國立政治大學法律科際整合研究所

碩士論文

指導教授：何賴傑　博士

刑事偵查中數位資訊之保全

研究生：高堅仁　撰

中華民國一〇一年七月

謝　辭

論文的完成代表在校園的學習生活即將告一個段落，帶著豐富的收穫向下一個階段邁進。

論文能夠順利的完成，首先要感謝何賴傑教授耐心的指導，從論文方向的選定以及內容的調整，經歷過許多次的討論，老師總是在尊重學生想要傳達的想法這個大原則之下，提供最好的建議。楊雲驊教授與李榮耕教授在口試過程中，對於內容中若干不成熟的見解提出建議，讓本論文有機會更臻於完善。

跨領域學習有機會能與不同專長的人交流，大家共同在法律學習這個平台上，相互提攜一起成長。也爲自己固有的專長領域打開另一扇窗，增廣了許多的見聞。

要感謝的人很多，在校園一隅偶遇的短暫交談，都有可能帶來新的啓發，若要一一列名可能會有掛一漏萬之虞。在有昭龍學長參與的課堂上，總是能激盪出討論的火花，讓在場成員帶著滿滿的收穫離開課堂，令人吮指回味。圖書館蔡斐雯小姐在資料蒐集方面以及陳相如小姐在圖書館資源使用方面所提供的協助，讓圖書館的功能在整個論文撰寫的過程中發揮了最大的效益。

家人的支持是走在自己所選擇的道路上最堅實的後盾，也因爲有家人的信任與期許，才能有足夠的動力在既定的目標上繼續前進。

摘要

資訊科技的發達爲人類的生活帶來了便利，同時也嘉惠犯罪實施的便利性，許多與犯罪相關的證據已經普遍以數位化的形式存在，在刑事偵查中對於這類數位資訊之保全成效，將直接影響到後續的刑事訴訟程序是否能順利地進行。因此有必要對於相關的法規範加以檢視，以期在顧及偵查效率的同時，亦能縮減對人民基本權利之侵害。

本文第二章介紹進入資訊數位時代之後，刑事偵查程序因數位資訊之保全所帶來的改變。第三章美國偵查實務討論美國法制對於數位資訊之保全在刑事偵查中的相關程序規定。第四章我國偵查實務探討我國法制對於數位資訊保全的相關規定，以及是否有可以借鏡外國法制優點改進之處。

關鍵字

憲法第四增修條文、犯罪偵查、通訊監察、電磁紀錄、搜索、扣押

國立政治大學
National Chengchi University

目次

國立政治大學
National Chengchi University

第一章 緒論

第一節 研究動機

隨著網路科技的進步，越來越多的商業行爲是架構在網路的平台上而進行的，網路上所傳遞的信號由工程的角度來看是一連串的 0 與 1 的電位信號，由商業的角度來看其蘊含著資訊流與金流，而由法律的角度來看當其儲存在載具[1]上成爲電磁紀錄時，也就成爲現今法律保護的客體。隨著資訊科技的進步，促成硬體運算速度與軟體功能性的大幅提升，已經徹底地改變人們的生活，相較於早期電腦的功能還相當受到侷限時，電腦給人的一般印象，是學生在學校必修的一門課，是架設在特定管制區域內一般人不得任意接近，僅供專業的科學家執行大量運算的重要工具，然而現今的電腦已經呈現一種不同於以往的面貌，除了桌上型電腦與筆記型電腦等大家所熟悉的樣貌外，手機、電子醫療儀器與公車定位系統都可以稱得上是廣義的電腦，經由網路將各個電腦連接起來讓信號可以在其間傳遞，也就構成了手機的通訊網路，醫院的診療、病歷網路，以及公車動態資訊系統。在科學技術發展的過程中，再精密的系統設計仍免不了因思慮不週而有漏洞的存在，這樣的漏洞若是讓存有善意的人先發現，則有助於協助系統開發者將漏洞修補，讓整個系統更加的穩定，但是在大多數的情形下都是存有惡意的人早先於善意的人發現了這樣的漏洞，而對於這樣的漏洞加以利用，通常能獲得財產上的利益，因而誘發犯罪行爲的實施。惡意程式的發展原本只是電腦玩家在發現了系統上的漏洞之後，著手開發撰寫程式，想要炫耀自己有操弄這個漏洞的能力，但是對有犯罪意圖的人，就會對這個漏洞加以利用，想要藉機獲取財產上的利益。以蠕蟲程式爲例，當系統上的漏洞被有心人士發現之後，針對這個弱點開發出蠕蟲程式，恰如其名，蠕蟲會自動的爬行，不斷的經由網路向外擴散，找尋有系統上漏洞的電腦加以感染、控制，而受感染的電腦其內部所存放的資料，也將落入蠕蟲散播者的掌控之中。受到這樣的啓發，有犯罪意圖的人加以改良其架構，增加縱深以躲避追查，例如，攻擊發動者(bot master/herder)，透過下一層的命令與控制中心(command and control，簡稱 C&C)，指揮再下一層的殭屍電腦[2](簡稱 bots)，由殭屍電腦去執行攻擊任務，這就形成所謂的殭屍網路(簡稱 botnet)。

[1] 何賴傑，錄音、錄影、電磁紀錄等之調查(刑事訴訟法第一六五條之一第二項)，全國律師，8 卷 9 期，2004 年 9 月，頁 34。

[2] 依據賽門鐵克 2009 年的全球網路安全威脅研究報告指出，台北市已成爲全球最多殭屍電腦的城市。由於台北 IT 基礎建設普及，以及國人電腦網路使用的安全防護習慣問題，使台北市成爲全球最多殭屍電腦

命令與控制中心會有數個，用來承接攻擊發動者的命令，以及避免因單點故障導致整個網路無法運行，每個命令與控制中心指揮受其管轄的許多殭屍電腦以執行攻擊任務，事實上命令與控制中心與殭屍電腦也都是受害者，該些電腦的擁有者並不知道其電腦已經被操控且用於犯罪行爲的實施。掌握了殭屍網路就等於是擁有了一支存在於虛擬空間(cyberspace)的兵團。可以自己發動攻擊以獲取財產上的利益、竊取存放在電腦上的敏感資訊、散佈垃圾郵件、點擊詐欺或是出租殭屍電腦供他人犯罪之用。由於透過網路所進行的攻擊具有跨境與匿蹤的特性，在犯罪的訴追上帶來相當程度的挑戰，以分散式阻斷服務攻擊爲例，在短暫的時間之內對所欲攻擊的網頁發出大量的瀏覽網頁的請求，使其超出該網頁主機所能負荷的程度，因而癱瘓該網頁主機，與該網頁有關的商業活動將被迫終止，所造成營業上損失的範圍，將視主機癱瘓的時間長短而定。待攻擊流量退去，受攻擊主機再度恢復正常時，從系統的記錄檔所能掌握的，只是在整個攻擊結構中最底層的殭屍電腦所在的網際網路位址(Internet Protocol，簡稱 IP)，而真正的攻擊行爲發動者卻仍逍遙法外。殭屍網路有一個特性就是，當電腦被感染成殭屍電腦之後，第一個動作就是與上一層的命令與控制中心聯絡/報到，這就是所謂的「打電話回家」(phone home)，命令與控制中心接受殭屍電腦的報到之後，會將其納入管轄，攻擊發動者也是下達攻擊指令給命令與控制中心，命其操控殭屍電腦執行攻擊任務。殭屍網路雖然是三階層的結構，但是從另一個角度來觀察，卻是以命令與控制中心爲樞紐的網路，所有的指令都需透過命令與控制中心來傳遞。發現殭屍電腦後，可以進一步追查命令與控制中心，掌握命令與控制中心之後，藉由搜索儲存在命令與控制中心電腦內的記錄檔，或是監聽命令與控制中心與攻擊發動者之間溝通的網路封包，就有機會可以找出下達指令的攻擊發動者的網路位址，透過網路服務提供者(Internet service provider，簡稱 ISP)查詢該網路位址的註冊資訊，就可以進一步找出行爲人的真實地址。

網路的發明，爲人們的生活帶來了便利，伴隨著也改變了人們的生活習慣，購買商品以往必須親臨展場選購，藉由網路可以在網頁上瀏覽商品，在網路上下訂單之後，經由宅配到府可以達到足不出戶還是能買到所想要的商品，金融轉帳以往必須親臨金融機構辦理，或是操作設置在特定地點的自動櫃員機，使用網路銀行可以不用出門而完成金融轉帳，這樣的便利帶來了許多時間與交通成本的節省，也將衍生相關的問題。行爲人與行爲結果發生地不再相伴而生，網路的特性之一，就是網路信號能輕易地穿越地理疆界的限制，而抵達位在網際網路另一端的電腦。電腦科技的進步，除了加快電腦運算的速度，也使得儲存媒體容量的增大成爲可行，資料經過數位化之後，交互混雜儲存在儲

的城市。參照 iThome online<http://www.ithome.com.tw/itadm/article.php?c=60894>(最後瀏覽 2012 年 6 月 22 日)。

存媒體之中，儲存的特性之一，就是資料混雜。現行的法律都是爲了規範—相對於網路所代表的虛擬世界—真實世界的行爲所設計，現行用於偵查犯罪的相關法律規定是否依然適用在虛擬世界，有加以檢視的必要。當行爲人透過網路實施犯罪行爲並產生犯罪結果時，想要藉由找尋目擊者、犯罪工具與指紋等傳統犯罪足跡，以指認行爲人將不再可行，取而代之的是，行爲人在網路連線的過程中，承載行爲人連線指令的網路信號，以行爲人所在地的電腦爲出發點，朝向目標電腦前進的過程中，所形成之網路連線路徑，該路徑是由許多的路由器或網路伺服器串接而成，伺服器上之記錄檔(log)將記載有關行爲人連線指令的到訪細節，此即新型態數位足跡。監聽與搜索扣押是掌握犯罪證據的重要方法，不論是在真實世界與虛擬世界均一體適用。監聽是對現在正在進行或未來即將發生的通訊內容的蒐集行爲，因爲對通訊雙方的隱私權有極大的侵害，因此監聽行爲的核准有著極高的門檻，網路通訊基於承載信號網路的特質，必須將通訊的內容切割成單位長度的封包(packet)分批傳送，等到達目的端之後再依序組合成完整的通訊內容，因爲是封包交換(packet switch)網路，線路不再專屬於通訊的雙方使用，線路中會傳送著來自不同的來源端以及前往不同目的端的封包，資料混雜是監聽網路通訊經常面臨的問題，在越接近目標端裝置監聽設備比較容易只單純截收到通訊雙方的內容，越遠離目標端的監聽截收行爲越容易截取到不相干第三人的通訊內容。由於網路犯罪經常有反覆實施的可能，因此以監聽的方式偵查網路犯罪有其實益。證據是證明犯罪行爲的重要依據，除了行爲人自願提出之外，在大部分的情況都需要國家以強制處分的方式取得，爲了保障人民的基本權避免國家力量的恣意干擾，對搜索的發動設有嚴格的要件，必須符合要件才能提出聲請，並經中立的法官加以審核以及核發令狀才得以執行，並應於令狀中詳細記載所欲搜索的地點，以及所欲尋得的標的，令狀的特定是爲了將搜索對人民的侵害限制在最小的範圍，以避免浮濫的概括搜索(general search)。因此，在搜索有體物時，有了以容器理論來判斷搜索行爲是否逾越了令狀的範圍，例如，搜尋槍枝就不能開拆信封，搜尋犯罪嫌疑人就不能打開書桌的抽屜，因爲依據容器理論，所欲搜尋的標的是不可能存在於該等容器空間之中。在網路犯罪的偵查中，爲了掌握儲存在儲存裝置中的數位證據必須對其加以搜索，但是資料儲存的方式卻是以混雜的方式儲存在該裝置中，因此，所欲搜索的容器該如何特定，搜索的方式該如何進行，才不至於超出令狀所劃定的範圍，在搜索儲存裝置內的數位資料時，將有別於搜索一般的有體物。

美國憲法第四增修條文是規範以國家力量對人民搜索的最上位的概念，只要符合要件即構成憲法上所定義的搜索行爲，要件的演進從早期的物理入侵到後來的合理隱私期待，可以看出隨著時代的進步，對人民基本權的保護也亦趨周延，隨著科技的發展與進

步，許多增進感官功能的偵查設備也相繼問世，對於偵查效率的提升有著顯著的幫助，但也進一步侵蝕對人民基本權的保障。當人民不覺得權利被侵害時，是否便不需要加以保障？許多基本權保障亦是相同道理，隨著科學技術的進步以及偵查技巧的改進，致使人民於當下並未及時的感受到有權利遭受到干預，但該等自由權利之保障卻具實質必要性，特別是表面上看起來不痛不癢之權利干預，往往造成人民無法想像之後遺症，故憲法保障「社會一般人觀念理解」上覺得無礙的權利，事實上是極爲重要的，進而避免無可挽救的局面發生，此係憲法所承載之使命，亦爲本文研究網路犯罪相關偵查作爲之動機所在。隨著人民對權利意識的覺醒以及要求加以保障的呼聲日漸高漲，執法人員於辦案程序上受到正當法律程序的檢驗亦日趨嚴格，爲因應這個趨勢刑事訴訟法亦同步修正，以保障被告或犯罪嫌疑人在訴訟程序上的權利，以抗制國家機器的權力過度擴張，有關此類因科學技術的進步所衍生的新型態偵查技術，亦應植基於正當法律程序之思考上進行研究與檢討。

當國家公權力相當程度干預人民基本權的情形下，基於法治國家原則，國家公權力之發動依據與運作均應依循符合憲法精神之法律及正當程序，遵守法律保留原則與比例原則，甚至受司法令狀原則之拘束方能使所欲維護之國家秩序，與所欲促進之人民福祉有其正當性可言，故本文將針對執法人員執行網路犯罪之偵查作爲時所應遵守的相關法律規定進行探討；此外，保障人權是世界潮流，現今實施民主憲政國家，國家各項施政作爲，亦皆以人權之保障爲依歸，惟在遇有社會之公益與個人之私益相衝突情形時，個人之私益便須受到限制，國家限制人民基本權，必須謹守「人權只能限制不能剝奪」、「基本權的『本質內涵』不容侵犯」、「以法律限制基本權利時，應顧及比例原則」之界限，以法律明文規範保障，本文亦將檢視我國目前在刑事訴訟法上相關規範情形如何？在我國法律漏未規範之處，是否有外國相關法律可供借鏡。

立憲主義國家之特色在於以憲法保障人民基本權，使人民免於無端受到國家行爲之干預、限制或侵害，在偵查網路犯罪的過程中，必須藉由網路監聽與搜索人民的電腦，以發現犯罪行爲人的蹤跡以及掌握犯罪證據，係涉及人民基本權干預的司法偵查權力行使，必須藉形式之法律規定以及實質內涵合憲性把關，並非可以毫無節制地行使，唯有明確劃分行使界限，使執行偵查任務的執法人員有所依循，方能不悖離憲法保障人民基本權的精神。

第二節 研究方法

本文研究方法將以文獻分析與比較研究法爲主。

一、文獻分析法：自網路科技發達以來已經顯著地爲人們的生活帶來了便利，然而，利用網路的特性所產生的犯罪問題，亦是相當困擾著執法單位，爲了達到對於犯罪跡證以及犯罪行爲人蹤跡的有效掌握，必須採取有別於一般傳統犯罪的偵查方法，引進新的科學技術的協助似已成爲不可避免的趨勢。此外，面對新興科技的發展對於偵查行爲所帶來的協助，亦引發是否過度侵犯人民基本權的疑慮。本文嘗試整理、歸納國內外學界、實務界對此相關議題探討之法規、期刊、論文、著作、研究報告及判例等文獻，勾勒本文研究主題之基本爭議、相關法律問題，並就上述文獻資料加以歸納、整理與分析，藉以建立本研究之理論架構。

二、比較研究法：我國是屬大陸法系成文法典之國家，法制建置初期繼受德國法，至今仍影響著我國法制的發展，隨著美國在資訊科技的發達以及已漸居於領先的地位，其相關法律的發展亦漸漸發揮其影響力。本文將歸納上述國家相關法制作爲比較法研究對象，針對我國法制規範不足、未臻成熟之處參考其他國家相關規定與實務見解，省思值得我國借鏡之相關外國法制可行性，期能截長補短進而勾勒未來修法或立法方向。

第三節 本文架構

本文係以網路犯罪之偵查爲主軸目標，藉由檢視電腦與網路技術的發展歷程，以對比這項科學技術所構築的虛擬空間與真實世界的差異，以及檢視經由監聽網路通訊之封包、調閱通訊內容以外之紀錄、搜索電腦等偵查作爲，對基本權的影響，並檢視現行的法律是否足以規範網路犯罪相關偵查作爲，以掌握相關法律問題之精神與內涵。

本文研究章節架構如下：

第一章爲緒論，主要介紹本文研究動機並說明研究方法，最後呈現全文架構。

第二章探討網路犯罪偵查的方法，首先說明傳統犯罪之偵查是以人證與物證之發掘爲中心，接著介紹網路的特性，以瞭解該特性使得傳統之犯罪偵查方法運用於網路犯罪偵查時所面臨的挑戰，最後並列舉一個真實的網路犯罪偵查案例，以瞭解偵查過程中所涉及的相關法律。

第三章探討美國網路犯罪偵查實務，首先介紹隱私權在美國發展的歷程，以及憲法第四增修條文對基本權保護的演進過程。面對有別於傳統犯罪的網路犯罪所帶來的挑戰，第一個要克服的問題是，如何追蹤犯罪嫌疑人，藉由監聽網路通訊之封包、調閱通訊內容以外之紀錄、要求揭露儲存在第三方的通訊資料等，相關的法律規範爲何以及其監督程序。第二個要克服的問題是，如何搜索犯罪嫌疑人的電腦，搜索策略該如何建立、搜索令狀該如何特定，在何種情形下允許例外的無令狀搜索，以及扣押後的電腦鑑識該

如何與搜索過程銜接，以使數位證據能確實獲得保全。

第四章探討我國網路犯罪偵查實務，首先介紹隱私權在我國受肯認的過程。通訊保障及監察法是用以規範現在正在進行與未來即將發生的通訊內容蒐集行爲，其是否亦可適用於網路通訊之監察。爲了確認犯罪嫌疑人的身分，必須取得個人註冊資料與通訊紀錄，此類非通訊內容資訊經常可以顯現網路使用者的喜好與習性，該些資訊的取得是否應有較高的規範門檻，以提高對非通訊內容資訊的保障。1997 年刑法修正首次肯認電磁紀錄具有保護的法益，並在 2001 年刑事訴訟法的修正中成爲得搜索扣押的客體，電磁紀錄的特性之一爲易於毀損與變造，在執行搜索與扣押的過程中，是否應命專家在場協助，以落實保全數位證據的目的，在搜索過程中若同時適用刑事訴訟法與通訊保障及監察法，其競合關係爲何。

第五章結論，將統整歸納本文各章節所得結論，將外國法制可爲我國參考之處加以具體化，針對現行法令未盡周全處提出具體可行之修法建議並作成結論，以兼顧抑制犯罪危害的擴大，找出犯罪行爲人與維護人權。

第二章 犯罪的偵查

第一節 傳統犯罪的偵查

偵查乃調查犯罪嫌疑人犯罪情形及蒐集證據之程序[1]。我國刑事訴訟法第 228 條第 1 項規定有，偵查機關在知有犯罪嫌疑者，應即開始偵查。偵查與起訴、審判以及執行共同構成廣義的刑事訴訟之一環。犯罪的偵查作爲是刑事訴訟的開端，而刑事訴訟是爲了要確定具體刑罰權之有無及其範圍所進行之程序，是以認定事實、適用法律，爲其主要內容，認定事實的過程中，必須仰賴證據爲之，有證據始得認定事實，事實明瞭，法律適用始得正確，所謂的證據，是指能使事實達到明瞭之原因(憑藉)[2]。因此，是否能有效地掌握犯罪嫌疑人以及其犯罪跡證，將影響到後續的刑事程序能否順利的進行。能夠成爲證據的類型可以區分爲人證與物證兩種。

傳統的犯罪手法，犯罪嫌疑人必須親身經歷犯罪現場以實施犯罪行爲，因此有可能會遭到第三人之目擊以及在現場留下犯罪跡證。

第一項 人證

學者將人證定義爲：「人證係以人之知識經驗爲材料之證據方法，因以人之知識經驗爲證據，故須以人之口頭爲陳述[3]。」人證的範圍包括證人與鑑定人。

證人係指在他人之刑事程序中，陳述自己所見所聞具體事實之第三人，除了存在有法律所允許的例外情形[4]，均有在以他人爲對象之偵查或審判程序中作證之義務[5]。證人屬於重要的證據方法之一，其所陳述的「證言」是屬於供述證據[6]，陳述內容之真僞將影響到事實認定與法律適用的結果。證人到場後開始作證程序之前，應先告知具結之義務與僞證之處罰，並當場由證人踐行具結程序[7]，經具結後若仍爲不實之陳述則將被課以僞證罪[8]之處罰。證人之陳述在審判中應經被告之詰問[9]，才能採爲認定被告犯罪事實

[1] 林俊益，刑事訴訟法概論(下)，新學林，2009 年 2 月，頁 3。
[2] 林俊益，刑事訴訟法概論(上)，新學林，2008 年 9 月，頁 352。
[3] 蔡墩銘，刑事訴訟法論，五南，2001 年 2 月，頁 223。
[4] 例外情況規定於刑事訴訟法第一百七十九條、第一百八十條、第一百八十一條、第一百八十二條。
[5] 林俊益，刑事訴訟法概論(上)，頁 513。
[6] 林鈺雄，刑事訴訟法(上)，元照，2004 年 9 月，頁 466。
[7] 刑事訴訟法第一百八十六條。
[8] 刑法第一百六十八條。

之判斷依據。

證人可以進一步區分爲與本案無關的第三人以及與本案有關的第三人[10]，前者即一般所稱之目擊證人，例如目睹車禍發生或銀行搶案發生之人，後者係指共同參與犯罪之人亦即同案之共同被告，例如共同參與銀行搶案之人，兩者均因親眼目睹事件之發生而具有陳述其所觀察到事實之能力。

被害人與告訴人亦得爲證人，惟兩者係使被告之受刑事訴追爲目的，其陳述之真實性相較一般之證人爲薄弱，仍應調查其他之證據以增強其證明力[11]。

基於訴訟經濟等原因，由檢察官合併或追加起訴或由法院合併審判之結果，而形成刑事訴訟上之共同被告，爲使刑事被告享有憲法第十六條所保障人民之訴訟權，其中包含充分之防禦權，亦即必須賦予刑事被告詰問證人之權利，經詰問後該證人之陳述始得作爲認定被告犯罪事實之判斷依據，因此共同被告對其他共同被告之案件而言，爲被告以外之第三人，本質上仍屬於證人[12]。

鑑定人係指第三人依其特別知識經驗，就某事項陳述其判斷意見之人，以行使一種替代證據調查之方法，證人與鑑定人之區別在於，證人所陳述其所觀察的事實是過去的事實，並無替代性，鑑定人係憑其特別知識經驗就現在之事實陳述其判斷意見之人，具有替代性，故證人得拘提，但鑑定人不得拘提[13]。

第二項 物證

學者將物證定義爲：「物證足供辨識事實，亦即可藉物證以推定所發生之犯罪事實，故物證可謂爲與犯罪有關之物體，通常爲有體物[14]。」

物證的功能在於能將犯罪嫌疑人與犯罪事實連接[15]，經由遺留在犯罪現場的掌紋、毛髮、筆跡、械彈之類有體物的掌握，藉由鑑定或勘驗之方式，對於既存的證據資料以法律特定的方式將之呈現成爲證據[16]，以使該類之物證扮演證明犯罪之功能。

鑑定的目的在於取得鑑定經過與結果之報告，鑑定人並應以言詞或做成鑑定報告之方式踐行報告義務[17]。若以言詞的方式在法庭上報告鑑定結果，則應踐行證人的作證程

---

[9] 有關詰問之程序請參照，刑事訴訟法第一百六十六條以下。
[10] 蔡墩銘，刑事訴訟法論，頁 224。
[11] 林俊益，刑事訴訟法概論(上)，頁 514。
[12] 釋字第 582 號解釋。
[13] 林俊益，刑事訴訟法概論(上)，頁 523-524。
[14] 蔡墩銘，刑事訴訟法論，頁 226。
[15] Kerr, Orin S., Digital Evidence and the New Criminal Procedure, 105 Colum. L. Rev. 279, 282 (2005).
[16] 楊雲驊，證據保全的規定與實務—以偵查階段爲中心，月旦法學雜誌，114 期，2004 年 11 月，頁 96。
[17] 蔡墩銘，刑事訴訟法論，頁 250。

序，並經被告對其鑑定內容的詰問，才能採爲有效的證據。

勘驗係調查證據與犯罪情形所實施之處分，由法官或檢察官就勘驗物，本其五官作用所實施或認識之結果做成得以爲證據資料之勘驗筆錄[18]。同樣的事實狀態爲證據時，將因其呈現的方式不同而適用不同的證據方法，以身體之物理性質狀態爲例，被害人陳述被告抓傷其手臂，是屬於證人之證據方法，法官當庭勘驗其手臂是否受傷，則是屬於勘驗之證據方法[19]。

第二節 網路的特性

第一項 匿名性

網路的特性之一就是具有高度的隱密性，行爲人身處於某一個角落，可使其行爲的效果發生於遙遠的另一端，行爲人的實體位置與行爲結果的發生地並沒有緊密的連接關係，行爲人在電腦前所下達的指令，經由網路設備轉換成封包透過網路的傳送，即可使其行爲結果發生於網路的另一端[20]。

網路上信號傳送的最小單位稱爲封包，封包表頭(header)記載著信號的來源位址與目的位址，封包到達目的地後被組合成服務請求，目的地主機依服務請求，將內容回應給請求端(來源端)主機，目的地主機的系統記錄檔會記錄服務請求主機的位址(IP)，至於下達服務請求指令的行爲人的識別資訊，並無法單純由 IP 來判斷。

網路管理人員基於網路架構的設計與安全性的考量，經常會劃定區域網路，僅由一特定端口對外連接網際網路，在該區域網路中之電腦主機均被配發虛擬 IP，只有需要存取該區域網路以外之資訊時，服務請求才會經由該對外端口向目的地主機發出，此時，該對外端口主機將扮演網路位址轉換(Network Address Translation，簡稱 NAT)的功能，記錄提出服務請求主機的虛擬 IP、目的地主機 IP 與服務請求類型，目的地主機回應的內容，亦是經由該對外端口進到發出服務請求的區域網路中，由該對外端口主機依據先前的記錄內容，將目的地主機所回應的內容，轉送至發出該服務請求的主機，此時，目的地主機的系統記錄檔所記錄服務請求主機的 IP，是該對外端口的 IP，並非真正發

[18] 林俊益，刑事訴訟法概論(上)，頁 549-550。
[19] 林鈺雄，刑事訴訟法(上)，頁 466。
[20] 身處於赤道島國的一個小朋友，透過網路瀏覽美國白宮網站，赤道的炎熱一如往昔，與現正處於冰天雪地的美國華盛頓特區，形成強烈的對比，負責白宮安全的警衛與監視設備，並無法察覺小朋友的到訪，而白宮網站的網管人員，是唯一有機會經由主機的系統記錄檔得知有一個來自該赤道島國的 IP 的瀏覽請求的人，至於小朋友的身分與性別並無所悉。

出該服務請求主機的虛擬 IP，除非能掌握到該對外端口主機的轉換記錄內容，才能找出真正發出該服務請求主機的 IP。

後門程式早先起源於系統管理人員基於管理上便利的需要所設計的一個便利通道，這個概念後來被有心人士加以利用，藉由各種方法植入後門程式，以躲避進入電腦系統所需要的帳號與密碼等安全性的驗證，經由後門程式進入電腦系統後，除了可以竊取該電腦內的資料，更常見的是被用來當成跳板，以做爲發動攻擊的起點，運用跳板主機可以阻斷反向追蹤，使真正發動攻擊主機的 IP 可以隱匿無蹤。

帳號與密碼可以用來識別合法的使用者，正如同真實世界中鑰匙可以拿來開門一樣。想要使用網路世界的資源，帳號與密碼的驗證時機，通常出現在設備使用、服務使用與連線使用這三種情形。

使用一台有帳號與密碼驗證要求的電腦，必須要先向系統管理者申請帳號與密碼的核發，通過系統管理者對申請者身分的審核，才能取得帳號與密碼。這是真實世界通往虛擬(網路)世界的入口，因此會有較嚴格的審核。

網路服務的使用型態之一就是單純的網頁瀏覽，在一般情況下並不需要任何的帳號與密碼的驗證，但是在電子布告欄(Bulletin Board System，簡稱 BBS)或網頁討論區，發表文章或參與討論時，必須要先進行會員註冊，一般而言對於所提供的註冊資訊並沒有很嚴格的驗證機制，因此該會員帳號持有者的真實身分依然具有相當的隱匿性。

使用個人電腦連接網路，必須向網路服務提供者(ISP)提出撥接(dial-up)或非對稱式數位用戶線(Asymmetric Digital Subscriber Line，簡稱 ADSL)連線申請，或是申請經由無線網路存取點(access point)連線，經過服務提供者驗證使用者的身分後，核發 IP 才能連接上網路。同樣的，這也是真實世界通往虛擬世界的入口，會有較嚴格的審核，政府對於網路服務提供者對其用戶的管理亦有相關的規範。

綜合以上的討論可以得知，要確認網路使用者的身分，必須要有 IP 與帳號兩者同時的配合，若有其中一項缺漏，將會造成網路使用者身分上的隱匿性。

第二項 無地域性

網路是由一段段的實體電路串接而形成一個資訊網路，路由器在其中巧妙地扮演起連接每一段實體電路的角色，除了具有實體層的連接功能之外，路由器也負責封包信號的繞送(routing)，經由傳送路徑上的眾多路由器的通力合作，能將服務請求的封包信號送達目的地端主機，過程中並不受真實世界的地形、地物等障礙的阻隔。

網際網路最大的特色之一就是全球化[21]，位在美國加州矽谷的網路公司提供免費電子郵件帳號，給全球的用戶申請、使用，提供服務的郵件伺服器，基於服務效率與異地備援的考量，經常會跨越不同的地理區域部署，以避免因爲天災所造成的設備毀損，導致所儲存資料的滅失，服務使用者經由代表該伺服器的網域名稱或 IP，與該伺服器建立連線取得服務，並不會真正計較該伺服器真實的座落位置。

在網路世界中，事件幾乎可以橫跨很長的距離而瞬間發生，網路上的疆界不再與領土、政治上的疆界一致，在網路上任何人都可能是鄰居[22]。

網路行爲的行爲人、行爲地以及網站設備的所在地、犯罪被害人以及犯罪結果可能分屬不同的國家，如果想要制定法律對於網路犯罪行爲加以規範，可能會因爲各國的法律規定不同以及無域外效力，而使得法律之執行無法貫徹[23]。

網路犯罪對於法律之挑戰在於網路無疆界[24]，網路的佈建跨越傳統的領土界線，基於對各國司法管轄權的尊重，執行犯罪的偵查必須特別倚賴國際合作，也因爲各國看待此類犯罪行爲嚴重性的態度不一而有執法效率上的落差[25]，因此提供網路犯罪行爲良好的滋長機會。

第三項 資料混雜

網路通訊與傳統電話通訊在傳輸協定上有著不同的特性，傳統電話通訊其資料的傳輸係藉由電路交換(circuit switch)系統進行，亦即通訊過程中會建立一條專屬線路以負責該次通訊資料的傳輸，線路頻寬不會與他人共享；網路通訊則是採用封包交換(packet switch)系統進行，在通訊過程中所欲傳送的資料會被切割成較小的傳送單位分批傳送在交織縱橫的網際網路實體線路上，不會有專屬線路的建立，抵達目的地端的資料並不一定會經過相同的傳輸路徑，由於每一段線路都將協助傳送不同目的地端的資料，因此線路頻寬是共享的[26]。

受限於網路的特性，因此必須將所欲傳送的資料切割成許多單位長度的較小資料，稱爲承載資料(payload)，並將接收端與發送端的位址等路由(routing)資訊記載於封包表

[21] 王銘勇，網路犯罪相關問題之研究，司法院，2002 年 11 月，頁 25。
[22] Balkin, Jack M. et al., Cybercrime: Digital Cops in a Networked Environment, New York University Press, 2007, p. 2.
[23] 謝明冠，網路行爲規範之研究，臺灣臺北地方法院檢察署，2001 年，頁 28。
[24] 謝明冠，網路行爲規範之研究，頁 29。
[25] Brenner, Susan W., Cybercrime : Criminal Threats from Cyberspace. Santa Barbara, CA: Praeger, 2010, p. 209-210.
[26] 陳信郎，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，2004 年，頁 106。

頭(header)，兩者構成一個封包(packet)，封包是網路傳送資料的最小單位。在傳送路徑上的路由器(router)讀取每個經過的封包表頭的目的地資訊，將封包往下一個路由器遞送，最終抵達目的地端主機。

一份傳送資料所分割的許多封包，在遞送過程中可能會經由不同的路徑抵達最後的終點，也因爲網路是共用的，在一段網路中會有來自不同來源端的封包經過其中，由路由器判斷其最佳路徑，將封包往下一個路由器遞送。

網際網路是一個階層式的架構，越上層的節點、骨幹越是許多資料遞送的必經之路，以台灣爲一個島國來說明，島外連接至台灣的電纜，均連接至位於屏東枋山或宜蘭頭城的海底電纜通信中心，也因爲有這些對外連接的電纜，台灣島內的網路才能成爲全球網際網路的一部份，台灣與外界的信息溝通若是要透過實體線路，一定會經過其中一個海底電纜通信中心，才能將需要離開台灣的封包信號，傳送離開台灣，或是接收欲進入台灣的封包信號。

基於犯罪的偵查所進行的封包截取，必須架設截取設備以收集所欲分析的封包，截取設備在整個網路架構中所處的位置，將會決定該設備所需面對的資料量的多寡，如果將該設備架設在較上層的節點，將會收集到較多犯罪偵查對象以外第三人的通信資料，造成隱私權侵害的問題，將設備架設在受偵查對象的住家網路或辦公室網路端口，亦有可能收集到與偵查案件無關第三人的通信資料，即使縮小收集的範圍，如何特定出只與偵查案件有關的資訊，亦是偵查技術所需面對的挑戰。

第三節 網路犯罪的偵查

在網路犯罪中，行爲人在電腦前下達指令，透過網路對網路另一端的電腦施以攻擊行爲，行爲人不需要親臨受害電腦的所在地，經由網路信號承載攻擊指令即能達成侵害的結果，相較於傳統犯罪的模式，網路犯罪的行爲人不會面臨被第三人目擊的危險，因而有較好的身分上的隱匿性，在傳統犯罪中所留下的生物與實體跡證，在網路犯罪模式中，已經轉換爲系統記錄檔[27]等數位型態跡證，也因爲受攻擊的標的是電腦與網路，其受侵害的特徵主要爲功能而非外觀，除非是該電腦的使用者或管理者發現其功能上已經產生異常，一般對該電腦沒有使用權限之人，並無法藉由外觀而察覺該電腦已經成爲網路犯罪行爲的客體。

[27] 系統記錄檔會定期的紀錄系統運行上的情況，一般簡稱爲 log，其中包括遠端連線電腦的 IP、連線時間以及使用何種連線服務，系統記錄檔是系統管理者在維護系統運行上重要的參考檔案，一般的電腦使用者並沒有權限可以接觸該檔案，駭客爲了湮滅犯罪的跡證，在入侵系統後會設法取得管理者的權限以更改或刪除系統記錄檔。

第一項 犯罪的發現

刑事偵查作爲之發動，必須要有犯罪行爲的發現爲前提，因爲該行爲已經侵害法律所保護的法益，因而必須採取刑法的手段加以介入，在電腦網路犯罪的情況中，犯罪的發現可以是受害者自行發現，經由網路誘捕發現或是經由網路巡邏發現，進而向執法機關舉報，而有偵查作爲的開端。

