觀，授權截收之命令或許可並不適當；或

---

[60] United States v. Ojeda Rios, 495 U.S. 257, 110 S.Ct. 1845, 109 L.Ed,2d 224(1990)

[61] United States v. Steiger, 318 F.3d 1039,(11th Cir. 2003)

[62] 18 U.S.C.A.§2518(10) **(a)**Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that—
(i)the communication was unlawfully intercepted;
(ii)the order of authorization or approval under which it was intercepted is insufficient on its face; or
(iii)the interception was not made in conformity with the order of authorization or approval.
Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

3.截收並未遵守於授權命令或許可。

第 2515 條[63]規定非法截收之有線或口語通訊之內容不得在任何審判、聽證、或在法院、大陪審團等之任何程序中作為證據，其他自此內容衍生所得之內容亦不得採為證據。

本條所稱之被害人係指其隱私權受到侵害，此定義係參照憲法第四修正案之證據排除原則所定之範圍[64]，然而二者仍有些許差異，即監聽法之證據排除規定，關於受到私人或政府非法監聽所取得之證據均適用，然唯一持反對見解係第六巡迴法院在 United States v. Murdock 案[65]採取「淨手」原則(clean hands)[66]。第六巡迴法院在 United States v. Murdock 案認為，只要政府未參與非法監聽，即允許政府得使用竊聽所取得之證據。在 Murdock 案，被告妻子竊錄丈夫在其所經營之殯儀館之電話通訊，妻子因此得知丈夫在擔任學校董事會主席時，曾接受某牧場為取得政府標案而交付之 9 萬元美金之賄款，被告妻子以匿名方式將受賄過程洩露予政府標案之投標廠商，該廠商持錄音向政府檢舉，執法機關因而起訴 Murdock 因未將該 9 萬美元之所得提報予政府而逃漏稅之罪。Murdock 就該錄音證據主張應予排除，惟法院認為雖然被告之妻錄下電話通話，係違反監聽法，惟該違法行為並未禁止該錄音證據使用於審判程序，且被告之妻之錄音行為與第四修正案之私人搜索類似，監聽法並未排除檢察官使用形成落入檢察官手裡之證據。

美國法典 2518 條 10 項 a 款(iii)規定，證據排除只限於截收未遵守授權命令或許可，最高法院指出只有當授權命令或許可之瑕疵係未能滿足在明顯要求使用特殊監聽設備之情況下，直接且本質性貫徹立法意旨要求限制截收程序之法律要

[63] 18 U.S.C.A.§2515 Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

[64] Scott v. United States, 436 U.S. 128, 139, 98 S. Ct. 1717 56 L.Ed.2d 168(1978)

[65] United States v. Murdock 63 F.3d 1391,1404(6th Cir. 1995)

[66] 即在他人被起訴之案件中，某人行為係正當、合法。

件時，始足當之[67]。因此，此授權之瑕疵必然是在防止無票監聽或電子監控時扮演核心或功能性的角色[68]，是以法院在判斷時需區分技術性之瑕疵或是本質性瑕疵。

例如，在 United States v. Donovan 案[69]，執行機關探員合法執行監聽票，得知受監察人與其他人討論賭博，探員聲請延長監聽時，未在聲請書列舉其他人，最高法院認為雖然監聽票違反法規規定之姓名要件，但並不會排除因此所取得之證據，因為該要件並未扮演本質性之角色。當有兩人之姓名並未列舉在清單上，導致該二人在起訴後八個月始收到監聽通知，最高法院仍認為該監聽所得之證據不應被排除，因為立法時並未將依據監聽程序之監聽後通知視為獨立限制條件。

第七項　撥號記錄器法(The Pen Register Statute)

一、撥號記錄器法概述

撥號記錄器法可細分為二部分：撥號器法（Pen Registers statute）和監測追踪法（Trap and Trace Devices statute），規定於美國法典 18 編 3121 條至 3127 條。撥號記錄器法可以類比為監聽法中，監聽與內容無關之資訊。相較於監聽法，撥號記錄器法較少受到公眾關注，且限制較寬鬆、例外部分更廣泛，其刑事處罰亦較輕微。

本法於 1986 年由國會通過，制定目的係為呼應最高法院於 Smith v. Maryland 案[70]宣示，認為以撥號記錄器監控自電話撥出之號碼，並非第四修正案所定義之搜索，本法係為規範二種監聽與內容無關之電話通訊設備使用，一是電話記錄器，另一則是監測追踪器，監測追踪器係記錄來電電話號碼。之所以稱為監測追踪器，因為搜集來電電話號碼原來需依靠電話公司使用 terminating trap[71]追踪電話

[67] United States v. Giordano, 416 U.S. 505, 527, 94 S.Ct. 1820,40 L.Ed.2d 341(1974)
[68] United States v. Chavez, 416 U.S. 562, 578, 94 S.Ct. 1849,40 l.Ed.2d. 380(1974)
[69] United States v. Donovan 429 U.S. 413,97 S.Ct. 658,50 L.Ed.2d 652 (1977).
[70] 442 U.S. 735, 99 S.Ct. 2577,61 L.Ed.2d 220(1979).
[71] 參見 United States, 610 F.2d. 1148, 1151 (Cir. 1979)

號碼。本法除有法院命令或其他規定之例外情況，不得安裝撥號記錄器和監測追踪器。

科技之進展使撥號記錄器法之使用顯得不合時宜，因為現今電話網路皆以電腦化，電線公司不再使用撥號記錄器或是監測追踪器判斷去電及來電的電話號碼。而 2001 年所制定美國愛國者法案(USA Patriot Act)修正撥號記錄器法，使本法得以適用於與內容無關之網際網路通。國會以最小變動之方式，透過修正第 3127 條第 3 款、第 4 款對於撥號記錄器及監測追踪器定義之方式，使本法能適用於網際網路之監聽上。

愛國者法案第 216 項(section)將 1986 年撥號記錄器法中以電話監控為中心轉換為聚焦於電話及網際網路通訊中與內容無關之住址資訊。撥號記錄器定義為:記錄或解碼(decode)經由電線或電子通訊轉換之設施或設備而傳送之撥號、路由、位址或信號資訊裝置或程序，惟不包括任何與內容相關之通訊[72]。監測追踪器則為:捕捉進來之得以識別原始號碼或其他撥號、路由、位址和信號資訊電子或其他脈衝而得以辨識有線或電子通訊之來源之裝置或過程，惟不得捕捉與內容有關之資訊[73]。

因為賦予舊法新定義，執法單位得依本法之規範搜集與內容無關之電話與網際網路通訊之撥號、路由、位址或信號資訊。本法所規範在於資訊搜集而非裝置性質本身，舉例來說，若是執法單位裝設嗅探器(sniffer)[74]以搜集與內容無關之

---

[72] 18 U.S.C.A.§3127(3) the term “pen register” means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

[73] 18 U.S.C.A.§3127(4) the term “trap and trace device” means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

[74] 嗅探器原本係網路監聽側錄產品名，現多用以成為封包監聽之代名詞。嗅探器秘密捕捉經由網路數據之過程，駭客用之盜取用戶名稱與密碼。

位址資訊，例如 IP 標頭(header)，嗅探器之功能就如同撥號記錄器(搜集來源資訊)和監測追踪器(搜集終點資訊)。網際網路通訊通常結合來源及目的資訊，因此監聽裝置變成兼具兩種功能即撥號追踪功能(pen/trap)，法院核准監聽時，通常亦是指撥號追踪令(pen/trap order)。

二、撥號記錄令(Pen Register Order)之聲請

任何檢察官均得向管轄區域之法官聲請撥號記錄令，其聲請書應載明:1.敘明聲請人係政府檢察官或是州執法單位、調查單位之檢察官身分；2.聲請人釋明即將取得之資訊與現在進行之犯罪調查相關[75]。聲請者只需具備以上要件，法院進行形式審查後，即應核發撥號記錄令。

三、撥號、路由、位址或信號資訊

美國愛國者法案以修正對於撥號記錄及監測追踪定義之方式，闡明撥號記錄器法得完整適用於網際網路通訊，修正後，撥號記錄器及監測追踪器係泛指所有得截取撥號（dialing）、路由（routing）、位址（addressing）或信號（signaling）資訊（簡稱為 DARS）之設備，惟截取之標的不包括與內容有關之資訊。

DARS 概念為現代通訊網路產生許多與內容無關，但包括傳送通訊以及通訊狀態之資訊，這些資訊或用來撥打目的電話號碼、按規定路線從電腦間發送封包、或將電子郵件寄往指定之位址，因此 DRAS 概念已擴及所有與內容無關之通訊資訊，如：撥打過之電話號碼、通話之長度、IP 位址以及電子郵件位址等。

DARS 與和內容資訊之界線，在一致資源定址器（Uniform Resource Locator, URL）案例，顯得非常模糊。當使用者在瀏覽器輸入 URL，瀏覽器寄送查詢指令至區域名稱伺服器（domain name server, DNS）要求伺服器回傳在 URL 之區域名

[75] 18 U.S.C.A.§3122(b) An application under subsection (a) of this section shall include—
(1)the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and (2)a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

稱 IP 位址，例如：www.moj.gov.tw，當區域名稱伺服器回應，第二個指令寄送指向區域名稱 IP 位址，因為 IP 位址聯繫不同區域名稱係屬公開資訊，因此區域名稱 URL 應如同 IP 位址一樣，被視為 DRAS。另一方面，但 URL 包括搜尋字串時，該搜尋字串應屬於監聽法下之「內容」而非撥號記錄器下所定義之 DARS。

行動通信基地台（cell-site）資訊既非 DRAS 亦非內容，行動通信基地台資訊搜集行動電話位置之即時資訊。則搜集行動電話位置之即時資訊應如何規範？在 United States v. New York Telephone 案[76]，聯邦法院得在監聽法外，適用聯邦刑事訴訟法（Federal Rule of Criminal Procedure）第 41 條和 All Writs Act 核發監聽票，依 41 條核發監聽票之門檻為合理根據（probable cause）。

四、撥號記錄器法之例外規定

原則上，撥號記錄器法在法院未核發追踪令時，禁止裝設撥號記錄器或監測追踪器，惟例外規定於第 3121 條 b 項，例外規定最重要者為使用者同意，如此一來，可確保來電顯示（caller ID）服務不會是非法服務。

在下列情況下，撥號記錄器法允許通訊服務提供者得安裝及使用撥號記錄器與監測追踪器：1.關於有線或電子通訊服務之運行、維護以及測試或保護服務提供者之權利或財物；或 2.為保護服務提供者及服務使用者免於詐欺、非法濫用使用服務，而記錄有線或電子通訊之開啟、終結。

第八項　聯邦儲存通訊法（The Stored Communications Act）

一、聯邦儲存通訊法之綜觀

監聽法與撥號記錄法規範如何截取經由網路傳送，且係未來發生(prospective)通訊之資訊，而聯邦儲存通訊法則是針對儲存於正常交易中之使用者帳戶資訊。

[76] 434 U.S. 159, 98 S.Ct. 364, 54 L.Ed.2d. 376(1977)

聯邦儲存通訊法規定於美國法典第 18 編第 2701 條至第 2700 條。監聽法和撥號記錄器法適用範圍較廣泛，包括經由網路傳送通訊之取得，相反的，聯邦儲存通訊法則僅規定關於兩種特別服務提供者之合法顧客和註冊者。

因對於第四修正案是否適用於儲存之電腦網路通訊有所疑義，是以國會於 1986 年制定聯邦儲存通訊法。制定本法之目的係為取得政府執行機關和持有使用者隱私資訊之服務提供者兩種間之衡平，本法限制政府強制提供者揭露其客戶與註冊者之資訊，同樣地，也限制 ISP 業者自願向政府揭露關於其客戶與註冊者之資訊。

二、電子通訊服務和遠端計算服務(remote computing service)提供者

聯邦儲存通訊法創設關於兩種特定網路提供者之顧客與註冊者之權利，電腦網路帳戶持有者在制定法律當時，通常以下列兩種方式使用第三方網路服務提供:一是帳戶持有者使用其等帳戶來傳送及接收通訊，例如:電子郵件。使用電腦網路傳送資訊，引發侵害隱私權之疑慮，因為在傳送及接收之過程中，通常會複製訊息及將訊息暫存於待傳送資料區。這些因為電子通訊服務提供者在傳送過程中所產生之複本，服務提供者將之存放於電子存儲設備中，但儲存之日期可能長達數月之久。

帳戶持有者亦使用網路服務提供者來從事電腦工作之外包，在 1980 年代，電腦容量有限，不足以存放及處理所有資訊，因此使用者付費使用遠端電腦儲存額外大量檔案或是處理大量數據。當使用者付費使用此種商業遠端計算服務，為保存及處理數據，會寄送使用者私人資訊複本至第三方計算服務，任何人均得註冊使用此種服務，會引發隱私疑慮在於此種商業服務會長時間存儲客戶私人檔案之複本。

聯邦儲存通訊法規範兩種服務提供者--電子通訊服務(electronic communication service, ECS)提供者和遠端計算服務(remote computing service, RCS)提供者。電子通訊服務提供者之定義為:任何提供使用者其傳送或接收有線或電

子通訊功能之服務[77]；而電子存儲設備(electronic storage)則指任何因電子傳送產生有線或電子通訊之暫時、中介之存儲設備[78]，以及任何在暫存時產生之檔案備份。遠端計算服務提供者係指藉由電子通訊系統提供公眾電腦存儲或處理服務[79]，電子通訊系統為任何傳送電子通訊之有線、廣播、電磁、光電、光學設備，以及任何儲存上開通訊之電腦或相關電子設備[80]。

三、命令提供與內容無關資訊之規定

聯邦儲存通訊法規定政府得以下列兩種方式，命令電子通訊服務業者、遠端計算服務業者提出與內容無關之資訊：其一為政府得以傳票（subpoena）命業者提出註冊者基本資料，如：姓名、住址、市內及長途電話通聯、服務時間（包括開始之日期）、電話號碼或其他註冊者號碼、身分與付款方式（包括信用卡卡號或付款銀行帳戶帳號）等。行政調查傳票（administrative subpoena）係依據聯邦法規或州法規所核發，或聯邦、州大陪審團（grand jury）以及審判中所發出之傳票均得命業者提出上開資訊，如欲以較嚴謹之程序，如聲請搜索票或依美國法典第 2703 條聲請法院命令亦可命業者提出資訊。

聯邦儲存通訊法允許政府以傳票命提出與合法客戶或註冊者無關之記錄，因法條明文所保護對象僅限客戶或註冊者之記錄或內容，因此不屬於客戶或註冊者之記錄或內容應摒除於本法限制範圍。例如：駭客連結網路之登入資訊就不在本法保護範圍，因為駭客並非合法之客戶或註冊者。

如政府欲取得除註冊者基本資料外之與內容無關之資訊時，則需較傳票更嚴謹之程序，例如，政府欲取得在一段特定時間窗中，某人傳送或接收電子郵件

[77] 18 U.S.C.A.§2510(15)(2000) “electronic communication service” means any service which provides to users thereof the ability to send or receive wire or electronic communications.

[78] 18 U.S.C.A.§2510(17)(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof

[79] 18 U.S.C.A.§2711(2) the term “remote computing service” means the provision to the public of computer storage or processing services by means of an electronic communications system.

[80] 18 U.S.C.A.§2510(14) “electronic communications system” means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.