第一款 受害者

電腦使用者發現目前所使用的電腦有異常[28]，經由電腦專家的診斷或是防毒軟體的掃瞄，而發現自己的電腦已經感染了電腦病毒，或是已經成爲供他人驅使的殭屍電腦，或是公司所駕設的網路平台遭受分散式阻斷服務攻擊(Distributed Denial of Service，簡稱 DDoS)，使得電腦網路系統無法負荷源源不斷來自網路上的服務請求，超出系統所能承載的極限而導致系統癱瘓被迫終止提供服務，或是一早醒來登入網路銀行帳戶後，卻發現帳戶中的存款已經藉由網路轉帳的方式遭到盜領一空，驚覺自己的帳號與密碼在不知情的情形下，已經落入駭客的掌握之中。

第二款 誘捕

誘捕是精心設下的陷阱，在一個事先規劃好的環境下，等待犯罪的發生，在該環境中可以全程觀察犯罪發生的經過，並且完整的蒐集犯罪的證據。

蜜罐(Honeypot)是一種普遍使用的「誘捕系統」，是一種被設計用來吸引攻擊者並刻意讓其攻陷的系統，藉由拖延攻擊者在蜜罐的停留時間以達到管理者的追蹤與分析目的，就如同一個用來吸引昆蟲的蜂蜜罐一般，蜜罐最主要的價值在於讓未授權者或非法者加以使用，由於蜜罐可以提供其它工具所無法獲得的獨特攻擊資訊，所以其所蒐集到的資訊都具有很高的價值[29]。

蜜網(Honeynet)是由數個蜜罐所組成，它是一個用來蒐集駭客相關資料的網路陷阱，以瞭解其團體屬性、感興趣的標的、使用的軟體、利用的電腦弱點等資訊，在蜜網中除了蜜罐之外，還需要一些網路軟硬體相關的裝置，例如防火牆、路由器、交換器以

[28] 異常的情況可能有以下的情形之一：系統非常的緩慢、硬碟不斷的讀取或是使用者在沒有使用網路服務的情形下，網路卡信號卻不斷的傳送。

[29] 葉昭熙，以開放始碼爲基礎的蜜罐系統設計與實現，國立高雄師範大學資訊教育研究所碩士論文，2007年，頁 8-9。

及日誌記錄工具與封包分析器等，在蜜網中最重要的元件就是資料控制(Data Control)和資料捕捉(Data Capture)單元，資料控制單元定義了怎樣將攻擊者的活動限制在蜜網中而不被攻擊者察覺，資料捕捉單元則是指在攻擊者不知情的情況下，如何掌握其所有的攻擊活動，而兩者之中又以資料控制單元最爲重要[30]。

分析誘捕環境所蒐集到的資訊，可以學習入侵者所使用的工具以及手法[31]，除了可以追溯犯罪足跡採集做爲犯罪的證據之外，亦可以提供資訊安全人員改善電腦系統現有的弱點，強化系統抵抗資訊安全威脅的能力。

經由誘捕系統所取得的犯罪資料，都是犯罪行爲發生當時的細節記錄，對於犯罪發生的整個過程有較好的掌握度，而實務上比較常遇到的情況是，犯罪行爲發生後才開始進行證據的蒐集，比較容易會面臨資料蒐集不完整的困難[32]。

第三款 網路巡邏

網路巡邏是藉由分析網路上的流量，以判斷是否有電腦因爲感染電腦病毒而有不正常網路信號的發送，網路服務提供者爲了確保在其所提供服務網路上的其他網路使用者的資訊安全，常常會有相關的機制以進行網路巡邏。

隨著資訊安全風險意識的覺醒，政府與民間機構已經體會到資訊安全防護的重要性，而普遍藉由防毒、防火牆，甚至入侵偵測系統等資訊安全設備的部署，試圖防護或偵測資訊安全事故的發生，由於欠缺對資訊安全設備所發出的危險預警信號加以解讀與判斷並採取適當措施的專責單位，資訊安全事故還是時有所聞，使得代價昂貴的設備沒有發揮應有的功能，資訊安全維運中心(Security Operation Center，簡稱 SOC)於是因應而生[33]。

資訊安全維運中心對於資安事件的管理主要區分爲四個階段：準備與預防階段、偵測與分析階段、封鎖與復原階段、蒐集與存證階段。準備與預防階段的重點在於加強安全認知與教育訓練，以提升資安人員的應變能力；偵測與分析階段的功能在於針對所發現的事件徵兆，加以初步分析並確認是否爲事故，以及持續監控與偵測該事故；封鎖與復原階段的功能爲進行通報應變作業、執行封鎖作業與證據蒐集以及資安事故還原；蒐集與存證階段的功能爲經驗學習以及蒐集事故資料與保留證據[34]。

---

[30] 葉昭熙，以開放始碼爲基礎的蜜罐系統設計與實現，頁 9。
[31] 黃佩倫，入侵電腦行爲之研究，國立交通大學科技法律研究所碩士論文，2004 年，頁 107。
[32] 黃佩倫，入侵電腦行爲之研究，頁 107。
[33] SOC 參考指引，九十五年度國家資通安全技術服務與防護管理計畫，available at http://www.rdec.gov.tw/public/Data/74217484571.pdf (last visited June 19, 2012)。
[34] SOC 參考指引，九十五年度國家資通安全技術服務與防護管理計畫。

行政院資通安全會報所統籌規劃推動之資訊安全資訊分享與分析機制，在學術網路方面的具體實現是分別在北區與南區建立學術資訊安全維運中心(簡稱 A-SOC)，北區學術資訊安全維運中心是由台灣大學負責管理，並在台灣大學、政治大學與中央大學成立維運點部署相關的資訊安全設備，將所蒐集到的資料彙整至北區學術資訊安全維運中心[35]。

北區學術資訊安全維運中心目前所達成的具體成果包括，部署入侵防禦設備並可以配合緊急應變機制即時阻擋惡意連線；建置資訊分析平台以蒐集各監控點資訊安全事件，進行初步關聯性分析，使北區學術網路的安全防護機制獲得強化。在網路犯罪偵防所可能提供的協助包括，建立學術網路區域聯防機制，透過學術資訊安全維運中心所監看之資安事件可以追蹤至校園網路之問題來源；建立校園網路資安事件之鑑識機制，對受害重要主機進行鑑識與蒐證，並配合學術資安維運中心之資安紀錄進行交互分析；以及提供資安事件追蹤與鑑識之經驗分享，以協助北區學術網路之連線單位資訊安全人員專業能力的提升[36]。

第二項 犯罪偵查單位

第一款 美國

網路科技的進步爲人類社會的生活型態帶來了改變，在享受該項科技爲生活上帶來便利的同時，也伴隨著隱憂，美國是目前網路科技最進步的國家，其所面臨的網路犯罪的挑戰也最爲嚴峻。爲了提升網路犯罪偵查的效率，以及因應不斷進步的犯罪手法，經由訓練以持續加強執法人員的素質，而有相關的網路犯罪偵查單位與計畫的產生。

第一目 美國司法部電腦犯罪防制中心

美國司法部電腦犯罪防制中心(Computer Crime and Intellectual Property Section，簡稱 CCIPS)，成立於 1996 年，其前身爲美國司法部電腦犯罪組(Computer Crime Unit)，負責推行美國司法部電腦犯罪防制計畫(The Justice Computer Crime Initiative)，以解決日益猖獗的電腦犯罪問題[37]。

---

[35] 李美雯，北區 A-SOC 建置與管理，available at http://tais2011.ntu.edu.tw/docs/2-7-3.pdf (last visited June 19, 2012)。

[36] 李美雯，北區 A-SOC 建置與管理。

[37] 蔡美智，美國重要之網路犯罪防制相關單位組織簡介，資訊法務透析，2000 年 3 月，頁 37。

CCIPS 的律師負責解決因電腦與通訊科技所引發的特殊爭議與參與訴訟案件，此外，該中心也提供訴訟資源給其他檢察官，訓練聯邦與地方執法人員，提供立法與修法建議，以及發起與參與國際合作以共同打擊電腦犯罪[38]。

CCIPS 的律師提供合作的對象包括，政府單位(例如，FBI、國防部、NASA)，私人機構(例如，硬體、軟體以及通訊科技公司)，學術機構以及國外對口單位等[39]。

第二目 聯邦調查局網路犯罪部門

美國是由 50 個州組成一個聯邦的國家，各州擁有獨立的司法管轄權[40]，只有憲法明文規定的事項，或是經憲法的授權才受聯邦管轄，除此之外都是屬於州法的管轄範圍[41]，當犯罪的偵查需要跨州的聯繫，或是案件的性質過於龐大或複雜，已經超過地方政府的能力，聯邦調查局(Federal Bureau of Investigation，簡稱 FBI)才會介入處理，網路犯罪在 FBI 的任務優先順序中，被列爲屬於與國家安全有關的事項[42]，因此由 FBI 主導偵辦。

聯邦調查局網路犯罪部(cyber division)，是第一線從事網路犯罪偵查工作的專業單位，偵查工作會依據不同的網路犯罪類型，而有不同的分組，例如，駭客入侵與兒童色情的犯罪特性不同，而有不同的組別負責，偵查駭客入侵的案件，所需要的技術能力甚高，因此偵辦駭客入侵案件的組員，通常在未進入 FBI 工作之前就已經具備有電腦技術背景[43]。

聯邦調查局的網路犯罪部，下轄有三個單位，網路犯罪打擊小組(cyber squads)部署在 FBI 的總部與 56 個地區辦公室，該組的成員專長於偵查網路入侵、智慧財產與個人資料的竊取、兒童色情與剝削兒童以及網路詐欺，網路犯罪行動組(Cyber Action Team)負責境外網路犯罪資訊的蒐集與分析，經常因任務的需要必須飛往世界各地，並與外國當地的執法機構共同打擊網路犯罪，電腦犯罪專案組(Computer Crimes Task Forces)在全國共有 93 個專案組，結合最先進的科技與來自聯邦與州政府的資源，配備有先進的實驗室，並持續提供執法人員增強犯罪偵查能力所需要的訓練，基於打擊網路犯罪的考量，FBI 有越來越多的機會與其他聯邦機構共同合作，其中包括國防部、國土安全部

[38] 請參照美國司法部 CCIPS 網頁，http://www.cybercrime.gov/ccips.html (最後點閱日：2012 年 2 月 17 日)。
[39] 蔡美智，美國重要之網路犯罪防制相關單位組織簡介，頁 37。
[40] 請參照美國憲法第四條第一項條文前段，各州對於他州之法律、紀錄與司法程序，應有完全之尊重與信任。
[41] 請參照美國憲法增修條文第十條，本憲法所未授予美國政府或未禁止各州行使之權限，皆保留於各州或其人民。
[42] 請參照 FBI 網頁，http://www.fbi.gov/about-us/quick-facts (最後點閱日：2012 年 2 月 16 日)。
[43] 蔡美智，美國重要之網路犯罪防制相關單位組織簡介，頁 38。

等[44]。

在 2007 年 6 月與 11 月，FBI 曾經執行兩次駭客掃蕩專案[45](Operation Bot Roast)，相當的有成效，發現數以百萬計的殭屍電腦，且分別逮捕多位殭屍網路的首腦(botherder)並加以起訴。

第三目 國家網路犯罪偵查聯合專案組

現今的網路威脅是以各種的方式來呈現，在治安層級，罪犯利用網路來進行詐欺、竊盜與侵害兒童。在國家安全的層級，間諜與恐怖份子利用網路以竊取機密與攻擊國家重要基礎設施。

有鑑於要根除來自於網路上的威脅，很難僅藉由單一機構的力量來達成，在 2008 年由美國總統發佈命令，指派國家網路犯罪偵查聯合專案組(National Cyber Investigative Joint Task Force，簡稱 NCIJTF)做爲所有政府機構進行國內網路威脅偵查時，相關資訊協調、整合與分享的匯聚點[46]。

該聯合專案組由 FBI 負責發展與支援，主要成員的組成來自於相關的情報機構與執法單位，其中亦包括國防部與國土安全部，希望能達到有效預測與防止網路犯罪的發生，以及追擊發動網路攻擊的幕後組織。

第二款 臺灣

我國主要偵查網路犯罪的機關，分別是台灣高等法院檢察署「電腦犯罪防治中心」、法務部調查局資訊室第四科、刑事警察局偵查第九隊等，其主要的功能介紹如下：

第一目 高等法院檢察署「電腦犯罪防治中心」

法務部於八十六年四月十六日在臺灣高等法院檢察署下成立電腦犯罪防治中心負責協調、整合相關單位資源，並在各地方法院檢察署指派專責檢察官辦理電腦犯罪相關案件，該中心主要五大工作目標如下[47]：

---

[44] 請參照 FBI 網頁，http://www.fbi.gov/about-us/investigate/cyber/computer-intrusions (最後點閱日：2012 年 2 月 22 日)。

[45] 參照美國聯邦調查局所發佈的新聞稿，http://www.fbi.gov/news/pressrel/press-releases/bot-roast-ii-nets-8-individuals (最後點閱日：2012 年 2 月 16 日)。

[46] 請參照 FBI 網頁，http://www.fbi.gov/about-us/investigate/cyber/ncijtf (最後點閱日：2012 年 2 月 22 日)。

[47] 林孟瑤，網際網路色情犯罪與刑事偵查之研究，中國文化大學法律學研究所碩士論文，2006 年，頁 128。

1.研擬防治電腦犯罪及網際網路犯罪的政策。

2.溝通檢、警、調及各相關執行、研究機關的見解及作法。動員各機關的人力、物力，經由防治中心的代表成員建立聯繫管道，並加強協調功能，給予辦案支援，以落實查緝成效。

3.加強執法人員在職訓練、研討、溝通法律意見及查緝技術以建立正確觀念及共識。

4.強化國內外電腦犯罪及網際網路犯罪之研究，並對國內辦理電腦犯罪及網際網路犯罪加以列管、追蹤並建立研究資料庫。

5.加強教育宣導，以建立適用電腦及網際網路社會的倫理及秩序，以減少網際網路犯罪的發生。

第二目法務部調查局資訊室第四科

電腦犯罪的防制是法務部調查局組織法第二條所規定的業務執掌之一，爲了更有效的打擊網路與電腦犯罪，於八十九年在調查局資訊室下成立第四科專責電腦犯罪偵防工作。其工作內容爲[48]：

1.防制網路暨電腦犯罪，主動發掘及協助本局各內外勤單位偵辦電腦犯罪案件，提供相關偵查技術，解析數位證據。

2.建置支援偵查、偵辦之資訊系統環境，提升辦案效能。

3.辦理有關防制電腦犯罪之宣導及教育訓練。

4.研擬防制電腦犯罪對策，力求偵查與預防並重，開展國內外合作管道，共同打擊網路暨電腦犯罪。

爲了立即有效的打擊網路犯罪，於該局所屬台北市調查處與高雄市調查處，並成立查緝電腦犯罪機動專組，專責網際網路犯罪案件之偵辦[49]。

第三目刑事警察局偵查第九隊

刑事警察局偵查第九隊是我國主要打擊網路犯罪的單位，該隊的前身乃是八十五年九月成立於刑事警察局資訊室下的電腦犯罪組。八十八年七月將原隸屬於資訊室之電腦犯罪組，擴編爲專責高科技犯罪偵查之偵查第九隊(第一組和第二組)，隨後於九十年十一月成立偵查第九隊第三組，進而於九十二年一月成立電腦技術組，編制成員三十位，

[48] 請參照法務部調查局網頁，http://www.mjib.gov.tw/cgi-bin/mojnbi?/newworkitem/crime/crime-7.html (最後點閱日：2012 年 2 月 23 日)。

[49] 林孟瑤，網際網路色情犯罪與刑事偵查之研究，頁 129。

分四組偵辦高科技犯罪案件[50]。

目前該隊主要的工作內容有「偵查重大科技犯罪案件」及「高科技犯罪資訊科技之蒐集研究」等二項，前者係指偵辦電腦惡意程式及網路入侵等案件；蒐集電腦駭客攻擊活動，分析駭客攻擊路徑，追蹤電腦駭客；協助各治安機關處理偵辦電腦犯罪發生的問題與疑慮；研究、破解不法人士利用科技設備犯罪；整合警察資訊、通信技術單位與人力，並結合民間科技人才支援偵辦刑案[51]。

而後者則包含蒐集高科技犯罪最新犯罪手法、工具，並分析罪犯所應用之技術；運用資訊技術蒐集並分析網路上隱藏之犯罪資訊，以達有效防制之效；研發新穎高科技犯罪偵查技術，研發與運用科技設備，協助犯罪偵查，預擬科技犯罪防制作爲；建置智慧型網路犯罪蒐證系統，蒐集網路不法犯罪資料，建立電腦犯罪檔案庫；規劃成立電腦鑑識單位，建置數位證據鑑識標準作業程序，做爲數位證據鑑識人員參考等工作[52]。

近來資訊與通訊發展已朝向結合之趨勢，科技產品不斷推陳出新，電腦犯罪、白領犯罪、經濟犯罪問題上升，獲取不法經濟利益，危害社會治安，九十五年四月一日經行政院核准整合刑事研究發展室、通訊監察中心、資訊室及偵九隊等單位成立任務編組「科技犯罪防制中心」，並於同年四月七日正式掛牌運作[53]。

刑事警察局偵九隊自成立以來所查獲案件已超過百起，並不定期掃蕩非法網站，對於遏止網路犯罪及網路色情等不法行爲已經發揮積極正面的功效，對外並曾協同 FBI 共同偵辦以台灣電腦主機爲跳板入侵美國政府機關網站的駭客案[54]。

第三項 犯罪事實與犯罪者的連結

不同的犯罪機制將會產生不同的證據，也影響著不同的偵查步驟，而產生不同於傳統犯罪的法規範的需求。刑事程序法是有機的法律，其緊緊依附在它所規範的犯罪偵查事實上，事實的改變，將會導致對現行法規範的改變帶來壓力[55]。

證據，是指能使犯罪事實達到明瞭之原因(憑藉)[56]，在網路犯罪中資料是以數位的方式呈現，其可能存放在儲存媒體上或是正處於傳送的狀態中，數位資料的特性之一爲易於毀損與變造，因此必須立即加以保全，其所展現的行爲就是搜索與扣押。

---

[50] 張承瑞，科技犯罪偵查暨數位鑑識出國參訪報告書，台中市警察局，2010 年 11 月，頁 7。
[51] 李相臣，網路科技犯罪專責隊-刑事局偵九隊，透視犯罪問題，4 期，2004 年 9 月，頁 66。
[52] 李相臣，網路科技犯罪專責隊-刑事局偵九隊，頁 66。
[53] 請參照刑事警察局網頁，http://www.cib.gov.tw/aboutus/aboutus02.aspx (最後點閱日：2012 年 2 月 26 日)。
[54] 請參照刑事警察局網頁，http://www.cib.gov.tw/news/news01_2.aspx?no=28 (最後點閱日：2012 年 2 月 26 日)。
[55] Kerr, Orin S.，Digital Evidence and the New Criminal Procedure，頁 281。
[56] 林俊益，刑事訴訟法概論(上)，頁 352。

第一款 儲存在第三方的資料

電腦的普及讓很多以電腦進行處理的資料得以數位化的方式儲存，網路的發達讓儲存資料的媒體不在侷限於本機電腦的硬式磁碟，網路應用的多樣化使得透過網路可以取得許多種類的服務，也因此產生各種不同類型的資料，這些資料分別存放在提供該項服務的伺服器主機中，例如，郵件伺服器會存有其郵件帳號使用者的電子郵件，網頁伺服器會存有網頁內容的資料，網路硬碟會存有使用者所儲存的個人檔案，這些伺服器除了儲存有其所扮演功能的資料外，也因爲這些伺服器是透過網路提供服務，通常都會有一個記錄連線的記錄檔，記錄與其連線的他方主機的 IP 或是使用者帳號的登入記錄。

使用者所發送與收取的電子郵件，所建立供人瀏覽的網頁，或是在使用網路或電腦的過程中，伺服器所自動產生的系統記錄檔，這些資料都是因爲使用者的行爲所產生，卻因爲資料分別位於提供服務的伺服器中，而產生使用者對該些資料有使用上的權限，伺服器的管理者也同時有管理上的權限。

在網路犯罪偵查的過程中，犯罪嫌疑人身分資料的掌握通常不是那麼的直接與明確，必須以結果發生地或是被害人爲起點，往上游追溯試圖重建整個犯罪路徑，偵查人員必須調閱相關伺服器的連線記錄或是帳號登入記錄，在相關資料都保存良好的最理想情況下，有機會可以找出犯罪行爲人。

過程中，偵查人員會要求伺服器管理者的協助，提供相關的連線記錄資料或是使用者的註冊資訊，以連結犯罪事實與犯罪嫌疑人。

第二款 傳輸中的資料

在上一款中提及，在相關資料都保存良好的最理想情況下，有機會可以掌握犯罪嫌疑人的身分，但是在追溯犯罪來源的過程中，經常會面臨犯罪嫌疑人使用跳板主機或是修改連線記錄檔，使犯罪路徑的重建被迫中斷，藉以躲避法律的訴追。

基於，犯罪會重複發生的經驗或是爲了掌握正在進行中的犯罪行爲，因此可以藉由監聽的方式將可能與犯罪行爲有關的封包信號收集起來，加以分析過濾之後做爲證據之使用。

本章第二節第三項曾提及，封包信號傳輸的過程中會有資料混雜的問題，監聽設備所裝設的位置會影響到將來需要處理過濾的資料量的多寡，過濾條件的設定除了將決定是否會接觸過多與偵查案件無關第三人的通訊資料，也將決定是否能完整的收集原來發

送訊息所切割而成的全部封包信號，唯有收集到完整的封包信號才能重組還原成原來發送的訊息。

第三款 搜索扣押

爲了防止證據遭到變造或滅失，必須在證據可能存在的位置進行搜索，除了應以侵害最小的方式進行，當找到所欲找尋的證據之後隨即加以扣押，並應立即停止搜索行爲。

網路犯罪偵查所面對的資料型態都是以數位化的方式存在，在法律上被稱爲電磁紀錄[57]，必須藉由搜索犯罪嫌疑人的電腦以找出犯罪事實與行爲人的關連，受惠於現今電腦科技的進步，儲存媒體的容量可以存放大量的資料，想要搜索其中的資料將會耗費相當長的時間，在現場進行即時的搜索已經是不可行並會有毀損資料的危險，因此必須先行在現場扣押該儲存媒體，接著帶回實驗室進行仔細的鑑識分析。

回到實驗室後首先必須對該被扣押的儲存媒體以位元流或鏡像的方式將存放在其中的資料製作一個備份，執行搜索的過程都是針對該複製的備份資料進行，才不至於在搜索的過程中毀損或更改存放在儲存媒體中的資料[58]。

在本章第二節第三項曾提及，封包信號傳輸的過程中會有資料混雜的問題，儲存媒體儲存有大量的資料同樣會面臨資料混雜的問題，執行搜索的人員應採用適當的方法搜尋出與犯罪有關的資料，以避免接觸到與偵查中案件無關的資料並造成對他人權利的侵害。

電腦作業系統在運作的過程中所記錄的許多資料，經由電腦鑑識將會重建許多的犯罪細節，甚至有機會可以回復已經被刪除的檔案[59]，並顯示犯罪行爲是否由該受鑑識的電腦所執行，以反駁犯罪嫌疑人聲稱該電腦是遭到駭客入侵或被當成跳板的無辜抗辯。

爲了使電腦鑑識的過程中不至於污染證據，鑑識人員必須遵守許多的程序，甚至是扣押的方式是否符合程序的要求，都會影響到後續鑑識的結果，例如，在扣押現場不經意的開啓一個檔案，雖然沒有更改到檔案的內容，但是該檔案最後被存取的時間已經被這個錯誤的行爲所更動，將有可能影響到對於犯罪行爲發生時間點的認定。

[57] 有關電磁紀錄的定義，請參照刑法第十條第六項。
[58] Kerr, Orin S.，Digital Evidence and the New Criminal Procedure，頁 288。
[59] Kerr, Orin S.，Digital Evidence and the New Criminal Procedure，頁 287。

第四節 一個實際的案例

以下是一個實際的案例[60]，藉由描述偵查人員其親身經歷的執法過程，可以普遍呈現電腦網路犯罪的偵查過程中，偵查人員爲了取得證明犯罪的數位資訊，經常面對的處境與所採取的因應措施，並於確實遵循相關法律的規範下，順利達成偵查的目標。本文將就過程中所涉及的相關法律加以探討。

Lance Mueller(以下簡稱 Mueller)，是前加州電腦與科技犯罪高科技專案組的成員。在當時是加州河邊郡的一位犯罪偵查員，並被指定爲州與聯邦聯合打擊電腦犯罪的成員，也就是一般所熟知的 CaTCH(Computer and Technology Crime High-Tech Task Force)，其主要的任務是執行電腦相關的偵查，以及執行進一步的電腦鑑識工作。

在 2003 年 1 月 3 日當日接獲河邊郡資訊技術部門通知，有未被授權的軟體被發現在三台提供公眾服務的網頁伺服器上之後，Mueller 展開了與駭客集團 Thr34t Krew 成員一連串的鬥法過程。經快速的檢查後，在以下的資料夾路徑上，發現未被授權的軟體：

C:\Program Files\Microsoft\Update\DLL\tk

該資料夾含有數個檔案，經過分析後發現它是 IRC 殭屍，使用 mIRC 程式來控制它。

該殭屍電腦在控制程式的執行下會連回 8 個 IRC 伺服器[61]之其中一個。嫌犯爲了混淆該些伺服器的所在位置，以增加偵查的困難度，因而對該些伺服器名稱進行加密，在純文字模式下看起來像是一堆亂碼。解密的方式也同樣在該 mIRC 程式中，經過解密之後才可以正確顯現該些伺服器的名稱。

該些嫌犯採用預先指定的網域名稱，並直接將它寫在程式中，而不是採用靜態的網際網路位址(IP)，因此他們可以快速地更換以連接到其他的網際網路位址[62]。該些網域

[60] 摘錄自 Malicious Bots，頁 9。
[61] 在此所指的 IRC 伺服器，就是命令與控制中心。連回的動作就是向命令與控制中心報到，接受指揮。
[62] DNS 是執行將網域名稱(domain name)對應至網際網路位址(IP)的功能，正如同在第二章第二節第六項所述，網域名稱是網路使用者比較容易理解與使用的資訊，而網際網路位址所表示的數字是封包信號在傳遞的過程中，相關的網路設備例如路由器等能夠解讀的資訊，網際網路位址所代表的是該台主機在網路上的位址，可以藉由配發該網際網路位址的 ISP 的協助，得知該台主機的所在地點。爲了躲避追查以及方便管理，在 mIRC 程式中只能定義 IRC 伺服器的網域名稱，至於由哪一台主機擔任 IRC 伺服器，則可以臨時指定與隨時更換，只要將網域名稱以及其所代表的網際網路位址的對應關係，記錄在 DYNDNS 所提供的服務內。

名稱都是註冊在 DYNDNS(http://www.dyndns.com)這家服務公司。

從該些被感染的電腦中，Mueller 取得了惡意程式的樣本，並將它感染至一台虛擬機器上，以觀察該 IRC 殭屍的行爲模式與能力。在解讀了 IRC 伺服器的網域名稱之後，Mueller 連線到其中一台 IRC 伺服器，觀察到底有多少受害電腦連接到該命令與控制中心(Command and Control，簡稱 C&C)。

Mueller 所連線的其中一台伺服器，當時連線的殭屍電腦有數百萬台，其歷史紀錄顯示最高曾經有過上千台殭屍電腦連接至該伺服器。CaTCH 通常不會偵辦普通的病毒或惡意程式的攻擊，但是在本案中，受害的電腦中其中一台是屬於政府單位的，而且可能有另外數百台的受害電腦。因此正式的調查行動在 2003 年 1 月 3 日開始展開。

開始的偵查步驟之一是聯絡 DYNDNS 服務提供者。依據電子通訊隱私法(Electronic Communication Privacy Act，簡稱 ECPA)與愛國者法案(USA PATRIOT Act)所賦予的權利，亦即依據 18 USC 2703(f)，Mueller 立刻要求涉及上述網域名稱的紀錄全數加以保存，直到 Mueller 能獲得正式的法院命令以合法的接收它們。

在 1990 年代電腦相關犯罪開始增加的初期，通常公司都很願意配合執法單位的偵查，但是隨著時間的經過以及有越來越多的電腦犯罪案件，很多公司已經被執法單位的配合偵查要求所淹沒而不堪負荷。此外，很多想協助犯罪偵查的公司，擔心因爲提供執法人員資料或協助執法人員，而遭到控訴。因此，通常需要提示法院命令，才能從一家公司取得任何的指認資訊。

Mueller 寫了一張宣誓書，描述上述發生的犯罪情況，並取得治安法官所核發的法院命令，以向該服務提供者取得該網域名稱的相關註冊細節。

Mueller 發現在 mIRC 程式中所指定的 8 個 IRC 伺服器網域名稱，只有 7 個被使用，因此 Mueller 將尚未被使用的那個網域名稱，對應至其所架設的一台 IRC 伺服器的網際網路位址上。

Mueller 同時也在自己架設的 IRC 伺服器的 6667 埠[63]，執行一個封包擷取的動作，

[63] 被感染成 IRC 殭屍後，會透過 6667 埠向 IRC 伺服器(命令與控制中心)報到，這就是所謂的 phone home。

以統計有多少的殭屍電腦想要跟命令與控制中心聯絡。在一個 24 小時的統計區間，有將近 10,000 台的殭屍電腦試圖與其所架設的 IRC 伺服器聯絡，這也讓 Mueller 瞭解到整個情況有多嚴重。Mueller 也注意到，嫌犯所控制的網域名稱所對應的網際網路位址，每天都會被重新對應到一個新的網際網路位址。

第一個 DYNDNS 帳號

向 DYNDNS 提示法院命令後，DYNDNS 提供 7 個網域名稱的註冊資訊給 Mueller，正如同 Mueller 所預料的，大部分的註冊資訊都是假的。該 7 個註冊的網域名稱，分別屬於 3 個不同的使用者帳號。第一個使用者帳號是 ARDOG1085，被用來控制 2 個網域名稱。DYNDNS 記錄著當帳號開啓後，用來傳送啓動連結的網際網路位址與電子郵件位址。該嫌犯最初使用的網際網路位址，與隨後嫌犯每天用來連線以重新更改該網域名稱所對應的網際網路位址，是相同的。

法院核發一個法院命令，以取得用來註冊 ARDOG1085 這個帳號的網際網路位址的用戶資訊，這個網際網路位址被確認是位於伊利諾州尚普蘭。Mueller 聯絡了一位在該地區的警探，並與他討論這個偵查行動。依據網際網路位址之用戶資訊所記載的地址，在警方的檔案中搜尋後得出該地址住著一個名叫 Arwin 的人，以及他的生日爲 1985 年 10 月。回顧 DYNDNS 所提供的紀錄，Mueller 注意到使用者帳號 ARDOG1085 與 Arwin 以及 10-85 有著些許的相似性。

提出宣誓書並獲得法院允許，在伊利諾州尚普蘭當地的網際網路服務提供者處安裝撥號記錄器以及追蹤裝置。該裝置允許 Mueller 捕捉進出嫌犯住處的網路流量的封包表頭資訊(header information)。該法院命令並不允許 Mueller 捕捉封包內容，封包表頭資訊包含來源 IP，目的 IP，通訊埠，通訊協定以及序號。捕捉資料的內容等同於監聽(wiretap)，也就等同於聽取電話線上的對話，這需要更高等級的法院命令，也就是一般所指的 Title III，也只有在特定類型的犯罪上才能使用。在這個時間點，一個撥號記錄器與追蹤裝置的安裝，已經足以提供 Mueller 所需要的資訊。

Mueller 安裝了一台 Linux 作業系統筆記型電腦，並開啓兩個網路介面。一個用來當成管理介面，另一個介面被用來收集所需要的資料。一位探員將 Mueller 的筆記型電腦帶至當地業者的機房安裝。機器安裝完成後，Mueller 可以坐在辦公室遠端登入那台

筆記型電腦，並監看所收集到的封包表頭資訊。Mueller 的目的主要是要證明，從嫌犯住處的網際網路位址所送出的封包，是傳送到 DYNDNS 的服務，用以組態該網域名稱，在當時並沒有對應的流入封包進入到嫌犯的電腦中，這樣的做法是要預防嫌犯辯稱他的電腦遭受攻擊，被拿來當成跳板(stepping stone)或代理伺服器(proxy)。

經過數天的收集封包表頭資訊，很明顯地嫌犯確實住在該地址，嫌犯不止從他的住處連線到 DYNDNS 服務，同時也連線到 IRC 伺服器。以上這些資訊，讓 Mueller 可以斷定住在伊利諾州尚普蘭的嫌犯，參與了 IRC 殭屍的攻擊。

第一次的搜索與扣押

搜索行動在 2003 年 2 月 6 日，分別於英國與美國兩地針對三個嫌疑犯同時展開。逮捕了三個嫌疑犯，以及扣押了電腦並隨後送往電腦鑑識實驗室加以分析。

經由以上的實際案例描述可以得知，偵查過程中為了取得數位資訊，必須適用通訊紀錄的緊急保存、使用者身分的揭露、撥號記錄器與追蹤裝置、搜索與扣押、以及電腦鑑識等相關法律規範，若涉及通訊內容的截取則有通訊監察法律規範的適用。本文將就刑事偵查過程中數位資訊之保全所涉及的相關法律加以探討。

第三章 美國偵查實務

第一節 隱私權

第一項 美國隱私權的發展及內容

美國隱私權的概念，首先在普通法侵權行爲的領域發展，歷經普通法原則的建構過程，隱私權的概念首先出現在十九世紀末[1]，由獨處的自由發展出美國侵權行爲法上的隱私權，至於美國憲法上是否亦有隱私權，則不無疑問[2]。

隱私權的文字並未見諸於美國憲法的條文上，在對隱私權提供保護的發展過程中聯邦最高法院並未直接定義隱私權，而是改以界定隱私權的保障範圍或內容[3]，經由具體個案的判決中呈現，肯認隱私權是憲法所保障的基本權利，將隱私權提升至憲法的層級。

在犯罪偵查的過程中必須以國家的力量介入私人的領域，以蒐集證據或是確認行爲人的身分，這些國家行爲已經對人民的隱私權造成侵害，基於隱私權是憲法所保障的基本權利，此類國家行爲必須符合相關的法律要件才能執行。

第一款 權利法案的擴張

於 1787 年通過的美國憲法本文共有七個條文，其中並未規定人民的基本權利，對於人民的權利雖然規定有禁止人身保護令狀特權之終止、禁止公權剝奪法案與追溯既往法律之通過[4]，以及除彈劾案外一切的罪案應以陪審團審判之[5]等侷限性的保障，依然招致不少的批評。

關於人民基本權利的保障後續係分階段以憲法修正案的條文加以規定，憲法修正案的條文視爲憲法的一部份，具有憲法的效力，首先於 1791 年將人民重要的權利一一的列舉共有十個條文，經各州議會之認可而生效，這十條增修條文被稱爲「權利法案」(Bill of Rights)。權利法案的效力最初僅適用於聯邦政府，並不及於聯邦以外的州政府與地方

[1] 陳起行，資訊隱私權法理探討—以美國法爲中心，政大法學評論，64 期，2000 年 12 月，頁 298。
[2] 陳起行，資訊隱私權法理探討—以美國法爲中心，頁 309。
[3] 陳信郎，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，2004 年，頁 16。
[4] 請參照美國憲法第一條第九項條文。
[5] 請參照美國憲法第三條第二項條文。

政府[6]，之後透過聯邦最高法院的判決才逐漸的擴張其適用範圍至各州。

南北戰爭後於 1856-1870 年間陸續增修的第十三條、第十四條與第十五條，從實體及程序上全面地保障了人民的自由權利，也彌補了「權利法案」有名無實的缺憾，尤其是增修條文第十四條第一項所明定之「正當法律程序」(Due Process of Law)與「平等保護」(Equal Protection of the Law)二法則，影響更是深遠，由於增修條文第十四條的制定，使聯邦法院可以審查各州之立法與行政行爲，依據該「正當法律程序」條款可以審查州議會所制定的法律是否符合實質性正當程序(Substantive Due Process)，以及州政府所行使的行政行爲是否違背程序性正當程序[7](Procedural Due Process)。

1925 年 Gitlow v. New York[8]一案中開啓了將第一增修條文中所保障的言論自由併入第十四增修條文中「自由」的內涵解釋的序頁，自此憲法的爭論出現是否「權利法案」之全部內容均應併入憲法增修條文第十四條而一體適用於各州，聯邦最高法院在 Palko v. Connecticut[9]一案中，由 Cardozo 大法官所提出的「選擇性合併原則」(Doctrine of Selective Incorporation)，主張將「權利法案」中具有基本重要性的部分，應選擇性地併入第十四增修條文第一項「正當法律程序」之內容[10]。至 1970 年，第十四增修條文已經吸收了大部分的「權利法案」內容，因此使得聯邦最高法院有權複查案件，有權建立指導各州、各地方以及聯邦政府的行爲標準[11]，「權利法案」的保障擴及於各州政府與人民，成爲各州應遵守的本國最高法律[12](the Supreme Law of the Land)。

「權利法案」對於人民的基本權利分別以列舉與概括式條文的方式呈現[13]，隱私權的文字雖未直接記載在憲法的條文之中，因爲隱私權所蘊含自我決定的權限被認爲是包括在「自由」的概念之中可以免於國家力量無理的干擾，因此學者認爲增修條文第十四

---

[6] Barron v. Baltimore, 32 U.S. 243 (1833)。在該案中巴隆(Barron)控告市政府，由於市政府的道路建築工程改變了巴爾的摩港附近的水流，致使他所經營的巴爾的摩港淤積了大量的泥沙，許多的船隻由於水深不夠無法停靠因而遭受損失，於是訴請地方法院判決賠償。地方法院基於市政府違反憲法增修條文第五條「非有相當賠償，不得將私產徵爲公用」的規定，判決市政府應賠償 45,000 元，後遭上訴法院所否定。巴隆向聯邦最高法院提起上訴，遭到聯邦最高法院以對此無管轄權爲理由，駁回。Marshall 首席大法官所表示的法院意見認爲，憲法增修條文第五條的賠償條款，其立法意旨在對聯邦政府的權利有所限制，並不適用於各州的立法，所以州行爲與憲法並無衝突。節錄自陸潤康，美國聯邦憲法論，文笙，1993 年，頁 325-326。

[7] 史慶璞，美國憲法與政府權力，三民，2001 年，頁 68。

[8] Gitlow v. New York, 268 U.S. 652 (1925)。聯邦最高法院在該判決中指出，言論與出版自由，受到憲法第一增修條文的保護，國會不得予以剝奪，受憲法第十四增修條文正當法律程序條款的保護，是各州不得予以損害的個人基本權利與自由。

[9] Palko v. Connecticut, 302 U.S. 319 (1937)。

[10] 史慶璞，美國憲法與政府權力，頁 70。

[11] Corwin, Edward S. & Peltason, J. W.，美國憲法釋義(Understand the Constitution)，廖天美編譯，結構群，1992 年，頁 203。

[12] 史慶璞，美國憲法與政府權力，頁 68。

[13] 美國憲法增修條文第一條至第八條爲列舉式的權利，第九條與第十條是概括式的權利。

條的「正當法律程序」也保障了美國人民的隱私權，在 1965 年以前，美國聯邦最高法院的見解認爲，人民的隱私權來自於增修條文第一、三、四、五、九條交相適用的結果，到了 1973 年，聯邦最高法院才直接了當的說，隱私權是增修條文第九條[14]所謂保留給人民的權利，因而有增修條文第十四條正當法律程序的適用[15]。

第二款 資訊隱私權

隱私權應該予以保護的觀念最早始於 1890 年 Warren 與 Brandeis 發表於哈佛法學評論關於隱私權(The Right to Privacy)的論文中，作者將隱私權界定爲「生活的權利」(the right to life)和「不受干擾的權利」(the right to be let alone)，並指出在普通法上已經保護個人決定其思想、情緒與感受(thoughts, emotions, and sensations)在什麼範圍之內傳達給他人，即使傳達給他人之後，個人仍保留限制這些思想、情緒與感受對公眾公開的程度，這些保護並非基於私人財產應受保障，而是基於人格的不可侵犯(an inviolate personality)，因此心靈的平靜(peace of mind)才是保護的焦點[16]。作者於文中主張隱私權應受刑法的保護，對於隱私權受到的侵害可以採取損害賠償與禁制命令的方式加以救濟，但是在涉及公共利益或一般利益時、依據法律有傳播的權利時、口頭散布而未造成特定的損害時、由本人或經其同意而散布時，對隱私權的保護必須加以限制[17]。

美國聯邦最高法院對隱私權的討論起源於有關婚姻生活、避孕與墮胎相關的爭議，1961 年在 Poe v. Ullman[18]一案中，多數大法官的意見認爲 Connecticut 州禁止避孕物使用的法律並不構成司法上的爭點，該州政府並無意強求執行此項規定，因此並不違憲，但是 Harlan 大法官的不同意見書指出，該州的此項法律違反了正當法律程序，侵犯了已婚者的婚姻隱私權，因爲對使用避孕物者加以追究，必然會涉及夫妻之間的親密關係，而夫妻之間的親密關係，當然涉及隱私權[19]。

Harlan 大法官在 Poe 一案中不同意見的主張，在 1965 年 Griswold v. Connecticut[20]一案中成爲法院的多數意見，在 Douglas 大法官主筆的法院意見中表示，有關 Connecticut 州法律禁止任何人使用藥物或其他儀器以達到避孕的目的，同時也禁止任

[14] 美國憲法增修條文第九條：「本憲法所列舉之各種權利，不得解釋爲否認或取消人民所保有之其他權利。」
[15] 陸潤康，美國聯邦憲法論，頁 331。
[16] Warren, Samuel D. & Brandeis, Louis D., The Right to Privacy, 4 Harv. L. Rev. 193 (1980)，轉引自陳起行，資訊隱私權法理探討—以美國法爲中心，頁 299。
[17] Warren, Samuel D. & Brandeis, Louis D., The Right to Privacy, 4 Harv. L. Rev. 193, 214-220 (1980).
[18] Poe v. Ullman, 367 U.S. 497 (1961)。
[19] 節錄自陸潤康，美國聯邦憲法論，頁 443。
[20] Griswold v. Connecticut, 381 U.S. 479 (1965)。

何人提供爲達成避孕目的的協助與諮詢，係對夫妻之間的親密生活，以及該夫妻與其醫生之間的信賴關係加以國家管制力量的介入[21]。

法院接著論述，第一增修條文揭示表達意見的自由；第三增修條文禁止軍隊於非戰時未經房屋所有權人的同意，駐紮在平民百姓的住家，是隱私權的另一個面向；第四增修條文明白肯認，人民有保護其身體、住所、文件與財物，抵抗不合理搜索與扣押的權利；第五增修條文的不自證己罪條款，允許人民創造一個政府不能強迫其放棄以對自己造成不利的隱私領域；第九增修條文提到，本憲法所列舉之各種權利，不得解釋爲否認或取消人民所保有之其他權利；前述個別基本權所擔保(guarantee)的權利所散發出來以形成一個暈影(penumbra)區域，構成一個隱私領域(zone of privacy)[22]。

如同第四與第五增修條文在 Boyd v. United States[23]一案中，對人民住宅的聖潔與生活的隱私，提供對抗各種政府入侵的保護，以及在 Mapp v. Ohio[24]一案中，第四增修條文所創造出的隱私權，其重要性不亞於保留給人民的其他權利[25]。

本案係關於架構在憲法所擔保之權利所創造出的隱私領域上的關係，亦即婚姻關係中的隱私，以及關於禁止使用，而非管制生產與銷售避孕物的法律，爲了達成該項目的所採用的方法將會對該關係產生破壞性的衝擊，這樣的法律掃蕩太過寬廣以至於侵犯了受到保護的自由區域，因此認定 Connecticut 州的該項法律違憲[26]。

在 Griswold 案之後，聯邦最高法院以及聯邦與州之下級法院，在解決涉及隱私權爭議案件時都會援引「權利法案」中第九增修條文與其他增修條文的協助，成爲這個時期法院處理隱私權爭議的特點[27]，直到聯邦最高法院在 Eisenstadt v. Baird[28]一案中依據第十四增修條文中「平等保護」原則，宣告 Massachusetts 州禁止對已婚夫婦以外之人出售避孕物的法律違憲，此後對隱私權的討論開始進入第十四增修條文的正當法律程序

---

[21] 林建中，隱私權概念之再思考—關於概念範圍、定義及權利形成方法，國立台灣大學法律研究所碩士論文，1999 年 1 月，頁 23-25。

[22] Griswold v. Connecticut, 381 U.S. 479, 484 (1965)。

[23] Boyd v. United States, 116 U.S. 616, 630 (1886)。

[24] Mapp v. Ohio, 367 U.S. 643, 656 (1961)。

[25] Griswold v. Connecticut, 381 U.S. 479, 484-485 (1965)。

[26] Griswold v. Connecticut, 381 U.S. 479, 485 (1965)。

[27] Corwin, Edward S.，美國憲法(The Constitution and What It Means Today)，Chase, Harold W. & Ducat, Craig R.修訂，王震南譯，陽明管理發展中心，1992 年 5 月，頁 538。

[28] Eisenstadt v. Baird, 405 U.S. 438 (1972)，該判決理由不採隱私權係存在於某一種關係之固有立場，在 Brennan 大法官所主筆的法院意見中表示，在適用第十四增修條文的「平等保護」原則時，並不反對州政府對不同的族群可以施以不同的對待的權力，但是反對違背法律規範目的的差別待遇，因此具有相同處境的人民必須被施以相同的對待。Massachusetts 州的該項禁止未婚婦女使用避孕物的法律，並無法對已婚與未婚婦女必須被施以不同的對待提出合理的解釋。依據 Griswold 案的精神，不能禁止已婚婦女使用避孕物，因此禁止未婚婦女使用避孕物亦將是不可行。Griswold 案討論存在婚姻關係中的隱私權，然而已婚的夫婦不是具有思想與軀體的單獨個體，而是兩個分別具有思想與情感個體的結合，隱私權就是個人不論已婚或單身，有免於政府介入干擾影響是否決定懷孕的權利。

條款。

在 Roe v. Wade[29]一案中，Blackmun 大法官所主筆的法院意見表示，憲法並未明白地提及任何的隱私權，在相關的一系列判決中，聯邦最高法院肯認的個人隱私權或者所擔保的隱私領域，確實存在憲法之中。在不同的判決中，法院以及個別的法官在第一、四、五、九增修條文、在權利法案所形成的暈影中，或是在第十四增修條文所擔保的自由的概念中，發現了隱私權的根據[30]。這些判決闡明只有當被認爲是「基本的」(fundamental)或是「蘊含在有秩序的自由的概念中」(implicit in the concept of ordered liberty)的個人權利，才能包括在被擔保的個人隱私之中，而這樣的隱私權可以擴展至婚姻、生產、避孕、家庭關係以及孩子教養的決定[31]。

法院進一步論述，隱私權的依據不論是在我們所認爲的第十四增修條文個人自由權利的概念以及限制州的行爲，或是地方法院認爲是第九增修條文保留給人民的權利，將足以包括婦女是否終止懷孕的決定，但是這樣的權利並不是絕對的，在涉及墮胎法律合憲性的爭議中，從聯邦至州法院各有不同的意見，卻也達成一致的結論，也就是隱私權足以包括婦女是否終止懷孕的決定在內，但是該項權利並不是絕對的，當州對於保障健康、保持醫療水準與保護未出生的生命有重大迫切的利益(compelling state interest)時，可以對該項權利有所限制[32]。

本案中，Texas 州法律規定只有當懷孕婦女面臨生命危險，爲拯救生命的唯一目的之外，禁止實施墮胎手術，而沒有考慮懷孕各個期間胎兒脫離母體存活的機會，與該法律保護未出生生命的迫切利益不符，已經違反第十四增修條文正當法律程序條款，因此宣告該項法律違憲[33]。

由以上的案例可知，聯邦最高法院對隱私權保障的討論，集中在是否係憲法上所稱的基本性權利以及其形成的法源依據，由早期的權利法案所形成的暈影理論出發，進展到凡符合有秩序的自由這個概念，均應依第十四增修條文的正當法律程序條款加以保障，在各個階段擔負起對權利法案中非列舉基本權利保障的責任[34]，這些案例的討論也都針對隱私權在自主性與自我決定權這個面向的保障。

部分聯邦最高法院大法官的主張傾向於將自由與隱私有所區隔，而有不同的憲法保障依據。White 與 Harlan 兩位大法官在 Griswold 案的協同意見書中，明白指出本案所

[29] Roe v. Wade, 410 U.S. 113 (1973)。
[30] Roe v. Wade, 410 U.S. 113, 152 (1973)。
[31] Roe v. Wade, 410 U.S. 113, 152-153 (1973)。
[32] Roe v. Wade, 410 U.S. 113, 153-155 (1973)。
[33] Roe v. Wade, 410 U.S. 113, 163-164 (1973)。
[34] 陳信郎，資訊隱私權保障與網路犯罪通訊監察法制，頁 15。

涉及的是自由是否受到侵犯，應該是屬於第十四增修條文正當法律程序是否受到侵害的問題[35]。以及 Rehnquist 大法官在 Roe 案的不同意見書中，不同意多數意見的看法而認爲本案並不涉及隱私權，指出隱私這個字的一般用法並不包括墮胎的決定在內，本案所決定的隱私與第四增修條文所保障免於搜索與扣押的自由有很大的距離[36]。

關於隱私權的面向學界的見解可約分爲二，狹義的詮釋認爲 Roe 案並不涉及隱私的問題，如同 Rehnquist 大法官於反對意見書中所持的見解，廣義說則認爲 Roe 案所涉及的個人重大決定，亦屬於隱私的意義所及[37]。

Parent 教授認爲美國聯邦最高法院在 Griswold 與 Roe 案中，混淆了自由與隱私的概念，因爲自由正是免於外在的限制，前述兩個案件所侵害的是人民的自由而非隱私，有別於憲法第十四增修條文正當程序所保障的自由，憲法所保障的隱私則是第四增修條文免於不合理的搜索與扣押的預設，而隱私也應該是憲法第一增修條文所保障各項自由的限制，例如新聞自由應受個人隱私的節制[38]。

歸納現今隱私權的範圍與內容包括以下二大部分[39]：

1、個人針對其相關資訊予以保密或限制傳播的權限：包括對個人資料的保護，例如個人的身體完整性、影像、聲音、過去經歷、醫療紀錄、醫療關係、財務資料、人事資料的保護；以及對個人通訊內容的保護，例如郵件、通話的保護。

2、個人對其私密空間的自我決定權限：包括生育自主權限，例如避孕、終止懷孕、懷孕與生育、強制絕育的權限；家庭自主權限，例如子女教養、結婚與離婚、家庭關係的權限；個人自主權限，例如性偏好、藥物使用、個人形象、姓名、自殺及安樂死的權限。

其中就個人針對其相關資訊予以保密或限制傳播的權限，有學者將之定義爲資訊隱私權[40](the right to information privacy)，早期資訊傳播的途徑必須倚賴口耳相傳與紙張，隨著電腦與網路科技的進步，能夠承載訊息的不再只有紙張，而有可以儲存電子、磁性與光學等信號，我國刑法將這類信號的儲存定義爲電磁紀錄，這類信號型態的儲存媒體(例如，硬式磁碟、軟式磁碟與光碟)，資訊的傳遞也不再只是侷限於傳遞口語的電話，而有藉由無線電波、光波與各種網路應用服務經由網路傳遞的封包所攜帶的資訊。今日資

[35] 陳起行，資訊隱私權法理探討—以美國法爲中心，頁 312。
[36] Roe v. Wade, 410 U.S. 113, 172 (1973)。
[37] 陳起行，資訊隱私權法理探討—以美國法爲中心，頁 311。
[38] 陳起行，資訊隱私權法理探討—以美國法爲中心，頁 312。
[39] 陳信郎，資訊隱私權保障與網路犯罪通訊監察法制，頁 17。
[40] Volokh, Eugene, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You, 52 Stan. L. Rev. 1049 (2000), 1050-1051. “[T]he right to information privacy - my right to control your communication of personally identifiable information about me - is a right to have the government stop you from speaking about me.”。

訊隱私權的內容以其狀態來區分可以包括二個部分[41]：就靜態而言，是指對個人已儲存資料的保護，就動態而言，是指對通訊過程中通訊內容的保護。這也是在網路犯罪刑事偵查的階段，蒐集犯罪證據與發現行爲人身分的過程中，最常碰觸的將是這類與個人相關的資訊。對於資訊隱私權的保障有聯邦最高法院針對第四增修條文所做的一系列判決，以及爲了讓以電子形式儲存的資料、檔案受到完善的保障與享有隱私，美國國會在二十世紀後期又通過了相關的法案，其中包括電子通訊隱私法、通訊輔助偵查法以及在 2001 年通過的愛國者法案[42]。

1977 年的 Whalen v. Roe[43]一案，是聯邦最高法院就資訊隱私權所做出最直接的判決。本案涉及 1972 年紐約州所通過的藥物控制法(New York State Controlled Substances Act of 1972)，該法爲加強控制同時流通於合法市場與非法市場的藥物，規定所有關於第二類最危險藥物的處方，應當用紐約州特別印製的官方表格(official form)。官方表格要求載明開具處方的醫師、提供該藥物的藥局、藥物名稱及劑量，以及病人的姓名、地址及年齡。這些資料一份將交給紐約州健康部門，該部門將這些資料輸入電腦處理。所有的表格資料保存五年，有確保其安全的保全系統，五年後該些表格資料將會被銷毀。病人資料禁止公開，且只有有限的州健康部門官員或調查人員能接觸這些資料。上述規定引起一些病人與醫生的反對，認爲 1972 年藥物控制法追蹤接受第二類最危險藥物病人的規定違憲。聯邦地方法院基於「醫師與病人關係是憲法保障的隱私權範圍所及」以及該範圍確因本法對於第二類藥物所採取「不必要且過於廣泛」的病人追蹤規定所侵害，而判決禁止受原告質疑的條款的執行[44]。

聯邦最高法院推翻這項地方法院的判決，由 Stevens 大法官所主筆的法院意見，從三個方面提出其推翻聯邦地方法院判決的理由[45]。

首先，針對聯邦地方法院指出紐約州在新法實施 20 個月之後，不能由其經驗證實追蹤病人身分的必要。Stevens 大法官指出，在 Lochner[46]案時期，這項認定本身便足以宣告法律無效。但 Lochner 一案已被推翻，新法是一項有秩序、有理性的立法決定，並且是經由特別任命的委員會經過長期聽證並參考其他州的經驗之後所做的建議。提供病人身分的要求(the patient-identification requirement)可能有助於降低危險藥物誤用法律的執行，是一項合理的假設。這項要求能合理地期待嚇阻可能的違法者，並有助於偵

[41] 陳信郎，資訊隱私權保障與網路犯罪通訊監察法制，頁 18。
[42] 法思齊，美國法上數位證據之取得與保存，東吳法律學報 ，22 卷 3 期，2011 年 1 月，頁 119。
[43] Whalen v. Roe, 429 U.S. 589 (1977)。
[44] 陳起行，資訊隱私權法理探討—以美國法爲中心，頁 316-317。
[45] 陳起行，資訊隱私權法理探討—以美國法爲中心，頁 317。
[46] Lochner v. New York, 198 U.S. 45 (1905)。

測具體的濫用事例。至少，州控制危險藥物散佈的重要利益能支持實驗一項新的控制方式的決定，若實驗失敗，州可以經由立法程序停止這項實驗。聯邦地方法院基於州未能提出提供病人身分要求的必要性而判定新法違憲的理由，並不充分[47]。

第二，針對原告病人指出新法侵犯其憲法保障的隱私範圍(zone of privacy)，其中包括，避免公開個人事物的個人利益與獨立做出某種重要決定的利益，Stevens 大法官認爲就公開的個人資訊而言，可能揭露處方上資訊的人有醫生、藥局或病人本身，這與新法實施之前並無不同。所不同者，是新法使健康部門員工有接觸的權利，但沒有任何經驗可以證明有不當揭露的事實，無論是新法執行期間，或是加州與伊利諾州實施這項制度的期間，因此，將這些資訊揭露於州健康部門，並不足以自動構成對個人隱私之侵害。另外，新法並未阻止大眾接觸這些藥物，病人獨立決定的權利也未受阻，在合法的藥量之內，藥物的使用完全由醫師與病人決定，故不會有原告主張可能影響病人就診決定的情形發生。至於原告中部分醫師的主張，法院認爲與病人並無不同，前述判決理由於醫生亦有適用[48]。

最後，Stevens 大法官指出，現代政府行政每每需要電腦處理大量的個人資訊；相對地，對於政府防範個人資訊不當地揭露也是法律上重要的一環。本案由於所涉及的州政府在個人資料的處理上展現了對於個人資料適當的保護，因此沒有必要決定無理揭露(unwarranted disclosure)的問題。本案判決僅指出本案的事實不足以構成侵害第十四增修條文對於任何權利或自由的保護[49]。

雖然憲法對於基本權的保障可以對抗國家行爲，但是各個基本權的絕對性並不相同，基本權的相對性將藉由迫切的重大利益的出現而浮現。由本案的結果可以得知，資訊隱私所受到的保障係相對的，往往在與其他相較的公共利益平衡之下，必須退居其次[50]。

New York 州的該項法律因爲對所蒐集的個人資料有周全的保護措施，而可以通過第十四增修條文的檢驗，然而新科技的引進也帶來些許的隱憂。Brennan 大法官在協同意見書中表示，雖然州政府主張新科技的使用幫助政府的運作更有效率，但是第四增修條文不只規範政府資訊蒐集的類型，也規範資訊蒐集的方法，將資料加以電腦化後集中

[47] 陳起行，資訊隱私權法理探討—以美國法爲中心，頁 318。
[48] 陳起行，資訊隱私權法理探討—以美國法爲中心，頁 318-319。
[49] 陳起行，資訊隱私權法理探討—以美國法爲中心，頁 319。
[50] 陳起行，資訊隱私權法理探討—以美國法爲中心，頁 322。如同 Douglas 大法官在 Roe 案協同意見書中指出，受美國憲法第一增修條文所保護的自由是絕對的，其他基本權的保障，則受有限制，就隱私而言，除了個人在家中受憲法的高度保障外，資訊隱私所受到的保障係相對的，往往在與其他相較的公共利益平衡之下，必須退居其次。

儲存以及使其易於存取，將潛在地增加該資訊被濫用的危險[51]。

第二項 憲法第四增修條文

美國憲法第四增修條文與「權利法案」中的第五、六與八增修條文共同組成刑事被告的「人權法案」，這組人權法案在當時以及多年之後相較於其法律發源地的英國相關法律，還是有顯著的進步[52]，第四增修條文的通過顯示在當時殖民地人民對於通用令狀(general warrants)的深惡痛絕[53]。

美國憲法第四增修條文[54]：「人民身體、住所、文件及財產免於不合理搜索及扣押的權利不得違背；搜索票或拘票，除本於相當理由，並經宣示或代誓宣言，且特別指明被搜索之處所及被扣押的人或物外，不應簽發。」

普通法中的侵權行爲法用以規範私人的入侵行爲，憲法第四增修條文前段保障人民身體、住所、文件及財產免於不合理搜索及扣押的權利，係指只有涉及政府行爲才有第四增修條文的適用。聯邦最高法院在 Burdeau v. McDowell[55]一案中表示，第四增修條文提供抵抗不合法搜索與扣押的保護僅適用於政府行爲(governmental action)，由該條文的起源與歷史明白顯示，其目的是用來節制國家權力(sovereign authority)的活動，以確保人民享有住居與持有財產不受干擾的權利，該限制並不及於政府機關[56]以外的單位。

即使政府沒有親自參與搜索行爲，私人搜索在一些情形仍然有第四增修條文的適用，亦即私人搜索是基於政府的指示或與政府人員共同進行[57]、或是私人搜索之後政府人員的搜索行爲超越先前私人搜索的範圍[58]、抑或是非屬於執法人員的政府人員所爲之搜索[59]，本文將於本章第三節第一項第四款私人搜索中，進一步論述。

基於第四增修條文是對於人民隱私保障的預設，對於搜索的定義也隨著科技的進步而有所不同，在以保護財產權爲主的年代，搜索被定義爲執法人員進入人民財產權所管領的一特定空間之中，以親眼目擊的方式蒐集證據，因爲其在該空間的所見所聞將在法

---

[51] Whalen v. Roe, 429 U.S. 589, 607 (1977)。

[52] Corwin, Edward S.，美國憲法，頁 451。

[53] Corwin, Edward S.，美國憲法，頁 421。

[54] 原文：The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.；轉引自，楊竹生，論美國憲法第四修正案所述搜索與扣押，中原財經法學，第 1 期，1995 年 6 月，頁 111。

[55] Burdeau v. McDowell, 256 U.S. 465, 475 (1921)。

[56] 此處的政府機關應該是指在刑事訴訟程序中，具有犯罪偵查功能的單位，以與行政機關中上級對下級的行政搜索有所區別。

[57] Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602 (1989)。

[58] United States v. Jacobsen, 466 U.S. 109 (1984)。

[59] New Jersey v. T. L. O., 469 U.S. 325 (1985)。

庭上做出證詞，藉由限制執法人員可以進入的空間將可以限制證據蒐集的範圍，在電子資訊時代所進行的電話監聽，雖然沒有物理入侵受監聽對象的住家範圍或辦公室，但是已經侵犯了受監聽對象對於通話內容的合理隱私期待，而被認爲是搜索行爲的一種[60]。從實務發展的脈絡觀察，憲法第四增修條文的適用最早是從財產權保護的觀點出發，進展到對於合理隱私期待的保護，以及將面臨隨著科技的進步偵查輔助設備的大量被採用，對第四增修條文所帶來的挑戰。

第一款 物理入侵

17 世紀的英國普通法有一句著名的法諺“an Englishman's home is his castle”，即在表彰個人的家是一個不可侵犯的神聖空間，基於保護家園的安全可以擊退入侵者，以確保生活上的平靜與財產上的安全。美國聯邦最高法院早期對憲法第四增修條文的解讀，著重在對人民財產權的保護。

在 Boyd v. United States[61]一案中，Bradley 大法官所主筆的法院意見指出，憲法第五增修條文保障人民在刑事案件中有免於證明自己罪刑的權利，本案中檢察官要求被告提出帳冊與文件在法庭中供其檢視並將採爲定罪的證據，已經落入第五增修條文所禁止的範圍。法院進一步表示，憲法第四與第五增修條文都是有關人民的人身安全，兩者關係密切而且相互投射光影[62]，第五增修條文禁止強迫人民提出對自己不利的證據以證明自己的罪行，而該證據也就是第四增修條文所指的不合理搜索與扣押的標的，並不需要真正的入侵房宅[63](actual entry upon premises)才有第四增修條文意義下的不合理搜索與扣押，在刑事案件中強迫被告提出對其人身或財產不利的帳冊與文件，已經有搜索與扣押的本質與精神且已相當達成其目的[64]，因此有憲法第四增修條文的適用。

在 Boyd 一案之後，法院皆以政府是否物理入侵憲法所保障的區域(a constitutionally protected area)，作爲判斷是否構成搜索的標準，該區域的範圍依據聯邦最高法院的解釋，即憲法第四增修條文中所提到的「人民身體、住所、文件及財產[65]。」

---

[60] Kerr, Orin S., Digital Evidence and the New Criminal Procedure, 105 Colum. L. Rev. 279, 290 (2005).

[61] Boyd v. United States, 116 U.S. 616 (1886)。

[62] Boyd v. United States, 116 U.S. 616, 633 (1886)。Bradley 大法官所稱相互投射光影是指，第四增修條文所禁止的不合理搜索與扣押，通常是爲了取得第五增修條文所禁止的強迫人民提出對自己不利的證據；第五增修條文所禁止的強迫人民證明自己的罪行，也將對什麼才是第四增修條文意義下的不合理搜索與扣押這個問題投射光影。使用不合理扣押的帳冊與文件來證明一個人的犯罪與強迫人民證明自己有罪，兩者之間法院不認爲有所差別。

[63] Boyd v. United States, 116 U.S. 616, syllabus (1886)。

[64] Boyd v. United States, 116 U.S. 616, 635 (1886)。

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

在 Olmstead v. United States[66]一案中，四個聯邦官員在調查走私烈酒的過程中，在上訴人 Olmstead 辦公室所在大樓的地下室以及在其他共犯住家外的街道上裝設竊聽器，法院採用其所蒐集到的通話內容作爲定罪的證據，上訴人主張以竊聽的方式蒐集通話內容並在法庭上採爲證據，同時違反其受憲法第四與第五增修條文[67]所保障的權利，Taft 首席大法官所主筆的法院意見中表示，除非對被告的身體所爲之搜索與逮捕，或是扣押其文件或是其有體財產，或是爲了扣押的目的而物理入侵(physical invasion)其住所之外，將不構成對憲法第四增修條文的違反，因此，法院認爲本案中竊聽裝置的使用並不構成憲法第四增修條文意義下之搜索與扣押行爲[68]。

Brandeis 大法官於本案的不同意見書中，引用聯邦最高法院在 Ex parte Jackson[69]一案中，認爲封緘的信件受有憲法第四增修條文保護的看法，認爲本案私人間電話談話內容本質上與封緘的信件並無不同，附隨於侵犯電話隱私的邪惡更甚於毀壞郵件的封緘，電話一旦遭到竊聽，電話線兩端通話者的隱私已經被侵犯，就刺探的方法而言，往昔被統治者採爲工具的援助令狀與空白搜索票，與現今的監聽相比就顯得微不足道[70]。

回顧權利法案的制定過程，制憲者肯認人民心靈、情感與思維的重要性，藉由憲法的制定著手營造一個適合追求幸福的環境，該些增修條文所擔保的有較廣的保護範圍，以尋求保護美國人民的信仰、思想與情感，他們賦予人民獨處的權利，政府任何對個人隱私不正當的入侵，不論其所採用的方法，必須被視爲違反憲法第四增修條文，將違反第四增修條文所取得的證據用於刑事訴訟程序上，必須被視爲違反憲法第五增修條文[71]。因此，藉由憲法第四與第五增修條文中特定的語言，以提供對抗政府入侵人民住家的聖潔與生活的隱私的保護[72]。

Brandeis 大法官接著論述，法律與憲法的制定都是爲了防制過去所發生的罪惡，但是對法律與憲法的解讀不應只侷限於過去所發生過的態樣，時間帶來改變，隨著新的情況與目的的出現，必須藉由更廣的適用才能賦予憲法原則的生命力，而擔保個人權利以對抗政府權力濫用的條文，也必須要有相同的適應能力以面對一改變中的世界[73]。在憲

[66] Olmstead v. United States, 277 U.S. 438 (1928)。
[67] Olmstead v. United States, 277 U.S. 438, 462 (1928)。法院認爲本案沒有適用憲法第五增修條文的空間，除非第四增修條文先被違反。法院進一步論述，沒有證據顯示被告在電話中的通話內容是被強迫的，該些被告持續與自願地透過電話進行交易，只是不知道有竊聽行爲的存在，因此本案必須將討論限制在第四增修條文。
[68] Olmstead v. United States, 277 U.S. 438, 466 (1928)。
[69] Ex parte Jackson, 96 U.S. 727 (1878)。
[70] Olmstead v. United States, 277 U.S. 438, 475-476 (1928)。
[71] Olmstead v. United States, 277 U.S. 438, 478-479 (1928)。
[72] Olmstead v. United States, 277 U.S. 438, 473 (1928)。
[73] Olmstead v. United States, 277 U.S. 438, 472-473 (1928)。

法的應用上，我們的思考不能只是侷限在過去曾經是什麼(what has been)，而是將來可能有什麼(what may be)，科技的進步對於政府刺探方法的協助將不會僅止於監聽[74]，藉由更精良的方法將有可能將人民在密室內的竊竊私語揭露於法庭之上[75]。

Brandeis 大法官於本案的不同意見與 40 年前的隱私權論述，強調人格不可侵犯的神聖目標脈絡依然一致，只是從普通法侵權行爲法下個人隱私免於新聞媒體的挖掘報導，擴展到免於政府監聽的憲法第四增修條文意義之下[76]。

類似的政府監聽案件在 Silverman v. United States[77]一案中，因爲有了稍微的物理入侵，而有不同的結果。警察在與上訴人 Silverman 住家只有一牆之隔的隔壁空屋，將竊聽器釘入牆內直到與上訴人住家的暖氣管接觸，此時上訴人家中的整個暖氣系統即被轉換成爲聲音收集器，上訴人在家中的對話內容將透過該釘牆式麥克風爲警察所知悉，法院認爲暖氣系統是住家的一部分，警察的行爲已經物理入侵憲法所保障的區域[78]，而構成憲法第四增修條文意義下的搜索行爲。法院的論述並未針對屋內的對話內容是否受有憲法第四增修條文的保護加以討論，認爲若是貼著牆壁竊聽一牆之隔另一屋內的對話，則不構成憲法第四增修條文意義下的搜索行爲[79]。

當時聯邦最高法院的見解認爲，只有對人民財產權所管領的空間的物理入侵，才構成搜索行爲。依據那個時期聯邦最高法院對憲法第四增修條文文義的解讀，憲法所保障的區域並不包括電話的通話內容[80]以及在屋內的對話內容。

第二款 合理隱私期待

政府的行爲是否構成憲法第四增修條文意義下的搜索行爲，早期是以是否有物理入侵以財產權保護的觀念所構築的憲法保障區域爲判斷，這個判斷依據直到 1967 年 Katz v. United States[81]一案，才被聯邦最高法院所摒棄。

聯邦調查局探員在上訴人 Katz 於街上所使用的共用電話亭外裝設竊聽器以蒐集上訴人的通話內容，Stewart 大法官所主筆的法院意見表示，第四增修條文保護的是人(people)而不是場所(place)，當一個人有意識地暴露在公眾之前，即使是在他的住家或辦公室，將不受憲法第四增修條文的保護，然而當一個人尋求保持隱私，即使是在公眾

[74] Olmstead v. United States, 277 U.S. 438, 474 (1928)。
[75] Olmstead v. United States, 277 U.S. 438, 473 (1928)。
[76] 陳起行，資訊隱私權法理探討—以美國法爲中心，頁 301。
[77] Silverman v. United States, 365 U.S. 505 (1961)。
[78] Silverman v. United States, 365 U.S. 505, 506-507, 510-511 (1961)。
[79] Silverman v. United States, 365 U.S. 505, 510 (1961)。
[80] Olmstead v. United States, 277 U.S. 438, 472 (1928)。
[81] Katz v. United States, 389 U.S. 347 (1967)。

可任意進出的地方，也將受到憲法的保護[82]。上訴人進入透明玻璃的電話亭，他所要排除的並不是不讓別人看到他在裡面做什麼，而是不讓別人聽到他在講什麼，他所享有保持通話隱私的權利，並不因爲他的一舉一動可以在電話亭外被看得一清二楚而有所退讓，因此，一個人在電話亭的通話內容可以享有憲法第四增修條文的保護[83]。法院同時也宣告過去所依據的入侵原則(the trespass doctrine)不再適用[84]。

Harlan 大法官的協同意見，是以財產權的觀點出發但是引進了對於合理隱私期待(reasonable expectation of privacy)保護的概念，認爲一關起門的電話亭就如同一個人的住家，已不再是一個開放區域，即使是短暫的佔領當時，身處其中之人享有受憲法保護的合理隱私期待，對該具有隱私意涵的空間的有形(物理)與無形(電子)入侵，已經構成憲法第四增修條文的違反[85]。