之電子郵件帳戶清單，或是政府欲取得某人在網路搜尋資料時，試圖以遠端登入之 IP 位址清單，這種與內容無法之紀錄，政府應依 2703 條 d 項規定取得法庭命令或搜索票[81]。政府為取得法庭命令，應提出特定可述事實（specific and articulable facts）顯示有命令提出之資訊與進行之犯罪調查有關且為關鍵之合理依據。上開條文使用「特定可述事實」似乎是援引最高法院關於 Terry 攔阻（Terry Stop）[82]應具備之依據程度之解釋。

四、命令提供有關於內容資訊之規定

電子通訊服務提供者持有保留在電子存儲設備 180 日內之內容資訊，僅得聲請搜索票強制命其提出，依 2703 條 a 項，聲請搜索票應達到合理根據門檻，此種搜索票執行方式與傳票類似，政府依一般程序取得搜索票後，傳真 ISP 業者令其提交。

對公眾開放之遠端計算機服務提供者所持有之內容和電子通訊服務業者所持有存放於電子存儲設備超過 180 日之內容資訊[83]之處理程序與上述不同，政府得以取得搜索票或傳票之方式強制令持有者提出資訊。政府亦得依 2703 條 d 項之命令結合 2705 條之事先通知（prior notice）或延緩通知（delayed notice）。2705

---

[81] 18 U.S.C.A.§2703(d) A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

[82] Terry v. Ohio, 392 U.S. 1, 21, 88 S.Ct. 1868, 20 L.Ed.2d. 889(1968) "[I]n justifying the particular intrusion the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant the intrusion. "員警必需能表明特定可述事實，從事實中加以理性推論而取得侵入之合理依據。

[83] 18 U.S.C.A.§2703(b) 區分 180 日內與超過 180 日內容之處理程序，係因推定超過 180 日之電子郵件通常為放置在垃圾桶內之郵件，無隱私權之合理期待，參見 United States v. Trimble, 986 F.2d 394, 399(10th Cir. 1993)，此判決認為丟棄之財物並無隱私權之合理期待。惟在 180 日原則提出後，電子郵件之使用習慣有巨大變化，今日有大量存放於遠端伺服器超過 180 日之電子郵件，持有者並無丟棄之意思。

條之延緩通知令允許若有理由相信通知會造成下列之有害結果，則得核發首次不逾 90 日之延緩通知：1.危及個人生命或身體安全、2.逃避追訴(flight from prosecution)、3.滅證或偽造證據、4.恐嚇潛在證人、或 5.其他嚴重危及調查程序或不當延滯訴訟。

在本法於 1986 年制定時，電子通訊服務與遠端計算服務之分類相當清楚，惟科技進步，現今許多電腦服務，如免費網頁式界面之電子郵件服務，即可提供訊息功能以及資訊存儲之功能。功能結合後，電子通訊服務業者與遠端服務業者之分類困難，應適用何法條令其等提出內容資訊更顯複雜，因此首要需判斷通訊之提供者在通訊中，扮演何種角色。譬如：當 ISP 業者伺服器內有未讀取之電子郵件時，就該未讀取之郵件而言，此時 ISP 業者之角色屬於電子通訊服務。或當使用者編輯檔案後透過檔案傳輸協助（File Transfer Protocol, FTP）方式傳送檔案至 ISP 業者主機之電子郵件帳戶內，則 ISP 業者對於該傳送之檔案而言，屬於遠端計算服務性質。

五、自願揭露資訊之規定

2702 條對於自願揭露之限制，僅適合於對公眾提供服務之業者，若服務提供者未提供服務予公眾，則不適合聯邦儲存通訊法。若任何人則註冊該服務，不論付費或是免費，即屬提供服務予公眾。若僅限有特殊關係始得註冊服務，則非屬對公眾提供服務，例外:律師事務所提供事務所之電子郵件帳號供職員註冊使用，則事務所並非對公眾提供服務者，因為該電子郵件服務僅職員得註冊。法條區分二種之意義在於，私人公司提供電腦帳戶之目的，一般來說，係為該公司之利益，然註冊者或客戶自營利性質之服務提供者取得電腦帳戶，目的多屬個人使用。

2702 條 b 項係針對內容資訊，2702 條 c 項係規範非內容資訊之揭露。服務提供者原則上不得揭露通訊資訊，惟在 2702 條 b 項、c 項例外情況下，服務提供者得揭露資訊。

2702 條 b 項之例外情況包括:服務提供者為傳遞通訊，而揭露資訊予通訊接收者或其代理程式(agent)[84]；或在傳送資訊過程，揭露資訊予網路中介(intermediary)[85]；或法律授權得揭露者[86]。而 2702 條 b 項其他得揭露之規定，係其他法益與個人隱私權權衡下，他法益高於隱私權。

2702 條 b 項 3 款，在通訊發信者、收件人或擬接收者或是遠端計算服務註冊者之同意下，服務提供者得提供通訊之內容[87]。第 2702 條 b 項第 5 款，服務提供者在提供服務所必需情況下或為保護其財產或權利得揭露資訊[88]。服務提供者得揭露資訊予國際失蹤及被剝削兒童保護中心（National Centerfor Missing andExploited Children）協助提供關於童工及兒童猥褻照片犯罪偵辦[89]。或服務提供者善意取得之內容資訊與犯罪有關時，服務提供者得揭露予執行單位[90]，此條文原則上係採「一望即知原則」(plain view doctrine)[91]，在將服務提供者置於與第四修正案賦予執行單位之權責相同地位。而 2502 條 b 項 8 款[92]則是第四修正案例外情況即緊急情況(exigent circumstances)和公共安全(public safety)之體現，服務提供者善意(in good faith)相信有危及個人生命或對身體有重大傷害之緊急情況時，得揭露資訊予政府單位。

關於與內容無關之資訊揭露之限制，大致和內容資訊揭露規定無異，最大

---

[84] 18 U.S.C.A.§2702(b)(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

[85] 18 U.S.C.A.§2702(b)(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

[86] 18 U.S.C.A.§2702(b)(2) as otherwise authorized in section2517,2511(2)(a), or2703of this title;

[87] with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service

[88] 18 U.S.C.A.§2702(b)(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

[89] 18 U.S.C.A.§2702(b)(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

[90] 18 U.S.C.A.§2702(b)(7) to a law enforcement agency—(A)if the contents—(i)were inadvertently obtained by the service provider; and(ii)appear to pertain to the commission of a crime;

[91] 一望即知原則允許執法者在無搜索票情況下，扣押在合法觀察下一望即知與犯罪有關之證據或違禁物。

[92] 18 U.S.C.A.§2702(b)(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

的差別在服務提供者得揭露與內容無關之紀錄予除政府單位以外之人，因此服務提供者得將與內容無關之紀錄出售予廣告商或其他商業機構。

總結美國關於通訊監察依電子通訊隱私權保護法案（Electronic Communication Privacy Act，ECPA）之聲請程序分析，並製作表格如下:

監聽程序	監察標的	所依據之法令	美國憲法第四修正案	實質上標準（substantive standard）	法院命令是否必要(Court Order Required)	是否需司法審查(Judicial Scrutiny)	通知受監察人（Notice）	證據排除法則之適用（Suppression）
通訊紀錄與追蹤令 Pen/Trap order	通聯紀錄、帳單地址等	撥號記錄器法（Pen Register Act）	不受保護	相關證據（Relevance）	是	否	否	否
搜索票 Warrant	任何通訊標的（例如電話基地台位址）	搜索票有權核發機關（例如：聯邦刑事訴訟法 Federal Rules of Criminal Procedure）	無定論	相當理由（Probable Cause and Particularity）	是	是	否	未定
監聽票 Wiretap order	通訊內容	監聽法（Wiretap Act）	超級監聽票 Super-Warrant	相當理由或需更高舉證責任（Probable , Cause,	是	是	是	依法規及憲法之規定

				Particularity and More）				

第三章　網際網路之通訊監察

第一節　網際網路通訊監察與傳統監聽之比較

網路通訊監察與傳統電話監聽相異之處在於，傳統的電話資料交換方式係採迴路交換(Circuit Switch)，亦即當發話端與受話端通話時，系統會建立一專屬線路供雙方使用，完全不受其他線路干擾，而網際網路則採封包交換（Packet Switch），彼此之間的傳遞是以廣播方式在傳送，以封包辨識認定傳送對象，網路提供通信資源供大眾使用，並未專屬某一使用者，因此同一實體線路上有許多輾轉通道存在同時通信。因此，在網際網路實施某一人之通訊監察時，很有可能截聽受監察人以外之人之通訊。

一般傳統郵件通常會以信封彌封，執行過濾郵件之人無法直接自外觀察知信件內容，但過濾電子郵件時，除寄收電子郵件的帳號外，在電子郵件內容與電子郵件帳號，皆屬於文字模式層次的情況下，以文字模式層次截取該電子郵件帳號之通聯紀錄時，亦可輕易取得信件內容[93]。

第二節　網際網路通訊監察之法制依據

第一項　適法性要件

一、重罪原則

因通訊監察本質上屬於侵害人民隱私權，因此監聽之前提需符合憲法第 23 條之比例原則，始得為之，是以通訊保障及監聽法第 5 條規定，除最輕本刑為三年以上有期徒刑之重罪外，尚列舉刑法或刑事特別法上之若干罪名，作為得以實

[93] 參照蔡美智著，「通訊保障及監察法」關於網路監聽之相關爭議，資訊法務透析，民國 88 年 12 月，頁 32。

施通訊監察之罪名範圍，本法係兼採概括及列舉之方式立法。惟目前採刑度與罪名併列的「重罪原則」，有學者認應採取「列舉重罪原則」才能對於基本權提供較完整的保障。而所謂「列舉重罪原則」，是指僅列舉之重罪方是屬於得實施監聽之範圍，以作為犯罪偵查的手段，亦即縱然是屬於「重罪」，但非法律所明確列舉出的，仍不得對其實施監聽，避免國家公權力過於恣意。然若僅採列舉重罪原則，不免有掛一漏萬之缺失，因我國刑事特別法多如牛毛，且法條變動頻繁，若採列舉重罪原則，本法將時時翻修。

二、必要性原則

所謂「必要性原則」係指監聽案件除為重大犯罪之外，在實際執行上應有實施監聽之必要，此乃因為監聽對人民基本權，即秘密通訊自由造成嚴重侵害，所以對重大犯罪之監聽，必須是在已窮盡其他方法仍無法取得犯罪證據時，始得實施，此即本法第 5 條第 1 項中所規定：「…不能或難以其他方法蒐集或調查證據者，…」之意旨，亦即監聽之實施，在犯罪偵查行為是具有「最後手段性」。

而新修正之通訊保障及監聽法第 5 條第 2 項後段，規定法官得於通訊監察書對執行單位作適當之指示，且執行機關應至少每 15 日作為 1 次以上之報告書說明通訊監察進行之狀況，且檢察官或法官有隨時命執行機關提出期中報告之權，以檢視通訊監察之執行有無符合最小侵害原則，自新修法之通保法第 5 條第 4 項規定可知。

三、相關性原則

所謂「相關性原則」是指監聽之手段與犯罪偵查之目的之間必須且具有相關性，亦稱「合理性原則」。由於電話、及網路是目前最便利之通訊設備，雖然被告或犯罪嫌疑人有可能利用電話傳遞犯罪信息，但並非指一切電話通訊皆與犯罪有關。為保護秘密通訊自由，對於監聽應限於與犯罪有關者，如與犯罪無關，即令為被告或犯罪嫌疑人之電話通話，實不應予以監聽。例如，就追捕逃犯而言，須是該逃犯固定或經常聯繫之密友方屬監聽之對象，而不得任意將與該逃犯熟識之人列入監聽之範圍。另偵查機關需已獲得客觀之證據，始得予以聲請監聽，不

得僅憑執法單位主觀臆測而聲請，此即是本法第五條第一項規定：「有事實足認…，而有相當理由可信其通訊內容與本案有關，…」及第六條規定：「有事實足認為…」之立法意旨。

四、書面許可原則

所謂「書面許可原則」是為使監聽的實施有明確的依據及界限，並且使法官核發監聽票程序更為慎重，所以在本法第 11 條規定，通訊監察書應記載事項有：案由及涉嫌觸犯之法條、監察對象、監察通訊種類及號碼等足資識別之特徵、受監察處所、監察理由、監察期間及方法、聲請機關、執行機關等項目，使執行監聽者能有明確執行依據及界限，不能任意的變更，以保障人民基本權，故在實施監聽前應獲得書面之許可。

五、一定期間原則

一定期間原則主要是認為實施監聽應有期限，以保障人民的基本權，免受不必要之侵害，藉由期限的規定以加強法官審核及監督的功能。在本法第 12 條規定，一般犯罪偵查之監聽期間，每次不得逾三十日，而有關國家情報之通訊監察期間，則每次不得逾一年；其有繼續監察之必要者，得於期間屆滿前，聲請繼續。但若在期間屆滿前，事實上已無監聽之必要者，應即停止實施監聽。另外，對於監聽所得資料，除已供案件證據留存於該案卷或為監察目的有必要長期留存者外，由執行機關於監察結束後，保存五年；逾期予以銷燬，此亦是一定期間原則的精神。

六、令狀原則

所謂「令狀原則」，即要求政府在對人民基本權利為侵犯前，必須先由司法機關審核實質理由，以防止無相當理由的強制處分[94]，蓋因行政機關為執法機關(為限制、剝奪人民權利的執行者)，故自憲法精神解釋，此一「中立及超然」的機關應為司法機關，而非行政機關[95]。令狀原則亦為法官保留原則，因監聽對人

[94] 參照王兆鵬，令狀原則，刑事訴訟法講義（一），92 年 3 月，頁 91。
[95] 參照前揭註，頁 103。

民基本權有所侵害，應事先經由中立之司法審查程序，是通訊監察之執行，以法院事先核准並核發通訊監察書後始得為之，此觀諸通訊保障及監察法第 5 條第 2 項之規定可知。

七、事後通知原則

按「第五條、第六條及第七條第二項通訊監察案件之執行機關於監察通訊結束時，應即敘明受監察人之姓名、住所或居所、該監察案件之第十一條第一項各款及通訊監察書核發機關文號、實際監察期間、有無獲得監察目的之通訊資料及救濟程序報由檢察官、綜理國家情報工作機關陳報法院通知受監察人。」、「法院對於第一項陳報，除有具體理由足認通知有妨害監察目的之虞或不能通知之情形外，應通知受監察人。」通訊保障及監察法法第 15 條第 1 項、第 3 項定有明文。受告知權為程序正義保障之一環，且為使受監察人於監聽結束後，得知監聽之相關事項，以作為救濟程序之依據，特立此條以維受監察人之權益。

第二項　法條依據

網際網路通訊，是否為我國通訊保障及監察法所涵蓋？依通訊保障及監察法第 3 條第 1 項所示，答案是肯定的，目前已知科技所得溝通方式皆包括本法範圍內。網際網路通訊監察係對流通於網際網路之電子資料進行監察，持有機關為網路服務業者或公司內部網路管理單位，本法第 3 條第 1 項第 1 款所謂通訊包括「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』」，而「電信」依電信法第 2 條第 1 款定義「指利用有線、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」，另「電信設備」依同條第二款則指「電信所用之機械、器具、線路及其他相關設備」。依據電信法定義，發送網路通訊之電腦設備應屬於「電信設備」的一種當無疑義。而網路通訊係利用電信設備發送、傳輸或接收符號、文字、影像等訊息，自屬通訊保障及監察法適用範圍。

而通訊保障及監察法第 3 條第 2 項，又加上「前項所稱之通訊，以有事實足認受監察人對其通訊內容有隱私或秘密之合理期待者為限」之限制，可知此原則係援引美國最高法院在 Katz v. United States 案中所建立之「合理隱私權期待原則」，認為僅在能夠合理期待且與隱私或秘密有關者，始屬本法所保障通訊範圍。

第三節　網際網路通訊監察之方式

第一項　監察客體[96]

一、以特定 IP 為對象

IP 係電腦主機在網路上之地址，每一主機在連上網際網路後均有獨立 IP 位址，因此若已知發出郵件或連線主機之 IP 位址，即可以此追踪至該 IP 之物理位置。另目前 ISP 業者多有提供虛擬主機或網路空間租用服務，若網站並非架設在個別主機以專線連線後取得獨立 IP，而係附屬在 ISP 主機內，但仍可透過對提供虛擬網路業者 IP 主機監控，間接查出租用人資料。

在某網頁可能含有網路犯罪內容，或是其主機是犯罪者經常入侵或藉此轉站、或傳輸郵件以外的資料時所使用的主機或網路電話、影音電話或視訊會議的監控，都可以監聽 IP 的方式來達成。但由於主機傳輸資料龐大，且除非設定為點對點的監控，否則將會取得許多與本案無關之使用者傳輸資料，若以比例原則及偵查經濟效益觀之，使用 IP 監控方式應審慎為之，是除非在已調閱通聯紀錄並掌握通訊來源，如犯罪者在國內而在國外主機租用網頁，即可在國內聯外的關鍵節點，監控聯往國外主機資料，從中找出國內聯繫者。

二、以特定電子郵件帳號為對象

監聽特定電子郵件帳號有二目的，一是以特定郵件通聯紀錄，查詢出寄件

[96] 參見陳信郎著，資訊隱私權保障與網路犯罪通訊監察法制，國立政治大學法律學研究所碩士論文，頁 107-108。

者及收件者電子郵件帳號，再由帳號追查使用者基本資料；另一則是監看查知特定電子郵件內容，藉以了解電子郵件內容是否與犯罪相關。

第一種為追查使用者基資，依通訊保障及監察法第 3 條之 1 規定，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。而前述通訊使用者資料，依同法第 3 條之 1 第 2 項，則指電信服務使用者姓名或名稱、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。因此如欲向電子郵件信箱業者調取電子郵件信箱申請人個人資料，應依同法第 11 條之 1 向法院聲請調取票。

若偵查機關欲監控特定郵件內容時，由於涉及通訊內容之「攔截」及「開拆」，則應符合通訊保障及監察法規定，取得通訊監察書。而對於傳輸中之電子郵件監看之做法有三[97]：一、偵查人員提供截錄機器予業者，於監察之機房裝設上網及通信紀錄器協助進行節點封包之截錄後，交由執行機關透過解讀電子郵件內容；二、要求電信業者或 ISP 業者，利用管理電子郵件伺服器軟體，將受監察人所收受的所有電子郵件，轉寄予聲請監察的執行者[98]。三、執行者直接進入業者之機房同步截收、解譯受監察人之電子郵件。

第二項　監察方式[99]

一、主機內監聽

此種監聽方式適用於向 ISP 業者租用網頁主機、信件主機，或是機關內部網路主機等情形，僅需在其主機內置放監聽程式複製通訊內容或通聯紀錄即可，範圍固定，不致截收他人資料。

---

[97] 參見許慈健著，網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究，國立交通大學管理學院碩士在職專班科技法律組碩士論文，頁 83。
[98] 參見林岡輝著，前揭文，頁 22。
[99] 參見陳信郎著，前揭文。

二、節點監聽

所謂「節點」，通常是指在骨幹網路（backbones）上通訊交換點，在網路節點上放置監聽設備，攔截封包之方式，極易攔截到與犯罪嫌疑人毫不相關之人之電子郵件，因此在越下游攔截越能監察到特定受監察人。因為網際網路與電話監聽之差別，主因為在電話對話係點對點傳播，而網路則是透過封包交換原理來處理許多使用者的封包，所以通過該節點之所有使用者資料，均會因此而遭截收，不無侵害不特定人通訊隱私權之疑慮。此種監察方式不但能監看受監察人之電子郵件，亦能監看所有瀏覽紀錄。但使用此種通訊監察方式，須先查明犯罪行為人使用上網連線之市內電話，透過業者裝設上網及通信紀錄器於受監察人最近之機房，藉以攔截行為人之郵件及儲存上網瀏覽紀錄，再透過機器解譯紀錄還原行為人網路行為[100]。

此種網路通訊監察方式似乎能有效掌握犯罪行為人所有上網行為，但實務上成效不彰，除受限於有些電信業者使用之系統而無法裝設機器與解碼外，另一方面，這種方式只限於受監察人使用固定線路時，始得行之，倘行為人係使用撥接帳號或在外免費網路連線，因無法確定犯罪嫌疑人上網連線地點，當然無法對之實施通訊監察。此外，一旦行為人進入需使用密碼之網頁，例如會員制之聊天室，偵查人員也會因無法取得該行為人之使用者代碼及通行密碼而無法取得網頁資料。

第四節　具加密功能之通訊軟體之通訊監察

第一項　概述

因智慧型手機之普及，以及網路速度大幅提升，民眾使用智慧型手機通訊、

[100] 參見許慈健著，前揭文，頁 85。

瀏覽網頁、傳送資料益見普遍。臺灣目前居主流通訊軟體如：Line、WhatsApp、WeChat、Facebook Messenger 或 Skype 均兼具通話、文字簡訊、傳檔等功能，加上具私密性、免費取得、立即性傳送等特點，民眾使用意願更高。正因為如此，目前犯罪均有使用此類具加密功能之通訊軟體之趨勢，更增加偵辦犯罪之困難度。

第二項　對以具加密功能之通訊軟體監察之方式

一、加密通訊軟體運行模式

以我國常見數種加密通訊軟體，Skype 係屬於網際協議通訊模式(voice-over-IP)以及即時通訊客戶端（instant messaging client）混合運行模式。Skype 用戶除得使用網路通話外，亦可以撥打至一般室內或手機電話，與其他大部份 VoIP 系統不同之處在於，Skype 是 P2P 與主從式架構（Client-Server System）混合。WhatsApp 功能不只傳送文字訊息，照片、影片、聲音檔以及所在地位置訊亦得透過 WhatsApp 傳送，WhatsApp 較惹議在於隱私與安全問題，因為 WhatsApp 使用者需上傳整個手機通訊錄至 WhatsApp 伺服器，讓 WhatsApp 能找尋出通訊錄上之聯絡人何人為 WhatsApp 使用者，因為即使非 WhatsApp 用戶之聯絡方式亦有可能一併上傳至 WhatsApp 伺服器，雖然上傳的僅電話號碼，但從電話號碼已足以辨識出聯絡人。

在所有之通訊軟體中，Facebook Messenger 起步較晚，雖然得傳送文字或聲音訊息，但基本上是附屬在 Facebook 網頁介面，近二年方單獨開發手機應用程式。Line 使用者可用軟體交換文字、位置、聲音及影像訊息，Line 因為貼圖市場吸引，近年一躍成為臺灣最普遍通訊軟體。

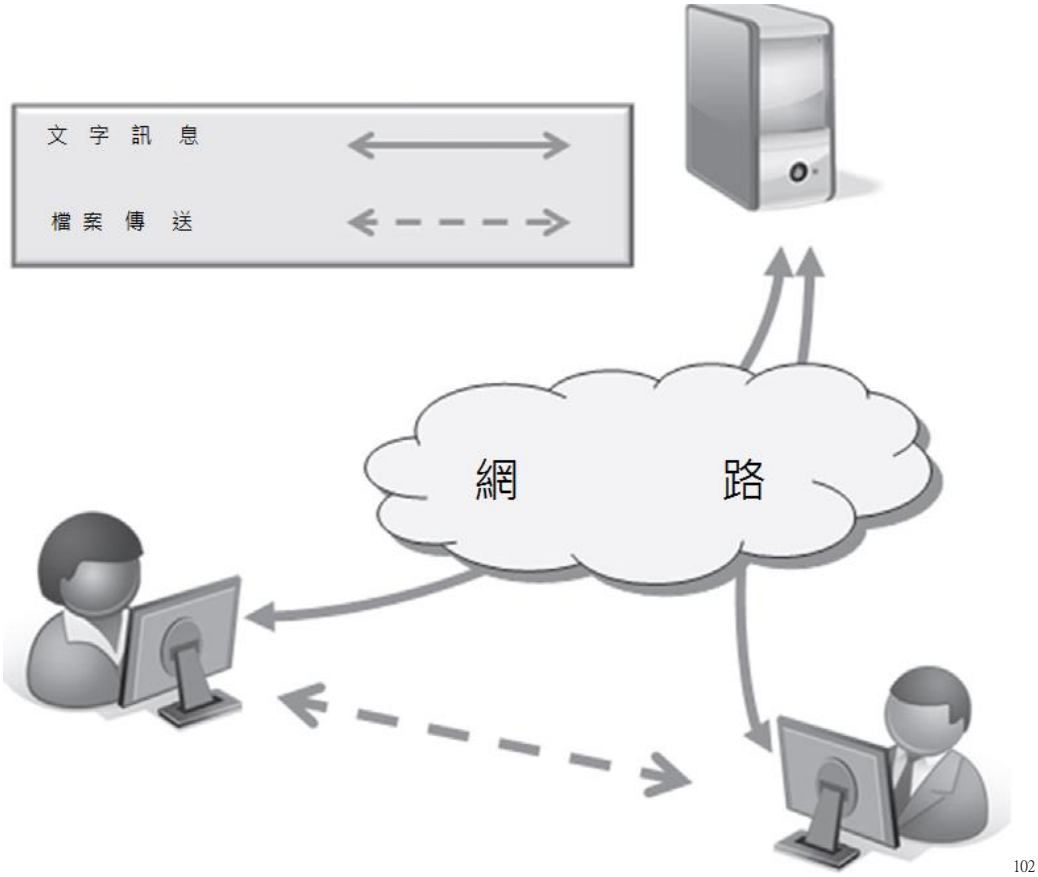
主從式架構是客戶端使用軟體與伺服器連結，經由伺服器控制連線和資料傳送。運作模式如下圖所示：

[101]

即時通訊軟體、IRC(Internet Relay Chat)、FTP（File Transfer Protocol）和聊天室多使用主從式架構。主伺服器具有連結數個使用者之功能，當用戶加入連結，主伺服器通知其他用戶有人傳送連結，使雙方可以連結。但即時通訊軟體亦有使用點對點連結方式（P2P），但僅限於傳送檔案時，雙方得使用軟體直接連繫對方，無須透過伺服器，但點對點連結方式，會曝露雙方之 IP 借址，且每一通訊軟體公司均有其獨立通訊協定，因此不同公司之通訊軟體間無法互傳訊息。

即時通訊軟體係藉由用戶登入訊息伺服器或是登入用戶端之電腦或手機運作，當訊息伺服器確認用戶之聯絡人名單，回傳聯絡人何人已登入於伺服器中，用戶選擇聯絡人後告訴系統連結聯絡人，雙方即可互傳訊息，傳訊之模式如下圖：

[101] Todd G. Shipley, Art Bowker,Investigating Internet Crimes-An Introduction to Solving Crimes in Cyberspace,p346



102

以往，即時通訊軟體係以未加密純文字方式傳送，但因此傳送過程中容易受到封包攔截，所以目前每家通訊軟體廠商多對其軟體傳送過程加密，且不時宣稱連其公司都無法解密來招攬客戶[103]。

二、加密通訊軟體之通訊監察方式

(一)、後門程式（Backdoor）

所謂「後門程式」係指可以「繞過」、「規避」電腦內部安全系統的另一個管道。可能是在軟體設計之初，程式設計師為方便未來進入系統維護所留下的程式，亦可能是電腦遭受到入侵而被植下的程式。許多駭客會經由後門繞過安全驗

[102] 同前註，頁 348

[103] 蘋果公司拒絕依司法部指示提供取得 iMessage 通訊內容，表示所有的服務均以加密，因此無法讓執法者取得通訊內容。參見報導 Apple, in refusing backdoor access to data, may face fines，http://www.zdnet.com/article/apple-in-refusing-backdoor-access-to-data-faces-huge-fines/ ，最後瀏覽日 2015 年 9 月 20 日。

證，非法進入電腦進行破壞或竊取資料[104]。如通訊軟體在事先預留「後門」，則執行監控單位即可透過後門程式進入目標系統，惟缺點是該後門程序可能遭有心人士濫用。

美國司法部前取得法院命令要求蘋果公司提出後門程式，使司法單位得以監控蘋果公司 iMessenge 以及 Facetime 訊息內容，嗣因反彈過鉅，司法部決定暫緩立法要求科技公司在其軟體中加入後門程式

(二)、特洛伊木馬程式（Trojan Horse）

木馬程式能暗中監視通訊、偵測被植入手機或電腦之網路活動、紀錄鍵盤敲擊，被將所有取得資訊透過網路傳送，甚至得截取被植入手機之螢幕。執法單位植入木馬程式藉以取得通訊資訊，木馬程式包括兩部分：服務端（伺服器部分）和用戶端（控制器部分）。而伺服器部分即是被植入木馬之標的，用戶端為植木馬的駭客，當駭客進入執行服務端的電腦。執行木馬程式的服務端後，在被植入者不知情下打開連結埠（Port），向指定地點發送資料（如網路遊戲的密碼，即時通訊交談內容等）。因通訊軟體傳訊過程中，多以加密方式傳送，業如前述，因此最佳之方式，係在訊息尚未加密前截收，即發送方發送訊息時，木馬程式發揮作用，在訊息尚未加密處理前，同步將發送方之訊複製並傳送至監察單位。

各國現有執行木馬程式以進入受監聽者資料之案例，如:瑞士政府與 ISP 業者合作，植入木馬程式至電腦內，以電腦配置之麥克風紀錄交談內容；或德國執行單位在嫌疑人硬碟內植入木馬程式，錄下所有麥克風、網路攝影機使用之活動，以及藉木馬程式掃瞄硬碟以取得與犯罪相關之檔案。美國 FBI 使用 CIPAV(computer and Internet Protocol address verifier)可紀錄 IP 位址，以將搜集之數據寄送回政府電腦。

[104] 教育部全民資安素養網資安小字典，https://isafe.moe.edu.tw/dictionary_detail.php?sn=11，最後瀏覽日 2015 年 9 月 1 日。

(三)、基地台模擬器(cell site simulator)

基地台模擬器係一極具爭議監聽軟體，其模擬無線電信商基地台運作模式。在基地台模擬器周遭之無線通訊裝置，如手機、平板電腦等之通訊以及與基地台間之連接，將由基地台模擬器所取代。基地台模擬器會記錄手機位置、無線裝置之電子識別碼並儲存所有通訊資料，無須經由網路服務或通訊服務提供者，即能取得手機基地台位置、截取通訊內容等資料。基地台模擬器可以被安裝在交通工具上、飛機上、直升機甚至無人機上。基地台模擬器強迫在覆蓋區域內所有無線裝置與原先之電信提供業者(如中華電信、遠傳等)斷訊，然後強迫無線裝置與基地台模擬器建立新的連線，基地台模擬器會發出比原先電信商設置之基台地更強的訊號，或是發出更強的訊息，無線裝置自然會連接到最強的基地台。

基地台模擬器包括許多軟硬體:StingyRay、KingFish、IMSI catcher[105]、triggerfish, 及 digital analyzer[106]等，在司法部電子監聽電子裡描述基地台模擬器之性能如下:設備包括天線、處理手機頻率信號傳送電子裝置、分析信號和配置蒐集證據之電腦，當用戶在使用手機時，基地台模擬器可讓執法單位辨識出方向及信號強度。藉由設備之移動，操作者可以三角定位法精確定位手機位置[107]。

對於犯罪偵查機關而言，使用基地台模擬器有如下益處:一、無須透過通訊服務提供者之協助。在需得服務提供者協助之監聽案件中，服務提供者一定知道監聽正在進行中，且需依據撥號追踪令之要求保存紀錄。在使用基地台模擬器的情況下，僅使用者知悉監聽刻在進行中。第二，基地台模擬器可以產出精確手機使用位置，最精密的情況，誤差不超過 180 公分[108]，在一聯邦案件審判中，執法

[105] IMSI 是 International mobile subscriber identity 縮寫，為手機獨特識別號碼。
[106] 參見司法部電子監聽手冊 http://www.justice.gov/sites/default/files/criminal/legacy/2014/10/29/elec-sur-manual.pdf 最後造訪日 2015 年 11 月 20 日。
[107] 同前註。
[108] PKI Electronic Intelligence, GSM Cellular Monitoring System (product brochure) , http://docstoc.com/docs/99662489/GSM-CELLULAR-MONITORING-SYSTEM 最後造訪日 2015 年 11 月 20 日。

單位承認可以在公寓大廈中定位出哪一間套房在使用受監聽之手機[109]，佛羅里達州塔拉哈西市警員在法庭上證述，只要持手提基地台模擬器，在大型公寓逐樓掃瞄，可以查出手機訊號發出之特定區域[110]。

美國執法機關至少從 1990 年代起就開始使用基地台模擬器[111]，因為從基地台模擬器所取得之資料包括手機之撥號號碼、路由、住址或信號資料，因此基地台模擬器長久以來被認為與撥號紀錄器法中撥號紀錄器和監測追踪器相當，是以美國司法部建議檢察官在犯罪偵查中若使用基地台模擬器前需取得撥號追踪令(pen/trap order)[112]，根據撥號紀錄器法，執法單位僅需提出將受搜索之資料與調查中之犯罪有關即可取得撥號追踪令。

但最近三年，法官及辯護人不斷質疑基地台模擬器之使用[113]，例如在 2012 年，一在德州南區聯邦法院治安法官駁回執法單位認為撥號追踪令足以做為安裝基地台模擬器之主張，法院認為基地台模擬器之性質類似於手機追踪器，所以應依據 Mobile Device statute 規定，至少應有合理依據始得聲請安裝基地台模擬器[114]。

第三項　對具加密功能之通訊軟體監聽之困難處

一、軟體業者協力意願低落

---

[109] United States v. Rigmaiden, 844 F. Supp. 2d 982, 996 (D. Ariz. 2012)

[110] Florida v. Thomas, No. 2008-CF-3350A (Fla., Leon Co. Cir. Ct., Aug. 23, 2010), https://www.aclu.org/files/assets/100823_transcription_of_suppression_hearing_complete_ 0.pdf 最後造訪日 2015 年 11 月 20 日。

[111] 參見 In re Application of the U. S. for an Order Authorizing the Use of a Cellular Tel. Digital Analyzer, 885 F. Supp. 197, 198 (C.D. Cal. 1995); Stephanie K. Pell & Christopher Soghoian, A Lot More Than a Pen Register, And Less Than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities, 16 YALE J. L. & TECH. 134, 142 (2014).

[112] Jon Campbell, LAPD Spied on 21 Using StingRay Anti-Terrorism Tool, LA WEEKLY, Jan. 24, 2013, http://www.laweekly.com/news/lapd-spied-on-21-using-stingray-anti-terrorism-tool-2612739 最後造訪日 2015 年 11 月 20 日。

[113] Linda Lye, In Court: Uncovering Stingrays, A Troubling New Location Tracking Device, ACLU (Oct. 22, 2012, 12:42 p.m.), https://www.aclu.org/blog/free-future/court-uncovering-stingrays-troubling-new-location-tracking-device?redirect_blog/national-security-technology-and-liberty/court-uncovering-stingrays-troubling-new-location 最後造訪日 2015 年 11 月 20 日。

[114] In re Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747, 752 (S.D. Tex. 2012)

以我國目前使用頻率最高前幾名通訊軟體而言，其軟體業者或是主機均設在國外，如 Line 為韓國公司、WhatsApp 係美國公司、WeChat 是中國大陸廠商開發、Facebook Messenger 為美國公司，主機均在海外，開發軟體商為外國公司，不受本國法律之監督，再因國內外法律有差異，外國公司本不受約束，例如在美國，任何人均可合法持有槍枝，若我國以持有槍械為申請調閱之理由向 Facebook 申請調取資料，極可能會被以與該國法有違而拒絕。

二、App 發展一日千里

因應使用者需求，或是軟體程式錯誤修正，手機通訊軟體不僅需推陳出新，連舊軟體亦不斷更新。為監察而破解應用程式往往緩不濟急，且偵查單位花費人力、物力破解應用程式後，程式又再更新，形同所有努力付諸流水。且通訊軟體數量驚人、發展蓬勃，而通訊監察建置機關有限，通訊軟體實為現在實務上通訊監察之漏洞。

三、通訊軟體加密[115]破解困難

現今軟體開發商為保護通訊安全，且運算功能提高，為軟體加密輕而易舉，是通訊軟體多以加密方式運送。以往電信業者依通訊監察及保障法第 14 條，對於執行監聽有協力義務，提供解密金鑰，然而目前國外軟體商並不願提供解密金鑰，一來此舉將降低民眾使用其軟體之意願，另一方面，我國通訊保障及監察法對軟體商是否有強制力，仍有疑義。

網路服務提供業者配合實施通訊監察之法源依據在通訊保障及監察法第 14 條規定，而其具體配合義務，則規定於通訊保障及監察法施行細則第 21 條、26 條，電信事業應使其通訊系統之軟硬體設備具有配合執行通訊監察時所需之功

[115] 所謂加密係指雙方在進行網路通訊時，使用相同資料編碼加密和解碼規則。當寄送方將訊息傳送出去，該訊息被內建之加密規則予以編碼，收受者因具有相同解碼規則之裝置，在接收訊息時，自動將加密之訊息解碼，因此收受者得以閱覽訊息，但第三人之裝置內因不具備同一編碼設置，縱然截收到訊息，仍是一堆亂碼。

能，並於執行機關執行通訊監察時予以協助，必要時並應提供場地、電力及相關介接設備。具體配合項目，前交通部電信總局為因應網路科技發展及配合網路犯罪偵查之需要，於 93 年 7 月 22 日增列幾項通訊監察項目：

1.網路電話服務

網路電話服務中提供 PC to Phone 或 Phone to PC 服務者需能自業者設備端（如 TDM Switch 或 VoIP Gateway），將依通訊保障監察法特定監察對象於通訊監察書許可期間內通話內容、時間及傳送路徑紀錄儲錄或轉送至通訊監察機關。

2.語音單純轉售服務

需能將依通訊保障及監察法特定之監察對象於通訊監察書許可期間內通話內容、時間及傳送路徑紀錄儲錄或轉送至通訊監察機關。

3.電子郵件服務

需能提供依通訊保障及監察法特定之監察對象於通訊監察書許可期間內收、送電子郵件內容、時間及傳送路徑紀錄儲錄或轉送至通訊監察機關。

於 95 年 10 月 14 日國家通訊傳播委員會復公告非 E.164 用戶號碼網路電話服務(不含不透過業者 VoIP Gateway 直接於網際網路間互相傳輸語音者)、E.164 用戶號碼網路電話服務、語音單純轉售服務及由網際網路接取服務經營者附加提供之電子郵件服務等 4 種第二類電信事業。