法院的多數意見指出憲法第四增修條文所保護的是人而非場所，揚棄了狹隘的物理入侵原則，進而採取合理隱私期待的判斷標準，但是場所並非從此就完全自外於判斷過程，Harlan 大法官所提出合理隱私期待的內容爲[86]：首先，必須要有主觀隱私期待的呈現，其次，這個隱私期待必須被社會認爲是合理的，因此受憲法第四增修條文保護的範圍，從早期的「人身、住所、文件及財產」等有形的區域擴展到無形的合理隱私期待所界定的區域。

自 Katz 案之後，合理隱私期待變成了判斷是否有憲法第四增修條文適用的標準。由以上的聯邦最高法院實務見解的演進可以得知，政府對於人民合理隱私期待的不合理侵犯即構成搜索行爲。

對於合理隱私期待的認定，並非主觀上有隱私期待的呈現即可達成，客觀上尚須有，這個隱私期待必須被社會認爲是合理的，這兩個要件缺一不可。

主張在開放地域(open field)的活動具有隱私期待通常是被認爲不合理的，在 Oliver v. United States[87]一案中，被告將大麻種植在隱密的區域、架設阻隔的圍籬並豎立禁止入侵(No Trespassing)的警告牌，在主觀上呈現有隱私的期待，法院認爲，如同在開放地域的農耕活動一樣，保護在開放地域的活動的隱私並不具有社會利益[88]，只有環繞住家與住宅緊密連接的土地，才能被視爲住宅的一部分而受有憲法第四增修條文的保護，

[82] Katz v. United States, 389 U.S. 347, 351 (1967)。
[83] Katz v. United States, 389 U.S. 347, 352 (1967)。
[84] Katz v. United States, 389 U.S. 347, 353 (1967)。
[85] Katz v. United States, 389 U.S. 347, 360 (1967)。
[86] Katz v. United States, 389 U.S. 347, 361 (1967)。
[87] Oliver v. United States, 466 U.S. 170 (1984)。
[88] Oliver v. United States, 466 U.S. 170, 179 (1984)。

因爲在這樣的延伸土地上經常伴隨著人民住家的聖潔與生活的隱私的親密活動[89]。本案政府的行爲已經構成普通法下對人民土地的入侵，但並不構成憲法意義下的搜索，財產權的存在只是決定是否具有隱私期待正當性的一個因素而已[90]。

被丟棄的垃圾無法主張合理的隱私期待，在 California v. Greenwood[91]一案中，警察在被上訴人 Greenwood 放置在屋外等待被收集的垃圾中，找到毒品犯罪的證據，以此建立相當理由申請對被上訴人住家的搜索票，並在隨後的搜索行動中找到定罪的證據，被上訴人主張其等待收集的垃圾是以不透明的袋子包裝，在固定收集的時間前短暫的放置在街道上，在主觀上呈現有隱私的期待[92]，法院認爲，隱私期待不一定會受到憲法第四增修條文的保護，除非客觀上社會認爲該期待是合理的[93]，法院並引用在 Katz 一案中的見解，認爲一個人有意識地暴露在公眾之下，將不受到憲法第四增修條文的保護[94]，法院指出社會上普遍認爲，放置在街道旁的垃圾，很容易遭到動物、兒童、清道夫、偷窺者以及其他公眾的接觸，因此不具有合理的隱私期待[95]。

在非法入侵的室內或是乘坐於非自己擁有的汽車當中亦無合理的隱私期待，在 Rakas v. Illinois[96]一案中，上訴人 Rakas 涉及服飾店的搶案於乘坐在由汽車所有人駕駛的汽車逃逸途中，遭警方攔檢並於車內置物箱以及座位底下的空間，分別起出子彈與槍械，上訴人主張其係合法的出現在所乘坐的汽車之中，因此對該些區域具有合理的隱私期待，法院認爲上訴人對於遭搜索的汽車並沒有財產或持有上的利益，對於遭扣押的子彈與槍械亦無財產上的利益[97]，基於憲法第四增修條文所保障的是個人的權利，如同其他憲法權利一樣，不能被代位行使[98](vicariously asserted)。

法院進一步論述，一個人經由汽車所有人的同意而合法的出現在汽車之中，這個前提並不能唯一決定，對遭搜索的汽車中的特定區域是否具有正當的隱私期待，法院指出在過去很多的案例中顯示，在憲法第四增修條文的保護目的下，對於汽車的保護並不能完全等同於住宅，尤其是當上訴人只是一個乘客，如同乘客以乘客的資格不能主張對其所搭乘汽車的後行李箱具有正當的隱私期待[99]。類似於 Katz 案中對電話亭同樣不具有所

[89] Oliver v. United States, 466 U.S. 170, 180 (1984)。
[90] Oliver v. United States, 466 U.S. 170, 183 (1984)。
[91] California v. Greenwood, 486 U.S. 35 (1988)。
[92] California v. Greenwood, 486 U.S. 35, 39 (1988)。
[93] California v. Greenwood, 486 U.S. 35, 39-40 (1988)。
[94] California v. Greenwood, 486 U.S. 35, 41 (1988)。
[95] California v. Greenwood, 486 U.S. 35, 40 (1988)。
[96] Rakas v. Illinois, 439 U.S. 128 (1978)。
[97] Rakas v. Illinois, 439 U.S. 128, 130 (1978)。
[98] Rakas v. Illinois, 439 U.S. 128, 133-134 (1978)。
[99] Rakas v. Illinois, 439 U.S. 128, 148-149 (1978)。

有權，但是當一個人進入電話亭關起門以將他人排除在外，可以對通話內容具有正當的隱私期待，然而本案並未呈現在被搜索的部分與被扣押的證物具有這樣的隱私期待[100]。

第三款 科技設備的進步所帶來的衝擊

Brandeis 大法官在 Olmstead 案的不同意見書中，已經清楚的預告科技的進步將會對政府刺探人民的隱私提供更多的協助，也將對憲法所保障的人民基本權利帶來衝擊。聯邦最高法院在個案所建立的原理原則，將在這些科技設備出現的過程中再度受到檢驗。

早期是以不能有物理入侵的行爲劃設一條明確的紅線，任何逾越這個界線的行爲即是明顯的違法，在 Katz 案所建立的合理的隱私期待原則，擴大了憲法第四增修條文的保護範圍，但是必須要先決定什麼是社會所認可的合理的隱私期待，才能判定政府的行爲是否已經侵入這個受保護的領域。隨著科技的進步很自然地增進感官功能的設備因此被運用於偵查作爲之中，使得以旁敲側擊(beat around the bush)的方式刺探人民的隱私可以輕易達成，也因此與人民合理的隱私期待展開了一連串的攻防過程。

以緝毒犬嗅聞行李，不構成憲法第四增修條文意義下的搜索行爲，在 United States v. Place[101]一案中，被上訴人 Place 在機場遭到緝毒官員的攔阻，並以緝毒犬嗅聞被上訴人的行李以判斷是否藏有毒品，被上訴人主張此舉已經侵犯其對行李箱內容物的隱私期待，法院遵循憲法第四增修條文保護人民正當的隱私期待免於政府不合理的入侵的精神，肯認個人行李內容物的隱私利益受有第四增修條文的保護[102]。法院進一步論述，以緝毒犬嗅聞行李並不需要打開行李箱而且也不會暴露箱內其他非違禁品的物品，相較於傳統的開箱翻找搜索，有較小的侵入性也不會帶來困窘與不方便，以緝毒犬嗅聞只會揭露是否有毒品的存在這個有限的資訊，沒有其他的偵查方式可以如此同時限縮資訊的取得方式與所揭露的資訊內容，因此認定緝毒官員以緝毒犬嗅聞行李的行爲，並不構成憲法第四增修條文意義下的搜索行爲[103]。

從飛行在合法巡航高度的飛行物觀察地面目標區域，不構成憲法第四增修條文意義下的搜索行爲，在 California v. Ciraolo[104]一案中，警察接獲匿名線報指稱被上訴人 Ciraolo 住家的庭院種植大麻，受制於雙層圍繞的高聳圍牆無法從地面觀察，因而租用

[100] Rakas v. Illinois, 439 U.S. 128, 149 (1978)。
[101] United States v. Place, 462 U.S. 696 (1983)。
[102] United States v. Place, 462 U.S. 696, 606-607 (1983)。
[103] United States v. Place, 462 U.S. 696, 607 (1983)。
[104] California v. Ciraolo, 476 U.S. 207 (1986)。

私人飛機從空中鳥瞰，被上訴人主張在緊鄰住家的土地圍上雙層圍牆，顯示主觀上有保持隱私的期待，法院認爲儘管與住家緊鄰的土地一向被認爲受有隱私期待的保護[105]，但是憲法第四增修條文對住家的保護，並沒有要求執法人員在公路上經過人民的住家時必須遮蔽雙眼，儘管有障礙物的阻隔，執法人員依然有權找一個有利的觀察地點以清楚地觀察其內部的活動，本案的執法人員在合法的巡航高度下以肉眼清楚地辨認出地面上所種植的大麻，任何在相同高度下的其他飛機乘客同樣能觀察到相同的結果，因此法院認爲被上訴人這樣的隱私期待並不能被社會所接受[106]。

同樣是從空中觀察大麻種植的案例，在 Florida v. Riley[107]一案中，警察搭乘直昇機從被上訴人 Riley 住宅旁溫室屋頂的缺口觀察到大麻的種植，法院認爲本案仍然受 Ciraolo 案的結果所拘束[108]，指出直昇機飛行在聯邦飛行總署所允許的高度觀察地面的活動，被上訴人對於溫室內的活動沒有合理的隱私期待，除非，有觀察到與住家相關的親密細節或是不當的造成噪音、風、灰塵或是傷害的威脅[109]，將不構成憲法第四增修條文意義下的搜索行爲。

O'Connor 大法官在協同意見書中指出，法院多數意見對憲法第四增修條文保護範圍的解讀，太過仰賴於聯邦飛行安全法規，該法規是用來促進飛行的安全，而不是用來保障人民有免於不合理的搜索與扣押的權利[110]。對於人民合理的隱私期待的解讀，應該回歸到與 Katz 案一致，亦即本案警察所搭乘直昇機的飛行高度是否也是其他直昇機所經常採用，而使得社會認爲這樣的隱私期待並不合理[111]。

綜合以上兩個案例可以得知，警察搭乘飛行器從空中觀察人民的住宅，只有當同時符合，飛行在法令允許的高度、不會造成噪音與灰塵等侵權行爲法概念下的物理入侵以及不能觀察住家與庭院的親密活動這三個條件之下，才不構成憲法第四增修條文意義下的搜索行爲[112]。

若只單純檢測特定藥物的存在與否，不構成憲法第四增修條文意義下的搜索行爲，在 United States v. Jacobsen[113]一案中，聯邦快遞職員在檢視一個破損的包裹中發現有白色的不明粉末於是通知緝毒官員前來處理。法院認爲本案仍然受 Place 案的結果所拘

[105] California v. Ciraolo, 476 U.S. 207, 213 (1986)。
[106] California v. Ciraolo, 476 U.S. 207, 213, 214 (1986)。
[107] Florida v. Riley, 488 U.S. 445 (1989)。
[108] Florida v. Riley, 488 U.S. 445, 449 (1989)。
[109] Florida v. Riley, 488 U.S. 445, 452 (1989)。
[110] Florida v. Riley, 488 U.S. 445, 452 (1989)。
[111] Florida v. Riley, 488 U.S. 445, 454 (1989)。
[112] 王兆鵬，重新定義高科技時代下的搜索，頁 171。
[113] United States v. Jacobsen, 466 U.S. 109 (1984)。

束，指出緝毒官員在現場進行的化學方式檢測，只能顯示該白色粉末是否爲古柯鹼這個有限的資訊，並不會侵犯到其他的正當隱私期待[114]。與 Place 案的案例事實稍微有不同的是，本案的可疑白色粉末的取得是附隨於私人搜索行爲之後，因此緝毒官員取得該白色粉末並不構成憲法第四增修條文意義下的搜索行爲[115]。

若是藥物檢測的過程中能夠揭露過多的私人資訊，則將構成憲法第四增修條文意義下的搜索行爲，在 Skinner v. Railway Labor Executives' Ass'n[116]一案中，聯邦鐵路管理局要求涉及鐵路意外事故的員工必須要接受血液與尿液的檢查，以確定是否服用被禁止的酒精與藥物，法院認爲採集血液與尿液等生物樣本以及後續的化學檢測，不只能檢測酒精與藥物的存在，更能得知疾病等身體健康狀況，已經侵犯該員工的隱私期待，而構成憲法第四增修條文意義下的搜索行爲[117]。法院進一步論述，基於酒精與藥物的濫用是導致鐵路意外事故的主因，政府保障鐵路運輸安全的迫切利益更勝於員工的隱私利益，而認爲這樣的藥物檢測規定是合理的[118]。

使用紅外線熱能顯像儀以顯示在屋內人員的活動情況，將構成憲法第四增修條文意義下的搜索行爲，在 Kyllo v. United States[119]一案中，警察使用熱能顯像儀掃瞄上訴人 Kyllo 的住家，發現部分區域有異常的高溫反應，與在室內種植大麻必須採用密集的燈光照射所產生的溫度上升的情形相符，法院不同意被上訴人主張在屋外偵測房屋表面所散發的熱能不構成搜索行爲，認爲這樣的看法過於機械式解讀 Katz 案的精神，儘管本案執法人員所使用的設備只能粗略的顯示屋內溫度的差異情形，我們的考量必須延伸到可以清楚辨認屋內人員活動的這類更精良設備的出現，違背 Katz 案所揭示的精神，將會使得人民的隱私期待受到科技進步的宰制[120]。

法院進一步論述，憲法第四增修條文對住家的保護並不取決於從住家中所取得資訊的質或量的多寡，而是如同本法院許多的案例所揭示的精神，在家中所有的細節都是私密細節，整個區域是可以免於政府的刺探，藉由熱顯像儀的使用可以知道上訴人將家中的暖氣設定到幾度，也可以知道女主人每天晚上幾點鐘使用三溫暖設備，這些都是住家的細節也就是私密細節，本案中執法人員所使用的設備並非一般大眾所普遍使用，其所取得的住家中的資訊，在過去除非經由物理入侵否則無法得知，該監視行爲已經構成憲

[114] United States v. Jacobsen, 466 U.S. 109, 123 (1984)。
[115] United States v. Jacobsen, 466 U.S. 109, 119 (1984)。
[116] Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602 (1989)。
[117] Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 618 (1989)。
[118] Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 633 (1989)。
[119] Kyllo v. United States, 533 U.S. 27 (2001)。
[120] Kyllo v. United States, 533 U.S. 27, 35-36 (2001)。

法第四增修條文意義下的搜索行爲[121]。

將全球衛星定位系統(Global Position System，簡稱 GPS)追蹤裝置貼附於特定對象所駕駛的汽車以追蹤其行蹤，將構成憲法第四增修條文意義下的搜索行爲，在 United States v. Jones[122]一案中，執法人員在被上訴人 Jones 的汽車底盤安裝衛星定位系統以追蹤被上訴人的行蹤，上訴人主張安裝追蹤器的位置以及汽車係停靠於公共道路上，均處於公眾可目視的狀態，依據 Harlan 大法官在 Katz 案所建立的標準，並不構成搜索行爲[123]，法院指出從憲法第四增修條文的文字特別指明對「人身、住所、文件以及財產」的保護，顯示其與財產權的緊密關係[124]，直到 Katz 案所揭示的第四增修條文保護的是人而非場所，才偏離以財產權爲唯一的檢驗標準[125]，Katz 案建立財產權並不是衡量憲法第四增修條文違反的唯一標準的看法，但不因此排除第四增修條文對財產權的保護，法院強調 Katz 案的合理的隱私期待檢驗標準，是附加於而不是用來取代，普通法入侵原則的檢驗標準[126]。

上訴人並試圖援引在 Oliver 案中，對開放地域的入侵以蒐集資訊，即使已經構成普通法下的入侵行爲，仍不構成第四增修條文意義下的搜索行爲的見解，法院認爲本案停放在公共空間的汽車，仍屬於憲法意義下的財產，執法人員在汽車底盤安裝追蹤器，已經構成憲法第四增修條文意義下的搜索行爲[127]。

法院最後重申，其並未偏離行駛在公路上汽車的移動路徑並不具有合理的隱私期待，亦即單純的目視觀察並不構成憲法第四增修條文意義下的搜索行爲這樣的看法，並指出協同意見的看法將造成以 Katz 案的合理的隱私期待爲唯一的檢驗標準，法院在此採用的入侵原則並不是唯一的檢驗標準，而是希望提供對抗不合理搜索的最小程度的保護[128]。

本案雖然經過 9 位大法官一致同意判決的結論，但是說理的方式卻呈現 5：4 的分歧，多數意見爲了取得最後的結論，採取退回到 Katz 案之前的物理入侵原則檢驗標準，認爲上訴人在被上訴人汽車安裝追蹤裝置已經構成搜索行爲，少數意見堅持以 Katz 案之合理隱私期待爲唯一的檢驗標準，認爲短暫的追蹤一個人在公共街道的移動路徑並不構成搜索行爲，由於上訴人的追蹤時間過長而被認定構成搜索行爲。

---

121 Kyllo v. United States, 533 U.S. 27, 37-40 (2001)。
122 United States v. Jones, 132 S. Ct. 945 (2012)。
123 United States v. Jones, 132 S. Ct. 945, 950 (2012)。
124 United States v. Jones, 132 S. Ct. 945, 949 (2012)。
125 United States v. Jones, 132 S. Ct. 945, 950 (2012)。
126 United States v. Jones, 132 S. Ct. 945, 951-952 (2012)。
127 United States v. Jones, 132 S. Ct. 945, 953 (2012)。
128 United States v. Jones, 132 S. Ct. 945, 953 (2012)。

Scalia 大法官所主筆的法院意見指出，法院是要確保人民保有如憲法第四增修條文制定當時，相同程度的隱私保障以對抗政府[129]。這樣的見解呈現出法院面對科技進步對隱私保障所帶來的挑戰，而因應產生的平衡調整(equilibrium adjustment)措施，以取得警察權力與隱私保障之間的平衡。亦即當新科技的出現已經對警察權力的擴張或縮減帶來重大的改變時，法院相對地提高或降低憲法第四增修條文的保護程度，以企圖回復到該科技方法介入之前的平衡狀態，正如同在地形高低起伏的山區想要維持定速行駛，上坡時要加踩油門，下坡時要鬆開油門一般[130]。

本案依然存在許多的問題尚待解決，例如要持續追蹤多久才會轉變爲搜索行爲，少數意見並未畫出一條明確可供遵循的界線[131]，以及在 Katz 案之後物理入侵原則似已含括於合理隱私期待的概念之中，是否仍有獨立成爲一個檢驗標準的必要[132]。面對這許多的疑問法院意見僅就其中一部分加以論述，本案後續的發展仍值得持續的觀察。

科技始終來自於人性，科學技術的進步爲人類的生活帶來了便利，同時也嘉惠政府對人民隱私的刺探行爲。在地面上有圍籬阻隔的隱私期待，在經由飛機的協助所呈現的三度空間下，該隱私期待將不再成爲可能。經由掃瞄房屋所發散出來的熱能，即能清楚地窺知屋內人員的活動狀態，以及以往必須耗費大量人力的跟尖行爲，如今只需貼附一個衛星定位系統追蹤器，就可以在電腦前輕易地接收被追蹤對象的行蹤。

如果有人聲稱憲法第四增修條文對人民隱私的保障並不受科技進步的影響，將是一廂情願的想法，今日我們所面對的問題是如何對科技的力量施以適當地限制，以減少受憲法保障的隱私領域的縮小[133]。

第二節 犯罪者的追蹤

傳統犯罪的偵查必須倚賴目擊者的指認與犯罪嫌疑人所遺留的生物跡證來找出犯罪嫌疑人，在網路通訊時代，犯罪嫌疑人不再以有形的形體出現在犯罪現場，而是改以電子信號的方式來遂行其犯罪行爲，例如無論是入侵電腦或是發動網路攻擊以癱瘓受害者的電腦，使得行爲人與犯罪結果發生地不再有緊密的連接關係，想要確認犯罪嫌疑人

[129] United States v. Jones, 132 S. Ct. 945, 950 (2012)。At bottom, we must "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."
[130] Kerr, Orin S., An Equilibrium-Adjustment Theory of the Fourth Amendment, 125 Harv. L. Rev. 476, 480 (2011).
[131] Hill, D. Garrison "Gary", United States v. Jones and the Search for Fourth Amendment Coherence, 23 S. Carolina Lawyer 28, 31 (2012).
[132] Millcarek, Lauren, Eighteenth Century Law, Twenty-First Century Problems: Jones, GPS Tracking, and the Future of Privacy, 64 Fla. L. Rev. 1045, 1109 (2012).
[133] Kyllo v. United States, 533 U.S. 27, 33-34 (2001)。

的位置與身分就變得相當的有挑戰性，隨著通信監察設備的相繼問世，因此對於電子信號的監察，變成是一種不可避免且有效的方法。

第一項 電子通訊隱私權法案

第一款 立法背景

竊聽(eavesdropping)是一種古老的行爲，在普通法下被認爲是一種騷擾行爲，早在美國南北戰爭時期 Stuart 將軍就以運用斥侯在戰場上攔截敵對陣營的軍事通訊而聞名[134]。剛開始的竊聽只有用耳朵並沒有倚賴器材的輔助，在屋簷(eaves)下、窗外或牆的另一邊蒐集私密的對話內容，隨著電話成爲人們常用的溝通工具，以在原本的電話線上連接額外線路的方式攔截通話內容，成爲新的竊聽(wiretaps)方式，如今設計精良的電子裝置已經可以用來竊聽(bugs)在各種情況下人與人之間的對話[135]。

竊聽所採用的不莊重的方法以及容易被濫用的特性很快地就被發現，早在 1862 年 California 已經立法禁止竊聽的行爲，1928 年的 Olmstead 案是聯邦最高法院第一個電話竊聽的案子，在該案中聯邦最高法院認爲政府沒有入侵受憲法保障領域的竊聽行爲沒有憲法第四增修條文的適用，國會爲了回應 Olmstead 案的結果，在 1934 年的聯邦通訊法[136](the Federal Communication Act of 1934)中，明文禁止對於電話通訊未經許可的攔截與內容的揭露[137]。

在 1967 年的 Berger v. New York 一案中，聯邦最高法院對於 New York 州法律允許以竊聽的方式蒐集犯罪的證據，認爲該法律的文字規定掃蕩太過寬廣已經侵入人民受憲法保障的領域，而構成憲法增修條文第四與第十四條的違反，法院意見表示[138]：(a)憲法第四增修條文的保障範圍及於對話，使用電子裝置以取得對話構成該增修條文意義下的搜索行爲；(b)New York 州法允許竊聽的執行，不需要確信任何特定犯罪的發生，或指明特定所欲蒐集的對話；(c)該法未能對所欲蒐集的對話予以特定性地描述，等於賦予執法人員一個扣押全部對話的變動權限；(d)一個長達兩個月的竊聽許可，等於是僅倚賴一個相當理由的提示而進行一連串的搜索與扣押，同時也避免立即執行的要求；(e)該法允許竊聽時間的延長，只需符合公共利益而不用提出相當理由；(f)該法並未要求取

[134] Berger v. New York, 388 U.S. 41, 45-46 (1967)。
[135] Berger v. New York, 388 U.S. 41, 45-47 (1967)。
[136] 47 U.S.C. §605
[137] Berger v. New York, 388 U.S. 41, 50-51 (1967)。
[138] Berger v. New York, 388 U.S. 41, syllabus (1967)。

得所欲扣押的對話即應停止竊聽，而是由執法人員自行決定是否停止；(g)該法並未要求除了在緊急情狀與秘密竊聽的必要下，才能排除通知的義務；(h)該法並未要求執法人員繳回法院所核發的令狀，而是任由執法人員用以扣押不論是否涉及犯罪嫌疑之人的對話。

爲了弭平偵查實務上所引發的紛爭，方法之一是由聯邦最高法院藉由個案進行原則性的揭示，國會經由立法程序將該些原則加以落實使執法人員易於遵循。國會爲了因應通訊監察的相關問題，依循 1967 年的 Katz v. United States 與 Berger v. New York 兩案所揭示的精神[139]，於 1968 年通過綜合犯罪防制及街道安全法(Omnibus Crime Control and Safe Street Act of 1968)，其中的第三篇(Title III)係規範針對有線通訊(wire communication)與口頭通訊(oral communication)之監聽行爲。

隨著科技的進步傳遞訊息的方式也隨之多樣化，對話的方式除了以當面交談或以有線電話的方式進行外，尚能藉由無線電話或電腦網路以達成相同的效果，而訊息溝通所憑藉的形式除了聲音以外還可以是文字與影像，傳統以針對聲音的攔截所進行的監聽行爲已經不再能夠滿足所欲達成的偵查目標，因此思考將攔截的對象擴及於電子信號。

國會在 1986 年通過電子通訊隱私法(the Electronic Communication Privacy Act of 1986，簡稱 ECPA)，將原來的 Title III 加以擴充納入對電子通訊(electronic communication)通訊監察的規範，成爲新的聯邦監聽法[140](the Federal Wiretap Act of 1986)用以規範現在正在進行中或未來可能發生的通訊內容的截取。除了聯邦監聽法，ECPA 還包括撥號記錄器與追蹤裝置法[141](the Pen Registers and Trap and Trace Devices chapter of Title 18)與儲存通訊法[142](the Stored Communication Act of 1986，簡稱 SCA)共三個部分。撥號記錄器與追蹤裝置法用以規範通訊過程中通訊內容以外資訊的取得。對於非屬正在進行中的通訊，存取已經儲存的電子通訊則應符合儲存通訊法的規範。ECPA 的三個部分分別規範動態(通訊中)與靜態(經儲存)的通訊，以及是否涉及通訊中內容與非內容通訊的取得方式，違反 ECPA 的相關規範將面臨民、刑事上的責任，在訴訟中的案件若有違法監聽取得的證據將會有證據禁止的效果[143]。

[139] Kerr, Orin S., Are We Overprotecting Code? Thoughts on First-Generation Internet Law, 57 Wash & Lee L. Rev. 1287, 1299 (2000).
[140] 聯邦法典第 18 章第 2510 至第 2522 條。
[141] 聯邦法典第 18 章第 3121 至第 3127 條。
[142] 聯邦法典第 18 章第 2701 至第 2712 條。
[143] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (2009 年版)，頁 151。

第二款 內容介紹

第一目聯邦監聽法

聯邦監聽法(Federal Wiretap Act)是用以規範正在通訊中的通訊內容的截取，爲了要符合該監聽法的相關規範，首先必須先確認即將受到監察的通訊是否屬於 18 U.S.C. §2510 所定義之受保護的通訊、其次是即將採用的通訊監察方式是否導致對該通訊的截取，如果都符合上述兩種條件，則是否有任何法律上的例外允許實施該通訊監察[144]。

在聯邦監聽法中規範有三種受保護的通訊類型，分別是有線通訊、口頭通訊與電子通訊。該法的有線通訊被定義爲：全部或一部聲音的傳送，是藉由有線線路、電纜或其他在發送端與接收端之間的連接(包含在一轉接站中使用該項連接)協助之通訊傳輸設備的使用，該設備是由從事提供或經營這類設備之人所提供或經營，用以州際或外國商業通訊之傳輸或影響州際或外國商業通訊之傳輸[145]。因此，家中的有線電話對話是有線通訊的一個典型，使用行動電話的通訊亦是有線通訊的一種，因爲行動電話以無線電波與基地台雙向傳輸信號，當信號進到基地台之後，其傳輸過程中有一段路徑會是以有線的方式傳遞，即使是行動電話對行動電話的通訊也必須透過基地台傳輸信號，因此符合有線通訊的定義。

口頭通訊則被定義爲：由人所發出之任何口頭通訊，其人顯示該通訊內容有不被截取的期待，且依當時情況足認此一期待爲正當，惟此一名詞並不包括任何電子通訊[146]。

將電子通訊定義爲：全部或一部藉由有線線路、無線電、電磁波、光電或光學系統傳送之任何足以影響州際或外國商業之記號、信號、文書、影像、聲音、資料或任何具有信息性質之傳送，但不包括下列情形：(A)任何有線或口頭通訊；(B)僅依語音呼叫裝置做成之任何通訊；(C)從追蹤裝置所發出之通訊；(D)儲存在金融機構通訊系統中用以

---

[144] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 162。

[145] 18 U.S.C. §2510(1) ‘‘wire communication’’ means 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。

[146] 18 U.S.C. §2510(2) ‘‘oral communication’’ means 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，轉引自陳信郎，資訊隱私權保障與網路犯罪通訊監察法制，頁 123。

電子儲存與資金轉帳之電子資金轉帳資訊[147]。

仔細區別以上三個受保護通訊的文字描述內容可以知道，口頭通訊的定義是爲了回應 Katz 案禁止對具有合理的隱私期待的對話，任何侵犯該隱私的竊聽(bugs)行爲，口頭的對話要能受到免於被竊聽的保護必須要符合具有合理的隱私期待這個條件才能成立，而有線通訊的定義則是爲了回應 Berger 案禁止對有線線路上的對話的竊聽(wiretapping)行爲，很明顯地在定義文字中並未出現合理的隱私期待這一個要件，主要是在 1968 年立法當時的環境下，所有的有線通訊都是人與人之間的電話對話，其本質上已經具有私密的特性，若再加上合理的隱私期待這個條件將是多餘的[148]。

有線通訊的另一個要件是所傳輸的聲音(the aural transfer)必須是由人所發出[149]，在寬頻網路尚未普及的年代使用網路的方式都是透過電話線連接數據機以撥接的方式連接網路，此時該電話線所執行的功能並不符合有線通訊的定義，而是電子通訊。

在 1986 年國會將受保護通訊的類型擴及網際網路通訊，依循有線通訊的定義架構增加第三個類型亦即電子通訊，使電子資料受到等同於聲音的保護，然而在定義文字中並未出現合理的隱私期待的要件，使得電子資料的傳輸本質上均構成受保護的電子通訊，學者認爲這樣的保護太過寬廣，由於網際網路上充斥著各式各樣的資料流，其中包括具有通訊性質的與不具有通訊性質的資料流，並非全部類型的資料都值得受到隱私的保護，建議必須依資料的性質加以區別採取適當的保護[150]。

瞭解了受保護通訊的類型，取得該些類型通訊的方式也將影響是否有聯邦監聽法的適用情形，該法對截取的定義爲：由聽覺或藉由任何電子、機械或其他裝置的使用，以取得任何有線、電子或口頭通訊的內容[151]。因此，隔著牆聆聽密室內的對話內容、蒐集行動電話與基地台雙向傳輸的無線電波加以解密或是蒐集網路上的封包信號加以組合還原以得知其通訊內容，都是聯邦監聽法所定義對受保護通訊的截取行爲而有該法的適用。在網路與電腦犯罪的通訊監察，通常是對有線與電子通訊的監察，比較少涉及口頭

[147] 18 U.S.C. §2510(12) ‘‘electronic communication’’ means 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 in section 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，轉引自陳信郎，資訊隱私權保障與網路犯罪通訊監察法制，頁 124。

[148] Kerr, Orin S.，Are We Overprotecting Code? Thoughts on First-Generation Internet Law，頁 1299。

[149] 18 U.S.C. §2510(18) ‘‘aural transfer’’ means a transfer containing the human voice at any point between and including the point of origin and the point of reception。

[150] Kerr, Orin S.，Are We Overprotecting Code? Thoughts on First-Generation Internet Law，頁 1299-1300。

[151] 18 U.S.C. §2510(4) ‘‘intercept’’ means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device。

通訊的監察[152]。

聯邦監聽法普遍禁止故意對於他人受本法保護通訊內容的截取，除非有例外的情形發生[153]。該法規定多種允許例外監聽的情形，在電腦網路犯罪的偵查有七種例外情形經常被使用[154]：1 依據聯邦監聽法第 2518 條法院命令允許的監聽、2 同意的例外、3 服務提供者的例外、4 電腦入侵者的例外、5 電話分機的例外、6 意外取得犯罪證據的例外、以及 7 公眾可取得的例外。

第二目撥號記錄器與追蹤裝置法

撥號記錄器與追蹤裝置法(Pen Registers and Trap and Trace Devices Statute)用以規範定址資訊與通訊中非內容資訊之蒐集，早期的撥號記錄器與追蹤裝置分別只具有記錄從某一被監管電話所撥出的號碼與捕捉撥入該電話的外來號碼(類似今日的來電號碼顯示)這樣簡單的功能，隨著通訊型態的多樣化今日的撥號記錄器與追蹤裝置，能夠捕捉通訊過程中內容資訊以外之其他資訊。例如將該法應用在電腦網路通訊上，可以蒐集電子郵件帳號與網際網路位址等資訊，2001 年的美國愛國者法案，再次確認撥號記錄器與追蹤裝置法的適用對象，應及於現今社會上各種之通訊技術，在實務的應用上撥號記錄器與追蹤裝置法較聯邦監聽法經常被使用[155]。

撥號記錄器與追蹤裝置法將撥號記錄器定義為：用以記錄或解碼由傳送有線或電子通訊的設備所發出之撥號、路由、定址或信號資訊的裝置或方法，且該些資訊不能包含任何的通訊內容，以及該撥號記錄器不包含有線或電子通訊服務的提供者或使用者用於帳務或附隨於帳務的紀錄、用於該提供者所提供之通訊服務的裝置或方法，或是有線通訊服務的提供者或使用者用於成本計算或是在其日常營業範圍內其他類似目的的裝置或方法[156]。

對追蹤裝置的定義為：捕捉足以識別有線或電子通訊來源的來源號碼或其他之撥

---

[152] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 162。

[153] 18 U.S.C. §2511(1)(a)。

[154] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 167-182。

[155] 法思齊，美國法上數位證據之取得與保存，頁 127。

[156] 18 U.S.C. §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。

號、路由、定址或信號資訊的到來電子或其他脈衝的裝置或方法，且該些資訊不能包含任何的通訊內容[157]。

以上兩個定義在今日的有線與電子通訊傳輸過程，牽涉相當廣泛的科技運用在其中，通訊傳輸設備其類型可以包括有線電話、行動電話、網際網路使用者帳號、電子郵件帳號與網際網路位址等等，而撥號、路由、定址或信號資訊幾乎包含在一通訊過程中所有可能出現的非內容資訊，定義文字同時包含裝置與方法更是將軟體與實體裝置都規範在適用範圍之內[158]，這樣的定義方式已經幾乎涵蓋現今所有的科技以及其可能發送的非內容資訊。

在通訊傳輸過程中所截取的非內容資訊，是否具有合理的隱私期待則引起相當的爭議，在 1979 年 Smith v. Maryland[159]一案中，法院認爲警察要求電信公司在其中央機房安裝撥號記錄器以蒐集上訴人 Smith 從家中電話所撥出的號碼，不構成憲法第四增修條文意義下的搜索行爲，所以沒有申請法院核發令狀的必要，法院的理由是必須政府的行爲構成對人民合理的隱私期待的侵犯才構成搜索行爲，由於該撥號記錄器所架設的地點是位於電信公司的中央機房上訴人無法主張對其受憲法保障區域的物理入侵，撥號記錄器的使用無法聽到通話的內容、無法識別通話雙方的身分以及無法確認通話是否完成，剩下需要受到檢驗的是上訴人對其所撥出的電話號碼是否具有合理的隱私期待[160]，法院依循在 Katz 案所建立的主客觀標準，認爲上訴人在撥打電話的過程中自願地將受話方的電話號碼揭露給電信公司，以完成通話線路的建立，已經承擔電信公司可能將該電話號碼資訊洩漏給警察的風險，即使上訴人主觀上對該撥出的電話號碼具有隱私的期待，客觀上社會不會認爲這樣的期待是合理的[161]。