雖然依前揭前交通部電信總局之函文或國家通訊傳播委員會之公告，要求網路服務提供業者配合實施通訊監察之項目已包含網路電信、語音單純轉售服務及電子郵件收、送內容等，惟實務上網路服務提供業者實際配合實施通訊監察項目，仍僅侷限於協助監看電子郵件及上網瀏覽紀錄，對於日益盛行之即時通訊，業者並無法實施通訊監察。

又通訊軟體廠商是否為通訊保障及監察法所稱之「電信事業」?依國家通訊傳播委員會 103 年 8 月 20 日通傳法務字第 10300514490 號函覆法務部之意見，答案似乎是否定。國家通訊傳播委員會認為網際網路服務提供業者(Internet Service Provider, ISP)可分為 4 種:網際網路接取服務提供者(Internet Access Service Provider,

IASP)、網際網路平臺提供者(Internet Platform Provider, IPP)、網際網路內容提供者(Internet Content　Provider , ICP)以及應用服務提供者(Application Service Provider, ASP)，僅 IASP 屬於電信法第 2 條第 5 款所稱之電信事業，因此依國家通訊傳播委員會見解，應用服務提供者並非電信事業，自不受通訊保障及監察法約束，而負監聽之協力義務。

四、接取速度增加[116]

臺灣 4G 高速上網服務已經上路，加上光纖技術成熟，民眾使用 4G 或是申請 50M 以上寬頻網路已是趨勢，惟使用高速網路傳輸，對於監聽亦是一大挑戰，常有監聽對象以通訊軟體傳送大量影音檔案或是觀看影音服務等與監聽無關之內容，為保有監聽之完整性，因此此等內容亦一併傳輸至建置機關，造成建置機關設備之負荷，亦無法達成即時截收監聽資料目的。再自大量資料中，篩選過濾可用線索，亦如大海撈針。另如前述，網際網路係以封包方式傳輸資料，若僅欲截取某特定應用程式內容，因封包到達時間不一，該應用程式之訊息截收會有資訊不連貫之情況。

五、難以定位追蹤與個化加密通訊軟體使用者[117]

智慧型手機多具備兩種上網功能:4G 與 Wi-Fi，加上可選擇之通訊軟體眾多，當監察對象同時使用數種通訊軟體加上不同上網方式，增加監聽之困難度。另現在免費 Wi-Fi 隨處可見，通訊軟體使用者只要連上免費、匿名網路，則對於通訊軟體使用者更是難以追查。

(一)、服務與接取提供者分離

欲監察對象若使用同一通訊軟體，惟通訊時變換連線方式，如 4G 與 Wi-Fi，則偵查人員需逐層進行資料調閱，先向通訊軟體業者調閱該用戶所使用之 IP 資

[116] 黃茂穗著，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，102 年 3 月，頁 74。
[117] 同前註，頁 74-75。

料，再向該 IP 之接取提供者(如 4G 業者)調閱用戶 資料及即時位置。惟通訊軟體業者不願配合提供用戶資料時，即難個化分析何人為該通訊軟體之使用人。

(二)跨層 ID 無法對應:

各項通訊服務使用者均有不同帳號名稱，而這些帳號名稱常無直接關聯性，如知悉嫌疑人之 IP 位址，但不知嫌疑人係使用何種通訊軟體，或是僅知道通訊軟體之帳號名稱，惟不知對應之 IP，亦是徒勞無功。

六、跨國犯罪使犯罪更難偵查

所謂網路無國界，犯罪者使用通訊軟體犯罪不必侷限在單一國家，此種跨國性犯罪，須透過國際合作機制，惟一來我國處境特殊，難完全突破跨國合作之困境，二是網路犯罪偵辦首重時效，方能第一時間確實掌握犯罪者，若需透過層層公文往返，恐緩不濟急。

第四項　美國網際網路服務提供者之反彈─後史諾登時代

2013 年 6 月美國國家安全局前外包承包技術員史諾登(Edward Joseph Snowden)洩露機密文件案，揭露國家安全局依愛國者法案[118]215 條[119]大量自美國電信業者處蒐集美國人電話以及網路通訊內容，及依據外國情報監聽法(Foreign Intelligence Surveillance Act Amendments, FISA Amendments)第 702 條，自國外九個主要網路服務提供者取得網路通訊情報[120]。

[118] 訂立愛國者法案之目的，在為防止恐怖主義之漫行，大幅擴張美國執法單位權限，得搜索電話、電子通訊、醫療、金融等紀錄等。

[119] 2015 年 5 月 30 日美國國會對於不延長本法案之決定達成共識，該法案於 2015 年 6 月 1 日失效。國會另立自由法案(The Freedom Act)削弱愛國者法案開放予國家安全局之監聽權。

[120] Glenn Greenwald, NSA Collecting Phone Records of Millions of Verizon Customers Daily, GUARDIAN (London), Jun. 6, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; 最後造訪日 2015 年 11 月 20 日 Glenn Greenwald & Ewen MacAskill, NSA Prism Program Taps in to User Data of Apple, Google and Others, GUARDIAN (London), Jun. 7, 2013,

在史諾登洩密案後，剎時間 Section 215、FISA Amendments、PRISM 成為熱門搜尋關鍵字，且引發民眾對於國家調查犯罪而侵入隱私領域之恐慌。同時各媒體不斷質疑執法單位對於網路及手機監聽之必要性，如: The Colbert Report 和 The Daily Show 報導執法單位使用之蒐證技術、紐約時報和華盛頓郵報報導手機定位技術[121]、華爾街日報專文介紹在飛機上安裝追踪手機訊號裝置[122]，這些報導如火上加油般加深民眾對於執法必要性與隱私間之疑慮。

2013 年 6 月，華盛頓郵報和衛報刊登史諾登提供有關於國家安全局稜鏡計畫(PRISM program)簡報[123]，簡報詳述網路用戶資料如何從數家大型電信業者、社群網路業者流向國家安全局，及國安局探員如何監控用戶之電子郵件、語音聊天訊息、影音聊天訊息、影像、儲存資料、網路電話、登入資料以及社群網路細節等。

這些服務提供者包括蘋果、谷歌、臉書、Skype、美國線上和微軟，這些公司瞬間成為眾矢之的，質疑聲浪不斷，這些電信、社群服務業者為止血，隨即採取必要措施與國家安全局保持距離。蘋果公司發出聲明，宣稱當記者在 6 月 6 日詢問時，第一次聽說政府稜鏡計畫，其公司並未提供政府單位任何直接讀取該公司伺服器權限，且政府單位必先取得法院命令，公司才會提供客戶通訊內容

---

http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data 最後造訪日 2015 年 11 月 20 日。

[121] Ellen Nakashima, FBI Clarifies Rules on Secretive Cellphone-Tracking Devices, WASH. POST, May 14, 2015, https://www.washingtonpost.com/world/national-security/fbi-clarifies-rules-on-secretive-cellphone-tracking-devices/2015/05/14/655b4696-f914-11e4-a13c-193b1241d51a_story.html 最後造訪日 2015 年 11 月 20 日; Tom Jackman, Experts Say Law Enforcement' s Use of Cellphone Records Can Be Inaccurate, WASH. POST, Jun. 27, 2014, http://www.washingtonpost.com/local/experts-say-law-enforcements-use-of-cellphone-records-can-be-inaccurate/2014/06/27/028be93c-faf3-11e3-932c-0a55b81f48ce_ story.html 最後造訪日 2015 年 11 月 20 日；Matt Richtel, A Police Gadget Tracks Phones? Shhh! It' s Secret, N.Y. TIMES, Mar. 15, 2015, http://www.nytimes.com/2015/03/16/business/a-police-gadget-tracks-phones-shhh-its-secret.html. 最後造訪日 2015 年 11 月 20 日

[122] Devlin Barrett, CIA Aided Program to Spy on U.S. Cellphones, WALL ST. J., Mar. 10, 2015, http://www.wsj.com/articles/cia-gave-justice-department-secret-phone-scanning-technology-1426009924 最後造訪日 2015 年 11 月 20 日 ; Devlin Barrett, Americans' Cellphones Targeted in Secret U.S. Spy Program, WALL ST. J., Nov. 13, 2014, http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533 最後造訪日 2015 年 11 月 20 日。

[123] Barton Gellman & Laura Poitras, U.S. Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program, WASH. POST, Jun. 6, 2012, A1 版。

[124]。臉書執行長馬克佐克伯表示:臉書從未，也不會是稜鏡計畫之一員而提供政府單位其伺服器之直接讀取權限。臉書從未接獲如同報導中 Verizon 一樣，來自政府之要求大量數據或資訊之概括請求或是法院命令，即使收受這種要求，臉書也會即力反抗[125]。

美國電信服務、社群服務提供企業為了不使其等公司看起來像政府之盟友，甚至而塑造公司是用戶隱私擁護者形象，其等所採取反制措施對於執法機關犯罪調查之影響既深且鉅。首先，蘋果公司和谷歌公司對於其公司之手機預設值予以加密，如此一來，即使執法單位取得搜索票，該等公司也無法協助執法單位進行解密。第二，眾服務供應商不若以往會主動合作，現今多挑戰執法單位之請求。

蘋果公司前於 2014 年 5 月間，在政府單位提出搜索票後，尚配合執法單位交出儲存在 iPhone 手機內之資訊，包括簡訊、照片 、影音、聯絡人名單、電話紀錄等[126]。然在 2014 年 10 月，蘋果公司宣布 iPhone 和 iPad 預設安全升級後，公司在無用戶密碼情況下，無法讀取在手機裝置上之任何資料[127]，且在其官方網站說明日後縱使面對政府請求交付資料之壓力下，仍將盡力保護用戶隱私[128]。在升級為 iOS 8.0 或更新版本後，即便在有搜索票之情況下，蘋果公司已無法配合政府做資料擷取，因為用戶資料被加密金鑰所保護，而加密金鑰與用戶密碼相連結，蘋果公司並不知道用戶設定的密碼，當然無法解密。谷歌迅速跟進，讓客戶

---

[124] 蘋果聲明“first heard of the government’s ‘Prism’ program when news organizations asked us about it on June 6. We do not provide any government agency with direct access to our servers, and any government agency requesting customer content must get a court order.” https://www.apple.com/apples-commitment-to-customer-privacy 最後造訪日 2015 年 11 月 20 日。

[125] 臉書聲明: “Facebook is not and has never been part of any program to give the U.S. or any other government direct access to our servers. We have never received a blanket request or court order from any government agency asking for information or metadata in bulk, like the one Verizon reportedly received. And if we did, we would fight it aggressively.” https:// www.facebook.com/zuck/posts/10100828955847631. 最後造訪日 2015 年 11 月 20 日。

[126] Andrew Cunningham, New Guidelines Outline, ARS TECHNICA (May 8, 2014), http://arstechnica.com/apple/2014/05/08/new-guidelines-outline-what-iphone-data-apple-can-give-to-police/. 最後造訪日 2015 年 11 月 20 日。

[127] Trevor Timm, Your iPhone is Now Encrypted, THE GUARDIAN, Sep. 30, 2014, http://www.theguardian.com/commentisfree/2014/sep/30/iphone-6-encrypted-phone-data-default. 最後造訪日 2015 年 11 月 20 日。

[128] Privacy--Government Information Requests, APPLE, http://www.apple.com/privacy/government-information-requests 最後造訪日 2015 年 11 月 20 日。

得在 Android 系統設備加密，縱使執法單位持有搜索票，亦無法進行解密[129]。

對於服務供應業者的新政策，司法部當然是首當其衝，且對於美國司法部而言是弊多於利，司法部副部長 Leslie Caldwell 對於執法單位在取得搜索票並扣得手機後，仍無法取得手機內之資料這種「無政府狀態」感到憂心[130]。同樣，美國聯邦調查局局長 Comey 表示無法理解為何會有企業銷售讓用戶得以超越法律的產品[131]，保護自身隱私之急切可以被理解，但我們也應該急切保護無辜的被害人[132]。在 2014 年 10 月，司法部與蘋果公司就此問題進行會議，司法部強調蘋果公司之加密政策將形成很大的危機[133]。美國總統歐巴馬亦表示，如果科技使我們在已鎖定恐怖份子，得知嫌疑人之手機號碼或社群網站帳號、電子郵件帳戶之情況下，仍無法取得這些裝備內的資料，那將會是個大問題[134]。

對此，谷歌執行長 Eric Schmidt 回應，政府仍有許多方式可以取得嫌疑者的資料[135]。蘋果執行長回擊:若政府想要取得資料，應向用戶索取，而不是要求公司提供客戶資料[136]。科技業者與美國執法單位的關係，自從史諾登洩密後，已降

---

[129] New Security Features in Android 5.0, ANDROID OFFICIAL BLOG (Oct. 28, 2014), http://officialandroid.blogspot.co.uk/2014/10/a-sweet-lollipop-with-kevlar-wrapping.html. 最後造訪日 2015 年 11 月 20 日。

[130] Julian Hattem, DOJ Fears Tech "Zone of Lawlessness," THE HILL http://thehill.com/policy/technology/230840-doj-fears-tech-zone-of-lawlessles 最後造訪日 2015 年 11 月 20 日。

[131] Brian Naylor, Apple Says iOS Encryption Protects Privacy, NPR http://www.npr.org/sections/alltechconsidered/2014/10/08/354598527/apple-says-ios-encryption-protects-privacy-fbi-raises-crime-fears 最後造訪日 2015 年 11 月 20 日。

[132] Ellen Nakashima, Tech Giants Don't Want Obama to Give Police Access, WASH. POST, http://www.washingtonpost.com/world/national-security/tech-giants-urge-obama-to-resist-backdoors-into-encrypted-communications/2015/05/18/11781b4a-fd69-11e4-833c-a2de05b6b2a4_story.html. 最後造訪日 2015 年 11 月 20 日。

[133] Devlin Barrett & DannyYadron，Apple and Others Encrypt Phones, Fueling Government Standoff, WALL ST. J., Nov. 18, 2014, http:// www.wsj.com/articles/apple-and-others-encrypt-phones-fueling-government-standoff-1416367801 最後造訪日 2015 年 11 月 20 日。

[134] 美國總統歐巴馬與英國首相卡麥隆聯合記者會談會 https://www.whitehouse.gov/the-press-office/2015/01/16/remarks-president-obama-and-prime-minister-cameron-united-kingdom-joint- 最後造訪日 2015 年 11 月 20 日。

[135] Danny Yadron, Google's Schmidt Fires Back Over Encryption, WALL ST. J., Oct. 8, 2014, http://www.wsj.com/articles/googles-schmidt-says-encrypted-phones-wont-thwart-police-1412812180 最後造訪日 2015 年 11 月 20 日。

[136]

到歷史性的冰點。

在 2015 年 5 月，美國科技界龍頭，包括蘋果公司、谷歌公司及密碼學家集體上書美國總統歐巴馬，請求美國總統否決政府關於命科技業者修改智慧型手機和其他通訊設備之安全性的法律提案，使執行機關得以取得解密後之資料。信中強調，堅強之加密技術是現今資訊經濟安全的基石。執法單位表示其支持加密程式之使用，但希望科技業提供執法單位讀取加密資料的合法管道—亦即後門程式，但後門程式形同對駭客開啟入侵的大門，這些網路服務提供商斷不可能答應。

第五項　以植入木馬程式為監聽方式之美國實務見解

一、簡介

美國執法單位近年來，以搜索犯罪嫌疑人之電腦為偵查犯罪方式有日趨增加之勢，其中最特別者是以植入木馬程式來蒐集犯罪證據。木馬程式有許多軟體，譬如 data extraction software、 network investigative technique (“NIT”)、 port reader、harvesting program、 remote search, CIPAV（ Computer and Internet Protocol Address Verifier）或是 IPAV（ Internet Protocol Address Verifier）。使用上述裝置最大之功能在於協助執法機關追踪使用代理伺服器或隱匿其網路活動者。在兩年期間，美國聯邦調查局使用木馬程式來蒐集證據，至少遍及全美十六個主要城市，包括水牛城、丹佛、休斯頓、洛杉磯、邁阿密、紐奧良、費城等處[137]，美國聯邦調查局在早期使用木馬程式時，主張無需取得司法授權[138]，惟此見解已為法院見解所推翻。

美國聯邦調查局植入木馬程式之目的，係為侵入嫌疑人之電腦以取得資料，蒐集之資料會自動寄往美國聯邦調查局位於東維吉尼亞州之伺服器，至於美國聯邦調查局如何使用取得之資料現仍屬機密。目前有紀錄中，調查局以木馬程式取

[137] 參見 Electronic Frontier Foundation，https://www.eff.org/files/filenode/cipav/FBI_CIPAV-10.pdf ，最後造訪日 2015 年 11 月 20 日。
[138] 同前註。

得之資料包括:電腦的 IP 位址、媒體存取控制位址(Media Access Control address，MAC address)[139]、運行之程式清單、系統版本及序號、瀏覽器種類、最近瀏覽網站、電腦註冊名稱、登入帳號等[140]。

二、美國憲法第四修正案及美國聯邦刑事訴訟規則第 41 條對聲植入木馬程式之搜索票之適用

執行單位若欲使用木馬程式，必先聲請搜索票，此觀諸第四修正案自明。再搜索票之核發基礎需有「合理依據」，且聲請書必需符合明確性(particularity)要件，即應敘明欲搜索之處所及欲扣押之人或物，特定搜索之標的。

美國聯邦刑事訴訟規則第 41 條規定執行單位聲請搜索票或其他扣押行，需具有合理依據，此亦為第四修正案所要求之標準。且搜索票之目的係為取得犯罪證據，或是供犯罪所用、預備使用或在犯罪中所使用之財物[141]，第 41 條 b 項規範治安法官有權得核發搜索票之情況:

1. 在轄區內有權核發之治安法官，若無得核發之法官，在轄區內登錄之州法院法官，得核發搜索票搜索、扣押在該轄區內之財物或人員[142]。

2. 有權核發搜索票之治安法官得核發搜索票時搜索、扣押轄區外之人員、財物，惟以於核發時該人員或財物在其轄區內，執行時已移居至他轄區者為限[143]。

---

[139] 媒體存取控制位址，或稱為實體位址，係用以定義網路裝置之位址，在 OSI 模型中，第三層網路層負責 IP 位址，第二層資料鏈結層則負責 MAC 位址。MAC 位址用於在網路中唯一標示一個網卡，一台電腦會有一或多個網卡，每個網卡都需要有一個唯一的 MAC 位址。

[140] 參見 Kevin Poulsen, FBI’s Secret Spyware Tracks Down Teen Who Made Bomb Threats。

[141] FED. R. CRIM. P. 41(c) Persons or Property Subject to Search or Seizure.A warrant may be issued for any of the following:
(1) evidence of a crime;(2) contraband, fruits of crime, or other items illegally possessed;(3) property designed for use, intended for use, or used in committing a crime; or (4) a person to be arrested or a person who is unlawfully restrained.
得以下列人員或財物為搜索、扣押標的而核發搜索票：(1)犯罪證據；(2)違禁物、犯罪所得之物或其他因犯罪之持有之物；(3)預備或意圖供犯罪所用之物或已用於犯罪所用之物；或(4)應受逮捕之人或受非法拘禁之人。

[142] FED. R. CRIM. P. 41(b)(1) a magistrate judge with authority in the district--or if none is reasonably available, a judge of a state court of record in the district--has authority to issue a warrant to search for and seize a person or property located within the district;

[143] FED. R. CRIM. P. 41(b)(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district

3. 就國內恐怖政擊或國際恐怖攻擊之調查，治安法官有權核發搜索票搜索在其轄區內或轄區外，與恐怖政擊相關之活動所在地之人員、財物[144]。

4. 治安法官有權核發搜索票准許其轄區內追踪器之安裝，以追踪其轄區內、轄區外或兩者間之人員、財物之移動情況[145]。

5. 在任何犯罪行為發生地之治安法官或是哥倫比亞特區之治安法官，得核發在美國國土外，但在下列範圍內之財物之搜索票[146]：

（1）在美國政府屬地、領地或邦聯內

（2）不論財物之所有權屬於何人，美國外交或領事在美國境外內因任務所持有之財物，包括附屬建築物、建築物之一部或因使用於任務之土地，或

（3）由美國政府所有或承租者以及在國外因美國外交、領事目的所使用之住所以及附屬土地。

第 41 條已明定五種治安法官得核發搜索票之情狀，因此任何聲請人聲請搜索票以安裝木馬程式時，應符合各條項所定之管轄要求，以下試分析各項情況：

適用第 41 條(b)(1)時，治安法官得核發其轄區內之搜索票[147]，因此治安法官就本款應考量者，並非犯罪發生地是否在其轄區內，而是搜索票之執行地應在其

---

when the warrant is issued but might move or be moved outside the district before the warrant is executed;

[144] FED. R. CRIM. P. 41(b)(3) a magistrate judge—in an investigation of domestic terrorism or international terrorism—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;

[145] FED. R. CRIM. P. 41(b)(4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both;

[146] FED. R. CRIM. P. 41(b)(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:
(A) a United States territory, possession, or commonwealth;
(B) the premises—no matter who owns them—of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or
(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

[147] 參見 United States v. Chipps, 410 F.3d 438, 446 (8th Cir. 2005)、United States v. Kernell, No. 3:08-CR-142, 2010 WL 1408437，認為本條限制治安法官僅能核發欲搜索之財物在其轄區內之搜索票。另United States v. Hernandez, No. 3:08-CR-142, 2008 WL 4748576 則指出治安法官，一般而言僅被授權處理其轄區內之事務，因為搜索之範圍應限縮在該法院之轄區內。

轄區內[148]。

第 41 條(b)項(2)款，係承前第 1 款之變動規則，規範原本在其轄區內受搜索之財物，然於執行搜索票時，已不在該轄區內之情況[149]。本款擴充傳統以為治安法官僅得核發其所在地轄區內財物之搜索票之見解。但大多數核發的決定是針對 41 條 b 項 2 款不適用之情況，例如:在 United States v. Glover 案[150]，FBI 追查一件販賣天使塵、海洛因案件，當 FBI 取得哥倫比亞特區聯邦法官核發之搜索票，授權其等得在嫌疑人 Glover 的卡車上安裝錄音裝置時，雖其聲請搜索票之際，Glover 的卡車停放在巴爾的摩，法官仍然核發搜索票授權 FBI 探員得進入停放在哥倫比亞特區外之卡車[151]，FBI 因此取得 Glover 在卡車上談論運送毒品之錄音，FBI 以該錄音證據逮捕 Glover 並取得被告之自白。在上訴審時，Glover 以准許核發搜索票在其卡車上安裝錄音器時，其卡車是停放在馬里蘭州為抗辯，然檢察官則主張治安法官有權就在美國境內，所有在運輸工具安裝電子錄音設備之案件核發搜索票。法院最後認為此搜索票違反第 41 條 b 項 2 款之規定，該錄音證據應被排除[152]。

同樣地，在 United States v. Krueger[153]案，聯邦探員調查一件持有、散布兒童猥褻圖片案件，在調查過程中，探員以為 Krueger 住所坐落於堪薩斯州安波瑞亞，因此向堪薩斯州法官聲請搜索票並獲核准，然而在搜索過程中，探員發現 Krueger 及其所使用之電腦均住在奧克拉荷馬州，惟探員仍向堪薩斯州之治安法官聲請搜索票，嗣雖依搜索票取得電腦，惟被告提出異議請求證據排除，因為第二次核發

---

[148] 參見United States v. McVicker, No. 3:11-CR-00101-SI, 2012 WL 860412 (D. Or. Mar. 13, 2012)。“traditionally warrants have only been allowed to search for property in that district.”(傳統來說，搜索票僅被授權搜索在該轄區內之財物。)

[149] 參見 United States v. Glover, 736 F.3d 509, 515 (D.C. Cir. 2013); United States v. Krueger, 998 F. Supp. 2d 1032, 1035 (D. Kan. 2014)。

[150] United States v. Glover, 736 F.3d 510.

[151] 參見 United States v. Vann, No. 07-CR-247(JMR/RLE), 2007 WL 4321969, 22 (D. Minn. Dec. 6, 2007) ，在明尼蘇達州之治安法官核發搜索執行地在威斯康辛州蘇必利爾市之搜索票。另參見 United States v. Jones, 132 S. Ct. 945, 948 U.S. 2012 搜索票授權裝置 GPS 定位系統，授權地在哥倫比亞特區，執行搜索票地點則在馬里蘭州。

[152] 參見前註 United States v. Vann 案，在明尼蘇達州之治安法官無權核發搜索位於威斯康辛州蘇必利爾市之房屋之搜索票;另參見前註 United States v. Jones 案 GPS 追踪裝置之安裝該當第四修正案之搜索，因此需符合最低程度之搜索保護要件。

[153] United States v. Krueger, 998 F. Supp. 2d 1032, 1033-34 (D. Kan. 2014)

搜索票係關於搜索在奧克拉荷馬州之財物，有違第 41 條 b 項規定，檢察官則主張在聲請搜索票時，該受搜索之財物得任意被移動，因此符合第 41 條 b 項 2 款之規定。地方法院裁決該搜索票自始無效，是以自被告電腦所搜得之證據及其自白均無證據能力[154]。

關於第 41 條b 項 3 款，國會在 2001 年通過美國愛國者法案，擴張恐怖攻擊犯罪調查範圍，授權治安法官得核發有關於國內外之恐怖政擊活動之搜索票，無論受搜索、扣押之財物是否在其轄區內[155]。

依第 41 條 b 項 4 款規定，治安法官得核發搜索票，准許在其轄區內安裝追踪裝置，追踪其轄區內或轄區外人員、財物之移動情況。本條係在 2006 年因修正美國聯邦刑事訴訟規則而變動[156]，過去，法院認為安裝追踪裝置在停放於公共區域之交通工具外部，是無需搜索票[157]，惟在 Jones 案[158]之後，最高法院認為不論安裝之地點，均需有搜索票始得在交通工具上安裝追踪器。

在 2008 年，美國聯邦刑事訴訟規則修正後新增第 41 條 b 項 5 款，雖執行搜索票之處所係在法院轄區外，惟受美國政府實際控管[159]，此範圍包括美國屬地之

---

[154] 相同案例參見 In re Emachines Computer Model No. S1940, No. C-12-740M, 2012 WL 3259897, (S.D. Tex. July 19, 2012) 德州南區法院法院駁回依第 41 條 b 項 2 款聲請之搜索票，因為受搜索之電腦已從該轄區移往德州西區。

[155] Section 219 (Single-jurisdiction search warrants for terrorism) 修正美國聯邦刑事訴訟規則，准許治安法官在調查國內、國際恐怖攻擊活動時，得簽發搜索票，無論受搜索標的是否在其轄區內。另參見 United States v. Vilar, No. S305CR621KMK, 2007 WL 1075041, (S.D.N.Y. Apr. 4, 2007); 參見 Gerald G. Ashdown, The Blueing of America: The Bridge Between The War On Drugs And The War On Terrorism, 67 U. PITT. L. REV. 753, 789-90 (2006).

[156] 參見 United States v. Asghedom, 992 F. Supp. 2d 1167,1168 (N.D. Ala. 2014); United States v. Hersman, No. 2:13-cr-00002, 2013 WL 1966047, (S.D. W.Va. May 10, 2013);
另參見美國法典第 18 編 3117 條 a 項:法院有權核發搜索票或其他命令，授權在其轄區內或於其轄區內安裝嗣後移動至轄區外之運輸工具追踪裝置。
18 U.S.C. § 3117(a) (“a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction”).

[157] 參見 United States v. Smith, 387 F. App’ x 918, 920-21 (11th Cir. 2010)。

[158] United States v. Jones, 132 S. Ct. 945 (U.S. 2012)本件 FBI 探員將追踪裝置安裝於被告 Jones 駕駛之車上，法院認為執法單位使用追踪裝置構成第四修正案之搜索，因此，因本件未取得搜索票即安裝追踪器，自追踪器所取得之證據應被排除。

[159] 參見 The Modest Role of the Warrant Clause 及 David A. Schlueter, Criminal Procedure Rules Pending Public Comment, 21 CRIM. JUST. 45 (2007):新增第 41 條 b 項 5 款，目的在於填補治安法官有權核發在美國領域外卻受美國管轄之搜索票之漏洞。

譬如關島或維京群島，以及全世界之美國大使館、領事館。

三、法院核發植入木馬程式之搜索票之案例討論

雖然時有所聞美國執行單位以現代科技調查犯罪，但受限於實務辦案考量，不想使植入木馬程式之監聽方法受到公眾之注目，因此釋出得供分析之案例並不多見[160]，且此類案例在聲請搜索票時多以彌封方式為之，且法官亦下令多封存此類案子[161]。

（一）華盛頓西區

A.案例經過：

在 2007 年六月，FBI 探員針對華盛頓萊西市高中一連串炸彈威脅案件進行調查，FBI 先聲請搜索票以便在嫌疑人之電腦內安裝木馬程式，取得嫌疑人使用之 MySpace 帳戶[162]，探員在聲請書上敘明合理根據可 MySpace 之 Timberlinebombinfo 帳號及其他電子郵件位址使用「電腦及 IP 位址驗證器」(Computer and Internet Protocol Address Verifier,CIPAV)[163]。CIPAV 可截收電腦往來之資訊，藉此找出嫌疑人之身分，但因為揭露 CIPAV 使用方式可能有害於其他同樣使用 CIPAV 之調查中案件，因此 CIPAV 使用方式被列為機密文件。

本案始於在 2007 年 5 月 30 日，學校人員發現手寫炸彈威脅之字條，學校發現字條後旋疏散 Timberline 高中師生。於 2007 年 6 月 4 日，學校又收到一封來自於dougbriggs123@gmail.com 帳戶之電子郵件，信中威脅將於 2007 年 6 月 4 日在學校引爆炸彈，嫌疑人稱在 Timberline 高中共藏放 4 顆炸彈，分別在數學教室、圖

[160] Declan McCullagh, FBI Remotely Installs Spyware to Trace Bomb Threat, CNET (July 18, 2007, 9:42 AM), http://www.cnet.com/news/fbi-remotely-installs-spyware-to-trace-bomb-threat/ 最後造訪日 2015 年 11 月 20 日。

[161] 參見 Brian L. Owsley, To Unseal or Not to Unseal: The Judiciary’s Role in Preventing Transparency in Electronic Surveillance Applications and Orders, 5 CALIF. L. REV. CIRCUIT 259 (2014)。

[162] 參見 Paul Ohm, Good Enough Privacy, 2008 U. CHI. LEGAL F. 1,

[163] CIPAV 係一包含木馬程式，由美國聯邦調查局控制，凡發送或接收 CIPAV 訊息之電腦，被遭到 FBI 監控。CIPAV 能夠蒐集大量資料，包括 IP 位址、MAC 位址、連接埠、正在運算之程式、操作系統型號等。CIPAV 會隱身在被植入電腦內，記錄 60 日內所有網路使用情況，以及與該電腦有通訊之每個電腦 IP 位址。

書館、主辦公室及一顆手榴彈。炸彈在 9 點 15 分起，每隔 15 分鐘引爆[164]，且在 8 點 45 分，學校電子郵件伺候器會先終止服務，接著學校會受到阻斷服務政擊(Denial-of-Service attack)[165]等語。學校因而再度疏散所有人員。

隔日，Timberline 高中人員收受一封來自於 dougbrigs @gmail.com 帳戶之炸彈威脅:「一顆炸彈放置在女子體育館置物櫃，藏放在一堆衣服下，其他四顆分別放在語言教室、數學教室，另一顆以膠帶黏住，只要有任何振動即會引爆，最後一顆放在置物櫃中。炸彈放置在隔音包內，是偵測不到。炸彈將在 10 點 15 分引爆。」員警未能從此封信取得任何訊息，因為電子郵件帳戶申請地在義大利，且無任寄件者資訊。

同日稍晚，學校收到另一封來自 dougbriggs234@gmail.com 帳戶的電子郵件，信中寫道: 「有六顆炸彈會在 10 點 45 分至 11 點 15 分間引爆，你們抓不到我，放棄吧!也許你們應該僱請 Bill Gates 來告訴你們，信是從義大利來的，喔!我已經告訴你們了，所以停止追踪信件來源，因為我早就告訴你們信是從義大利寄出，你們也只能追踪到義大利，所以，停止吧!」，因為這兩封郵件，學校因此疏散師生。

在 2007 年 6 月 6 日，Timverline 高中校長收到一封自 dougbriggs911@gmail.com 帳戶之電子郵件，信中表示 :「享受人生最後的時光」，稍晚，第二封電子郵件再度威脅師生安全，且嘲弄追查寄件人身分的人員:「這是最後的警告，兩顆炸彈將會在 10 點 45 分引爆，一顆是手榴彈，一顆藏放在不知名的地方。你們只能追查出信件來自於義大利，沒有任何證據會導向美國，所以，放棄吧! 你們應該僱用 Bill Gates 來協助你們追查，學校不該建議教師不讓學生得知這些信件，信就是寫來娛樂大家！」。學校因此疏散師生。

---

[164] 原文為“I will be blowing up your school Monday, June 4, 2007. There are 4 bombs planted throughout timberline high school. One in the math hall, library hall, main office and one portable. The bombs will go off in 5 minute intervals at 9:15 AM.”。 dougbriggs123@gmail.com 帳戶建立於 2007 年 6 月 3 日，IP 位址為 80.76.80.103。

[165] 阻斷服務攻擊亦稱洪水攻擊，目的在使受攻擊之電腦或網路資源系統耗盡，服務因而暫時中斷或停止。

在 2007 年 6 月 7 日，另一封來自 thisisfromitaly@gmail.com 電子郵件寫道:「已在學校安裝三顆炸彈，且已設好定時器，確保分秒不時地爆炸。鎖緊大門也許是個好對策，但太遲了！」學校因為此信，再度疏散師生。

在 2007 年 6 月 7 日，疑似嫌疑人在地方電子報上張貼三則威脅訊息，在報社移除訊息後，訊息再度被張貼在電子報上，直到報社關閉讀者回覆功能。經分析張貼資訊，恐嚇訊息來自於 IP 位址為 192.135.29.30 ，據調查，該 IP 位址是義大利核子物理學研究院(National Institute of Nuclear Physics in Italy)。

此外，在 2007 年 6 月 7 日警長告知萊西警察局，有民眾投訴收到來自 MySpace 帳號Timberlineinfo 的邀請，希望她能張貼 htttp://bombermails.hypephp.com 訊息在其 MySpace 頁面，若其不從，日後其姓名將出現在炸彈威脅上，同時也有 33 名家長也報案其子女收到同樣的邀請。其中有兩位民眾在收到訊息後接受邀請，其後就收到來自暱稱為「Alexspi3ring_09」即時訊息，當民眾要求寄件人寄送更多有關炸彈攻擊之資訊時，即時訊息就停止傳送。Alex Spiering 確有其人，且在當時是 Timberline 高中學生並使用 MySpace。

在 2007 年 6 月 8 日，學校當局收到兩封來自 Timberline.Sucks@gmail.com 帳戶的炸彈威脅，學校因而疏散師生。追查結果，dougbriggs123@gmail.com 和 MySpace 網站的“Timberlinebombinfo” 帳戶的 IP 位址都是 80.76.80.103，惟這個 IP 位址是義大利 ISP 業者使用中。

在 2007 年 6 月 12 日，聯邦治安法官核發搜索票准予搜索 MySpace 網站 Timberlinebombinfo 之帳戶，隔日 FBI 經由網路植入 CIPAV 至系爭電腦，並回傳取得資料，數日後，根據搜索取得之證據，以炸彈威脅等罪名逮捕一名十年級的學生[166]。該生當時是 15 歲，審判中承認炸彈威脅、騷擾和竊取身分等罪行，後法院判決其在少年機構執行 90 日刑罰。