本案所倚賴的風險承擔(assumption of risk)原則，首先揭示在 United States v. Miller[162]一案中，Powell 大法官在所主筆的法院意見指出，憲法第四增修條文並不禁止政府自第三人處取得他人所揭露給該第三人的資訊，既使該資訊的揭露是基於特定的用途以及確信該第三人不會洩漏的假設前提下。自此風險承擔原則經常被用在反駁，對於第三人所揭露的資訊主張具有合理的隱私期待的抗辯上。

---

[157] 18 U.S.C. §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。

[158] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 154。

[159] Smith v. Maryland, 442 U.S. 735 (1979)。

[160] Smith v. Maryland, 442 U.S. 735, 741-742 (1979)。

[161] Smith v. Maryland, 442 U.S. 735, 744 (1979)。

[162] United States v. Miller, 425 U.S. 435, 443 (1976)。

對於正在進行中的通訊所爲之通訊監察，在判斷何時該適用聯邦監聽法或撥號記錄器與追蹤裝置法，首先必須要區分所蒐集的資訊是屬於通訊的內容資訊，或是內容資訊以外的定址或其他的非內容資訊，使用有線電話或行動電話所進行的對話交談，其通話內容是屬於內容資訊，所撥打或是接收的電話號碼是屬於非內容資訊。

行動電話的可攜性所帶來的方便性，已經幾乎取代有線電話成爲現今社會的主要通訊工具，由於具有可移動的特性因此不若有線電話易於掌握通話的所在位置，對於犯罪的偵查造成了新的障礙，行動電話在移動的過程中會尋找最接近的一個基地台並與之建立連線，成爲電話網路的一員之後才能與該電話網路中其他的電話進行通訊。

行動電話與基地台的連線會記錄在基地台資訊中，基地台資訊記錄通話開始的地點與通話結束的地點但是並不會建立通話過程中行動電話的移動路徑，法院普遍認爲基地台資訊不屬於通訊的內容資訊，基地台的設置在郊外有較遠的間隔距離，在都市地區則較密集，若能同時輔以監視器的設置，這樣的資訊對犯罪的偵查是相當有幫助的，可以藉由調閱基地台附近的現場監視器畫面以過濾出可能的嫌犯[163]。

法院對於基地台資訊取得的方式則有分歧的看法，大部分的法院認爲必須要同時符合撥號記錄器與追蹤裝置法的第 3121(a)條與儲存通訊法的第 2703(d)條才能核發法院命令(court order)，其所持的理由爲基地台資訊符合第 3127(3)與 3127(4)條中所定義的撥號、路由、定址或信號資訊的類型，依據第 3121(a)條的規定要有法院命令才能裝設撥號記錄器與追蹤裝置以蒐集該些資訊，至於要求同時符合第 2703(d)條的規定是基於通訊輔助偵查法(the Communications Assistance for Law Enforcement Act of 1994，簡稱 CALEA)第 1002(a)條，禁止政府單獨只依撥號記錄器與追蹤裝置法的規定取得行動電話用戶的基地台資訊，至於其他不同看法的法院則認爲要有令狀(warrant)才能強制揭露這類資訊，法院目前在這方面尚未達成一致的見解[164]。

基於網際網路是共用的以及每次只能傳送不超過特定長度的資料，網際網路通訊的傳輸過程中，必須將所欲傳輸的通訊內容切割成許多的單位長度資料，並在每個資料片段附加來源與目的位址，以協助將每個資料片段順利送達目的地端，之後再將該些資料片段加以組合以還原成最初在發送端所欲傳送的通訊內容，網路科技的術語將含有通訊內容的該些單位長度的資料片段稱爲承載資料(payload)，而存放來源與目的位址資訊的非通訊內容資訊則被稱爲表頭(header)，兩者構成一個網路傳送資料的最小單位稱爲封

[163] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 159。

[164] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 160。

包(packet)。

依據撥號記錄器與追蹤裝置法只能收集封包表頭這類不含通訊內容的定址資訊，蒐集整個封包將構成對通訊內容的截取而有聯邦監聽法的適用，其主要的區別在於定址或非內容資訊只存在於封包的表頭之中，承載資料所承載的都是通訊的內容[165]。

使用電子郵件通訊時，發信者撰寫信件內容並指定收件者的電子郵件帳號按下傳送鍵之後，郵件軟體會將寄件者與收件者的電子郵件帳號以及傳送過程中相關的路由資訊寫在該封電子郵件的信件檔頭中。瀏覽特定網頁必須在瀏覽器輸入專屬於該網頁的網際網路位址(IP 位址)，才取得將該網頁的畫面呈現在自己的電腦螢幕上。

網際網路的通訊經常必需倚賴第三方設備的協助，電子郵件的信件檔頭與網頁瀏覽所輸入的網際網路位址，於通訊過程中用以提供導引傳輸設備之路由資訊，依據 Smith 案的精神，這樣的資訊不具有合理的隱私期待，且該兩項資訊符合撥號記錄器與追蹤裝置法對定址資訊的定義，亦不會構成對通訊內容的洩漏，因此對該些資訊的取得必須符合撥號記錄器與追蹤裝置法的規範[166]。要特別注意的是信件主旨(subject line)可能揭露通訊內容的相關訊息，依據聯邦監聽法對內容[167]的定義信件主旨被視爲通訊內容的一部分，不適用撥號記錄器與追蹤裝置法的規定[168]。

同樣是使用在瀏覽器的位址欄，統一資源定位器(uniform resource locators，簡稱 URL)可以揭露更多個人的網際網路活動情形，其差別在於網頁的 IP 位址只能將畫面帶到所欲瀏覽網頁的首頁，而 URL 可以精確顯示所瀏覽的內容，同樣地在搜尋網頁中所輸入的搜尋關鍵字有時也會被附加而成爲 URL 的一部分，將導致通訊內容的揭露[169]，因此對 URL 與搜尋關鍵字等資訊的取得，不適用撥號記錄器與追蹤裝置法的規定。

第三目儲存通訊法

儲存通訊法(Stored Communication Act，簡稱 SCA)規範政府如何自網路服務提供者取得所儲存的帳號資訊，舉凡儲存的電子郵件、帳號記錄與用戶資訊之取得，均需符合儲存通訊法的規定[170]。儲存通訊法將網路服務提供者區分爲提供電子通訊服務

---

165 USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 152。

166 United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008)。

167 18 U.S.C. §2510(8) ‘‘contents’’, when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication。

168 In re Application of the United States of America for an Order Authorizing the Use of a Pen Register and Trap, 396 F. Supp. 2d 45, 48 (D. Mass. 2005)。

169 United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008)。

170 USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，

(electronic communication service，簡稱 ECS)與遠端計算服務(remote computing service，簡稱 RCS)兩種類型。

對於電子通訊服務[171]的定義是依循聯邦監聽法對該通訊服務之定義：係指提供使用者使其具有發送與接收有線或電子通訊能力的服務。儲存通訊法將遠端計算服務[172]定義爲：藉由電子通訊系統提供公眾電腦儲存或處理之服務。其中電子通訊系統[173]係指：用於傳輸有線或電子通訊之任何有線線路、無線電波、電磁、光學或光電設備，以及用於電子儲存該些通訊之電腦或相關的電子設備。

任何的公司或政府單位提供他人以電子地方式進行通訊，可以被認爲是電子通訊服務的提供者，例如有線電話、行動電話、電子郵件與電子布告欄等服務的提供者都是屬於這個類型，而不問該服務提供者所扮演的主要營業功能，例如保險公司提供給員工的電子郵件服務也是屬於這個類型，然而附隨於提供服務的過程中局部使用的通訊工具，例如使用門口的對講機才能得到屋內人員開門的協助則不屬於這個類型[174]。

遠端計算服務係指，藉由遠端電腦以提供客戶儲存或處理資料的服務，例如以分時安排的方式使用該遠端電腦的運算設備，或是提供資料的儲存以供未來對該資料的存取，都是屬於這個類型，除了具有儲存或處理資料的功能外，還要能對公眾提供服務，因此，民眾支付相關費用就能取得電信公司的通訊服務是屬於這個類型，而只對公司員工提供的電子郵件帳號因爲不對公眾提供服務，將不屬於這個類型[175]。一個服務提供者可以同時具有這兩種服務功能，只要所提供的服務符合定義的內容，兩者並不具有互相排斥的條件。

網路服務提供者在提供用戶服務的過程中將會產生並儲存許多不同性質的資料，儲存通訊法將儲存的資料區分爲用戶的基本與連線資訊(basic subscriber and session information)、與用戶相關之紀錄或其他資訊(records or other information pertaining to a customer or subscriber)以及內容與電子儲存(contents and electronic storage)三種資

頁 115。

[171] 18 U.S.C. §2510(15) ‘‘electronic communication service’’ means any service which provides to users thereof the ability to send or receive wire or electronic communications。

[172] 18 U.S.C. §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。

[173] 18 U.S.C. §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。

[174] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 117-118。

[175] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 119-120。

訊類別[176]。用戶的基本與連線資訊[177]包括：(A)姓名；(B)地址；(C)區域與長途電話通聯紀錄，或是連線的時間與長度；(D)服務的長度與服務的類型；(E)電話或設備號碼或用戶號碼或其身分識別，其中包含任何臨時派發的網路位址；以及(F)支付該項服務的方式與來源，其中包含任何信用卡或銀行帳戶號碼。

與用戶相關之紀錄或其他資訊[178]：係指除了通訊內容以外之非內容資訊，亦即所有與用戶相關的資訊，其中包含帳號的使用紀錄、基地台的資訊以及該用戶通訊對象之電子郵件位址等等，並包括前述用戶的基本與連線資訊，之所以將兩類的非內容資訊加以區別，是基於立法者認爲後者將揭露更多的交易資訊並足以描繪出用戶在網路上的活動情形[179]。

儲存通訊法將通訊內容依其是否完成通訊傳輸過程，區分爲電子通訊服務提供者所持有處於電子儲存狀態中之通訊內容，以及儲存在遠端計算服務提供者處之通訊內容[180]。電子儲存[181]係指，(A)附隨於電子傳輸之有線或電子通訊之暫時或中間儲存；以及(B)由電子通訊服務基於備份保護該通訊目的之儲存該通訊。

舉一個電子郵件通訊傳輸的例子來說明，Joe 使用公司的電子郵件帳號(Joe@goodcompany.com)寄送一封信至 Jane 的個人電子郵件帳號(Jane@localisp.com)，這封信到達 LocalISP 公司的電子郵件伺服器等待 Jane 的讀取，此時 GoodCompany 與 LocalISP 公司都是電子通訊服務提供者，而該封電子郵件正處於電子儲存狀態中，當 Jane 讀取該封信件後，通訊傳輸過程即已完成且兩公司不再屬於電子通訊服務提供者，該電子郵件不再處於電子儲存狀態，Jane 可以選擇將該封信件刪除或是留在郵件伺服器上，如果選擇將信件留在伺服器上，LocalISP 公司的角色將轉變爲遠端計算服務提供者[182]。

接下來 Jane 回復信件給 Joe，信件到達 GoodCompany 公司的電子郵件伺服器等待 Joe 的讀取，Joe 讀取信件後選擇將信件留在伺服器上，此時的 GoodCompany 公司既不是電子通訊服務也不是遠端計算服務的提供者，因爲通訊傳輸已經完成且

[176] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 121-122。
[177] 18 U.S.C. §2703(c)(2)。
[178] 18 U.S.C. §2703(c)(1)。
[179] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 122。
[180] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 123。
[181] 18 U.S.C. §2510(17)。
[182] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 125-126。

GoodCompany 公司的郵件伺服器並未對公眾提供服務，對該封電子郵件的取得不再適用儲存通訊法的相關規定，而是必須符合憲法第四增修條文的規範，當 Joe 與 Jane 進一步分別將電子郵件下載至辦公室與家中的電腦儲存，Joe 與 Jane 由於不屬於儲存通訊法所定義的兩類服務提供者，他人欲取得在該些電腦中所儲存的電子郵件，同樣沒有儲存通訊法的適用，也必須遵守憲法第四增修條文的規範[183]。

立法者藉由對服務提供者與受保護資料的區分並給予不同程度的保障，提供儲存通訊資料一個完整的隱私保護陣列，在取得該些受保護的資料之前，執法人員必須對該資料的類型及其提供者先行加以區分才能適用正確的規定[184]。

電子通訊隱私法相較於憲法第四增修條文的差別在於，電子通訊隱私法規範的對象不再僅侷限於政府，而是可及於一般之個人，任何人想要從網路服務提供者取得儲存之電子郵件、帳戶紀錄或是用戶資訊，皆須遵守電子通訊隱私法中有關取得儲存通訊的相關規定，因此，電子通訊隱私法不僅就已儲存的通訊提供使用該服務用戶的隱私權保障，對於傳輸中的通訊也提供更高程度的保障[185]。

第二項 撥號記錄器與追蹤裝置法

第一款 許可程序

撥號記錄器與追蹤裝置的初次安裝或延長使用，必須依據撥號記錄器與追蹤裝置法中有關聲請主體[186]與內容[187]的規定，聲請法院命令(court order)的核發。由代表政府的檢察官或州執法官員，以書面宣示或相當的確信，向有管轄權的法院或該州法院提出申請。聲請書中必須指明提出聲請檢察官或州執法官員的身分以及指明執行該項偵查的執法單位，並由聲請人證明所要取得的資料與該單位正在進行中的犯罪偵查有關。

法院收到聲請書後確認聲請人所述安裝該項設備後所取得的資料與正在偵查中的犯罪有關，就會核發單方的法院命令，該命令適用的對象爲在美國境內任何提供有線或電子通訊的個人或單位，其協助有助於該命令執行之人，若對未列名於該命令中的個人或單位提示，經該些受提示對象的要求並由檢察官或執法官員以書面或電子形式證明該

[183] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 126。
[184] 法思齊，美國法上數位證據之取得與保存，頁 120。
[185] 法思齊，美國法上數位證據之取得與保存，頁 120。
[186] 18 U.S.C. §3122(a)(1)-(2)。
[187] 18 U.S.C. §3122(b)(1)-(2)。

命命對該些受提示對象亦有適用[188]。

在對公眾提供服務的封包交換網路安裝撥號記錄器與追蹤裝置則有較嚴格的規定，執法單位必須維護一個對該設備的全程使用紀錄，其中包括安裝該設備或從該設備取得蒐集資訊的人員身分、設備安裝與解除的時間日期以及從設備取得所蒐集資訊的時間日期長度、對於該設備的組態設定與後續修改以及該設備所蒐集的任何資訊，該設備的使用紀錄必須在設備使用結束後 30 天內送交核發該命令的法院[189]。執法單位在使用該設備時，應當採用當時科技可行的方法以避免蒐集到有關有線或電子通訊的內容[190]。

法院命令所載的內容必須指明，該設備所欲蒐集資訊之電話線或其他通訊設備，已知的租用或登記人的身分、已知的受刑事偵查之人的身分、適用該命令的通訊屬性其中包括號碼或其他識別資訊，以及該設備所欲蒐集資訊之電話線或其他通訊設備，已知的所在位置、該設備所欲取得之犯罪資訊、以及應聲請人之請求指明可以協助該設備安裝的資訊、設備與技術[191]。法院命令必須指示，該命令必須密封除非法院另有指示，且擁有或出租線路或其他通訊設備之人或是依據該命令有協助安裝義務之人，不得向該通訊設備用戶或其他人揭露該設備或是該偵查作爲的存在，除非法院另有指示[192]。首次執行撥號記錄器與追蹤裝置的安裝與使用期限不得超過 60 天，時間的延長必須獲得核發該命令法院的允許，且不能超過另一個 60 天的期間[193]。

法院在核發撥號記錄器與追蹤裝置的命令時並不要求相當理由的存在，也沒有限定特定的犯罪類型才能適用，聲請的條件相對寬鬆。在執行上也相當有彈性，聯邦法院所核發的命令，在該法院的管轄區域外依然具有效力[194]，網路犯罪的偵查過程中經常會遇到跳板電腦的使用以企圖阻斷對犯罪源頭的追溯，該命令對於未列名其中的第三人經適當的提示程序之後依然具有拘束力，可以順利建立起受害電腦與犯罪源頭之間的完整路徑。

第二款 違法的責任

違反本法律將會面臨民事與刑事的責任，在刑事責任方面，沒有取得法院所核發的命令，私自安裝或使用撥號記錄器與追蹤裝置的違法效果將只有罰款、一年以下之徒

188 18 U.S.C. §3123(a)(1)-(2)。
189 18 U.S.C. §3123(a)(3)(A)-(B)。
190 18 U.S.C. §3121(c)。
191 18 U.S.C. §3123(b)。
192 18 U.S.C. §3123(d)。
193 18 U.S.C. §3123(c)。
194 USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 155。

刑，或是兩者併罰[195]。其所取得的證據在刑事訴訟中沒有證據禁止的效果，法院認爲如果在訴訟中賦予法條所沒有的救濟方式，將會侵犯立法機關的權限[196]。在民事方面，因爲違反本法律而受有損害之人可以向加害人請求補償[197]。不當的揭露撥號記錄器與追蹤裝置所蒐集的資訊，亦構成本法律的違反[198]。

執法人員與提供協助的通訊服務提供者，善意信任法院所核發的命令、緊急安裝撥號記錄器與追蹤裝置的要求、立法或法律的授權，導致違反本法律所引起之任何民刑事訴訟中可以主張完全抗辯[199](good faith defense)。

第三款 監督

在個案中對於電子通訊業者提供公眾使用之封包交換網路安裝撥號記錄器與追蹤裝置，在法院命令所允許的蒐集資訊期限屆至後 30 天內，必須向核發命令的法院報告該設備的使用狀況。

除了個案的報告義務之外，聯邦檢察總長每年必須向國會呈報司法部所屬執法單位申請撥號記錄器與追蹤裝置的統計資料[200]，其中包括：

(1)法院命令允許的截取時間長度，以及延長執行命令的數量與時間長度；

(2)記載在法院命令、聲請書或延長命令上所涉及的罪名；

(3)所涉及的偵查次數；

(4)受影響設備的本質與數量；以及

(5)提出聲請的執法單位的人員身分與所屬區域，以及核准該命令之人。

第三項 聯邦監聽法

第一款 許可程序

對於通訊內容的截取必須取得法院所核發的令狀才能進行，聯邦監聽法對於令狀的聲請主體與要件，以及簽發令狀的主體與要件均有詳細的規定。該法將令狀核發的單位區分爲聯邦與州法院，聯邦法院令狀的執行客體又區分爲有線或口頭通訊以及電子通訊

195 18 U.S.C. §3121(d)。
196 United States v. Forrester, 512 F.3d 500, 512 (9th Cir. 2008)。
197 18 U.S.C. §2707(a)。
198 18 U.S.C. §2707(c)。
199 18 U.S.C. §3124(e)。
200 18 U.S.C. §3126。

兩種，不同的令狀類型各有不同的適格聲請主體。向聯邦法院聲請對有線或口頭通訊內容的通訊監察，其聲請書必須經檢察總長、副檢察總長、或由檢察總長指定在刑事部門或國家安全部門中之助理檢察總長、代理助理檢察總長、副助理檢察總長、或代理副助理檢察總長核准提出聲請[201]。向聯邦法院聲請對電子通訊內容的通訊監察，其聲請書只需經由聯邦檢察官核准提出聲請[202]。向州法院聲請的通訊監察，其聲請書須經由州檢察長核准提出聲請[203]。

只有符合該法所規定的犯罪類型才能實施通訊監察，向聯邦法院聲請對有線或口頭通訊內容的通訊監察，係正在進行中的偵查與該法第 2516(1)條所列的罪名有關。向聯邦法院聲請對電子通訊內容的通訊監察，必須是與聯邦重罪有關的偵查。向州法院聲請的通訊監察，必須是列明於第 2516(2)條中的罪名才符合要件。確認所欲截取的通訊內容可能提供所偵查犯罪的證據之後，以書面記載第 2518(1)條所規定的事項，向有管轄權的法院提出申請[204]：

(a)提出聲請的執法官員，以及核准提出聲請的官員身分；

(b)聲請人所倚賴的事實與情況之完整陳述，確信命令應該被核發，其中包括：(i)特定的犯罪，已經發生、正在發生或即將發生、(ii)除了有本條第十一節的例外情形，詳細描述即將被截取通訊的地點、(iii)詳細描述即將被截取的通訊類型、(iv)已知的犯罪嫌疑人其通訊即將被截取的身分；

(c)完整陳述關於，其他的偵查程序已經嘗試並且失敗，或是既使嘗試也不可能成功或是太過危險；

(d)陳述所需維持截取的時間。依偵查案件的性質，假如所核准的截取無法在第一次取得所描述的通訊類型自動終止，要詳細描述足以建立相當理由(probable cause)的事實，相信相同的通訊類型隨後將會發生；

(e)完整陳述關於，提出聲請以及核准提出聲請之人所已知，尋求法官核准對有線、口頭或電子通訊的截取以及在該聲請書中所提及的人員、設備或地點的所有先前聲請，以及法官在該些聲請所採取的決定；以及

(f)如果聲請延長截取的命令，陳述截至目前爲止所截取到的結果，或是合理解釋未能取得該結果；

對該偵查案件有管轄權的法院進行對聲請人單方的審查，並視需要要求補強證據

[201] 18 U.S.C. §2516(1)。
[202] 18 U.S.C. §2516(3)。
[203] 18 U.S.C. §2516(2)。
[204] 18 U.S.C. §2518(1)。

[205]，依據聲請書中所陳述的事實決定是否核發通訊監察令狀[206]：

(a)存在相當理由可以確信該個人正在進行、已經進行或即將進行本法第 2516 條所列的罪名；

(b)存在相當理由可以確信經由截取可以取得與該犯罪有關的通訊內容；

(c)一般的偵查方法已經嘗試並已失敗，或者即使嘗試有可能不會成功或是太過危險；

(d)除了有本條第十一節的例外情形，存在相當理由可以確信即將被截取內容的通訊設備或地點，正在被用於或即將被用於該犯罪的進行，或是被該個人所租用、登記在其名下或經常使用。

法院所核發的通訊監察令狀必須記載[207]：

(a)其通訊內容即將被截取的，已知的該個人的身分；

(b)允許截取通訊設備的本質與地點；

(c)描述即將被截取的通訊類型，以及所涉及的特定犯罪；

(d)核准通訊監察聲請提出的單位與該官員的身分；以及

(e)允許截取的時間長度，以及是否在第一次獲得所欲截取的通訊即應自動終止。

於令狀中另可應聲請人的要求，指示通訊服務的提供者、房東、監管人或其他人提供聲請人完成該截收所需要的資訊、設備與技術協助，並對該通訊設備產生最少的干擾。

聯邦最高法院在 Katz 案確認具有合理隱私期待的通訊內容是屬於憲法第四增修條文保護的客體，任何對進行中通訊內容的截取將構成該增修條文意義下的搜索行爲，聯邦監聽法的制定強化了對於通訊隱私的保障，該法提供法院在簽發通訊監察令狀時必須審酌的事實，除了該增修條文所要求的「相當理由」，聯邦監聽法增加「重罪原則」並可視需要要求聲請人提出補充證據以滿足相當理由的門檻。對於通訊內容的截收不若對傳統有體物的搜索與扣押，可以經由令狀的描述清楚地判斷是否屬於被允許的客體(人身、住所、文件以及財產)，依據該法所聲請與核發的令狀只須指明已知身分的受通訊監察對象並及於在核發令狀當時未知身分的其他人(others as yet unknown)，受通訊監察對象所及範圍的不確定，引來想當多的疑慮。

在 United States v. Kahn[208]一案中，被上訴人 Kahn 因涉及非法經營賭博罪，法院核准對被上訴人本人、未知身分的其他人，以及可能用於賭博經營的兩條電話線的通訊

[205] 18 U.S.C. §2518(2)。
[206] 18 U.S.C. §2518(3)。
[207] 18 U.S.C. §2518(4)。
[208] United States v. Kahn, 415 U.S. 143 (1974)。

監察，監聽過程中截取到被上訴人太太與一已知賭博參與者的對話並將採爲定罪的證據，被上訴人抗辯其太太並非未知身分的其他人，未能將其太太列名於令狀中受通訊監察的對象是違法監聽，聯邦最高法院在法院意見中指出，只允許對已知身分並明確記載於通訊監察令狀之人實施通訊監察，雖然可以將保護個人隱私的利益發揮到極致但也將引起相當的疑慮[209]。法院進一步論述，法條文義僅要求將確信犯有第 2516 條中的特定犯罪之人記載於通訊監察令狀之中[210]，如果要求政府將可能使用電話從事犯罪活動之人給予詳細的調查才能聲請通訊監察狀，將會嚴重影響偵查效率[211]。因此法院認爲，記載於通訊監察令狀中受通訊監察對象之身分，僅限於在聲請令狀當時有相當理由確信該個人正從事於犯罪之人，儘管在監聽開始之前沒有理由懷疑被上訴人太太亦涉及犯罪，其仍屬於令狀中所歸類未知身分之其他人[212]。

由該判決所揭示的精神可以得知，已知之人係指存在相當理由確信正在或即將從事犯罪之人，並非某特定犯罪嫌疑人之近親家屬或其日常生活中經常往來之人，於聲請通訊監察令狀當時未能將已知之人記載於令狀之中，僅是特定性不夠完備[213]，對其所爲之通訊監察不構成違法通訊監察。

聯邦監聽法所規範通訊監察聲請的要件，基於保護對話交談內容賦予口頭與有線通訊特定重罪的要求，而電子通訊只需符合聯邦重罪等較寬鬆的條件，隨著網路通訊所能提供的服務的多樣化，以及人們倚賴網路通訊的日漸加深，利用網路所進行的語音與視訊同樣能達到對話交談的功能，因此有是否應將核准電子通訊監察的門檻提高至與口頭與有線通訊相同的思考[214]。

第二款 執行

通訊監察無可避免地會接觸到與所偵查犯罪無關第三人之通訊內容，聯邦監聽法規範執行通訊監察時要以產生最小程度侵害的方式進行，令狀所允許執行通訊截取的期間不能超過達成其目的所需要的時間，最長不能超過 30 天，30 天的起算以最早開始進行截取的時間點起算或是令狀核發 10 天後起算，令狀延長的聲請必須符合聲請書記載與法院審查其所載內容等有關規定，所允許延長的期間不能超過法院認爲需要達成該目的的時間，最長不能超過另一個 30 天，令狀中並應記載(1)應儘快執行通訊截取、(2)以減

209 United States v. Kahn, 415 U.S. 143, 153 (1974)。
210 United States v. Kahn, 415 U.S. 143, 152 (1974)。
211 United States v. Kahn, 415 U.S. 143, 153 (1974)。
212 United States v. Kahn, 415 U.S. 143, 155 (1974)。
213 United States v. Donovan, 429 U.S. 413, 437 (1977)。
214 謝昆峰，網際網路與刑事偵查，國立台灣大學法律學研究所碩士論文，2002 年，頁 57。

少截取到與本令狀目的無關通訊內容的方式進行、(3)取得所欲截取的內容或是時間已達30 天即應立即終止[215]。

聯邦監聽法對於以產生最小程度侵害的執行方式並未提供明確的依據，執法人員在實務運作上必須倚賴其主觀上的判斷，法院在審查是否符合令狀所要求的最小化原則將會依據[216]：(a)主觀上，整體而言，執行監聽工作的人是否呈現對隱私權的高度尊重，以及是否已經採取所有可能避免不必要侵犯的合理措施、(b)客觀上，認爲該執法人員所採取的措施是合理的。

所截取的通話內容是否涉及正在偵查中的犯罪，必須要對該通話內容加以解讀才能判斷，若當時所掌握的內容與正在偵查中的犯罪無關則必須立即終止對該通訊的截取，等經過一適當時間間隔後，再度截取並判斷是否與偵查中的犯罪有關，若此時的內容涉及正在偵查中的犯罪，則可以同步監聽並加以儲存記錄，這個在偵查實務上經常被採用的方式，執法人員在主觀上已經呈現對受通訊監察對象隱私的尊重[217]。

截取全部的通訊一般會被認爲沒有積極採取達成最小化原則的措施，除非是有法定的例外情形[218]，當所截取的通訊是以執法人員無法解讀的編碼或外國語言所組成且現場並沒有專家可以提供即時的協助，可以例外允許將該些通訊全部加以儲存記錄，事後再由專家解譯該些通訊中與正在偵查中的犯罪有關的部分交給執法人員，並將其他不相關的部分封存在法院，以達到類似於最小化措施的效果[219]。

通訊監察在執行當時必須要保持秘密性，不僅不能告知受通訊監察之對象，依據法律協助執行通訊監察之人亦不能洩漏通訊監察作爲的存在，通訊監察執行完成後的告知義務可以向社會確保通訊監察這項科技有被合理的使用，任何依法核准的通訊監察將因告知義務的履行，最終讓受通訊監察之人有所知悉，使其在隱私覺得受不合法侵犯之時有機會可以尋求適當的民事救濟[220]，因此國會在聯邦監聽法賦予事後告知的義務。

在通訊監察令狀聲請提出後，最晚不得超過第 90 天，無論是被駁回、期間屆滿或是延長期間屆滿，核准或駁回該聲請的法官應使列名於通訊監察令狀或聲請書上之人，以及法官基於公平利益之考量，使居於受截取通訊另一端之其他人，受下列事項之通知[221]：

---

[215] 18 U.S.C. §2518(5)。
[216] Scott v. United States, 425 U.S. 917, 921 (1976)。
[217] Wuslich, Julie P., An Overview of Electronic Surveillance in the United States; Law, Policy, and Procedure，下載自 http://www.unafei.or.jp/english/pdf/PDF_rms/no59/ch26.pdf (最後點閱：2012 年 5 月 1 日)。
[218] 18 U.S.C. §2518(5)。
[219] Wuslich, Julie P.，An Overview of Electronic Surveillance in the United States; Law, Policy, and Procedure。
[220] United States v. Donovan, 429 U.S. 413, 438 (1977)。
[221] 18 U.S.C. §2518(8)(d)。

(1)該通訊監察令狀核發或聲請提出的事實；

(2)核准或不核准截取或是駁回聲請的日期，以及核准的期間；以及

(3)在該期間之內是否截取有線、口頭或電子通訊的事實。

法官基於公平利益之考量，得依受通訊監察之人或其辯護人之聲請，允許其檢視該受截取之通訊、聲請書以及令狀。對法官單方提示正當理由(good cause)之後，本節所規定的告知義務可以被延遲。

第三款 違法的責任

執行電子監控時違反聯邦監聽法的相關規定，將面臨刑事處罰(18 U.S.C. §2511(4))、民事責任(18 U.S.C. §2520)以及在訴訟上證據禁止(18 U.S.C. §2518(10)(a))的效果[222]。

任何受侵害之人可以主張對該通訊截取的內容，或自該通訊內容取得證據的禁止，當有下列的情形發生時[223]：

(i)該通訊係非法截取；

(ii)該截取行爲所依據的令狀，形式不完備；或是

(iii)該截取行爲並未以令狀所允許的方式進行。

聯邦監聽法對於通訊監察的聲請與令狀的執行都有相關的規定，違背該些相關規定並不必然面臨證據禁止的效果，在 United States v. Giordano[224]一案中，執行助理檢察總長核准了通訊監察聲請書向法院的提出，聯邦最高法院認爲法律將通訊監察限定用在特定類型的犯罪，在呈現相當理由的情形下，並要求經由司法部門資深官員的核准才能向法院提出聲請，國會的目的是要節制通訊監察的使用，本案令狀的核發係依據不適格的核准者所核准提出的通訊監察聲請，係屬於違法通訊監察而有證據禁止的適用[225]。

未將全部已知的犯罪嫌疑人列名於通訊監察聲請書上，以及沒有確實履行告知義務，不產生證據禁止的效果，在 United States v. Donovan[226]一案中，執法人員在聲請延長通訊監察時已經由前一次的通訊監察得知特定犯罪嫌疑人的身分，但是未能於聲請延長通訊監察時將該些人列名於聲請書上，在履行告知義務時亦疏漏未能通知部分受通訊監察之人，聯邦最高法院表示通訊監察令狀的核發，法院審核通訊監察聲請書上所載

[222] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 183。
[223] 18 U.S.C. §2518(10)(a)。
[224] United States v. Giordano, 416 U.S. 505 (1974)。
[225] United States v. Giordano, 416 U.S. 505, 527 (1974)。
[226] United States v. Donovan, 429 U.S. 413 (1977)。

的事實，認爲存在相當理由可以確信特定人正從事於犯罪、與該犯罪有關的通訊可以經由截取獲得、以及該通訊設備正用於犯罪的進行，即符合法律核發通訊監察令狀的要求，沒有列名全部已知的受通訊監察對象，不影響一合法令狀的效力[227]。

至於未確實履行告知義務的部分，聯邦最高法院表示法律的內容或立法紀錄並未賦予因疏漏未通知受通訊監察之人而使該通訊監察違法的效果，本案當法院對大部分受通訊監察對象送達通知時，該截取行爲已經完成且對話內容是依據一個有效的令狀加以扣押，即使該通知未能送達部分受通訊監察之人，並不構成違法的通訊監察[228]。

類似於將口頭與有線通訊的通訊監察限定於特定重罪的要求，電子通訊的通訊監察只需符合聯邦重罪等相對寬鬆的條件，立法者對於違法通訊監察的證據禁止的態度亦因通訊類型而有不同，違法通訊監察的證據禁止僅適用於口頭與有線通訊，並不及於電子通訊，只有未能依 18 U.S.C. §2518(8)(a)之規定將受截取電子通訊封存時，才例外有證據禁止的效果[229]。隨著電子通訊科技的進步其所能傳遞具有隱私期待的信息亦趨多樣化，也應該思考對電子通訊之違法通訊監察賦予證據禁止的效果。

證據禁止的效果可能導致將犯罪嫌疑人定罪的關鍵證據排除，而使得維護社會安全的重大利益遭受衝擊，法院曾經表示證據禁止並不是一個受歡迎的救濟方式，法院通常採爲最後的手段，只有當所欲嚇阻的利益遠大於排除該非法取得證據所犧牲的重大社會成本時才會加以採用[230]。

違法截取、使用或揭露通訊者[231]，在刑事部分將處以罰款、五年以下之徒刑，或是兩者併罰[232]，在民事部分受侵害之人可請求暫時處分、損害賠償與懲罰性賠償以及律師費與相關訴訟成本[233]。民事請求權在受侵害之人有合理機會知悉該侵害事實的存在之日起算，逾兩年不行使而消滅[234]。

執法人員或協助執行通訊監察之通訊服務提供者，善意信任下列事項所導致的違法通訊監察，在民刑事訴訟中可以主張完全的抗辯[235]：

(1)法院令狀或命令、大陪審團傳票、立法或法律授權；

(2)應執法人員要求的 2518(7)緊急通訊監察；或是

---

227 United States v. Donovan, 429 U.S. 413, 435 (1977)。
228 United States v. Donovan, 429 U.S. 413, 438-439 (1977)。
229 USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 184。
230 United States v. Forrester, 512 F.3d 500, 512 (9th Cir. 2008)。
231 18 U.S.C. §2511(1)。
232 18 U.S.C. §2511(4)。
233 18 U.S.C. §2520(b)。
234 18 U.S.C. §2520(e)。
235 18 U.S.C. §2520(d)。

(3)善意信任是 2511(3)或 2511(2)(i)所允許的行爲。

善意信任的抗辯必須是涉及公權力行使的違法通訊監察才有適用，國會的用意是要保護電信公司與依據法院令狀協助執法人員執行通訊監察之人，善意信任抗辯不及於民事竊聽案件[236]。除了善意信任抗辯之外，相當多的法院肯認在民事訴訟上有適格豁免抗辯(qualified immunity defense)，當執法人員合理地相信其行爲並未超出法律所允許的範圍，若因此而違法可以主張適格豁免抗辯[237]。

第四款 監督

通訊監察係以受監察對象無法察覺的方式蒐集其通訊的內容，過程中潛藏著侵害隱私的極大可能性，可能受到影響的範圍不僅是犯罪嫌疑人甚至包括與偵查中犯罪無涉之第三人，如果沒有適當的監督機制則很容易遭到濫用，要求對受通訊監察對象履行告知義務，是提供該受監察對象一個監督其所受通訊監察程序是否適法的機會。

對於個案的監督，聯邦監聽法規定在通訊監察令狀核准之後，核准該令狀的法官可以要求在規定期間向其報告執行的進度與繼續截取的需要[238]。此外，並要求核准或駁回該聲請的法官，在令狀期間屆至或駁回聲請 30 天內，向美國法院行政部門呈報下列事項[239]：

(a)令狀聲請或延長期間聲請的事實；

(b)令狀聲請或延長期間聲請的種類；

(c)令狀聲請或延長期間聲請所核准、更正或駁回的事實；

(d)令狀所核准截取期間與延長該令狀期間的次數與長度；

(e)令狀、聲請書或延長期間令狀所記載的罪名；

(f)提出聲請的執法人員以及單位，與核准提出該聲請官員的身分；以及

(g)被截取通訊設備的本質與地點。

對於通案的監督，聯邦監聽法規定在每年一月聯邦檢察總長、經聯邦檢察總長指定之助理檢察總長或州檢察長，應向美國法院行政部門呈報下列事項[240]：

(a)上年度中，聲請令狀或延長期間令狀時，有關 2519(1)(a)至(g)的資料；

---

[236] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 189。

[237] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 189。

[238] 18 U.S.C. §2518(6)。

[239] 18 U.S.C. §2519(1)。

[240] 18 U.S.C. §2519(2)。

(b)依令狀所執行截取之描述，包括：(i)截取到涉及犯罪通訊之性質與頻率、(ii)截取到其他通訊之性質與頻率、(iii)通訊受截取的人數、(iv)令狀遇到加密通訊的數量，該加密通訊是否妨礙執法人員依據該令狀取得截取通訊的明文、以及(v)用於截取行爲之人力成本、數量、性質與其他資源；

(c)依該令狀所執行之截取，所進行逮捕的次數與罪名；

(d)該截取所涉及審判的次數；

(e)該截取遭證據禁止聲請的次數，以及成立或駁回的次數；

(f)該截取促成定罪的次數與所涉及的罪名，以及截取行爲重要性的一般評估；以及

(g)上年度中，所取得的令狀或延長期間令狀，有關本節(b)至(f)的資料。

對於接受國會的監督，聯邦監聽法規定在每年四月美國法院行政部門應向國會提出上年度中有關通訊監察聲請數量，以及令狀或延長期間令狀核准或駁回數量的完整報告，該報告中應包括依據 2519(1)與 2519(2)之規定向美國法院行政部門呈報資料之整理與分析數據，美國法院行政部門授權發佈依據 2519(1)與 2519(2)規定呈報資料的內容與格式等有關的規定[241]。

第四項 儲存通訊法

電子通訊隱私法將處於傳輸中的通訊區分爲內容與非內容資訊，藉由制定聯邦監聽法與撥號記錄器與追蹤裝置法分別提供保護，欲取得這兩個類型的資料必須符合相關法律的規定。電子通訊傳遞的信息是以信號加以承載，信息若非處於傳輸狀態則必須處於儲存狀態，由於電能、光學與電磁等這類信號具有揮發性的特質，當其不處於傳輸狀態時必須將其所承載的信息附著於載體[242]使之處於儲存的狀態，以供後續之取得與利用。儲存通訊法的制定是爲了要提供處於儲存狀態中通訊的保護，並區分強制揭露與自願提供兩種方式，分別規範取得儲存通訊的方式。

第一款 強制揭露

儲存通訊法第 2703 條規範 5 種政府可以採用的機制以強制服務提供者揭露其所儲存關於用戶的通訊內容或紀錄，這 5 種機制分別爲[243]：傳票、事先通知用戶的傳票、法

[241] 18 U.S.C. §2519(3)。

[242] 何賴傑，錄音、錄影、電磁記錄等之調查(刑事訴訟法第一六五條之一第二項)，全國律師，8 卷 9 期，2004 年 9 月，頁 33。

[243] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 127。

院命令、事先通知用戶的法院命令以及搜索令狀。

1.傳票(Subpoena)：政府使用傳票可以取得用戶的基本與連線資訊[244]包括：(A)姓名；(B)地址；(C)區域與長途電話通聯紀錄，或是連線的時間與長度；(D)服務的長度與服務的類型；(E)電話或設備號碼或用戶號碼或其身分識別，其中包含任何臨時派發的網路位址；以及(F)支付該項服務的方式與來源，其中包含任何信用卡或銀行帳戶號碼。傳票的效力亦及於不受儲存通訊法保護的客體，員工將已讀取的電子郵件存放在公司的郵件伺服器上，此時公司並不屬於儲存通訊法定義下的電子通訊服務或遠端計算服務的提供者，政府可以使用傳票強制公司提供該已讀取的電子郵件[245]。

傳票的種類包括依據聯邦或州法律所核發的行政傳票、聯邦或州大陪審團傳票或審判傳票[246]。

2.事先通知用戶的傳票(Subpoena with Prior Notice to the Subscriber or Customer)：政府使用傳票並事先通知該用戶，或有符合 2705(d)允許延遲通知的事由，可以取得以下資訊：

(1)不要求事先通知的傳票所能取得的所有資訊[247]；

(2)儲存在電子通訊服務提供者超過 180 天之有線或電子通訊內容[248]；以及

(3)儲存在遠端計算服務提供者之有線或電子通訊內容[249]。

事先通知是指通知該用戶有關其儲存在服務提供者的資訊，將因傳票對服務提供者提示之後，政府將自服務提供者取得該用戶的資訊[250]。延遲通知規定在第 2705 條，有理由相信向用戶通知傳票的存在會阻礙正在進行的偵查或對個人的生命與安全造成危害，經上級督導長官簽署書面確認後可以延長 90 天，若前述不利的事實持續存在，經再次簽署書面確認可再延長另一個 90 天，並在延遲期間結束後，政府應將該傳票與書面解釋延遲通知的理由，送達該用戶[251]。

3.法院命令(Court Order)：政府使用法院命令，可以取得以下資訊：

(1)不要求事先通知的傳票所能取得的所有資訊[252]；

---

[244] 18 U.S.C. §2703(c)(2)。
[245] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 128。
[246] 18 U.S.C. §2703(c)(2)(F)。
[247] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 129。
[248] 18 U.S.C. §2703(a)。
[249] 18 U.S.C. §2703(b)(1)(B)(i)。
[250] 法思齊，美國法上數位證據之取得與保存，頁 123。
[251] 18 U.S.C. §2705。
[252] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 130。

(2)向電子通訊服務或遠端計算服務提供者取得有關該用戶的紀錄或其他資訊，不包括通訊內容[253]。

有管轄權法院依據政府單位所提出特定且描述清楚的事實，顯示有合理的基礎可以相信所欲取得的通訊內容、紀錄或其他資訊與正在偵查中的犯罪有關且重要，可以核發法院命令，當服務提供者立即對法院命令提出異議，指出該命令將造成其不適當的負擔時，法院可以對該命令撤銷或修改[254]。

核發法院命令的法官可以是，聯邦治安法官、聯邦地方法院或相對等州法院法官，聯邦法院所核發的法院命令在其管轄區域外，依然具有效力[255]。

4.事先通知用戶的法院命令(Court Order with Prior Notice to the Subscriber or Customer)：政府使用法院命令並事先通知該用戶，或有符合 2705(d)允許延遲通知的事由，可以取得以下資訊：

(1)不要求事先通知的法院命令所能取得的所有資訊[256]；

(2)儲存在電子通訊服務提供者超過 180 天之有線或電子通訊內容[257]；以及

(3)儲存在遠端計算服務提供者之有線或電子通訊內容[258]。

延遲通知規定在第 2705 條，有理由相信向用戶通知法院命令的存在會阻礙正在進行的偵查或對個人的生命與安全造成危害，經向核發該命令之法院呈報並經確認後可以延長 90 天，若前述不利的事實持續存在，經再次呈報並經確認可再延長另一個 90 天，並在延遲期間結束後，政府應將該傳票與書面解釋延遲通知的理由，送達該用戶[259]。

5.搜索令狀(Search Warrant)：政府使用搜索令狀不需事先通知該用戶，可以取得以下資訊：

(1)要求事先通知的法院命令所能取得的所有資訊[260]；以及

(2)儲存在電子通訊服務提供者等於或少於 180 天之有線或電子通訊內容[261]。

令狀的核發必須向法院提出宣誓書(affidavit)並符合聯邦刑事程序規則或州令狀程序相關規定，聯邦法院依據第 2703 條所核發的令狀，在該核發令狀法院管轄區外依然

[253] 18 U.S.C. §2703(c)(1)。
[254] 18 U.S.C. §2703(d)。
[255] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 130-131。
[256] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 132。
[257] 18 U.S.C. §2703(a)。
[258] 18 U.S.C. §2703(b)(1)(B)(ii)。
[259] 18 U.S.C. §2705。
[260] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 133。
[261] 18 U.S.C. §2703(a)。

具有效力[262]，令狀的執行並不需要由執法人員親自搜索服務提供者的電腦系統，而是將令狀提示給服務提供者，由服務提供者依據令狀所載的內容取得所指定的資料後交給執法人員[263]，對於通訊內容的搜索通常會採用兩步驟的搜索方式，首先由服務提供者整理出特定用戶帳號內的全部電子郵件，再由執法人員逐一檢驗是否屬於令狀所特定的應扣押的標的再加以扣押[264]。

以位階而言令狀高於法院命令，法院命令高於傳票，位階高者可以取得更多的資訊，也需要符合更高的條件門檻才能核發。以非內容資訊而言，就不要求事先通知的法院命令與傳票兩者相較，該法院命令可以取得更多類型的非內容資訊。內容資訊必須要有法院核發的搜索令狀才能取得，另一種取得內容資訊的方法即是以事先通知用戶的傳票或法院命令取得儲存在電子通訊服務提供者超過 180 天之有線或電子通訊內容，或是儲存在遠端計算服務提供者之有線或電子通訊內容。

受儲存通訊法保護的資料，有兩種情形允許政府不用傳票可以取得資訊，首先是經用戶同意之非內容資訊的提供，其次是偵查中的電話行銷詐欺案件，由執法人員向服務提供者提出正式書面請求，即可取得該從事電話行銷用戶之姓名、地址以及營業場所所在位置等資訊[265]。

第二款 自願提供

儲存通訊法普遍禁止對公眾提供服務的電子通訊服務與遠端計算服務提供者洩漏其用戶之紀錄、其他資訊以及通訊內容，除非有例外的情形發生[266]。當考慮是否符合自願提供的例外時，首先要考慮的是該服務提供者有沒有對公眾提供服務，如果不對公眾提供服務則不受儲存通訊法的限制[267]。

儲存通訊法允許服務提供者在下列情形，可以選擇自願提供用戶的通訊內容[268]：

(1)對該通訊的收受者、經發出通訊或收受通訊者的同意、對傳遞過程中經手該通訊

[262] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 134。
[263] 18 U.S.C. §2703(g)。
[264] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 134。
[265] 18 U.S.C. §2703(c)(1)(C), §2703(c)(1)(D)。
[266] 18 U.S.C. §2702(a)。
[267] Andersen Consulting LLP v. UOP, 991 F.Supp. 1041, 1043 (N.D. Ill. 1998)，UOP 公司提供給員工使用的電子郵件系統沒有對公眾提供服務，儲存通訊法不禁止該公司揭露員工存放在郵件伺服器內的通訊內容。
[268] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 136。

之人、依循特定法律程序、或經遠端計算服務提供者之用戶同意，所爲之揭露[269]；

(2)附隨於提供服務或保護服務提供者之權利或財產之所必需，所爲之揭露[270]；

(3)依據 2258A 對國家失蹤與剝削兒童中心，所爲之通報揭露[271]；

(4)由服務提供者所意外取得且與犯罪之進行有關，對執法人員所爲之揭露[272]；或是

(5)服務提供者善意信任，存在涉及他人死亡危險或嚴重身體傷害之緊急情狀，必須立即提供與該緊急情狀有關通訊，對政府單位所爲之揭露[273]。

儲存通訊法允許服務提供者在下列情形，可以選擇自願提供用戶的紀錄或其他資訊給政府單位或他人：

(1)經該用戶的同意或經第 2703 條的授權，所爲之揭露[274]；

(2)附隨於提供服務或保護服務提供者之權利或財產之所必需，所爲之揭露[275]；

(3)服務提供者善意信任，存在涉及他人死亡危險或嚴重身體傷害之緊急情狀，必須立即提供與該緊急情狀有關通訊，對政府單位所爲之揭露[276]；

(4)依據 2258A 對國家失蹤與剝削兒童中心，所爲之通報揭露[277]；或是

(5)對政府單位以外之其他人，所爲之揭露[278]。

第三款 網路犯罪偵查之證據保存

網路犯罪的偵查經常必須倚賴網路服務提供者的協助，服務提供者所持有的網路相關紀錄於追溯犯罪者的過程中經常提供重要的線索，沒有法律規定網路服務提供者應該將與其用戶帳號有關的紀錄保存多久或多完整，這將依各個服務提供著的經營規劃與其所擁有的資源而有所不同，有的保存完整且長達一定的時間，有的時間較短甚至沒有保存[279]。

爲了避免有助於犯罪偵查的證據遭到銷毀或遺失，執法人員著手偵查網路犯罪的第

[269] 18 U.S.C. §2702(b)(1)-(4)。
[270] 18 U.S.C. §2702(b)(5)。
[271] 18 U.S.C. §2702(b)(6)。
[272] 18 U.S.C. §2702(b)(7)。
[273] 18 U.S.C. §2702(b)(8)。
[274] 18 U.S.C. §2702(c)(1)-(2)。
[275] 18 U.S.C. §2702(c)(3)。
[276] 18 U.S.C. §2702(c)(4)。
[277] 18 U.S.C. §2702(c)(5)。
[278] 18 U.S.C. §2702(c)(6)。
[279] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 139。

一件事情就是通知網路服務提供者保存有關特定用戶帳號相關的資料，並同時向法院聲請強制揭露該些資訊的許可。

電子通訊服務或遠端計算服務之提供者，在收到政府單位的請求後應立即採用所有可能措施以保存其所持有的紀錄與其他證據，等待政府單位聲請法院命令或其他程序的核准向政府單位的強制揭露，前述紀錄應保存 90 天，在收到政府單位的延長請求之後，可以延長保存另一個 90 天[280]。

2703(f)並未規定提出通知的形式，因此一通電話將可以符合通知的要求，但是以書面的方式經由傳真或電子郵件的方式送達，不僅可以留下紀錄而且可以防止誤解，將是比較安全且可行的方法，但是要特別注意的是只能要求服務提供者保存當時已經儲存在服務提供者的紀錄，若要取得尚未發生的紀錄則必須符合通訊監察相關的規定[281]。

除了緊急保存的要求之外，基於偵查的秘密性，執法人員在聲請強制揭露許可時可以請求法院指示經提示該許可的服務提供者，不得洩漏該揭露許可的存在，當執法人員認爲存在下列可能性時[282]：

(1)危及個人之生命或身體安全；

(2)逃離法律訴追；

(3)使證據遭到破壞或竄改；

(4)恐嚇證人；或是

(5)嚴重妨害偵查或不當延遲審判。

第四款 違法的責任

執法人員依據儲存通訊法第 2703 條所爲之強制揭露，經常招致違反憲法第四增修條文的挑戰，而主張有證據禁止法則的適用，依據聯邦最高法院在 Illinois v. Krull[283]一案中所表示的看法認爲，執法人員的責任是確實履行令狀或法律所記載的規定，證據禁止的目的是要對執法人員違反第四增修條文的行爲產生嚇阻的作用，法院認爲若賦予客觀合理信任該法律所導致的憲法第四增修條文違反證據禁止的效果，將不會產生任何的嚇阻效果，因爲審核令狀或法律的合憲性並非執法人員的責任[284]。

遵守儲存通訊法所取得的證據沒有證據禁止的適用，違反儲存通訊法但不構成憲法

[280] 18 U.S.C. §2703(f)。
[281] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 140。
[282] 18 U.S.C. §2705(b)。
[283] Illinois v. Krull, 480 U.S. 340 (1987)。
[284] Illinois v. Krull, 480 U.S. 340, 249-350 (1987)。

第四增修條文的違反，所取得的證據也沒有證據禁止的適用，立法者在制定儲存通訊法當時僅提供民事救濟的方式[285]。

在民事部分受侵害之人可請求暫時處分、2707(c)所規定之損害賠償，若涉及故意違反將有懲罰性損害賠償的適用、以及律師費與相關訴訟成本[286]。美國政府的雇員若涉及故意違反將受行政處分[287]。民事請求權在受侵害之人有合理機會知悉該侵害事實的存在之日起算，逾兩年不行使而消滅[288]。

善意信任下列事項所導致的儲存通訊法違反，在民刑事訴訟中可以主張完全的抗辯[289]：

(1)法院令狀或命令、大陪審團傳票、立法或法律授權(包括政府單位依據 2703(f)所提出保存證據之要求)；

(2)應執法人員要求的 2518(7)緊急通訊監察；或是

(3)善意信任是 2511(3)所允許的行爲。

第五款 監督

儲存通訊法賦予執法部門向國會的報告義務，在每個年度聯邦檢察總長應向眾議院與參議院司法委員會提出包括下列內容的報告[290]：

(1)司法部依據 2702(b)(8)所接受自願揭露通訊內容的數量；以及

(2)該些揭露的基礎事實整理，其中包括：

(A)依據 2702(b)(8)對司法部的自願揭露；以及

(B)與該些揭露有關所終結的偵查，沒有提出刑事告訴的數量。

第三節 搜索與扣押

第一項 以合理隱私期待之存在為區分

美國憲法第四增修條文保障人民有免於不合理搜索與扣押的自由，憲法的文字並未對搜索與扣押做出直接的定義，而是藉由聯邦最高法院在個案中所確立的原則，勾勒出

[285] United States v. Reyes, 922 F. Supp. 818, 837-838 (S.D.N.Y. 1996)。
[286] 18 U.S.C. §2707(b)。
[287] 18 U.S.C. §2707(d)。
[288] 18 U.S.C. §2707(f)。
[289] 18 U.S.C. §2707(e)。
[290] 18 U.S.C. §2702(d)。

搜索與扣押的行爲態樣[291]。

政府對於人民受憲法保護區域的物理入侵，將構成憲法第四增修條文意義下的搜索行爲，依聯邦最高法院早期對該區域所及範圍的見解，即憲法第四增修條文中所提到的「人民身體、住所、文件及財產[292]。」在 Katz 一案中將受憲法保障的區域由有形的實體延伸至具有合理隱私期待的無實體形狀之通訊內容，任何對該具有社會認可的合理隱私期待的侵犯，即構成憲法第四增修條文意義下的搜索行爲[293]。

附隨於一個搜索行爲之後，對於個人財產持有利益的干預行爲即是扣押行爲[294]，在科技發達之前扣押行爲的客體僅限於有實體形狀的物件，隨著科技的進步具有個人合理隱私期待的通訊內容，亦能以無實體形狀的樣貌出現，在 Berger v. New York 一案中認爲對無實體形狀的通訊內容的截取亦是扣押行爲的一種[295]。

第一款 容器理論

聯邦最高法院在許多的判決中一再強調，處於無法一目瞭然(plain view)其內容物的封閉不透明容器(opaque closed container)，其合理的隱私期待受有憲法第四增修條文的保護，即使是在允許無令狀搜索的汽車搜索過程中所尋得的封閉容器，其所受憲法第四增修條文的保障，並不因爲發現該封閉容器的存在是基於一個合法無令狀搜索，而有所減損[296]。

電腦、行動儲存裝置(例如，隨身碟)或是行動電話，這類具有儲存數位資料功能的裝置，是否可以被視爲封閉容器而主張具有合理的隱私期待，取得這些裝置所儲存資料的行爲，是否構成憲法第四增修條文意義下的搜索行爲，而有令狀原則的適用，這將影響電腦網路犯罪偵查過程中，執法人員所應遵循的法定程序以避免因違法搜索而導致證據禁止的效果。

法院認爲可以將儲存裝置視爲一個封閉容器，將數位資料儲存在該容器中主觀上已經呈現對該儲存的內容具有隱私的期待，對於該容器的搜索將有令狀原則的適用[297]。儘管法院普遍採取將電子儲存裝置視爲封閉容器的看法，彼此間還是存在著些微的差異，第五巡迴上訴法院採用將一整個儲存裝置視爲一個封閉容器的看法，當私人搜索儲存裝

[291] 謝昆峰，網際網路與刑事偵查，頁 15-16。
[292] 王兆鵬，重新定義高科技時代下的搜索，頁 168。
[293] Katz v. United States, 389 U.S. 347, 360-361 (1967)。
[294] United States v. Jacobsen, 466 U.S. 109, 113 (1984)。
[295] Berger v. New York, 388 U.S. 41, 59 (1967)。
[296] Robbins v. California, 453 U.S. 420, 425-426 (1981)。
[297] United States v. Runyan, 275 F.3d 449, 458 (5th Cir. 2001)。

置的一部分之後，個人對該封閉容器內容的隱私期待已經因爲私人搜索的開啓與檢查而不復存在，警察接手搜索該儲存裝置內更多的檔案並不構成違法搜索，因爲警察的搜索行爲並未超出先前私人搜索的範圍[298]。

隨著資訊科技的進步，儲存裝置的容量已經幾乎具有承載相當於一個圖書館藏書的能力，其中交互混雜著各種類型的資料，如果將儲存裝置簡單的類比成封閉容器或檔案櫃，將隱藏著更多在搜索過程中侵害個人隱私的風險，法院必須明瞭儲存裝置的特性，並採取相應的措施[299]。

第十巡迴上訴法院，採取將個別的檔案視爲一個單獨容器的看法，認爲警察不依據令狀上的指示搜索儲存裝置中與非法販賣毒品有關的資訊，轉而搜索該儲存裝置中兒童色情的圖片，已經逾越令狀所允許的搜索範圍[300]。

無論是將一整個儲存裝置視爲一個封閉容器，或是其中的個別檔案分別視爲一個單獨的容器，將不影響儲存裝置中所儲存的資料具有隱私期待的看法，有差別的是令狀將如何特定搜索客體與一目瞭然法則適用的問題。

第二款 公開分享的資料

聯邦最高法院在 California v. Greenwood 一案中表示，被丟棄的垃圾無法主張合理的隱私期待，由於該被拋棄的物件已經處於公眾可接觸的狀態下，因此不具有合理的隱私期待[301]。Stewart 大法官在 Katz 一案的法院意見中指出，一個人有意識地暴露在公眾之下，即使是在其住家或辦公室中，將不受到憲法第四增修條文的保護[302]。

個人可以主張存放在其電腦中資料的合理隱私期待，但是將資料上傳到網路或公用電腦使其處於其他人可接觸的公開分享狀態，將不能主張對該些資料具有合理的隱私期待，或是透過網路使他人可以存取自己電腦的特定儲存區域內的資料，在連上網路的那一剎那就不能再主張對該分享區域的合理隱私期待[303]。

第三款 第三人持有

依據聯邦最高法院在 United States v. Miller 一案中，所揭示的風險承擔原則指出，

298 United States v. Runyan, 275 F.3d 449, 464-465 (5th Cir. 2001)。
299 United States v. Walser, 275 F.3d 981, 986 (10th 2001)。
300 United States v. Carey, 172 F.3d 1268, 1274 (10th Cir. 1999)。
301 California v. Greenwood, 486 U.S. 35, 39-40 (1988)。
302 Katz v. United States, 389 U.S. 347, 351 (1967)。
303 USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 5-6。

憲法第四增修條文並不禁止政府自第三人處取得他人所揭露給該第三人的資訊，既使該資訊的揭露是基於特定的用途以及確信該第三人不會洩漏的假設前提下[304]。由以上聯邦最高法院的判決精神可以推知，一個人將所管領具有合理隱私期待的物件或資訊交給第三人使其置於該第三人實力支配之下，原持有者將不能再主張對該物件或資訊之合理隱私期待。

郵件的寄送者在遞送過程中，仍保有對於該郵件內容合理的隱私期待，等郵件到達收件者之後，寄件者對該郵件內容的合理隱私期待才會消失，雖然在遞送的過程中必須藉由許多第三人的通力合作，才能將郵件往收件者的方向傳遞，仍不影響在郵件到達收件者之前，寄送者對該郵件內容的合理隱私期待。既使郵件被傳遞至一個錯誤的收件者並經該錯誤收件者的開啓，仍然不改變寄件者對該郵件內容合理隱私的期待[305]。

在 Smith v. Maryland 一案中，聯邦最高法院認爲在撥打電話的過程中自願地將受話方的電話號碼揭露給電信公司以完成通話線路的建立，不能對該撥出的號碼主張具有合理的隱私期待，因而認爲使用撥號記錄器與追蹤裝置以捕捉電話號碼的行爲不構成憲法第四增修條文意義下的搜索行爲[306]。在網路通訊的過程中必須對許多協助完成網路通訊的服務提供者揭露電子郵件位址或網際網路位址等路由資訊，以達成將信息傳遞至目的地，網路通訊使用者不能對電子郵件位址或網際網路位址等這類已經第三人持有的路由資訊，主張具有合理的隱私期待[307]。

法院普遍認爲將物件傳遞給第三人之後即喪失對該物件的合理隱私期待，例外的情形是短暫寄放於第三人處，且對該寄放之物件仍保有控制權，則依然可以主張對該物件的合理隱私期待，例如寄放的上鎖行李、磁片封存在信封內交給朋友保管或是租用的置物櫃[308]。要特別注意的是，一開始擁有的控制權可能會因爲時間的流逝而喪失，例如超過租用期限且沒有繼續給付租金的置物櫃，將會喪失對該置物櫃內容的合理隱私期待[309]。

---

304 United States v. Miller, 425 U.S. 435, 443 (1976)。

305 Walter v. United States, 447 U.S. 649, 658-659 (1980)。

306 Smith v. Maryland, 442 U.S. 735, 744 (1979)。

307 United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008)。

308 USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 9-10。

309 United States v. Poulsen, 41 F.3d 1330, 1337 (9th Cir. 1994)，Poulsen 租用的置物櫃已經超過期限且沒有繼續給付租金，遭到置物櫃所有人對存放在該置物櫃內物件行使留置權，此時 Poulsen 已經喪失對該置物櫃內容的合理隱私期待。

第四款 私人搜索

憲法第四增修條文保障人民有免於不合理搜索與扣押之自由，這個憲法誡命僅限於用以對抗政府對人民合理隱私期待的侵犯行爲，私人以自己的決定所進行的搜索與扣押行爲，只要不涉及扮演政府的代理人或是有政府官員的參與或知悉，即便該搜索與扣押行爲是不合理的，都沒有憲法第四增修條文的適用[310]。

一旦隱私期待遭到私人的入侵行爲破壞之後，憲法第四增修條文將不禁止政府使用已經不再具有隱私性質的資訊[311]。有關政府使用私人搜索的成果是否應該有任何的限制，聯邦最高法院在 Walter v. United States 一案中表示，如果經由令狀所允許的政府搜索行爲都要限制在令狀中所特定出的授權範圍內執行，政府利用私人侵犯他人隱私所取得的資訊，也必須受到如同令狀特定性相同的限制[312]。對於政府所接續的無令狀搜索行爲，必須加以檢視是否超出私人搜索的範圍，而構成另一個搜索行爲[313]。

電腦網路犯罪偵查作爲的發動，經常是起源於電腦維修工程師在檢修客戶電腦的過程中發現犯罪證據，將證據呈報給執法人員[314]，這是一種涉及電腦常見的私人搜索態樣，執法人員欲接續一個私人搜索而進一步檢視該私人行爲所發現的證據，此時因涉及電子儲存裝置，對於該私人搜索範圍的認定，將取決於不同巡迴上訴法院對容器理論的看法不同而有不同的結果。

採第五巡迴上訴法院將一整個儲存裝置視爲一個封閉容器看法的法院，其轄區下的執法人員在私人搜索儲存裝置的一部分之後，可以接手搜索該儲存裝置內更多的檔案而不構成違法搜索，因爲該搜索行爲並未超出先前私人搜索的範圍[315]。採第十巡迴上訴法院將個別的檔案視爲一個單獨容器看法的法院[316]，其轄區下的執法人員僅能就私人搜索所提供的資訊加以檢視，接觸未於私人搜索過程中所發現的檔案或資訊，將構成另一個新的搜索行爲而有令狀原則的適用。

私人搜索所發現的資訊經常連結後續的政府犯罪偵查工作，該私人搜索是否屬於政府行爲的一部分，是否只是政府爲了規避法律上的要求所採取的權宜措施，經常於個案中遭到欲主張證據禁止方的挑戰。對於區別私人搜索與政府搜索，歸納聯邦巡迴上訴法

---

310 United States v. Jacobsen, 466 U.S. 109, 113 (1984)。
311 United States v. Jacobsen, 466 U.S. 109, 117 (1984)。
312 Walter v. United States, 447 U.S. 649, 657 (1980)。
313 United States v. Jacobsen, 466 U.S. 109, 115 (1984)。
314 United States v. Hall, 142 F.3d 988, 991 (7th Cir. 1998)。
315 United States v. Runyan, 275 F.3d 449, 464-465 (5th Cir. 2001)。
316 United States v. Carey, 172 F.3d 1268, 1274 (10th Cir. 1999)。

院的判決可以獲得以下三個判斷要點：政府是否知悉或默許這個侵入行爲、執行搜索之一方是否基於協助政府的目的、以及政府是否確實鼓勵、發起或唆使該私人行爲[317]。

電腦駭客入侵他人電腦將所蒐集到的兒童色情犯罪證據，以電子郵件寄給聯邦調查局，觸發對該犯罪的偵查並導致犯罪嫌疑人的定罪[318]，事後聯邦調查局探員以電子郵件與該駭客聯繫表達對其協助行爲的感謝，並表示有類似的犯罪資訊可以繼續提供給他們[319]。經過數個月之後該駭客繼續基於協助政府的目的，提供其以相同的入侵方式所蒐集到另一個犯罪嫌疑人 Jarrett 電腦中的兒童色情犯罪證據，使聯邦調查局建立相當理由聲請對 Jarrett 的搜索令狀並導致逮捕，在審判中 Jarrett 主張該駭客是居於政府代理人的角色，聯邦地方法院核准該非法取得證據的禁止，第四巡迴上訴法院表示本案中政府操作在趨近禁止線的邊緣，然而政府事前對於該駭客入侵 Jarrett 的電腦以取得犯罪證據並未知悉與默許，因此不成立政府代理人的關係[320]。

第五款 政府工作場所搜索

聯邦最高法院在 O'Connor v. Ortega 一案中表示，政府部門的員工不因爲在政府部門之場所工作而失去憲法第四增修條文的保障[321]。因此，由政府部門管理者所執行對其員工私人財物的搜索與扣押行爲，仍有憲法第四增修條文的適用[322]。然而，基於該場所的實際營運情形，由其管理者而非執法人員所爲之入侵，將使員工部分的隱私期待成爲不可能，特別是依據辦公室的實際運作或正式的工作規則，將使員工在其辦公室、辦公桌、以及檔案櫃的隱私期待有所減損[323]。

法院在衡量由政府部門管理者所執行的搜索行爲是否合理時，要考量其員工之正當隱私期待所受到的侵犯與政府對於該工作場所之監督、控制、與營運效率之需求，兩方之間的平衡[324]。法院認爲政府部門管理者基於非犯罪偵查性質之工作相關目的以及調查與工作相關的不當行爲之必要，對其員工受憲法保護隱私利益之侵犯，若仍需要具備相當理由與符合令狀要求，將對政府部門的經營效率帶來重大的負擔[325]。

---

317 USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 12。
318 United States v. Steiger, 318 F.3d 1039 (11th Cir. 2003)。
319 United States v. Jarrett, 338 F.3d 339, 341 (4th Cir. 2003)。
320 United States v. Jarrett, 338 F.3d 339, 346-347 (4th Cir. 2003)。
321 O'Connor v. Ortega, 480 U.S. 709, 717 (1987)。
322 O'Connor v. Ortega, 480 U.S. 709, 715 (1987)。
323 O'Connor v. Ortega, 480 U.S. 709, 717 (1987)。
324 O'Connor v. Ortega, 480 U.S. 709, 719-720 (1987)。
325 O'Connor v. Ortega, 480 U.S. 709, 725-726 (1987)。

在衡量政府部門管理者的搜索行爲是否合理時，必須依據搜索的發動(inception)與範圍(scope)這兩個因素加以衡量，亦即是否有合理的基礎相信該搜索行爲可以取得該員工與工作相關不當行爲的證據，或是基於非犯罪偵查性質之工作相關目的之所必需，以及其範圍僅合理的及於搜索的目標，而不至於過渡擴大[326]。

法院受到 O'Connor 案的啓發，評估政府部門員工在工作場所是否享有合理隱私期待時，將會考量以下因素：該區域是否僅由該員工單獨使用、他人是否有權使用該區域、工作的性質是否需與他人密切合作、辦公室規則是否提醒該特定區域有被搜索的可能、以及被搜索的財產是公有的或私有的[327]。

在執行政府工作場所電腦搜索，考量政府部門員工對該政府電腦是否享有合理的隱私期待時，該工作場所之雇用政策與電腦登入畫面所揭露的訊息將扮演著重要的角色，經由文字的方式清楚的記載並提醒使用者對於存放在該電腦或網路中的資訊是否享有隱私期待，如果已經清楚地通知員工其在網路上的活動以及儲存在電腦中的資訊，將不定期的受到監看、稽核與檢查，則不能主張其在工作場所的電腦具有合理的隱私期待[328]。

第二項 無令狀搜索－令狀原則的例外

Harlan 大法官在 Katz 案的協同意見書中指出，政府對於人民受憲法保障區域的入侵普遍需要令狀的核發，除非是有特定的例外情形[329]。當執法人員欲執行搜索時，首先應考慮這樣的行爲是否構成對人民合理隱私期待的入侵，該行爲若構成憲法第四增條文意義下的搜索行爲，則進一步確認是否有符合無令狀搜索的例外情形，聯邦最高法院在判決中承認數種合法的無令狀搜索，以下僅就電腦網路犯罪偵查中較常用的無令狀搜索加以討論。

第一款 同意搜索

Katz 案指出任何人有意識地暴露在公眾之下將不具有合理的隱私期待，同意是一種放棄(waiver)其受憲法第四增修條文保護的意思表示，當一個人自願地同意(consent)接受執法人員的搜索，此時的政府行爲並不構成對人民合理隱私期待的侵犯，而政府負有

326 O'Connor v. Ortega, 480 U.S. 709, 726 (1987)。
327 USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 46-47。
328 United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000)。
329 Katz v. United States, 389 U.S. 347, 362 (1967)。

舉證責任證明被搜索對象是有意地放棄一個已知的權利[330]。法院在考量同意是否在自願地情形下發生，必需依據該決定是否在自由與沒有受到任何限制的情況下所做成、是否瞭解將有可能蒐集到對其不利的證據、以及是否遭受過度的壓迫與自我決定的能力已經受到嚴重的干擾且將導致正當程序的違反，等綜合情況加以考量[331]。

搜索之同意並不僅限於被告才能行使，對於受搜索標的有「共同權限」(common authority)之第三人，都可以行使同意搜索的權限，共同權限的判斷並不是基於對該標的物的財產所有權，而應該是基於對該標的物的共同使用與管理的權限，因此房東不能行使對其已出租房子的同意搜索，共同居住之人可以行使其共同使用區域的同意搜索，而共同使用該區域之全部成員也必須承擔其成員中有人會同意該共同區域被搜索的風險[332]。

同意搜索範圍的判斷必須依據，一般理性之人對於執法人員與被搜索對象之間所交換訊息之客觀合理性的解讀[333]，並以書面記錄同意的範圍以利後續之解讀與判斷。對於場所的同意搜索其範圍是否及於存在該場所中的電腦，第十巡迴上訴法院採用比較緊縮的見解，不同意政府主張的對公寓的同意搜索及於存放在電腦中的檔案[334]，因此務實的作法是當場經由被搜索人的同意將搜索的範圍擴及至電腦內的檔案，或是將該電腦扣押帶離現場，向法院聲請另一張令狀以搜索該電腦的內容。