B.法院理由

[166] 參見 Lacey 10th-grader Arrested in Threats to Bomb School, SEATTLE TIMES, http://www.seattletimes.com/seattle-news/lacey-10th-grader-arrested-in-threats-to-bomb-school/，最後造訪日 2015 年 11 月 20 日。

全案以事後之明來看，在搜索票核發時，系爭電腦實際所在地是在華盛頓州西區，但核發當時並無任何證據得以佐證此一事實。因此並不該當聯邦刑事訴訟規則第 41 條 b 項 1 款或是 41 條 b 項 2 款。同樣地，FBI 當時亦非向法院聲請安裝追踪裝置之搜索票，因此也無同規則第41 條 b 項 4 款之適用。最後，同規則第 41 條 b 項 5 款亦不適用在本案上，因為電腦並不處在美國屬地或外交使館、領事館屬美國政府所有之建築物內。

因此，第 41 條得適用作為土地管轄核發依據就只剩 41 條 b 項 3 款之情狀，雖然聲請書未註明係依據本款作為聲請理由，但聲請書已敘明本件屬州際間之對人身安全之威脅，以及使用電腦危害公眾安全之案件一炸彈威脅屬恐怖攻擊[167]。因此聲請符合恐怖攻擊之土地管轄要件，是以不問電腦所在地在何處，均非核准搜索票應審酌之重點。

(二)科羅拉多州法院

A.案例事實

在 2012 年 10 月，美國菸酒槍炮及爆裂物管理局(Bureau of Alcohol, Tobacco, Firearms and Explosives)探員向科羅拉多地方法院聲請搜索票，為使搜索標的之電腦能植入「網路調查器」(network investigative technique，NIT)，用以辨識出電腦、電腦位置、及其他電腦資訊、電腦使用者資訊。探員在聲請書上列出搜索標的清單:電腦 IP 位址、MAC 位址、，電腦運作之程式、瀏覽器名稱和版本、電腦作業系統、時區、有線及無線網路通訊資訊、使用之 URL 等。

據探員表示，本案開始於嫌疑人在 2012 年 7 月 22 日，撥打電話予 Arapahoe 郡警長告知已安裝炸彈，該帶有口音之來電者自稱 Andrew Ryan，威脅若不釋放 James Holmes[168]，將炸毀 Arapahoe 郡監獄，來電者當時係使用(760) 705-8888 門號

[167] United States v. Garey, 546 F.3d 1359, 1361 (11th Cir. 2008)

[168] James Holmes 因在 2012 年 7 月 12 日在科羅拉多州 Aurora 戲院槍殺 12 名民眾而被訴殺人。參見 Jack Healy, Mental Evaluations Endorse Insanity Plea in Colorado Shootings, Defense Says, N.Y. TIMES (May 13, 2013),

之網路電話，嗣後因網路收訊不佳以及來電者的口音難辨，警長進一步要求與來電者進行書面對話，所以取得來電者使用之電子郵件帳號為 soozanvf @gmail.com 。

接下來數日，帶有口音自稱 Andrew Ryan 的男子再度聯繫 Arapahoe 郡警局，並威脅如果不釋放 James Holmes，將炸毀監獄，電話來電顯示為(760) 705-8888，同時，副警長也接到來自 soozanvf@gmail.com 的電子郵件威脅訊息。在 2012 年 7 月 25 日，自稱 Andrew Ryan 之男子，以(760) 705-8888 門號聯繫警局並表示其與同夥已在 Cherry Creek 水庫殺死三人，棄屍在水庫，但經警搜查並未發現任何被害人。

在 2012 年 7 月 30 日，Greenwood Village 警局收到一通關於威脅將炸毀 Doubletree 飯店之來電，在來電者與警局通話時，員警前往 Doubletree 飯店查看，該來電男子英文帶有口音且自稱 Andrew Ryan，告訴員警他已經在飯店裡放置炸彈，當員警與來電者交談時，員警聽到另有一人告訴來電者炸彈已放置在飯店以及多久後炸彈會引爆，在疏散飯店後，員警進行搜查，並未發現任何炸彈。而本次通話，嫌疑犯是使用(877) 573-9800 門號之網路電話(VoIP)。

在 2012 年 7 月 31 日上午，該名帶有口音自稱 Andrew Ryan 男子聯絡丹佛國際機場，宣稱他和友人已在機場內安裝炸彈[169]，若不釋放 James Holmes，將引爆放置於行李區之炸彈，本此來電顯示號碼為(760) 705-8888，此門號屬於谷歌公司語音郵件系統所使用。繼於 2012 年 8 月 14 日下午，科羅拉多州 Aurora 郡監獄接獲炸彈威脅電話，來電者自稱 Alex Anderson，表示若不釋放 James Holmes 將引爆藏放在監獄之炸彈，來電顯示同樣為屬於於谷歌公司語音系統之門號(760) 705-8888。

---

http://www.nytimes.com/2013/05/14/us/james-holmes-aurora-shooting-suspect-enters-insanity-plea.html 最後造訪日 2015 年 11 月 20 日。

[169] Will C. Holden, Denver International Airport Confirms Non-specific Bomb Threat, FOX 31 DENVER (July 31, 2012, 2:11 PM), http://kdvr.com/2012/07/31/denver-international-airport-confirms-non-specific-bomb-threat/ 最後造訪日 2015 年 11 月 20 日。

在 2012 年 9 月 12 日下午，一自稱 Jason 男子撥打電話至丹佛國際機場，宣稱在美國聯合航空航班 6318 前往北達科塔州之班機放置炸彈，將會在班機抵達時引爆，其接著指出其為蓋達組織成員，此舉係為報復美國軍事攻擊，來電號碼同樣為谷歌公司語音郵件系統門號(760) 705-8888。

在 2012 年 9 月 9 日，嫌疑人以 soozanvf@gmail.com 電子郵件帳號寄送數張照片予丹佛警察，其中一張照片係一男子身著伊朗軍服，寄件者告訴警察其姓名為 Mohammed[170]。其後，於 2012 年 9 月 16 日，Mohammed 再次聯絡丹佛警方並指出，他已經在德州大學及北達科塔州立大學放置炸彈，他進一步解釋他原先使用之 soozanvf @gmail.com 帳戶已遭谷歌公司封鎖帳號，因此他目前使用 Texas.Slayer @yahoo.com 之帳號聯絡 ，丹佛警方後又多次收受以該新電子郵件帳戶寄出，宣稱在多所大學或機場放置炸彈之電子郵件。

在 2012 年 9 月 9 日，以 soozanvf@gmail.com 電子郵件寄送數張照片予丹佛警察，其中一張照片係一男子身著伊朗軍服，寄件者告訴警察他的名字是 Mohammed[171]。在 2012 年 9 月 16 日，Mohammed 再次聯絡丹佛警方指出，他已經在德州大學及北達科塔州立大學放置炸彈。他解釋他的使用的 soozanvf @gmail.com 帳戶遭谷歌公司取消帳號，他目前使用之帳號為: Texas.Slayer @yahoo.com ，丹佛警方又多次收受多封在大學或機場放置炸彈之電子郵件係來自於該新帳戶。

於 2012 年 10 月 9 日，治安法官核准在 Texas.Slayer @yahoo.com 帳號安裝 NIT 之搜索票，在 2012 年 10 月 9 日探員提出修正搜索票內容之聲請，目的為使 NIT 能充分發揮其功能，修正聲請中解釋 NIT 如何使用，及聲請人手寫之宣誓書，強調現調查中之犯罪涉及國際及國內恐怖攻擊，因此搜索票係依據聯邦刑事訴訟規則第 41 條 b 項 3 款所聲請，聲請人並擔保此次搜索並不會截收任何電子郵件中關於即時訊息內容的部分，治安法官於 2012 年 10 月 9 日核發修正使用 NIT 在

[170] 參見 Yale Law School Information Society Project
[171] 參見前揭註

Texas.Slayer@yahoo.com 搜索之搜索票。嗣於 2012 年 10 月 29 日，特別小組成員聲請第二次修正之搜索票，為修正前兩次聲請上印刷錯誤，同日治安法官即核發第二次修正後在 Texas.Slayer@yahoo.com 使用 NIT 的搜索票。在 2012 年 12 月 11 日，特別小組探員聲請第三次修正之搜索票，為在系爭電子郵件裝設新設計之 NIT，因原先安裝之 NIT 未能發揮其功能，同日治安法官核發第三次修正後得在 Texas.Slayer@yahoo.com 使用 NIT 的搜索票。探員於 2012 年 12 月 14 日，以寄送連結方式將 NIT 植入 Texas.Slayer @yahoo.com 帳戶，惟僅部分 NIT 成功，但也因此取得系爭帳戶之兩個 IP 位址，然該 IP 位址位在伊朗。

B.法院理由

本件治安法官核准針對 Mohammed 之炸彈攻擊威脅之搜索票，惟並未敘述簽發理由，但得從搜索聲請書看出端倪，聲請書明確指出法條依據為第 41 條 b 項 3 款，因為本件涉及恐怖攻擊，只有第 41 條 b 項 3 款建立土地管轄之依據。

聲請搜索之探員為建立第 41 條 b 項 3 款適用依據，其提供相當數量之證據，說明本件係與炸彈威脅有關，係屬恐怖攻擊案件，且這些證據亦闡明搜索明確性要件，聲請書內有充分之證據足以支持具有合理依據以核發搜索票之要件，因為本件為犯罪活動，且使用 NIT 之目的在於搜索電腦以獲取犯罪證據[172]。

(三)德州西區法院

A.案例事實

於 2012 年 12 月 18 日，美國聯邦調查局探員向德州西區法院治安法官聲請搜索票，為安裝 NIT 在系爭電腦，用來識別電腦、電腦所在地、其他有關電腦及使用者資訊，聲請人請求扣押之標的包括受搜索電腦之 IP 位址、MAC 位址、運作之程式、時區、電腦操作系統、預設語言及有線無線網路連結資訊、使用者姓名、帳戶及瀏覽過之網址等。聲請人強調本件係具有合理依據而聲請搜索票，搜

[172] In re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 758-59 (S.D. Tex. 2013)

索標的 512SocialMedia@gmail.com 是由嫌疑人 Donald Lee Phelps 所使用，Donald Lee Phelps 因金融詐騙遭聯邦通緝。

自 2005 年起，Phelps 即假冒其女友時在伊朗服役之已分居丈夫之身分進行詐騙，先更改德州駕駛執照，再以其女友之夫姓名取得佛羅里達州身分證，接著使用新取得之佛羅里達州身分證在信用合作社開戶，並在信用合作社謀得一職，最後，再使用信用合作社帳戶開立支票，並累積信用向銀行取得信用卡並申請貸款，聯邦在 2007 年 10 月 16 日發出對 Phelps 因銀行詐欺案之拘捕令。

在 2012 年 11 月 14 日，一秘密線民提供執法單位 Phelps 之手機門號，據線民指稱 Phelps 曾在德州奧斯汀居住約五年，使用假名 James Bridges，Phelps 以假名開立一名為 Extreme Social Media 的公司，在公司擔任程式設計師。線民因定期與 Phelps 使用上開手機門號交談，因此取得門號交予執法機關。

聯邦治安法官於 2012 年 11 月 20 日搜索票授權 FBI 得追踪線民提供 Phelps 使用中手機門號，隔日，FBI 即在德州 San Antonio 某家飯店追踪到該手機訊號，當探員到達飯店時，飯店人員自照片認出 Phelps 為飯店之旅客，但已於當日稍早時退房，Phelps 係假冒 Jack Rady 入住，並使用現金支付住宿費。

在 2012 年 12 月 3 日，FBI 查得 Phelps 係使用 JBridges007@gmail.com 電子郵件帳號，隔日即自谷歌公司取得登錄上開帳號之 IP 位址，進一步查出，Phelps 使用 HideMyAss.com[173]軟體用以掩蓋其登錄電子郵件使用之 IP 位址。

在 2012 年 12 月 10 日，第二位秘密線民提供 Phelps 使用之另一電子郵件帳號：512SocialMedia@gmail.com，線民能自照片中辨認出 Phelps，線民並提供 Phelps 在 Amplify Credit Union 信用合作社所開戶之銀行帳號，信用合作社帳戶是 Phelps 所經營之 Extreme Social Media 公司為戶名，雖然上開帳戶已經透支，但可以知道的是，登入銀行帳戶之 IP 位址，遭人使用 HideMyAss.com 隱藏。

聯邦治安法官於 2012 年 12 月 18 日簽署搜索票，授權聯邦探員在

[173] HideMyAss.com 為一提供用戶上網安全工具和網站之網站，讓用戶可以匿名上網，保護在線活動之隱私。參見 https://www.hidemyass.com/ ，最後造訪日 2015 年 11 月 20 日。

512SocialMedia@gmail.com 電子郵件帳戶 使用 NIT 程式。聯邦探員於 2012 年 12 月 20 日執行搜索植入 NIT，據回傳之資訊顯示，IP 位址之 ISP 業者位在德州奧斯汀，使用之裝置為電腦，配載 3561MB 之記憶體，電腦硬碟共有 589,663 MB 容量，作業系統版本為 Windows 7 Home Premium。

最後 Phelps 在阿拉巴馬州被捕，因銀行詐欺及加重身分竊用罪名在佛羅里達北區被起訴。在 2012 年 4 月 3 日 Phelps 承認上述兩項罪名，於 2012 年 7 月 17 日判決 5 年後入監執行[174]。

B.法院理由

治安法官在簽發對 Donald Phelps 之搜索票時，只授權可使用 NIT，然並未以書面敘述核發搜索票之理由，本件被告所涉犯之罪名為銀行詐欺案，亦即涉犯之罪名並非恐怖攻擊，所以科羅拉多州關於土地管轄限制（territorial limitation）[175]之案例，管轄限制並不適用在本案。

本件聲請書亦未提供任何證據釋明在聲請搜索票時，系爭電腦所在地位在該轄區內，因此，第 41 條 b 項 1 款並不適用在本案[176]。同樣的，因為沒有證據證明系爭電腦所在地，是以第 41 條 b 項 2 條亦不適用，因為第 2 款之要件為法官核發搜索票時，電腦在該法院轄區內[177]。本件搜索之標的，並非請求安裝追踪裝置，因此第 41 條 b 項 4 款並不適用於本案核發搜索票之理由[178]。最後，第 41 條 b 項 5 款也不適用於本案，因為電腦並非位於美國屬地或是外交使館建築物內。

綜上，本件亦不符合搜索明確性之要求，因此搜索票之核發有相當之爭議

---

[174] FBI, Jacksonville Division, Former Gainesville Resident Sentenced for Bank Fraud and Identity Theft (July 18, 2013), https://www.fbi.gov/jacksonville/press-releases/2013/former-gainesville-resident-sentenced-for-bank-fraud-and-identity-theft 最後造訪日 2015 年 11 月 20 日。

[175] 係指司法管轄權行使之地區限制。

[176] 參見 United States v. Chipps, 410 F.3d 438, 446 (8th Cir. 2005)、United States v. Kernell, No. 3:08-CR-142, 2010 WL 1408437, (E.D. Tenn. Apr. 2, 2010)

[177] United States v. Glover, 736 F.3d 509, 515; United States v. Krueger, 998 F. Supp. 2d 1032, 1035 (D. Kan. 2014)

[178] United States v. Asghedom, 992 F. Supp. 2d 1167, 1174-75 (N.D. Ala. 2014).

性，有「思慮欠周而核發」（improvidently granted）[179]之嫌，雖然就 Donald Phelps 之逮捕，此搜索票並未扮演任何角色，因此無從將此搜索票不合法做為逮捕不合法之理由。

(四)德州西區法院

A.案例事實

美國聯邦調查局探員於 2013 年初，向德州西區法院聲請搜索票搜索無法特定名稱之電腦，因有人使用該電腦從事聯邦法銀行詐欺、危害電腦安全及身分盜用等犯行，探員聲請搜索票之目的係為秘密在受搜索之電腦植入資料截收軟體，進而搜索標的電腦之硬碟、隨機存取存儲器（random access memory, RAM）及其他儲存媒體，並自動啟動電腦內建攝影機，及建立電腦所在地之經緯度座標，以及將上開資訊回傳在法院轄區內之 FBI 探員使用之電腦，聲請監控時間為 30 日[180]。聲請人聲請擬扣押之標的為電腦內之資料，包括使用者之 IP 位址、網路瀏覽紀錄、證明與受害銀行電子郵件伺服器往來之使用者 IP 位址、在犯罪時系爭電腦曾被使用及在犯罪期間內，由何人使用、持有或控制系爭電腦[181]。此外，因為監聽期間係自安裝監控程式後持續 30 日，聲請書也聲請對於未來發生的資料，包括得以辨識未來受詐騙被害人之會計分錄（accounting entries）、自系爭電腦內建攝影機拍下照片以辨識系爭電腦所在地及使用者以及系爭電腦所在地之資訊包括經緯度座標[182]之搜索，藉此可以調查使用者之臉部特徵以及定位出電腦所在地[183]。

---

[179] 係指法院在未經充份考慮或未獲與之有關之所有事實基礎，或基於錯誤之推測、誤導性之資訊，作出之判決、裁定。

[180] In re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013); 另參閱 Yale Law School Information Society Project。

[181] In re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d at 755-56; 另參見 Gus Hosein & Caroline Wilson Palow, Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques, 74 OHIO ST. L.J. 1071, 1089-90 (2013).