第二款 緊急搜索

聯邦最高法院在判決中基於保護證據或執法人員的安全，曾經允許下列數種不及聲請令狀的緊急情狀(exigent circumstances)搜索行為：證據正處於即將被破壞的危險、執法人員正在追緝嫌犯當中、保護執法人員的安全、嫌犯可能會逃逸[335]，當有類似上述四種情況發生時，政府的搜索行為將不被認為是對於人民合理隱私期待的侵犯。

儲存在電腦中數位資料的容易被毀壞是導致緊急搜索經常在電腦搜索中被採用的原因之一，電腦中的資料可能因為被刪除、受潮、高溫、或是儲存裝置實體遭到破壞，將使得讀取儲存在其中的資料不再可能，而有採取緊急扣押將該裝置隔離於該受搜索對象實力支配之外的必要，有限儲存容量的通訊裝置將因持續進入的訊息覆蓋先前儲存的

330 Schneckloth v. Bustamonte, 412 U.S. 218, 325 (1973)。
331 Schneckloth v. Bustamonte, 412 U.S. 218, 225-226 (1973)。
332 United States v. Matlock, 415 U.S. 164, 171-172 (1974)。
333 Florida v. Jimeno, 500 U.S. 248, 251 (1991)。
334 United States v. Carey, 172 F.3d 1268, 1274 (10th Cir. 1999)。
335 Georgia v. Randolph, 547 U.S. 103, 117 (2006)。

資料[336]，或是短暫存放在揮發性記憶體中的資料將因失去電源供應而消失，而有採取緊急搜索的必要，快閃記憶體是一種典型的非揮發性記憶體其所儲存的資料不會因電源消失而遺失資料，基於這項特性而被普遍使用於今日的行動電話或個人數位助理等行動電子裝置之中，對於這類含有快閃記憶體裝置若主張因失去電源供應將導致資料流失而採取的緊急搜索，是不合理的[337]。

緊急搜索必須被嚴格限制在只有面臨急迫而來不及聲請令狀的情況下，其發動才有正當性[338]。搜索與扣押涉及不同的憲法利益，與搜索相較下扣押本質上較不具侵略性，法院經常核准基於相當理由的無令狀扣押[339]。合法執行的無令狀緊急扣押電腦，當緊急情況已經不復存在時，並不代表存在緊急搜索該遭到扣押電腦的合理性[340]。該遭到扣押的電腦已經隔離於犯罪嫌疑人實力支配之外，不再處於可能遭受惡意毀損資料的危急情況之下，因此必須取得另一張令狀才能合法地搜索該扣押電腦的內容。

第三款 附帶搜索

附隨於犯罪嫌疑人的合法逮捕行為(incident to a lawful arrest)之後，執法人員可以在沒有令狀的情形下執行對該受逮捕對象的全身搜索以及搜索其立即可接之觸鄰近區域(the area within his immediate control)，這項例外允許是基於避免證據受到毀損與執行逮捕人員遭受傷害[341]。

執法人員在離開逮捕現場後才執行搜索附隨於逮捕行為所扣押的手提箱，聯邦最高法院認為此時該手提箱已經排除於該受逮捕對象的實力支配之外，且不存在該受逮捕對象從該手提箱中取得武器或毀損證據的緊急情狀危險，因此該搜索行為不再是附隨於逮捕的附帶搜索行為[342]。

應用以上的原則，附隨於逮捕所取得的電腦與類似的儲存裝置，基本上將有附帶搜索原則的適用。

除非面臨行動通訊裝置所儲存的號碼會被不斷進來的新號碼所覆蓋的情況外，現今

---

[336] United States v. Ortiz, 84 F.3d 977, 984 (7th Cir. 1996)，在逮捕的附帶搜索過程中，執法人員從呼叫器讀取號碼是合法的，因為呼叫器中的資訊容易被破壞。

[337] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 28-30。

[338] Terry v. Ohio, 392 U.S. 1, 25-26 (1968)。

[339] Segura v. United States, 468 U.S. 796, 806 (1984)。

[340] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 30。

[341] Chimel v. California, 395 U.S. 752, 763 (1969)。

[342] United States v. Chadwick, 433 U.S. 1, 14-16。

的行動通訊裝置已經幾乎等同於一部電腦，基於電腦作業系統的運作特性，不建議於逮捕現場進行電腦內資料的搜索，以避免因爲翻動資料夾的內容或開啓檔案，導致時間或相關系統狀態的改變，而影響到證據產生時間點的認定，比較安全可行的作法是先行將該電腦或行動通訊裝置扣押，取得令狀之後在實驗室以電腦鑑識的方法對該電腦或行動通訊裝置執行搜索[343]。

第四款 一目瞭然法則

當執法人員處於合法的地位得以觀察與接觸特定證據，且該證據具有明顯的犯罪特質，此時例外允許在沒有令狀的情形下，依據一目瞭然(plain view)法則對該證據進行扣押[344]。亦即執法人員必須先有一個合法的搜索行爲才能主張其無令狀扣押行爲是合法的，因此附隨於有令狀的搜索以及合法的無令狀搜索之後的扣押行爲，都有一目瞭然法則的適用。

在搜索電腦時合法搜索範圍的界定將取決於由容器理論所劃定的範圍，從本文有關容器理論的介紹中可以瞭解到，第五巡迴上訴法院與第十巡迴上訴法院對於容器理論不同的看法，在應用一目瞭然法則時也將帶來相當的差異，第五巡迴上訴法院所採取的將整個儲存裝置視爲一個容器的看法，當存在一個對該封閉容器的合法搜索行爲，將使得該容器內具有犯罪性質的資料，處於一目瞭然法則適用下的應扣押客體。

將整個儲存裝置視爲一個容器的看法以及輔以一目瞭然法則的應用，是最能有效掌握不在令狀所特定範圍內的其他犯罪證據，犯罪者經常會以變更或僞裝檔名的方式隱藏具有犯罪性質的資料，第九巡迴上訴法院質疑是否應限定特定的搜索方法，例如以關鍵字搜尋，而主張對整個儲存裝置的完全檢視，才是最能發現犯罪證據的方法[345]。

第十巡迴上訴法院基於一個檔案視爲一個單獨容器的看法，認爲執法人員必須清楚他想要在電腦上找到什麼樣的證據而且以避免碰觸到不在令狀所特定之其他檔案的方式執行搜索，執法人員所意外發現的犯罪證據可以立即扣押，但是要暫停搜索並聲請另一個令狀核准對該相同性質犯罪證據的搜索[346]。

---

[343] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 34。

[344] Horton v. California, 496 U.S. 128, 136 (1990)。

[345] United States v. Adjani, 452 F.3d 1140, 1150 (9th Cir. 2006)。

[346] United States v. Walser, 275 F.3d 981, 986-987 (10th Cir. 2001)。

第三項 令狀搜索

美國憲法第四增修條文後段規定，「搜索票或拘票，除本於相當理由，並經宣示或代誓宣言，且特別指明被搜索之處所及被扣押的人或物外，不應簽發。」亦即搜索與扣押必須要有令狀的核發才能進行。該項憲法誡命被稱爲令狀原則，違反令狀原則所取得的證據視爲非法證據，依據證據排除法則，非法取得的證據在審判中不得使用[347]，違法取證的人並應承擔相關的民刑事責任。

在聲請搜索令狀時必須先確立想要藉由搜索行爲的發動達成什麼樣的效果，爲了達成這個目標在事前應該詳細的規劃整個搜索的策略，找出足以說服核發令狀的法官存在相當理由可以經由搜索掌握相關的犯罪證據，以及證據均存在於令狀所特定的範圍之內，不至有疏漏的情形發生。

第一款 構思搜索策略

在撰寫搜索聲請書時，必須仔細考量在該即將發動的搜索行爲可以揭露什麼樣的證據，經由客觀事實的蒐集是否有相當理由的存在並足以支持證據存在該受搜索客體的確信，在今日的犯罪偵查電腦經常是一個被搜索的客體，除了物權性之外電腦的功能性是使其受到關注的另一個原因，電腦所扮演的角色可能是違禁品、犯罪證據的儲存裝置、或實施犯罪所使用的工具[348]。

要能夠先確定電腦在犯罪過程中所扮演的角色，才能確實掌握搜索的範圍與應扣押的標的。對場所的搜索發現電腦是屬於贓物之類的違禁品，則應該對該電腦的實體加以扣押。當電腦儲存有犯罪的證據，對該電腦實體的扣押並不足以使其成爲證明犯罪的證據，因此其儲存裝置的內容應被搜索，並扣押存放在該裝置中足以證明犯罪的證據。想要證明電腦曾經被當成實施犯罪的工具，除了犯罪嫌疑人遺留在電腦鍵盤上的指紋，搜索電腦系統在運轉過程中自動產生的相關系統檔案，將有助於掌握足以支持該電腦曾經被使用於犯罪的證據。

第二款 建立相當理由

搜索令狀的核發必須由中立的治安法官依據聲請書上所記載的整體事實所做出實

[347] 王兆鵬，重新定義高科技時代下的搜索，頁 166。
[348] USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 61-62。

際、普遍常識的決定，認爲存在違禁品或犯罪的證據將會在某特定場所發現的相當可能性[349]。此即滿足憲法第四增修條文所要求令狀的核發必須本於相當理由(probable cause)的標準。

依據搜索令狀對於搜索標的之特定描述，在執行搜索的過程中任何可能隱藏該標的的封閉容器將立即被打開，此時個人對於該容器的隱私利益將因爲核發令狀治安法官基於相當理由所做的決定而退讓[350]。電腦具有如同公事包一般收納文件與記錄的功能，依據這個聯邦最高法院所建立的原則，在搜索電腦的情形中並不需要特別指明對電腦的搜索，只要核准搜索的標的可能存在電腦之中即可[351]。而科技的進步也使得，在令狀中明確指定搜索標的將以何種形式存在，不再可能[352]。

當執法人員發現某個特定網際網路位址可能與犯罪的發生有關，並由服務提供者處取得該網際網路位址的實際裝機地址，將可以建立搜索該地址場所以及存在該場所電腦的相當理由，即使該受搜索之人抗辯網際網路位址是因爲不安全的無線網路遭到盜用所導致，仍不爲法院所接受，因爲相當理由的標準只需要存在相當的可能性將會發現犯罪證據即可滿足，並不需要達到超越合理懷疑(beyond a reasonable doubt)的證明程度[353]。

非法網站的網路會員帳號或電子郵件帳號，將成立對該會員帳號或電子郵件帳號持有者電腦搜索的相當理由，法院指出相當理由的建立必須在所懷疑的非法活動與將被搜索的財產之間找到連接點，因此可以合理的相信使用電子郵件寄送的色情圖片，將有可能在該帳號持有者的電腦或所附屬的儲存裝置中找到[354]。

第三款 特定搜索目標

搜索與扣押是對人民受憲法保障權利的干預，搜索侵犯人民的隱私期待，扣押將干預人民持有財產的利益，爲了避免空白搜索令狀的效果，必須藉由令狀將搜索與扣押的範圍加以特定，將侵害程度限制在最小的範圍內[355]。憲法第四增修條文的文字明確對於令狀的特定性作出指示，亦即必須指明「即將被搜索的場所」與「即將被扣押的人或物」。特定性的要求不僅沒有給予執行搜索與扣押的人員自行斟酌的空間，同時也可以達到避

[349] Illinois v. Gates, 462 U.S. 213, 238 (1983)。
[350] United States v. Ross, 456 U.S. 798, 823 (1982)。
[351] United States v. Giberson, 527 F.3d 882, 887 (9th Cir. 2008)。
[352] United States v. Reyes, 798 F.2d 380, 383 (10th Cir. 1986)。
[353] United States v. Perez, 484 F.3d 735, 740 (5th Cir. 2007)。
[354] United States v. Terry, 522 F.3d 645, 648 (6th Cir. 2008)。
[355] Andresen v. Maryland, 427 U.S. 463, 482 (1976)。

免扣押到不在令狀特定範圍內物品的效果[356]。

在涉及電腦的搜索與扣押時必須先確定電腦在犯罪中所扮演的角色，電腦如果是犯罪的證據、違禁品、實施犯罪的工具、犯罪的成果，則應該在令狀中指明對電腦實體的搜索與扣押[357]。電腦被用於駭客攻擊，被用於散佈色情圖片或是寄送恐嚇的威脅，在實施犯罪的過程中電腦的使用對於犯罪目的的達成具有相當的貢獻，才能將電腦認定爲實施犯罪的工具而符合將電腦實體扣押的規定，並不是只因其具有儲存資料的功能即可將電腦認定爲實施犯罪的工具[358]。

當電腦不具有違禁品或犯罪工具的特性，搜索電腦的目的只是爲了取得存放在其中的犯罪證據，有鑑於儲存裝置中經常混雜著各種與犯罪無關的資料，在令狀中特定搜索資料的類型是有其必要性[359]，若無法精確知道資料將以何種形式存在，以一種較廣或通稱的名詞來描述[360]，在搜索或扣押當時的環境下可以呈現特定性，亦符合特定性的要求[361]，但應儘量避免使用「任何以及全部之資訊或資料」這類的描述，且沒有附加任何的限縮條件，將被視爲一種範圍過廣的描述，而不符合特定性的要求[362]。

第四款 允許不在現場搜索

搜索電腦是一種相當耗時的工作，除了儲存裝置的容量可以容納數量龐大的檔案數目，犯罪者經常將具有犯罪屬性的資料加以更名、加密或隱藏，若僅簡單地以列出檔名目錄的方式加以檢視，將會遺漏或無法找出該具有犯罪屬性的資料，再者犯罪的證據不一定是以人爲產生檔案的形式來呈現，電腦作業系統運轉過程中所自動產生的各種記錄檔，亦詳實的記載各個時刻電腦的使用狀態，除非有適當的工具與方法否則將無法順利找出與取得這類檔案與紀錄[363]。

搜索過程中執法人員在現場停留過久將加劇搜索所帶來的侵害性，在搜索紙本文件時法院允許先行扣押整個檔案櫃，移至另一個地點檢視其中的文件，辨別何者是屬於令狀所記載應扣押的文件，並立即歸還其他不屬於令狀扣押範圍內的文件[364]。在搜索電腦

356 Marron v. United States, 275 U.S. 192, 196 (1927)。
357 Fed. R. Crim. P. 41(c)。
358 USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 70-71。
359 United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999)。
360 United States v. Bright, 630 F.2d 804, 812 (5th Cir. 1980)。
361 Davis v. Gracey, 111 F.3d 1472, 1478 (10th Cir. 1997)。
362 United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009)。
363 USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 76。
364 United States v. Santarelli, 778 F.2d 609, 616 (11th Cir. 1985)。

中的犯罪證據時，法院認爲將整部電腦扣押後移至一個有專家協助的適當環境下，執行搜索是合理的[365]。

在聲請令狀時應該說明現場搜索所面臨的限制，以及允許將整台電腦扣押移至一個適當場所進行搜索的必要性，讓核發令狀的治安法官可以瞭解執行犯罪證據扣押所面臨的限制與執法人員的意圖，並在令狀中記載允許不在現場(off-site)搜索，如此才能發揮法院的監督功能[366]。

第五款 限制搜索方法

憲法第四增修條文清楚的指明令狀核發的三個要件：由中立的治安法官所簽發、具備相當理由確信可以經由搜索掌握犯罪的證據、以及指明應被搜索的場所與應被扣押的人或物。除此之外，基於對該增修條文文字的解讀與聯邦最高法院判決對該條文的詮釋，並未發現令狀特定性的要求包括應該清楚的指示令狀的執行方式[367]。

搜索電腦內的資料是一種技術也是一種藝術，在大多數的情況下必須依現場所面臨的情境才能判斷決定下一步要採取什麼方法找尋搜索標的，關鍵字搜索經常被用於找尋以文字方式呈現存在的檔案內容與檔案名稱，但是無法運用於搜尋經過掃瞄成影像的文件內容，檔案名稱以代碼命名或經有意無意拼錯字亦無法以關鍵字搜索發生效果，在聲請令狀當時要求對於搜索方式加以特定，或要求指明將用於搜索執行的關鍵字，將可能影響到找出位於令狀特定範圍內的犯罪證據的機會[368]。

當簽發令狀的治安法官堅持在令狀中指定執行搜索時的限制條件，例如，限制只有記載在令狀中的關鍵字才能用來搜索，或是電腦鑑識必須在指定的時間內完成，倘若這些限制條件將對偵查行爲帶來嚴重干擾，美國司法部鼓勵聲請令狀的檢察官向上級法院提出抗告[369]。若選擇不提出抗告，則執行人員必須確實遵守令狀中所記載的限制條件，以免因違反限制條件而產生證據禁止的效果[370]。

執行令狀當時可能會發生什麼樣的情況，核發令狀的法官並無法事先預知，必須倚

---

365 United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000)。
366 United States v. Hill, 459 F.3d 966, 976 (9th Cir. 2006)。
367 Dalia v. United States, 441 U.S. 238, 257 (1979)。
368 USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 79。
369 USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 80。
370 USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 82。

賴執行令狀的人員依據當時所遇到的情境，以符合令狀目的所做出的最佳判斷執行[371]，令狀執行的合理性，事後將會以司法審查的方式來決定[372]，超越令狀所許可的範圍將可能面臨證據禁止的效果。

第四項 電腦鑑識

電腦鑑識(computer forensic)是指從電腦中取得證據的過程，通常是由受過訓練的電腦鑑識專家依據搜索令狀，在政府的鑑識實驗室中進行[373]。

如果不存在緊急取得存放在儲存裝置中資料的必要性，實務的運作方式偏好依據搜索令狀先對電腦加以扣押隨後再進行鑑識分析，一個受過訓練的專家工作在一個完整規劃的鑑識環境下，通常可以在該電腦中取得相關詳細的資訊，也可以避免匆忙執行搜索可能導致的資料毀損[374]。

現場的電腦若處於關機的狀態則不應任意啓動電源，以避免更改關機前的系統狀態紀錄，若正處於開機的狀態，則不可循作業系統的正常關機方式，而是要以切斷電源供應的強制關機方式，才能保存那一個瞬間系統的狀態。

第一款 第二階段搜索

第一階段搜索的目標在於找出應扣押之儲存裝置，且令狀允許不在現場搜索該儲存裝置的內容，接下來就是在電腦鑑識實驗室中，以電腦鑑識的流程與步驟，對該儲存裝置的內容進行第二階段搜索。

電腦鑑識的過程主要可區分爲二個步驟，首先是資料複製，其次是資料搜索。資料複製是指將扣押電腦的儲存裝置拆卸下來，連接至鑑識設備上以鏡像(imaging)或位元流(bitstream)的方式，將該儲存裝置的內容完整的複製到政府所持有的儲存裝置上，後續並在該政府儲存裝置上執行搜索的動作。

與一般電腦使用者複製磁碟內容所不同的是，一般電腦使用者只能複製看得到的檔案，而位元流的複製方式將完整呈現資料於原儲存裝置中分布的狀態，精確地複製每一個位元與位元組，其中包括使用者的檔案與電腦運轉過程中相關的記錄檔，例如記載磁

371 Dalia v. United States, 441 U.S. 238, 257 (1979)。
372 Dalia v. United States, 441 U.S. 238, 258 (1979)。
373 Kerr, Orin S., Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 537 (2005).
374 USDOJ，Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，頁 30-31。

碟使用狀態的主檔案表(Master File Table)、描述資料屬性的詮釋資料(metadata)等[375]。

對複製資料執行搜索的好處是可以避免更動原始證據的風險，以電腦鑑識的方式執行對儲存資料的重建，有可能回復已經遭到刪除的檔案，主要是因爲檔案的刪除並不是立即由儲存空間中抹除，而是在主檔案表中標示該遭刪除檔案所使用的儲存空間，已經允許以覆蓋的方式存放其他新的資料，在執行電腦鑑識當時若該遭釋放的空間尚未被使用，則有可能回復先前被刪除的檔案，電腦鑑識同時也可以從詮釋資料詳實的記載中掌握每一個時刻電腦被使用的過程[376]。

資料搜索是指在經複製的資料中揀選出符合令狀所特定的資料。搜索過程中對於每個出現在眼前的文件加以簡略的閱讀是有必要的，以判斷是否爲符合令狀所允許的扣押標的，當所獲得的資訊足以清楚地判斷該文件並不屬於令狀所特定的扣押標的時，即應立即停止閱讀[377]。

第二款 超出範圍的搜索

被扣押的電腦可能同時存在數種不同的犯罪證據，對電腦的搜索必須使法官確信存在發現特定犯罪證據的相當理由才能獲得令狀的核發，執法人員也被限制在令狀所特定的範圍內執行搜索，以避免導致違法搜索。

沒有經過實際執行搜索無法事先預知該電腦中還存在哪一種特定類型的犯罪證據，自然無從建立相當理由以取得對該類犯罪證據的搜索令狀。依據令狀所進行的合法搜索在過程中所意外發現的不在令狀所特定之犯罪證據，可以依據一目瞭然法則立即將該另案證據加以扣押。

至於是否可以立即對該另案犯罪執行搜索，則應遵循管轄法院對容器理論的見解，若法院採取將整個儲存裝置視爲一個容器的看法，則可以立即執行該另案犯罪證據的搜索。若法院採取將個別的檔案視爲一個單獨容器的看法，則不可以立即展開對該意外發現的犯罪搜索其他可能存在的證據，應以該意外發現的證據建立相當理由取得另一個令狀的許可，才能執行對該意外發現犯罪的證據搜索[378]。

[375] Kerr, Orin S.，Searches and Seizures in a Digital World，頁 541。
[376] Kerr, Orin S.，Searches and Seizures in a Digital World，頁 541-542。
[377] United States v. Heldt, 668 F.2d 1238, 1267 (D.C. Cir. 1981)。
[378] United States v. Walser, 275 F.3d 981, 987 (10th Cir. 2001)。

第四節 小結

美國隱私權的概念，首先在普通法侵權行爲的領域發展，歷經普通法原則的建構過程，由獨處的自由發展出美國侵權行爲法上的隱私權。至於隱私權受美國憲法保障之發展歷程，則應從憲法增修條文之「權利法案」，以及美國聯邦最高法院的相關判決觀察。美國憲法關於人民基本權利的保障係以憲法增修條文的方式加以規定，首先出現的十個列舉條文被稱爲「權利法案」，後續增修的第十三條、第十四條與第十五條，從實體及程序上全面地保障了人民的自由權利。

隱私權的文字雖未直接記載在憲法的條文之中，因爲隱私權所蘊含自我決定的權限被認爲是包括在「自由」的概念之中可以免於國家力量無理的干擾。起先美國聯邦最高法院的見解認爲，人民的隱私權來自於增修條文第一、三、四、五、九條交相適用的結果，後來聯邦最高法院才直接了當的說，隱私權是增修條文第九條所謂保留給人民的權利，因而有增修條文第十四條正當法律程序的適用。

隱私權應該予以保護的觀念最早始於Warren與Brandeis發表於哈佛法學評論關於隱私權的論文中，作者將隱私權界定爲「生活的權利」和「不受干擾的權利」，並指出在普通法上已經保護個人決定其思想、情緒與感受在什麼範圍之內傳達給他人，即使傳達給他人之後，個人仍保留限制這些思想、情緒與感受對公眾公開的程度，這些保護並非基於私人財產應受保障，而是基於人格的不可侵犯，因此心靈的平靜才是保護的焦點。

聯邦最高法院對隱私權保障的討論，由早期的權利法案所形成的暈影理論出發，進展到凡符合有秩序的自由這個概念，均應依第十四增修條文的正當法律程序條款加以保障，在各個階段擔負起對權利法案中非列舉基本權利保障的責任。

部分聯邦最高法院大法官主張將自由與隱私有所區隔，而有不同的憲法保障依據。學者認爲自由正是免於外在的限制，亦即憲法第十四增修條文正當程序所保障的自由，而憲法所保障的隱私則是第四增修條文免於不合理的搜索與扣押的預設，而隱私也應該是憲法第一增修條文所保障各項自由的限制，例如新聞自由應受個人隱私的節制。

學者將資訊隱私權定義爲，個人針對其相關資訊予以保密或限制傳播的權限。今日資訊隱私權的內容包括：靜態對個人已儲存資料的保護，以及動態對通訊過程中通訊內容的保護。對於資訊隱私權的保障有聯邦最高法院針對第四增修條文的相關判決，以及美國國會爲了保障以電子形式儲存的資料、檔案所享有隱私，所通過的包括電子通訊隱私法、通訊輔助偵查法以及在2001年通過的愛國者法案。

憲法第四增修條文保障人民身體、住所、文件及財產有免於政府不合理搜索及扣押

的權利。在普遍應用科技設備協助偵查作爲之前，搜索被定義爲執法人員以進入人民財產權所管領空間之方式蒐集證據，在電子資訊時代所進行的電話監聽，雖然沒有物理入侵受監聽對象所管領的空間，但是已經侵犯了受監聽對象對於通話內容的合理隱私期待，而被認爲是搜索行爲的一種。從發展脈絡觀察，憲法第四增修條文的適用最早是從財產權保護的觀點出發，進展到對於合理隱私期待的保護，以及將面臨隨著科技的進步偵查輔助設備的大量被採用，對第四增修條文所帶來的挑戰。

Brandeis 大法官曾表示，法律與憲法的制定都是爲了防制過去所發生的罪惡，但是對法律與憲法的解讀不應只侷限於過去所發生過的態樣，時間帶來改變，隨著新的情況與目的的出現，必須藉由更廣的適用才能賦予憲法原則的生命力，而擔保個人權利以對抗政府權力濫用的條文，也必須要有相同的適應能力以面對一改變中的世界。在憲法的應用上，我們的思考不能只是侷限在過去曾經是什麼(what has been)，而是將來可能有什麼(what may be)，科技的進步對於政府刺探方法的協助將不會僅止於監聽，藉由更精良的方法將有可能將人民在密室內的竊竊私語揭露於法庭之上。

以物理入侵判斷是否構成憲法第四增修條文意義下的搜索行爲，直到 Katz 一案才被聯邦最高法院所摒棄，進而採取合理隱私期待的判斷標準，其內容爲：首先，必須要有主觀隱私期待的呈現，其次，這個隱私期待必須被社會認爲是合理的，因此受憲法第四增修條文保護的範圍，從早期的「人身、住所、文件及財產」等有形的區域擴展到無形的合理隱私期待所界定的區域。

科技始終來自於人性，科學技術的進步爲人類的生活帶來了便利，同時也嘉惠政府對人民隱私的刺探行爲，在地面上有圍籬阻隔的隱私期待，在經由飛機的協助所呈現的三度空間下，該隱私期待將不再成爲可能，經由掃瞄房屋所發散出來的熱能，可以清楚地窺知屋內人員的活動狀態，以及以往必須耗費大量人力的跟尖行爲，如今只需貼附一個衛星定位系統追蹤器，就可以在電腦前輕易的接收被追蹤對象的行蹤。科技所帶來的便利性已經逐漸侵蝕人民受憲法保障的隱私領域，今日我們所面對的問題是如何對科技的力量施以適當地限制，以減少受憲法保障的隱私領域的縮小。

美國國會在 1986 年通過電子通訊隱私法，將原來的 Title III 加以擴充納入對電子通訊通訊監察的規範，成爲新的聯邦監聽法用以規範現在正在進行中或未來可能發生的通訊內容的截取。除了聯邦監聽法，ECPA 還包括撥號記錄器與追蹤裝置法與儲存通訊法共三個部分。撥號記錄器與追蹤裝置法用以規範通訊過程中通訊內容以外資訊的取得。對於非屬正在進行中的通訊，存取已經儲存的電子通訊則應符合儲存通訊法的規範。ECPA 的三個部分分別規範動態(通訊中)與靜態(經儲存)的通訊，以及是否涉及通訊中內

容與非內容通訊的取得方式，違反 ECPA 的相關規範將面臨民、刑事上的責任，在訴訟中的案件若有違法監聽取得的證據將會有證據禁止的效果。

聯邦監聽法是用以規範對有線通訊、口頭通訊與電子通訊這三種受保護通訊內容的截取。對於通訊內容的截取必須取得法院所核發的令狀才能進行，聯邦最高法院在 Katz 案確認具有合理隱私期待的通訊內容是屬於憲法第四增修條文保護的客體，任何對進行中通訊內容的截取將構成該增修條文意義下的搜索行爲，聯邦監聽法的制定進一步強化對於通訊隱私的保障，該法提供法院在簽發通訊監察令狀時必須審酌的事實，除了該增修條文所要求的「相當理由」，聯邦監聽法增加「重罪原則」並可視需要要求聲請人提出補充證據以滿足相當理由的門檻。

聯邦監聽法所規範通訊監察聲請的要件，基於保護對話交談內容賦予口頭與有線通訊特定重罪的要求，而電子通訊只需符合聯邦重罪等較寬鬆的條件，隨著網路通訊所能提供的服務的多樣化，以及人們倚賴網路通訊的日漸加深，利用網路所進行的語音與視訊同樣能達到對話交談的功能，因此有是否應將核准電子通訊監察的門檻提高至與口頭與有線通訊相同的思考。

通訊監察無可避免地會接觸到與所偵查犯罪無關第三人之通訊內容，聯邦監聽法規範執行通訊監察時要以產生最小程度侵害的方式進行，該法並未對產生最小程度侵害的執行方式提供明確的依據。

通訊監察執行完成後的告知義務可以向社會確保通訊監察這項科技有被合理的使用，任何依法核准的通訊監察將因告知義務的履行，最終讓受通訊監察之人有所知悉，使其在隱私覺得受不合法侵犯之時有機會可以尋求適當的民事救濟。

執行電子監控時違反聯邦監聽法的相關規定，將面臨刑事處罰、民事責任以及在訴訟上證據禁止的效果。違法通訊監察的證據禁止僅適用於口頭與有線通訊，並不及於電子通訊，隨著電子通訊科技的進步其所能傳遞具有隱私期待的信息亦趨多樣化，也應該思考對電子通訊之違法通訊監察賦予證據禁止的效果。未將全部已知的犯罪嫌疑人列名於通訊監察聲請書上，以及沒有確實履行告知義務，不產生證據禁止的效果。

除了向監察對象的告知義務。對於個案的監督，核准令狀的法官可以要求向其報告執行的進度與繼續截取的需要。審核通訊監察聲請的法官應在規定期限內，向美國法院行政部門呈報相關資料。對於通案的監督，每年聯邦檢察總長應向美國法院行政部門呈報統計資料。對於接受國會的監督，每年美國法院行政部門應向國會提出上年度中有關通訊監察聲請數量，以及令狀或延長期間令狀核准或駁回數量的完整報告。

撥號記錄器與追蹤裝置法用以規範定址資訊與通訊中非內容資訊之蒐集，這類的資

訊是在通訊過程中自願提供給通訊服務提供者以完成通訊服務的建立，通訊服務的使用者基本上已經承擔服務提供者可能將該些資訊洩漏給政府的風險，而不能主張具有合理的隱私期待。

撥號記錄器與追蹤裝置的安裝，由代表政府的檢察官或州執法官員，以書面宣示或相當的確信聲請法院命令的核發，法院在核發命令時並不要求相當理由的存在，也沒有限定特定的犯罪類型才能適用，聲請的條件相對寬鬆，在執行上也相當有彈性，聯邦法院所核發的命令，在該法院的管轄區域外依然具有效力。違反本法律將會面臨民事與刑事的責任，其所取得的證據在刑事訴訟中沒有證據禁止的效果。對於個案的監督，在法院命令所允許的蒐集資訊期限屆至後，必須向核發命令的法院報告該設備的使用狀況。對於國會的監督，聯邦檢察總長每年必須向國會呈報司法部所屬執法單位申請撥號記錄器與追蹤裝置的統計資料。

儲存通訊法規範政府如何自網路服務提供者取得所儲存的帳號資訊，舉凡儲存的電子郵件、帳號紀錄與用戶資訊之取得，均需符合儲存通訊法的規定。儲存通訊法將網路服務提供者區分爲提供電子通訊服務與遠端計算服務兩種類型。

該法規範 5 種政府可以採用的機制以強制服務提供者揭露其所儲存關於用戶的通訊內容或紀錄，這 5 種機制分別爲：傳票、事先通知用戶的傳票、法院命令、事先通知用戶的法院命令以及搜索令狀。使用傳票可以取得用戶的基本與連線資訊，隨著不同機制的聲請要件以及是否需事先通知，可以分別取得不同性質的資訊。

受儲存通訊法保護的資料，有兩種情形允許政府不用傳票可以取得資訊，首先是經用戶同意之非內容資訊的提供，其次是偵查中的電話行銷詐欺案件，由執法人員向服務提供者提出正式書面請求，即可取得該從事電話行銷用戶之姓名、地址以及營業場所所在位置等資訊。

儲存通訊法普遍禁止對公眾提供服務的電子通訊服務與遠端計算服務提供者洩漏其用戶之紀錄、其他資訊以及通訊內容，除非有例外的情形發生。當考慮是否符合自願提供的例外時，首先要考慮的是該服務提供者有沒有對公眾提供服務，如果不對公眾提供服務則不受儲存通訊法的限制。若存在經通訊一方之同意、保護服務提供者權利或財產、犯罪偵查、保護他人之緊急情狀等情形下，可以選擇自願提供用戶的通訊內容。若存在經用戶之同意、保護服務提供者權利或財產、犯罪偵查、保護他人之緊急情狀等情形下，可以選擇自願提供用戶的紀錄或其他資訊給政府單位或他人。

網路犯罪的偵查經常必須倚賴網路服務提供者的協助，沒有法律規定網路服務提供者應該將與其用戶帳號有關的紀錄保存多久或多完整。爲了避免有助於犯罪偵查的證據

遭到銷毀或遺失，執法人員著手偵查網路犯罪的第一件事情就是通知網路服務提供者保存有關特定用戶帳號相關的資料，並同時向法院聲請強制揭露該些資訊的許可。法律並未規定提出通知的形式，因此一通電話將可以符合通知的要求，但是以書面的方式經由傳真或電子郵件的方式送達，不僅可以留下紀錄而且可以防止誤解，將是比較安全且可行的方法，緊急保存只能要求服務提供者保存當時已經儲存在服務提供者的紀錄，若要取得尚未發生的紀錄則必須符合通訊監察相關的規定。

遵守儲存通訊法所取得的證據沒有證據禁止的適用，違反該法但不構成憲法第四增修條文的違反，所取得的證據也沒有證據禁止的適用，該法僅提供民事救濟的方式。儲存通訊法賦予執法部門向國會的報告義務，在每個年度聯邦檢察總長應向眾議院與參議院司法委員會提出司法部所接受自願揭露通訊內容的數量以及用於偵查但未提出刑事告訴數量的報告。

電子通訊隱私法相較於憲法第四增修條文的差別在於，電子通訊隱私法規範的對象不再僅侷限於政府，而是可及於一般之個人，任何人想要從網路服務提供者取得儲存之電子郵件、帳戶紀錄或是用戶資訊，皆須遵守電子通訊隱私法中有關取得儲存通訊的相關規定，因此，電子通訊隱私法不僅就已儲存的通訊提供使用該服務用戶的隱私權保障，對於傳輸中的通訊也提供更高程度的保障。

美國憲法第四增修條文保障人民有免於不合理搜索與扣押的自由，在 Katz 一案中將受憲法保障的區域由有形的實體延伸至具有合理隱私期待的無實體形狀之通訊內容，任何對該具有社會認可的合理隱私期待的侵犯，即構成憲法第四增修條文意義下的搜索行為。

電腦、行動儲存裝置(例如，隨身碟)或是行動電話，這類具有儲存數位資料功能的裝置，將數位資料儲存在其中主觀上已經呈現對該儲存的內容具有隱私的期待，法院認為可以將儲存裝置視為一個封閉容器，對於該容器的搜索將有令狀原則的適用。將電子儲存裝置視為封閉容器的看法，法院彼此間存在著些微的差異，第五巡迴上訴法院採用將一整個儲存裝置視為一個封閉容器的看法，第十巡迴上訴法院，採取將個別的檔案視為一個單獨容器的看法，這將影響到搜索範圍的認定與一目瞭然法則的應用。