[182] In re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d at 756

[183] Yale Law School Information Society Project

探員之聲請依據為被害人之個人電子郵件信箱以及銀行帳戶曾被入侵[184]，入侵帳戶所使用之 IP 位址在國外，一旦被害人採取電子郵件信箱防護措施，第二個與被害人電子郵件帳號相差無幾之電子郵件帳號就被申請。第二個電子郵件帳號與被害人之電子郵件信箱只差 1 個字母，嫌犯曾使用第二個電子郵件帳號試圖將被害人在銀行帳戶之存款電匯到國外銀行。

B.法院理由

本案聲請之案由為聯邦銀行詐欺罪，治安法官駁回搜索票之聲請，理由如下：欠缺該當第 41 條 b 項土地管轄限制（territorial limit ）原則、憲法第四修正案關於搜索明確性之要件以及憲法對於錄影監視之標準等之證據。

因為錄影監視(video surveillance)之無差別性及侵入之本質，第五巡迴法院某種程度上就錄影監視採取與監聽一樣較嚴格之標準[185]，治安法官強調四個本件採用高於「合理根據」標準之理由，亦即在法院要求之標準下，搜索票授權錄影監視需展現出超過「合理根據」之標準—有理由相信犯罪證據會因錄影監視而取得，且應包括:1.已嘗試過其他蒐證方且該蒐證方式未能達到取證目的，或是合理相信其他蒐證方式難以達取證目的、或其他方式過於危險。2..受截收之通訊種類明確性之聲明，以及與該通訊相關罪名之陳述 3.監聽之期間應以足以達蒐證目的為限，最長不得逾 30 日（但必要時得延長之）以及 4.監聽侵害最小化，達到監聽目的已足之陳述[186]。法院認為聲請人未能敘明其已經採取其他所有必要手段以取得欲扣押之資訊，且聲請人未採取其他措施，並以侵害最小性之手段以取得本搜索票所欲搜索之資訊[187]，未達法院採取之嚴格標準，因此駁回本件搜索之聲請。

治安法官同時也認為本件執行單位未能滿足第四修正案明確性(particularity)

[184] In re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d at 755.
[185] United States v. Cuevas-Sanchez, 821 F.2d 248, 250 (5th Cir. 1987); 18 U.S.C. §§ 2510-20 (2012).
[186] In re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d at 760
[187] Gus Hosein & Caroline Wilson Palow, Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques, 74 OHIO ST. L.J. 1071, 1089-90 (2013)

之要求，第一，法院認為聲請人未能解釋聲請人所欲裝設之木馬程式將如何搜索以及讀取系爭電腦，特別是聲請人未提及該軟體應如何被運用以及軟體如何發揮功能。此外，駁回理由亦強調聲請書未能指出對於系爭電腦之搜索行為如何取得犯罪證據，法官並質疑系爭電腦之所在地，指出電腦可能是放置在公眾得使用之場所，例如圖書館、網咖、工作場所等，或是系爭電腦同時被家人、朋友所共同，而家人和朋友可能與犯罪行為無涉，或使用者係在不知情之情況下所用電腦，但以上之使用情況都會被此次搜索行動所囊括，與犯罪無涉之私人資訊也被截收。

再者治安法官分析聯邦刑事訴訟規則第 41 條五種授權法官得核發搜索票之情況，但無一適用於本件聲請案，聲請書請求核發搜索票之依據為第 41 條 b 項 1 款，但聲請人承認目前並無證據證明系爭電腦在德州南區。聲請人另主張自系爭電腦所取得之證據將會首先於核發搜索票之法院轄區內被檢視，因此儘管本件缺乏電腦所在地之認識，聲請人主張仍得依第 41 條核發搜索票。惟法院否定這項主張，因為如這項主張得適用，則將會導致在該轄區內核發之搜索票得搜索全世界的電腦，因為自搜索電腦取得之資料，都可以在被取回至搜索票核發地前皆可不被檢視，再本件實際上有兩種搜索標的，一是欲查出電腦之所在地，另一是搜索儲存於電腦內資料，但上述兩種搜索皆非在本法院轄內完成，所以無法依據第 41 條 b 項 1 款核發搜索票。

其次，治安法官討論在第 41 條 b 項 2 款，法院認為本案並不該當該款所規範之情事，因為該款並非適用授權搜索之標的物在核准搜索時在管轄區域外，搜索後將搜索扣得之證物取回轄區內之情況，該款應適用的情況應是相反的況狀。另其他第 41 條規定之狀況，法官亦認為不適用於本件搜索票之聲請案，因本案之調查案由並非恐怖攻擊，因此第 41 條 b 項 3 款不適用，再即便法院認同木馬程式是追踪裝置之一種類型，因為木馬程序得追踪受搜索電腦的所在地，但本件聲請人仍無法證明此種「追踪裝置」是在其轄區內安裝，是以第 41 條 b 項 4 款亦未提供核發搜索票之依據。最後，聲請書亦未說明系爭電腦是在美國屬地或在美國政府持有、或大使館、領事館之建築物內，第 41 條 b 項 5 款亦不適用。

(五)內布斯加州法院

A.案例事實

美國聯邦調查局調查一件散布兒童猥褻物集團案件，集團成員都使用「洋蔥路由器」(The Onion Router, Tor)[188]以隱藏他們在內布斯加州 Bellevue 之電子佈告欄(bulletin board)之真實身分，集團成員在該電子佈告欄散布兒童猥褻照片及討論如何性虐待兒童[189]。使用 Tor 可以以加密方式寄出訊息，無法追查 IP 位址，如此可以匿名通訊，無法查出實際之使用者[190]。

因為不知這些參與兒童猥褻圖片討論版集團成員之 IP 位址，FBI 聲請搜索票在電子佈告欄安裝網路偵查器，法院授權在 2012 年 11 月 16 日至 2012 年 12 月 2 日間得在系爭電子佈告欄上使用網路偵查器，只要任何人進入佈告欄，偵查器即會自該人的電腦寄出資料至 FBI 的電腦，使探員得因此查出該人之電腦識別身分。使用網路偵查器，FBI 可以辨識出電腦真實之 IP 位址，以及登入該電子佈告欄真正存取之時間。查出 IP 位址只是偵查第一步，取得 IP 位址後，FBI 使用行政傳票(administrative subpoenas)令提出文件、再次聲請搜索票、對嫌疑人提出控訴後逮捕嫌犯。

本件被告等經起訴後，數名被告提出異議，請求法院排除因搜索票授權植入之網路偵查器所取得之證據，檢察官針對異議則主張，本件在數不同被告之放置於不同處所之電腦安裝網路偵查器該當第四修正案之搜索。本件進行審理後，治安法官建議駁回排除證據之異議，地方法院法官亦採同一見解。

---

[188] 程式設計目的在瀏覽網頁時可以不被監看，可以匿名傳訊，避免資訊在傳輸過程中被過濾、分析。使用者先在電腦上安裝客戶端程式，客戶端程式會連上一個 Tor 目的伺服器以取得節點清單，用戶之客戶端挑選出一條網路流量路徑，透過各個 Tor 節點來連繫目的地伺服器，所有節點間之通訊都被加密，因此不易查出 IP 位址，或查出 IP 位址也找不出使用者。

[189] United States v. Pierce, Nos. 8:13CR106, 8:13CR107, & 8:13CR108, 2014 WL 5173035, (D. Neb. Oct. 14, 2014).

[190] Fed. Trade Comm’n v. Asia Pac. Telecom, Inc., 788 F. Supp. 2d 779, 786-87 (N.D. Ill. 2011) (“[T]he Tor Project functions by rerouting a user’s online activity through an international network of servers, allowing the user to reach an online destination through one of many ‘exit nodes.’ The user’s destination site then records the exit node’s IP address rather than the user’s true IP address, making it very difficult to trace the user’s true identity.”)

B.法院理由

本件所涉犯之罪名為散布兒童猥褻圖片案並非國內外之恐怖攻擊活動，因此聯邦刑事訴訟規則第 41 條 b 項 3 款之屬地限制並不適用於本件搜索票之核發。再者，本件共有十五名被告，當被告等從事散布或是存取兒童猥褻圖片時，被告等之住所地不明，且於核發搜索票以安裝網路偵查器之際，被告等之身分不明，因為無從適用第 41 條 b 項 1 款。又雖然散布兒童猥褻圖片之電子佈告欄設於內布斯加州 Bellevue 境內，在聲請搜索票之當下，無證據顯示任何被告之電腦所在地在此轄區內，因為第 41 條 b 項 2 款亦不適用。

其次，聲請搜索票之目的係為安裝網路偵查器，並非裝置追踪裝置，因此第 41 條 b 項 4 款亦不適用[191]。最後，因為電腦並未在美國屬地或是領事館建築物內，所以第 41 條 b 項 5 款亦不適用。總而言之，本件搜索票之核發是否有第 41 條 b 項各款事由，仍有極大之爭議。

四、雖植入本馬程式達搜索目的為美國現行法及實務所許，惟仍應謹慎為之

除木馬程式外，執法單位尚有其他得取得與犯罪活動相關之電子資料之方式。例如，在已知嫌疑人所使用之電子郵件帳號之情況下，執法機關得聲請安裝撥號紀錄器或監測追踪器。就取得電話門號而言，撥號紀錄器可取得撥出資訊，監測追踪器可以蒐集來電資訊[192]。若搜索之標的為電子郵件，執法單位可能因此取得任何資訊收送之信箱、瀏覽網頁之 IP 位址，以及從該電子郵件帳戶傳送之資料數量等。執行單位使用前述工作之好處在於聲請安裝之標準較寬鬆，且只要達到以下所述之標準，治安法官核票幾乎無任何裁量空間:聲請人所提出證據顯示安裝此類工具，證據很有可能會被取得，且工具之使用與現在進行中之犯罪偵查有關。而因撥號紀錄器等工具所取得之資料，有助於進一步犯罪調查，且可提

[191] United States v. Asghedom, 992 F. Supp. 2d 1167, 1174-75 (N.D. Ala. 2014).
[192] 18 U.S.C. §§ 3121-27 (2012)

供為聲請搜索票或安裝木馬程式之基礎。

再者，在調查犯罪過程中，政府可能聲請從網際網路服務提供者取得與電子郵件帳戶相關之註冊者資料[193]，依美國法典第 2703 條，執行單位得取得手機門號或網路服務註冊者之姓名、生日、住址、電子郵件服務開始日期以及註冊時使用之金融帳戶資訊[194]。雖然聲請標準不若撥號紀錄器般寬鬆，但仍低於聲請搜索所必要之「合理根據」標準[195]，而取得這些使用者註冊資料，有助於進一步之犯罪偵辦，以及提供聲請搜索票，或執行木馬程式之基礎。

因為電腦及網路之性質，上述之裝置供法完美適用於聯邦刑事訴訟規則第 41 條外，仍存有若干疑慮。例如，當執行此類工具，工具會截收電腦內所有資料，縱然該資料與調查中之犯罪無關，更甚者，取得之資訊可能會涉及無辜第三人，因此核發時，不只應考慮與犯罪無關之資料應受保護，不應被截收，且這些資訊亦不能由執行單位保存。

國會為於 2006 年通過聯邦刑事訴訟規則第 41 條修正案，明確授權治安法官核發追踪裝置之搜索票，此係在是在電子通訊隱私權保護法案制定後 20 年，方立法授權使用追踪裝置。在美國，聯邦法院程序規則司法會議有權得提案修正關於搜索票是否應准許安裝木馬程式[196]，且最近司法部亦提案修正第 41 條，希望明定在刑事偵查中，法院授權准許木馬程式之安裝[197]，提案增修新的事由得搜索

---

[193] 18 U.S.C. § 2703.

[194] In re § 2703(d) Order; 10GJ3793, 787 F. Supp. 2d 430, 436 (E.D. Va. 2011); In re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d), 157 F. Supp. 2d 286, 288 (S.D.N.Y. 2001).

[195] 18 U.S.C. § 2703(d) 另參見 In re Application of the United States for an Order Directing a Provider of Elec. Commc' n Serv. to Disclose Records to the Gov' t, 620 F.3d 304, 315 (3d Cir. 2010)

[196] Laws and Procedures Governing the Work of the Rules Committees, UNITED STATES COURTS, http://www.uscourts.gov/RulesAndPolicies/rules/about-rulemaking/laws-procedures-governingwork-rules.aspx 最後造訪日 2015 年 11 月 20 日。

[197] Ellen Nakashima, FBI Wants Easier Process to Hack Suspects' Computers, WASH. POST (May 9, 2014), http://www.washingtonpost.com/world/national-security/fbi-wants-easier-processto-hack-suspects-computers/2014/05/09/f30c37b0-d78d-11e3-8a78-8fe50322a72c_story.html 最後造訪日 2015 年 11 月 20 日；Committee on Rules of Practice and Procedure, Meeting Minutes http://cryptome.org/2014/03/doj-hacker-attack.pdf 最後造訪日 2015 年 11 月 20 日

電子儲存資料[198]:

(b) 授權核發搜索票。聯邦執法單位官員或檢察官之請求:

(6)有以下情況，任何與犯罪活動有關地區之治安法官有權核發搜索票，以安裝遠端存取裝置而在轄區內或轄區外搜索電子儲存媒體以及扣押或複製電子儲存資訊:

(A) 媒體或資料所在地，業經由科技方式隱藏；或

(B)在案由為 18 U.S.C. § 1030(a)(5)[199]罪之調查程序中，媒體是未經授權已經損壞之受保護電腦以及該電腦所在地超過五處者。

若上開見解日後為最高法院採用，修正之提案極有可能會通過，因為國會不太可能拒絕適用最高法院之見解。

惟今日實務上所面臨之問題，在於執法單位使用木馬程式之範圍，已遠超過國會在 1986 年制定電子通訊隱私權保護法時之預期及理解，甚至超越 2001 年愛國者法案制定時之範圍[200]，Susan Freiwald 教授主張除非最高法院強力提議，國會一如既往不會修正關於電子監聽和隱私權之問題[201]，因為限於法律架構以及黨派間互不相讓，縱使法院強力推動下，國會亦不可能有辦法解決這些問題。

木馬程式之安裝，除了執行單位應提出符合第四修正案之合理依據之標準，

---

198 (b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:
(6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside the district if:
(A) the district where the media or information is located has been concealed through technological means; or
(B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

199 (A)knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
(B)intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
(C)intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

200 Orin S. Kerr, The Mosaic Theory of the Fourth Amendment, 111 MICH. L. REV. 311, 344 (2012)

201 Susan Freiwald, Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact, 70 MD. L. REV. 681, 687 (2011)

和符合聯邦刑事訴訟規則第 41 條之要件外，執法單位仍應提出自搜索電腦中取得之第三人資料或與犯罪無涉之私人文件之處理辦法。因此法院開始思索，應該在核發植入木馬程式之搜索票時，訂定執行規則[202]，例如:在使用基地台轉儲技術(cell tower dump)搜索，法院命執行單位繳回所有原始紀錄和備份紀錄，不論該備分紀錄是否為電子檔[203]。另有法院在搜索之標的為嫌疑人之臉書帳戶時，要求執行單位進行防護機制，避免執行單位蒐集或是存取無權取得之資訊[204]，哥倫比亞特區聯邦法院治安法官 John Facciola 特別要求執法單位在執行搜索票時，必須遵守保護在搜索票核准範圍外之私人資料[205]。

即便木馬程式之授權安裝符合憲法第四修正案及第 41 條之要求，執法單位就因此所取得之資訊，仍應恪遵以下標準:第一、執行單位禁止保留任何與犯罪調查無關之第三人資料，此種資料之所有備份均應被銷毀，任何電子紀錄應被刪除，惟犯罪偵查單位提出第三人係共犯時，則不在此限，政府得保留取得之第三人資料及文件。第二，執法單位必須有能力區別與嫌疑人電腦中與所調查之犯罪相關之資訊以及與犯罪無關之文件，例如與犯罪活動無關之私人照片以及財務資訊，當電子紀錄被刪除時，任何不相關之文件之備份均應銷毀。

第六項　對具加密功能之通訊軟體之通訊監察於現行法規範下之可行性

以後門程式方法監聽加密通訊軟體固然可行，惟此舉端賴軟體商之配合，願意在通訊軟體開啟後門程式，就美國而言，甚至以國家安全為由要求蘋果公司、

---

[202] In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d), 964 F. Supp. 2d 674, 678 (S.D. Tex. 2013)

[203] In re Cellular Telephone Towers, 945 F. Supp. 2d 769, 771 (S.D. Tex. 2013)

[204] In re Information Associated with the Facebook Account Identified by the Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc., 21 F. Supp. 3d 1, 9 (D.D.C. 2013)

[205] In re Apple iPhone, IMEI 013888003738427, 31 F. Supp. 3d 159, (D.D.C. 2014) (聲請搜索手機案件); In re ODYS LOOX Plus Tablet, Serial Number 4707213703415, in Custody of United States Postal Inspection Serv., 28 F. Supp. 3d 40, 46 (D.D.C. 2014) (聲請搜索電腦案件)

谷歌公司配合，仍引起軒然大波。

我國對於通訊監察之方式，並無太多限制，此可就通訊保障及監察法第 13 條第 1 項本文:「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」可見一斑，是以，植入木馬程式使其複製受監察人使用通訊軟體之通訊再回傳建置機關，似符合「截收」之方式，惟使用木馬程式之功能凡幾，有些甚可開啟麥克風及通話功能，如此即有違通訊保障及監察法第 13 條第 1 項但書:「但不得於私人住宅裝置竊聽器、錄影設備或其他監察器材。」以手機充作竊聽器。

或有謂網路監察記載「受監察處所」有其困難[206]，惟在實務上，受監察處所欄位均填載「電話裝機處」，即可表示受監察之客體為何，因此，如以植入木馬程式作為通訊軟體之監察方式，僅需填載通訊軟體裝設處即可。

使用木馬程式做為犯罪調查工具，有其優缺點，優點是，以往可以逍遙法外之罪犯，得以因新科技而被逮捕，且可以達到其他監聽工具無法達成之目的。然而，使用木馬程式較有爭議處在於，木馬程式常會截取將整個電腦或手機之資料，而取得與本案無關之內容，因此在使用木馬程式上應特別注意，受監察客體之特定。

[206] 蘇三榮著，網路時代通訊監察與個人資料保護之法制研究，國立交通大學科技法律研究所碩士論文，頁 50.

第四章　結論

隨著資訊科技進步，為查緝犯罪所需，在技術上得採取之偵辦手段經緯萬端，像本文提及植入木馬程式、後門程式即為一例。惟當執法機關以駭客手法取得犯罪證據，固然在技術上不成問題，惟在現行法之框架下，仍需進一步思考，以下係就我國通訊監察之困境而提出之可能改變方向:

一、放寬網路通訊監察限制

因使用網路從事犯罪行為，緝捕時機稍縱即逝，且現今通訊容易不只文字，尚有圖片、語音、影像等，通訊內容因容量龐大而保存不易，如通訊監察時，固守監察通訊種類及號碼等足資識之特徵，恐失制敵機先之時效，是在網路通訊監察或是通訊軟體監察時，不妨引進美國「機動式監察(roving wiretap)」方式，在限定之重罪，不特定通訊監察之地點、方式，僅針對所觸犯之罪名進行監聽，在犯罪嫌疑人頻頻更換通訊方式，或通訊種類時，方能收監聽之效。

二、建置網路通訊監察之標準機制

目前網路通訊之監聽仍以個案行之,不似手機或室內電話通聯建置統一掛線監聽中心，為避免事後無法監督，以及難解民眾對於過度網路監聽之疑慮，宜建立與現行電話通訊監察作業一般之流程與機置，包括取得監聽票後之投單、上線、現譯及監聽所取得之資料之保存與監聽後之通知、稽核作業。

對檢察官而言，科技搜證設備是水能載舟，亦能覆舟，雖然科技能蒐集數位證據，而數位證據在現今所有犯罪類型，扮演極重點之角色，但身為檢察官應該對於科技蒐證設備之挑戰有警覺性，過去不曾被質疑監聽工具現在飽受爭議，以往一些法律要件被視為常規而理所當然被忽視的，而今卻屢屢有爭執空間，就新型態之數位證據蒐集工具方面，檢察官應對於法官的懷疑，以及辯護人的異議有所準備，而美國科技設備進行監聽的實例，不失為我國之借鏡。

參考文獻

一、參考書籍

- Stephen A. Saltzburg Daniel J. Capra, American Criminal Procedure: Adjudicative,West Academic Publishing
- Russell L. Weaver, Leslie W. Abramson, John M. Burkoff, Catherine Hancock, Principles of criminal procedure, St. Paul, MN : West, c2012.
- Wayne Lafave, CriminalProcedure, 5th,HornbookSeries, Student Edition, 2014 Pocket Part, West Academic
- Lafave, Wayne;Israel, Jerold;King, Nancy, LaFave, Israel, King and Kerr'sCriminalProcedure, 5th (HornbookSeries), West Academic
- James J. Tomkovicz, Welsh S. White, Criminal Procedure: Constitutional Constraints upon Investigation And Proof
- William Burnham, Introduction To The Law And Legal System of The united States.
- Todd G. Shipley, Art Bowker,Investigating Internet Crimes-An Introduction to Solving Crimes in Cyberspace,
- 王兆鵬，令狀原則，刑事訴訟法講義（一）

二、期刊文獻

- 陳運財著，偵查之基本原則與任意偵查之界限，私立東海大學法學研究第 9 期
- 陳運財著，監聽之性質及其法律規範－兼評通訊監察法草案之爭議，東海法學研究第 13 期
- 張銘晃著，論違法監聽資料之證據價值，法學論叢，93 年 7 月
- 江舜明著，監聽在刑事程序法上之理論與實務，法學論叢第 168 期
- 蔡美智著，「通訊保障及監察法」關於網路監聽之相關爭議，資訊法務透析，民國 88 年 12 月
- 黃茂穗著，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
- 謝碩駿著，警察機關的駭客任務-論線上搜索在警察法領域內實施的法律問題，臺北大學法學論叢第 93 期
- 莊佳瑋譯，含基地台位址之通聯紀錄是否屬合理期待之隱私，檢察新論第 16 期
- 蔡美智著，「通訊保障及監察法」關於網路監聽之相關爭議，資訊法務透析，民國 88 年 12 月
- Gus Hosein & Caroline Wilson Palow, Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques, 74 OHIO ST. L.J. 1071, 1089-90 (2013)

- Kevin Poulsen, FBI’ s Secret Spyware Tracks Down Teen Who Made Bomb Threats
- Brian L. Owsley, To Unseal or Not to Unseal: The Judiciary’ s Role in Preventing Transparency in Electronic Surveillance Applications and Orders, 5 CALIF. L. REV. CIRCUIT 259 (2014)
- Paul Ohm, Good Enough Privacy, 2008 U. CHI. LEGAL F. 1
- Gus Hosein & Caroline Wilson Palow, Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques, 74 OHIO ST. L.J. 1071, 1089-90 (2013)
- Orin S. Kerr, The Mosaic Theory of the Fourth Amendment, 111 MICH. L. REV. 311, 344 (2012)
- usan Freiwald, Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact, 70 MD. L. REV. 681, 687 (2011)

三、學位論文

- 陳誌泓著，電腦、網路與刑事偵查——以網路犯罪公約於日本法的落實為中心，國立臺灣大學法律學研究所碩士論文
- 陳信郎著，資訊隱私權保障與網路犯罪通訊監察法制，國立政治大學法律學研究所碩士論文
- 許慈健著，網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究，國立交通大學管理學院碩士在職專班科技法律組碩士論文
- 蘇三榮著，網路時代通訊監察與個人資料保護之法制研究，國立交通大學技法律研究所碩士論文

四、實務案例

- Olmstead V. United State 277U.S.438(1928)
- Katz v.United States, 389 U.S. 347 (1967)
- United States v. Van Leeuvwen 397 U.S. 249, 251, 90 S.Ct. 1029, 25 L.Ed.2d 282(1970).
- United States v. Jacobsen 466 U.S. 109, 114, 104 S.Ct. 1652, 80 L.Ed2d 65(1984).
- Ex Parte Jackson 96 U.S. 727,24 L.Ed. 877(1987).
- United States v. Van Leeuwen 397 U.S. 249, 90 S.Ct. 1029, 25 L.Ed.2d 282(1970)
- United States v. Jacobsen, 446 U.S. 109, 104 S. Ct. 1652, 80 L.Ed.2d 85(1984)
- Berger v. New York 388 U.S. 41, 87 S.Ct. 1873, 18 L.Ed.2d. 1040(1967).
- Smith v. Maryland 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220(1979)
- Quon v. Arch Wireless Operating Co. 29 F.3d. 892(9th Cir. 2008).
- United States v. Forrester 495 F.3d 1041 (9th Cir. 2007).
- Nardone v. United States 302 U.S.379,384,58 S.Ct. 275, 82 L.Ed. 314(1937).

- Goldman v. United States, 316 U.S. 129. 133-134, 62 S.Ct. 993,86 L.Ed. 1322(1942)
- United States v. Scarfo 180 F. Supp.2d 572 (D.N.J. 2001).
- United States v. Baranek, 903 F.2d.1068, 1072(6th Cir. 1990)
- Pharmartrak, Inc.329 F 3d. 9, 18(1st Cir. 2003)
- United States v. Bynum, 763 F.2d 474(1st Cir. 1985)
- United States v. Nnfro, 64 F.3d 98 (2nd Cir.1995)
- United States v. Giordano, 416 U.S. 505, 94 S.Ct. 1820, 40 L.Ed.2d 341(1974).
- United States v. Kahn, 415 U.S. 143, 94 S.Ct. 977, 39 L.Ed.2d. 255(1974)
- United States v. Turner, 528 F.2d 143 (9th Cir. 1975).
- United States v. Ojeda Rios, 495 U.S. 257, 110 S.Ct. 1845, 109 L.Ed,2d 224(1990)
- United States v. New York Telephone 434 U.S. 159, 98 S.Ct. 364, 54 L.Ed.2d. 376(1977)
- Terry v. Ohio, 392 U.S. 1, 21, 88 S.Ct. 1868, 20 L.Ed.2d. 889(1968)
- United States v. Ojeda Rios, 495 U.S. 257, 110 S.Ct. 1845, 109 L.Ed,2d 224(1990)
- United States v. Steiger, 318 F.3d 1039,(11th Cir. 2003)
- Scott v. United States, 436 U.S. 128, 139, 98 S. Ct. 1717 56 L.Ed.2d 168(1978)
- United States v. Murdock 63 F.3d 1391,1404(6th Cir. 1995)
- United States v. Giordano, 416 U.S. 505, 527, 94 S.Ct. 1820,40 L.Ed.2d 341(1974)
- United States v. Chavez, 416 U.S. 562, 578, 94 S.Ct. 1849,40 l.Ed.2d. 380(1974)
- United States v. Donovan 429 U.S. 413,97 S.Ct. 658,50 L.Ed.2d 652 (1977).
- United States v. Rigmaiden, 844 F. Supp. 2d 982, 996 (D. Ariz. 2012)
- United States v. Chipps, 410 F.3d 438, 446 (8th Cir. 2005)
- United States v. Kernell, No. 3:08-CR-142, 2010 WL 1408437
- United States v. Hernandez, No. 3:08-CR-142, 2008 WL 4748576
- United States v. McVicker, No. 3:11-CR-00101-SI, 2012 WL 860412 (D. Or. Mar. 13, 2012)
- United States v. Glover, 736 F.3d 510
- United States v. Vann, No. 07-CR-247(JMR/RLE), 2007 WL 4321969, 22 (D. Minn. Dec. 6, 2007)
- United States v. Jones, 132 S. Ct. 945, 948 U.S. 2012
- United States v. Krueger, 998 F. Supp. 2d 1032, 1033-34 (D. Kan. 2014)
- United States v. Vilar, No. S305CR621KMK, 2007 WL 1075041, (S.D.N.Y. Apr. 4, 2007)
- United States v. Garey, 546 F.3d 1359, 1361 (11th Cir. 2008)
- United States v. Chipps, 410 F.3d 438, 446 (8th Cir. 2005)
- United States v. Kernell, No. 3:08-CR-142, 2010 WL 1408437, (E.D. Tenn. Apr. 2, 2010)
- United States v. Asghedom, 992 F. Supp. 2d 1167, 1174-75 (N.D. Ala. 2014)

●United States v. Cuevas-Sanchez, 821 F.2d 248, 250 (5th Cir. 1987)
●United States v. Pierce, Nos. 8:13CR106, 8:13CR107, & 8:13CR108, 2014 WL 5173035, (D. Neb. Oct. 14, 2014)
●Fed. Trade Comm’ n v. Asia Pac. Telecom, Inc., 788 F. Supp. 2d 779, 786-87 (N.D. Ill. 2011)
●United States v. Asghedom, 992 F. Supp. 2d 1167, 1174-75 (N.D. Ala. 2014).

五、網路資料

●Apple, in refusing backdoor access to data, may face fines，
http://www.zdnet.com/article/apple-in-refusing-backdoor-access-to-data-faces-huge-fines/
●教育部全民資安素養網資安小字典，
https://isafe.moe.edu.tw/dictionary_detail.php?sn=11
●司法部電子監聽手冊
http://www.justice.gov/sites/default/files/criminal/legacy/2014/10/29/elec-sur-manual.pdf
●PKI Electronic Intelligence, GSM Cellular Monitoring System (product brochure) ,
http://docstoc.com/docs/99662489/GSM-CELLULAR-MONITORING-SYSTEM
●Florida v. Thomas, No. 2008-CF-3350A (Fla., Leon Co. Cir. Ct., Aug. 23, 2010), https://www.aclu.org/files/assets/100823_transcription_of_suppression_hearing_complete_0.pdf
●Jon Campbell, LAPD Spied on 21 Using StingRay Anti-Terrorism Tool, LA WEEKLY, Jan. 24, 2013,
http://www.laweekly.com/news/lapd-spied-on-21-using-stingray-anti-terrorism-tool-2612739
●Linda Lye, In Court: Uncovering Stingrays, A Troubling New Location Tracking Device, ACLU (Oct. 22, 2012, 12:42 p.m.),
https://www.aclu.org/blog/free-future/court-uncovering-stingrays-troubling-new-location-tracking-device?redirect_blog/national-security-technology-and-liberty/court-uncovering-stingrays-troubling-new-location
●Glenn Greenwald, NSA Collecting Phone Records of Millions of Verizon Customers Daily, GUARDIAN (London), Jun. 6, 2013,
http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order
●Glenn Greenwald & Ewen MacAskill, NSA Prism Program Taps in to User Data of Apple, Google and Others, GUARDIAN (London), Jun. 7, 2013,
http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

- Ellen Nakashima, FBI Clarifies Rules on Secretive Cellphone-Tracking Devices, WASH. POST, May 14, 2015, https://www.washingtonpost.com/world/national-security/fbi-clarifies-rules-on-secretive-cellphone-tracking-devices/2015/05/14/655b4696-f914-11e4-a13c-193b1241d51a_story.html
- Tom Jackman, Experts Say Law Enforcement' s Use of Cellphone Records Can Be Inaccurate, WASH. POST, Jun. 27, 2014, http://www.washingtonpost.com/local/experts-say-law-enforcements-use-of-cellphone-records-can-be-inaccurate/2014/06/27/028be93c-faf3-11e3-932c-0a55b81f48ce_story.html
- Matt Richtel, A Police Gadget Tracks Phones? Shhh! It' s Secret, N.Y. TIMES, Mar. 15, 2015, http://www.nytimes.com/2015/03/16/business/a-police-gadget-tracks-phones-shhh-its-secret.html
- Devlin Barrett, CIA Aided Program to Spy on U.S. Cellphones, WALL ST. J., Mar. 10, 2015, http://www.wsj.com/articles/cia-gave-justice-department-secret-phone-scanning-technology-1426009924
- Devlin Barrett, Americans' Cellphones Targeted in Secret U.S. Spy Program, WALL ST. J., Nov. 13, 2014, http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533
- Andrew Cunningham, New Guidelines Outline, ARS TECHNICA (May 8, 2014), http://arstechnica.com/apple/2014/05/08/new-guidelines-outline-what-iphone-data-apple-can-give-to-police/
- Trevor Timm, Your iPhone is Now Encrypted, THE GUARDIAN, Sep. 30, 2014, http://www.theguardian.com/commentisfree/2014/sep/30/iphone-6-encrypted-phone-data-default
- Privacy--Government Information Requests, APPLE, http://www.apple.com/privacy/government-information-requests
- New Security Features in Android 5.0, ANDROID OFFICIAL BLOG http://officialandroid.blogspot.co.uk/2014/10/a-sweet-lollipop-with-kevlar-wrapping.html
- Julian Hattem, DOJ Fears Tech "Zone of Lawlessness," THE HILL http://thehill.com/policy/technology/230840-doj-fears-tech-zone-of-lawlessles
- Brian Naylor, Apple Says iOS Encryption Protects Privacy, NPR http://www.npr.org/sections/alltechconsidered/2014/10/08/354598527/apple-says-ios-encryption-protects-privacy-fbi-raises-crime-fears

●Ellen Nakashima, Tech Giants Don’ t Want Obama to Give Police Access, WASH. POST, http://www.washingtonpost.com/world/national-security/tech-giants-urge-obama-to-resist-backdoors-into-encrypted-communications/2015/05/18/11781b4a-fd69-11e4-833c-a2de05b6b2a4_story.html
●Devlin Barrett & DannyYadron，Apple and Others Encrypt Phones, Fueling Government Standoff, WALL ST. J., Nov. 18, 2014, http:// www.wsj.com/articles/apple-and-others-encrypt-phones-fueling-government-standoff-1416367801
●美國總統歐巴馬與英國首相卡麥隆聯合記者會談會 https://www.whitehouse.gov/the-press-office/2015/01/16/remarks-president-obama-and-prime-minister-cameron-united-kingdom-joint-
●Danny Yadron, Google’ s Schmidt Fires Back Over Encryption, WALL ST. J., Oct. 8, 2014, http://www.wsj.com/articles/googles-schmidt-says-encrypted-phones-wont-thwart-police-1412812180
●Electronic Frontier Foundation， https://www.eff.org/files/filenode/cipav/FBI_CIPAV-10.pdf
●Declan McCullagh, FBI Remotely Installs Spyware to Trace Bomb Threat, CNET (July 18, 2007, 9:42 AM), http://www.cnet.com/news/fbi-remotely-installs-spyware-to-trace-bomb-threat/
●Lacey 10th-grader Arrested in Threats to Bomb School, SEATTLE TIMES, http://www.seattletimes.com/seattle-news/lacey-10th-grader-arrested-in-threats-to-bomb-school/
●Jack Healy, Mental Evaluations Endorse Insanity Plea in Colorado Shootings, Defense Says, N.Y. TIMES (May 13, 2013), http://www.nytimes.com/2013/05/14/us/james-holmes-aurora-shooting-suspect-enters-insanity-plea.html
●Will C. Holden, Denver International Airport Confirms Non-specific Bomb Threat, FOX 31 DENVER (July 31, 2012, 2:11 PM), http://kdvr.com/2012/07/31/denver-international-airport-confirms-non-specific-bomb-threat/
●FBI, Jacksonville Division, Former Gainesville Resident Sentenced for Bank Fraud and Identity Theft (July 18, 2013), https://www.fbi.gov/jacksonville/press-releases/2013/former-gainesville-resident-sentenced-for-bank-fraud-and-identity-theft
●Laws and Procedures Governing the Work of the Rules Committees, UNITED STATES COURTS,

http://www.uscourts.gov/RulesAndPolicies/rules/about-rulemaking/laws-procedures-governingwork-rules.aspx

- Ellen Nakashima, FBI Wants Easier Process to Hack Suspects' Computers, WASH. POST (May 9, 2014), http://www.washingtonpost.com/world/national-security/fbi-wants-easier-processto-hack-suspects-computers/2014/05/09/f30c37b0-d78d-11e3-8a78-8fe50322a72c_story.html
- Committee on Rules of Practice and Procedure, Meeting Minutes http://cryptome.org/2014/03/doj-hacker-attack.pdf