Katz 案的法院意見指出，一個人有意識地暴露在公眾之下，即使是在其住家或辦公室中，將不受到憲法第四增修條文的保護。個人將資料上傳到網路或公用電腦使其處於其他人可接觸的公開分享狀態，將不能主張對該些資料具有合理的隱私期待。

憲法第四增修條文並不禁止政府自第三人處取得他人所揭露給該第三人的資訊，法院普遍認為一個人將所管領具有合理隱私期待的物件或資訊交給第三人使其置於該第

三人實力支配之下，原持有者將不能再主張對該物件或資訊之合理隱私期待。

憲法第四增修條文保障人民有免於不合理搜索與扣押之自由，這個憲法誡命僅限於用以對抗政府對人民合理隱私期待的侵犯行爲，私人以自己的決定所進行的搜索與扣押行爲，只要不涉及扮演政府的代理人或是有政府官員的參與或知悉，即便該搜索與扣押行爲是不合理的，都沒有憲法第四增修條文的適用。對於政府所接續的無令狀搜索行爲，必須加以檢視是否超出私人搜索的範圍，而構成另一個搜索行爲。若涉及電子儲存裝置，對於該私人搜索範圍的認定，將取決於不同巡迴上訴法院對容器理論的看法不同而有不同的結果。

同意是一種放棄其受憲法第四增修條文保護的意思表示，搜索之同意並不僅限於被告才能行使，對於受搜索標的有「共同權限」之第三人，都可以行使同意搜索的權限，此外尚應考量被告是否主客觀上承擔了共同權限之人可能會同意執法人員搜索的風險，美國聯邦最高法院認爲必須同時具備「共同權限」與「風險承擔」此二個要件，才能成立一個有效之第三人同意搜索。

儲存在電腦中數位資料的容易被毀壞是導致緊急搜索經常在電腦搜索中被採用的原因之一，或是基於證據保全的目的而有採取緊急扣押將該裝置隔離於該受搜索對象實力支配之外的必要。附隨於犯罪嫌疑人的合法逮捕行爲之後，執法人員可以在沒有令狀的情形下執行對該受逮捕對象的全身搜索以及搜索其立即可接之觸鄰近區域，這項例外允許是基於避免證據受到毀損與執行逮捕人員遭受傷害。應用以上的原則，附隨於逮捕所取得的電腦與類似的儲存裝置，基本上將有附帶搜索原則的適用。當執法人員處於合法的地位得以觀察與接觸特定證據，且該證據具有明顯的犯罪特質，此時例外允許在沒有令狀的情形下，依據一目瞭然法則對該證據進行扣押。

搜索令狀的核發必須由中立的治安法官依據聲請書上所記載的整體事實所做出實際、普遍常識的決定，認爲存在違禁品或犯罪的證據將會在某特定場所發現的相當可能性。此即滿足憲法第四增修條文所要求令狀的核發必須本於相當理由的標準。在聲請令狀時應該說明現場搜索所面臨的限制，以及允許將整台電腦扣押移至一個適當場所進行搜索的必要性，讓核發令狀的治安法官可以瞭解執行犯罪證據扣押所面臨的限制與執法人員的意圖，並在令狀中記載允許不在現場搜索，如此才能發揮法院的監督功能。

電腦鑑識是指從電腦中取得證據的過程，通常是由受過訓練的電腦鑑識專家依據搜索令狀，在政府的鑑識實驗室中進行。如果不存在緊急取得存放在儲存裝置中資料的必要性，實務的運作方式偏好依據搜索令狀先對電腦加以扣押隨後再進行鑑識分析，一個受過訓練的專家工作在一個完整規劃的鑑識環境下，通常可以在該電腦中取得相關詳細

的資訊，也可以避免匆忙執行搜索可能導致的資料毀損。

被扣押的電腦可能同時存在數種不同的犯罪證據，依據令狀所進行的合法搜索在過程中所意外發現的不在令狀所特定之犯罪證據，可以依據一目瞭然法則立即將該另案證據加以扣押。至於是否可以立即對該另案犯罪執行搜索，則應遵循管轄法院對容器理論的見解，若法院採取將整個儲存裝置視爲一個容器的看法，則可以立即執行該另案犯罪證據的搜索。若法院採取將個別的檔案視爲一個單獨容器的看法，則不可以立即展開對該意外發現的犯罪搜索其他可能存在的證據，應以該意外發現的證據建立相當理由取得另一個令狀的許可，才能執行對該意外發現犯罪的證據搜索。

第四章 我國偵查實務

第一節 我國隱私權保護的演進

我國憲法本文或增修條文之中，並沒有針對隱私權的明文規定，但是從一九九二年的司法院大法官會議第二九三號解釋開始，隱私權的概念與相關原則開始被援引爲說理與論證的依據[1]。大法官一開始並未對隱私權直接做出定義，而是藉由個案爭議的決議，逐漸勾勒出隱私權的面向與保障的範圍。

在釋字第二九三號解釋主文中提到：「銀行法第四十八條第二項規定『銀行對於顧客之存款、放款或匯款等有關資料，除其他法律或中央主管機關另有規定者外，應保守秘密』，旨在保障銀行之一般客戶財產上之秘密及防止客戶與銀行往來資料之任意公開，以維護人民之隱私權。」銀行法第四十八條第二項規定之目的即是針對客戶與銀行往來過程中所涉及的資料，限制客戶以外之人傳播的權限。該解釋主文進一步提到基於議會對於公營行庫監督之需要，在銀行不透露個別客戶姓名以及議會不傳播所取得資料的前提下，銀行應提供相關的資料供議會審查[2]。該前提呈現出大法官試圖藉由限制客戶資料的傳播以達到維護客戶隱私權的思維。

釋字第五０九解釋是有關刑法的毀謗罪是否違憲之爭議。大法官在解釋主文開宗明義即闡明言論自由是受憲法第十一條明文保障的人民基本權利，具有實現自我、溝通意見、追求真理及監督各種政治或社會活動之功能，國家應給予最大限度的維護，只有在顧及對個人名譽、隱私及公共利益之保護，才能以法律對言論自由依其傳播方式爲合理之限制[3]。在此所提及的隱私即是針對與公眾利益無關之個人私事，限制其傳播的權利。

釋字第五三五號解釋主文中提到：「臨檢實施之手段：檢查、路檢、取締或盤查等不問其名稱爲何，均屬對人或物之查驗、干預，影響人民行動自由、財產權及隱私權等甚鉅，應恪遵法治國家警察執勤之原則。」當臨檢實施於人民所管領的私密空間時，例如住宅或汽車，即對該空間內所保有不欲爲外人窺知的私密細節的侵犯。在此的隱私權所欲維護的是個人私密的空間不受侵擾的權利。

釋字第五八七號解釋理由書中提到：「此種訴訟雖係爲兼顧身分安定及子女利益而

[1] 蔡榮耕，Yes, I do! —同意搜索與第三人同意搜索，月旦法學雜誌，157 期，2008 年 6 月，頁 103-104。
[2] 釋字第 293 號解釋。
[3] 釋字第 509 號解釋。

設，惟得提起否認之訴者僅限於夫妻之一方，未規定子女亦得提起否認之訴，或係爲避免涉入父母婚姻關係之隱私領域，暴露其生母受胎之事實，影響家庭生活之和諧。」此處所提及的隱私領域是一種自我決定權限的展現，只有適格的主體才具有提起否認之訴的權限。

在釋字第六０三號解釋主文中提到：「隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並爲保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃爲不可或缺之基本權利，而受憲法第二十二條所保障。」大法官透過以上文字明白闡述，憲法第二十二條是我國保障隱私權的憲法依據。藉由隱私權對個人生活私密領域與個人資料自主控制權限的保護，達成人性尊嚴、個人主體性與人格發展能夠得到維護之目的。本解釋所指涉的基本權是以人性尊嚴爲核心，依序向外擴張至一般人格權、個別人格權之隱私權、隱私權中之資訊隱私權、以及涉及個人資料之資訊自主權[4]。

釋字第六三一號解釋理由書中提到：「憲法第十二條規定：『人民有秘密通訊之自由。』旨在確保人民就通訊之有無、對象、時間、方式及內容等事項，有不受國家及他人任意侵擾之權利。此項秘密通訊自由乃憲法保障隱私權之具體態樣之一，‧‧‧‧。」延續大法官將秘密通訊自由視爲隱私權態樣之一的看法，可以推論憲法第十條所保障之人民居住自由，亦同樣隱含著人民對於居住處所中所保有的私密空間，享有不受國家不當入侵的權利[5]的隱私權意涵。

綜觀上述大法官的解釋文可以得知，隱私權所呈現的面向包括限制個人資訊傳播、個人自我決定權限、以及個人私密空間不受侵擾等具體內容。有關控制個人資料流向的資訊自主權則蘊含著資訊隱私權、個人資料保護權、秘密通訊自由等內容[6]，分別對應至搜索電磁紀錄、調閱個人資料、通訊監察等強制處分實施時所將涉及的基本權侵害。隱私權並不是一個絕對的權利，在符合憲法第二十二條與第二十三條的情形時，國家可以對這個權利加以限制[7]。既使如搜索是對個人私密空間的侵擾，通訊監察是對個人通訊內容的蒐集等侵害基本權的態樣，只要經過適當法律的授權之後，即能對個人所享有的隱私權加以限制。

---

[4] 李震山，來者猶可追，正視個人資料保護問題－司法院大法官釋字第六０三號解釋評析，台灣本土法學雜誌，76 期，2005 年 11 月，頁 228。

[5] 蔡榮耕，Yes, I do! －同意搜索與第三人同意搜索，月旦法學雜誌，157 期，2008 年 6 月，頁 104。

[6] 李震山，來者猶可追，正視個人資料保護問題－司法院大法官釋字第六０三號解釋評析，台灣本土法學雜誌，76 期，2005 年 11 月，頁 228。

[7] 蔡榮耕，I Am Listening to You（上）－釋字第六三一號解釋、令狀原則及修正後通訊保障及監察法，台灣本土法學雜誌，104 期，2008 年 3 月，頁 49。

第二節 通訊保障及監察法

美國法將通訊監察認定爲對合理隱私期待侵犯的一種行爲，因此對於通訊內容的截取將有憲法第四增修條文的適用，進入電子通訊時代之後爲了加強對電子通訊隱私的保障於是制定聯邦監聽法賦予通訊監察行爲較嚴格的規範，並與撥號記錄器與追蹤裝置法以及儲存通訊法共同構成電子通訊隱私法。而我國法將通訊監察與搜索認定爲兩種不同的強制處分行爲，分別採用不同的法律加以規範。

我國法對於通訊內容具有隱私的期待才有通訊保障及監察法的適用。爲了因應網路通訊的普及所面臨的問題，以下將就網路監察容許性、監察的客體與方式、許可程序、執行與監督等各個面向加以討論。

第一項 網路通訊監察容許性

通訊保障及監察法規範三種受保障的通訊類型，該法第三條第一項將此三種通訊類型定義爲：「一、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。二、郵件及書信。三、言論及談話。」該條第二項進一步對受保護的通訊範圍加以限制「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爲限。」很明顯地係受美國聯邦最高法院在 Katz v. United States 一案所建立的「合理的隱私期待原則」的影響，立法者認爲只有能夠合理期待該通訊內容具有隱私性或秘密性者，才屬於本法所保障的通訊範圍[8]。因此，在大街上的高聲談話或是書寫在明信片上的通訊內容，將不被認爲具有合理的隱私期待。

通訊保障及監察法適用於具有隱私期待的聲音與文字的通訊方式，例如密室內的談話內容、封緘的書信以及電話的談話內容，是可以輕易地理解，而經由網路所進行的通訊是否同樣有該法的適用，則必須進一步加以檢視，該法第三條第一項以一種幾乎含括現今電子科技時代所有可能使用的通訊方式，定義了一類受保護的通訊類型，亦即藉由科技設備所傳送的通訊內容。

網際網路是由許多的電腦、有線傳輸線路、無線傳輸設備、路由器相互串接組合而成的資訊網絡，利用電腦進行網路通訊時通訊的內容無論是符號、文字、影像或聲音均被承載在封包之中，傳遞在有線傳輸線路上或藉由無線傳輸設備傳送，並經由路由器的導引將封包正確地傳送至目的地電腦。

[8] 陳信郎，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，2004 年，頁 106。

電信法第二條第二款將電信設備定義爲：「電信所用之機械、器具、線路及其他相關設備。」該法第二條第一款將電信定義爲：「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。」依據前一段對於網路通訊的概略描述，對照電信法對於電信設備的定義描述，電腦與路由器屬於器具或其他相關設備，有線傳輸線路與無線傳輸設備具有線路的功能，而封包中所承載的通訊內容符合電信法中對於電信的定義。利用電腦發送發送、儲存、傳輸或接收封包，應屬於受通訊保障及監察法保護之通訊類型[9]。

第二項 監察的客體與方式

網路的通訊監察可能是以網際網路位址(IP)或電子郵件帳號爲受通訊監察的客體[10]。IP 位址類似於網路世界的門牌號碼，理論上每台連接網際網路的電腦都應該被配置一個獨一無二的 IP 才能夠正確地發送與接收封包信號以進行網路通訊。現今網際網路所採用的 IPv4 版本的位址表示方式，是以 32 個二進位數字來表示一個 IP 位址，以 8 個位元爲一單位共分成 4 段，例如：11000000 10101000 00000001 00000010，爲了便利人們閱讀通常會以十進位的方式表示爲 192.168.1.2。

欲對某一特定電腦的網路通訊進行通訊監察，必須蒐集由該電腦所發送或即將接收的封包信號，加以組合還原才能解讀其通訊內容。網際網路是屬於封包交換的網路，用以傳輸封包信號的線路是由大家所共同使用，亦即在某一段時間區間內流經一特定線路的封包信號，將不會只專屬於一個封包信號發送者或接收者。資料的混雜性是封包交換網路的一個特性，爲了避免觸及與犯罪偵查對象無關的通訊內容，必須先過濾出屬於受通訊監察 IP 所發送或即將接收的封包信號，才能加以蒐集。

網路的普及使得有越來越多的電腦有上網的需求，因而以 IPv4 版本所定義的網際網路位址(public IP，公有 IP)即將面臨使用殆盡的窘境，除了積極發展新的 IPv6 版本以定義出更多數量的網際網路位址，目前無法取得足夠公有 IP 數量的單位，通常會將單位內的電腦配置只能在單位所屬的區域網路內通訊傳輸的私有 IP(private IP)，對於需要離開區域網路的通訊傳輸經過網路位址轉換，統一以一個公有 IP 位址爲代表與外界溝通，此時若在區域網路外對該公有 IP 位址實施通訊監察將無法判斷，所蒐集的封包信號是由區域網路內哪一台電腦所發送或即將接收，必須藉由該區域網路的管理者的協助，由網路位址轉換(Network Address Translation，簡稱 NAT)伺服器查表找出所對應

[9] 蔡美智，「通訊保障及監察法」關於網路監聽的相關爭議，資訊法務透析，1999 年 12 月，頁 38-39。
[10] 蔡美智，「通訊保障及監察法」關於網路監聽的相關爭議，資訊法務透析，1999 年 12 月，頁 37。

的區域網路內電腦。

同樣地，電子郵件帳號也必須是獨一無二的才能使電子郵件的發送與接收正常地運作，電子郵件帳號由兩部分組成，以 joe@goodcompany.com 爲例，goodcompany.com 是指郵件伺服器的名稱，該名稱在網際網路世界中是獨一無二的，如果同時存在兩個相同名稱的郵件伺服器將會使電子郵件發生不知該向那一個伺服器遞送的錯誤，Joe 是指使用者帳號，在 goodcompany.com 伺服器中只能允許有一個 Joe，但是並不妨礙在其他的伺服器中有另一個 Joe 的存在。帳號的擁有者必須要通過密碼的驗證，才能讀取與寄送電子郵件，偵查實務普遍認爲是一種由帳號的擁有者所專屬操控的通訊工具。

常見的網路通訊監察方式，可以區分爲在主機內取得或節點上蒐集通訊內容[11]。隨著資訊科技的發達網路上已經能夠提供許多種類的通訊服務，例如電子郵件、聊天室或類似 msn 之類的即時通訊等，每一種通訊服務都會有專屬的服務主機或伺服器，用以接收、儲存與傳遞該服務之使用者相互之間所傳遞的訊息，訊息是以使用者帳號爲單位個別管理，直接從服務主機執行通訊監察的好處是，不會觸及受通訊監察對象以外其他人之通訊內容。但是必須倚賴該服務主機管理者的協助，才能順利進行通訊監察的工作。

網路節點是傳輸線路的匯集點，通常是由路由器扮演起節點的角色以決定每一個流經該路由器的封包的下一個傳遞路徑，以在節點蒐集封包的方式執行網路通訊監察，必須要考量節點在網路架構中所處的位置，在越下游的節點蒐集封包與較上游的節點相較，所需要過濾的資料量會比較少也比較不會接觸到與受通訊監察對象無關第三人的資料，通訊監察設備的安裝涉及從網路服務提供者的通訊設備截取封包信號，同樣地也必須倚賴該節點管理者的協助，才能順利進行通訊監察的工作。封包蒐集裝置的附掛要有該節點設備管理者的協助，封包的蒐集與分析則可以由執行通訊監察之一方獨力完成。

第三項 許可程序

聲請通訊監察書的核發必須要符合通訊保障及監察法第五條第一項所列的事由：「有事實足認被告或犯罪嫌疑人有下列各款罪嫌之一，並危害國家安全或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者，得發通訊監察書。」亦即此一條文內涵所呈現出的重罪原則、相當性原則、必要性原則都具備的情況下，所核發的通訊監察書才具備適法性[12]。

[11] 蔡美智，「通訊保障及監察法」關於網路監聽的相關爭議，資訊法務透析，1999 年 12 月，頁 37。
[12] 陳信郎，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，2004 年，頁 111。

重罪原則：通訊監察是對人民受憲法第十二條保障「人民有秘密通訊之自由」的重大侵害，正在偵查中的犯罪必須是該法第五條第一項所明文列舉之十五款重大的犯罪類型，並「嚴重危害國家安全或社會秩序者」，才符合重罪原則的要求。

相當性原則：由所蒐集到的客觀事實加以判斷，存在相當理由可以支持「即將截取的通訊內容與本案有關」的確信。此原則在於說服法官在做出對人民基本權利侵害的處分之前，確實存在可以經由通訊內容的截取取得證明犯罪的證據之相當理由。

必要性原則：是要避免以國家力量對人民基本權利的恣意侵害，即使所呈現的客觀事實已經符合重罪原則與相當性原則的要求，若存在以侵害較小的方式取得證明犯罪的證據，仍不宜貿然發動對人民通訊內容的截取，當客觀事實已經呈現「不能或難以其他方法蒐集或調查證據者」，才存在通訊監察的必要性。

上述三項原則同樣出現在美國聯邦監聽法對於聲請通訊監察令狀的要求，顯見兩國的法系雖有不同，但是限制國家力量對人民基本權利侵害的目標實屬一致。

網路犯罪是藉由網路的環境著手實施與發生犯罪的結果，並於人們生活的真實世界產生效果，爲了克服網路的特性對於傳統偵查方式所帶來的障礙，通訊監察於是成爲偵查網路犯罪最有效率的方式。網路犯罪的特性能夠通過聲請通訊監察所要求之相當性原則與必要性原則的檢驗，然而該法並未將特定的網路犯罪罪名列舉呈現於條文之中而無法通過重罪列舉原則的檢驗，其中包括利用電腦或其相關設備觸犯洩密罪涉及刑法第三百一十五條以下罪名、竊取線上遊戲寶物涉及刑法第三百二十條的竊盜罪等[13]，以及駭客入侵電腦涉及刑法第三百五十八條、刪除變更電磁紀錄涉及刑法第三百五十九條、發動分散式阻斷服務攻擊涉及刑法第三百六十條。

有實務的研究指出，應就個別的網路犯罪類型加以檢討，就犯罪行爲的可非難性較高且不以通訊監察的方式進行偵查將面臨較高障礙的犯罪類型，依比例原則衡量，將其納入容許通訊監察的範圍[14]。學者並指出美國法制亦是採取重罪原則，但是能夠執行通訊監察的案件範圍遠較我國爲大，只要法院能確實審查通訊監察書的核發，應可考慮適度放寬得進行通訊監察的案件類型[15]。

該法對於有聲請提出權限之人的規定，與刑事訴訟法第一百二十八條之一司法警察官在經過檢察官的同意之後，可以向法院聲請搜索票的規範方式不同，該法第五條第二項的規定呈現出通訊監察書的聲請權是由檢察官所獨占，此與司法警察承擔第一線的犯

[13] 蘇三榮，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，2008年，頁 46。

[14] 謝名冠，網路行爲規範之研究，臺灣臺北地方法院檢察署，2001 年，頁 200-201。

[15] 蔡榮耕，I Am Listening to You（上）－釋字第六三一號解釋、令狀原則及修正後通訊保障及監察法，台灣本土法學雜誌，104 期，2008 年 3 月，頁 56-57。

罪偵查工作，最能確實評估聲請通訊監察必要性的現實運作方式不同，有學者建議可以採取刑事訴訟法第一百二十八條之一的模式，賦予司法警察官在取得檢察官的同意之後，向法院聲請通訊監察書的權限[16]。

第四項 執行

執行通訊監察必須取得法院所核發的通訊監察書，並依據通訊監察書所記載的內容確實執行。通訊保障及監察法第十一條規定有通訊監察書的應記載事項：「一、案由及涉嫌觸犯之法條。二、監察對象。三、監察通訊種類及號碼等足資識別之特徵。四、受監察處所。五、監察理由。六、監察期間及方法。七、聲請機關。八、執行機關。九、建置機關。」

身分隱匿是網路的特性之一，在網路犯罪偵查過程中如何特定犯罪嫌疑人的身分，一直是一個相當大的挑戰，通訊監察書要能具體描述應記載事項之內容，以避免給予執行人員裁量的空間。有關網路犯罪的「監察對象」或「監察通訊種類及號碼等足資識別之特徵」的內容規定並未見諸於通訊保障及監察法施行細則之中，實務上都由檢察官或法官依個別案件的具體事實加以審酌，一般而言「監察通訊種類及號碼等足資識別之特徵」內容，大多記載網路服務提供者被監聽主機所在地址、監聽對象的用戶編號(或撥接用戶的編號)以及分配的 IP 位址，若監聽的客體是電子郵件，則必須同時記載電子郵件主機與電子郵件位址兩項資訊[17]。

該法第五條第二項賦予法官「得於通訊監察書上對執行人員為適當之指示」之權力，執行人員必須遵循法官在通訊監察書上所指示的應注意事項，執行通訊監察。

該法第二條第二項規定通訊監察的執行「不得逾越所欲達成目的之必要限度」，且「應以侵害最少之適當方法為之。」此規範呈現出該法的「比例原則」與「最小侵害原則」內涵，其目的是要將執行過程中對人民的干擾減少至最低程度。針對執行行為的規範還包括時間的限制[18]、使用方法的限制[19]以及執行處所的限制[20]，亦是進一步具體落實該法第二條第二項所揭示的原則。

該法條文中並未如美國聯邦監聽法定有明文規定，執行人員第一次截取到足以證明

[16] 蔡榮耕，I Am Listening to You（上）－釋字第六三一號解釋、令狀原則及修正後通訊保障及監察法，台灣本土法學雜誌，104 期，2008 年 3 月，頁 58。
[17] 陳信郎，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，2004 年，頁 110-111。
[18] 通訊保障及監察法第十二條參照。
[19] 通訊保障及監察法第十三條參照。
[20] 通訊保障及監察法第十四條第一項參照。

犯罪的通訊內容後應立即停止通訊監察，而是由檢察官或法官藉由執行機關定期呈報的報告書[21]，判斷是否有繼續監察的必要才會做出停止監察的決定或是在通訊監察期間屆滿前由檢察官或法官審酌停止監察的必要性[22]，從第一次截取到足以證明犯罪的通訊內容到檢察官或法官做出停止通訊監察決定的這段期間，將會接觸更多監察對象的通訊內容，此與該法第二條第二項所揭示的「最小侵害原則」相悖。

違法執行的通訊監察，將會面臨證據禁止的效果。執行通訊監察過程中違反該法第五條或第六條所規定之事項且情節重大者、第七條或第三十二條所規定之事項者，所取得之內容或所衍生之證據，於司法偵查、審判或其他程序中，均不得採爲證據。此係立法者爲落實人權保障，故明定違反本條之相關規定執行監聽所取得之證據應予排除，至於違法之情節是否重大，則應由法官據個案予以審核[23]。

第五項 監督

通訊保障及監察法設有通訊監察的監督機制，要求依該法第五條、第六條所核准執行之通訊監察，於偵查中由檢察機關、審判中由法院派員至建置機關，或使用電子監督設備，監督通訊監察執行情形，偵查中案件，法院得隨時派員監督執行機關執行情形[24]。該法第十六條第一項規定執行機關於監察通訊後，除了定期應按月向檢察官、依職權核發通訊監察書之法官報告執行情形，檢察官、法官並得隨時命執行機關提出報告。

該法另一個有關通訊監察的監督規定見諸於第五條第四項：「執行機關應於執行監聽期間，至少作成一次以上之報告書，說明監聽行爲之進行情形，以及有無繼續執行監聽之需要。法官依據經驗法則、論理法則自由心證判斷後，發現有不應繼續執行監聽之情狀時，應撤銷原核發之通訊監察書。」

課以執行機關報告的義務是爲了落實人權保障，使執行機關負有應於通訊監察期間提出報告之義務，若發現無通訊監察之必要時，得由法院撤銷通訊監察書，儘早停止通訊監察，以維護人權並減少侵害的擴大[25]。

在英美普通法的傳統下，治安機關執行搜索原則上應該在事前告知，此即「敲門告知」(knock and announce)原則，這個原則是保障隱私權以及節制政府濫權的一個重要手段，被搜索人有機會當場防衛自己的權利[26](例如，指出搜索令狀上的地址錯誤，亦即

[21] 通訊保障及監察法第五條第四項參照。
[22] 通訊保障及監察法第十二條第二項參照。
[23] 通訊保障及監察法第五條立法理由參照。
[24] 通訊保障及監察法第十六條第二項參照。
[25] 通訊保障及監察法第五條立法理由參照。
[26] 廖元豪，多少罪惡假「國家安全」之名而行？一簡介美國反恐措施對人權之侵蝕，月旦法學雜誌，131

該處所並非令狀上記載應該被搜索的地點)，並親自在場監督搜索的範圍是否有逾越令狀所允許的界線，同時可以當場立即提出異議以防止侵害的擴大。

執行搜索是爲了掌握已經存在的犯罪證據，通訊監察是對於正在發生或未來即將發生通訊內容的截取行爲，犯罪嫌疑人若事先知悉其通訊內容將被蒐集以用於證明其犯罪之刑事程序上，將不再於通訊內容中透露任何對其不利的訊息，基於通訊的這項特質事先告知將有礙於通訊監察的執行。

通訊保障及監察法除了規範執行機關的報告義務之外，該法第十五條並課以執行完畢後對監察對象的通知義務。亦即除了認爲通知有妨害監察目的之虞或不能通知之情形外，或是不通知之原因消滅後，應即敘明受監察人之姓名、住所或居所報由檢察官陳報法院通知受監察人，或是敘明不能通知之原因陳報法院[27]。

事後的通知雖然不如事前通知能有效且即時防止侵害的擴大，事後的通知使監察對象有機會知悉並檢視其是否已遭受違法通訊監察或其受通訊監察內容是否遭到洩漏或濫用，該法並賦予受有損害之人損害賠償求償的權利[28]，損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅，或自損害發生時起，逾五年而消滅[29]。

對於執行機關不存在該法第十五條的不通知的例外情形，卻未能確實履行事後通知的義務時，該法並未規範任何的法律效果，有論者建議對於沒有正當理由未能確實履行該義務者應課以罰則，以促進該法第十五條規範的落實，且該法亦未如美國聯邦監聽法一般，要求執法機關對於每年通訊監察的聲請與核發資料加以記錄，並經過彙整後呈報立法機關備查，因而沒有公開的統計資料可以評估通訊監察的實施成效[30]，進而提供未來修訂相關法律時的參考依據。

第三節 使用者資料的揭露

美國電子通訊隱私法是以是否涉及通訊內容之接觸爲區分以適用不同的法律，我國法制亦採取相似的標準，涉及具有隱私期待通訊內容的截取必須適用較嚴格的通訊保障及監察法，對於通訊內容以外之非內容資訊則適用電信法與個人資料保護法相關規定。

期，2006 年 4 月，頁 40。

[27] 通訊保障及監察法第十五條參照。

[28] 通訊保障及監察法第十九條參照。

[29] 通訊保障及監察法第二十一條參照。

[30] 謝昆峰，網際網路與刑事偵查，國立台灣大學法律學研究所碩士論文，2002 年，頁 139。

第一項 個人資料的取得

申請電話或網路之通訊服務時，服務提供者基於營運管理的需求會要求申請人提供姓名、生日、身分證字號、裝機與帳單地址、甚至包括教育程度、婚姻狀態、職業等資訊，這些個人資訊已經足以拼湊出一個人的側寫以及在社會上的族群屬性，並在今日商業活動頻繁的社會中具有某種程度的商業價值，取得這類資訊藉由篩選出目標族群即可提高網路或電話行銷成功的機會。

在網路犯罪刑事偵查的範疇內通訊服務提供者所掌管的個人資訊亦具有相當的價值，犯罪偵查的過程中所掌握的電話號碼、IP 位址、電子郵件帳號或是網頁位址等資訊，只能確定該些資訊涉及犯罪或淪爲犯罪的工具，對於犯罪行爲人身分的掌握並未能發揮立即的貢獻，此時通訊服務提供者所掌管的個人資訊，能夠提供連結犯罪行爲人身分的最佳憑藉，例如，電話是由何人所申請安裝、IP 位址是配發給何人使用、電子郵件帳號或網頁位址是由何人所註冊申請、以及通訊設備的所在地點。

個人資訊足以表徵個人的特質與呈現歷史的紀錄，對其不當的蒐集或揭露將會構成個人對其自身資訊限制傳播權利的侵害，因此法學界多將個人資訊視爲隸屬於隱私權範圍的一環，而肯認應該對其加以保護，在大法官的釋憲實務中已經肯認隱私權是屬於受憲法保障的基本權，基於刑事偵查作爲的需要，取得個人資訊之要件與程序必須符合「法律保留原則」[31]，才不至於引發侵害人民受憲法保障權利的疑慮。

網路犯罪刑事偵查過程中爲了確定犯罪嫌疑人的身分而向通訊服務提供者請求提供其所掌管的用戶個人資訊，將涉及個人資料保護法、電信法與刑事訴訟法等相關法律之規定。

個人資料保護法用以規範個人資料之蒐集、處理及利用[32]。2010 年 5 月 26 日公布的個人資料保護法較其前身電腦處理個人資料保護法，具有保護客體的增加與保護義務適用主體的擴大等優點，受保護的個人資料將不再侷限於以電腦處理的資料類型，以人工紙本的方式處理的個人資料同樣屬於受保護的客體，受規範負有義務的主體不再採取行業別列舉的方式，而是普遍及於該法第二條所定義的公務機關與非公務機關[33]。

犯罪偵查過程中執法機關要求通訊服務提供者提供用戶的個人資料，依據個人資料保護法對於行爲的定義，服務提供者提供其所掌管的個人資料是屬於利用的行爲，執法

[31] 謝昆峰，網際網路與刑事偵查，國立台灣大學法律學研究所碩士論文，2002 年，頁 143。
[32] 個人資料保護法第一條參照。
[33] 劉靜怡，不算進步的立法：「個人資料保護法」初步評析，月旦法學雜誌，183 期，2010 年 8 月，頁 148。

機關取得個人資料是屬於蒐集的行爲，因此執法機關與通訊服務提供者同時受該法的規範。該法第八條[34]與第九條規範直接與間接蒐集個人資料應履行告知義務，但是第八條第二項允許若存在依法律規定得免告知、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要、或告知將妨害公務機關執行法定職務的情況下可以免除告知義務。實務上執法機關通常不會向偵查對象告知調閱其用戶個人資料的蒐集行爲，以避免偵查對象妨礙偵查的進行。

個人資料保護法禁止對所蒐集的個人資料進行特定目的以外之利用，除非有該法第二十條第一項所列各款的除外情形，才能爲特定目的外之利用：

一、法律明文規定。

二、爲增進公共利益。

三、爲免除當事人之生命、身體、自由或財產上之危險。

四、爲防止他人權益之重大危害。

五、公務機關或學術研究機構基於公共利益爲統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。

六、經當事人書面同意。

若不存在該條第一款的法律依據，執法機關欲引用第二款與第四款是否將導致浮濫取得個人資料，造成人民基本權利的侵害。有論者建議應依據法律保留原則明確訂定要件與程序規範[35]，以避免控辯雙方因所處立場不同而對於條文產生不同解讀的疑慮。

該法第三條規定該條所賦予個人資料當事人之權利不得預先拋棄或特約限制，以此大前提解讀第二十條第六款經當事人書面同意的除外規定，可以很清楚地瞭解當事人的同意必須是爲了該次的目的外利用所爲之特定徵詢而取得，倘若個人資料蒐集機關於當事人提供個人資料之時即聲明在特定的情況下有權對個人資料進行目的外之利用，例如基於協助司法機關調查犯罪之需要者，此類預先約定不免給人以契約約定凌駕法律條款的印象，且將因抵觸該法第三條的規定而不具有法律效力。

電信法第七條第一項要求電信事業及其從業人員對於電信之「有無」及其「內容」負有保密的義務。該法並未提及對於用戶個人資料的保密義務，卻於該條第二項明定電信事業受理有關機關查詢「通信紀錄」及「使用者資料」應遵循電信總局所訂定之相關作業程序規定，很明顯地未能賦予電信事業及其從業人員對於用戶個人資料的保密義務

[34] 個人資料保護法第八條第一項所規定的告知事項包括：「一、公務機關或非公務機關名稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得行使之權利及方式。六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。」

[35] 謝昆峰，網際網路與刑事偵查，國立台灣大學法律學研究所碩士論文，2002 年，頁 145。

此係立法上的疏漏。

實務上查詢電信用戶的個人資料必須遵循，依據電信法第七條第二項所授權訂定具有法規命令位階之「電信事業處理有關機關(構)查詢電信使用者資料實施辦法」中所規範的要件與程序。就要件要求而言，查詢機關應敘明其法律依據且存在該辦法第三條所列各款之情形，例如司法機關、監察機關或治安機關因偵查犯罪或調查證據所需者，才能依法向電信業者查詢使用者資料[36]。該辦法並將電信業者能夠提供的使用者資料範圍限制在電信使用者姓名或名稱、身分證統一編號、地址、電信號碼等資料，並以用戶申請各項電信業務所填列之資料為限[37]。

就程序要求而言，查詢機關應提出正式公文或加蓋機關印信之電信使用者資料查詢單正本記載該辦法第五條所規定之資訊辦理，緊急情況之查詢可以傳真為之，並於三個工作日內補具正式公文或加蓋印信之電信使用者資料查詢單正本，若經查詢機關與電信事業雙方事前認證同意，查詢申請的提出得以經加密之電子郵件為之，該電子郵件並視同正式公文或電信使用者資料查詢單正本[38]。

刑事訴訟法中，有關執法機關取得通訊服務提供者所掌管的用戶個人資料，可以藉由證據保全程序，依據法院所核發的搜索令狀執行搜索並經扣押程序而取得或命掌管該個人資料之通訊服務提供者依據提出命令之要求而提出。

第二項 通訊紀錄的取得

通訊紀錄記載著用戶使用該通訊服務的相關細節，最早的起源單純是為了收取通話費用的帳務需求，電信服務提供者記錄通話對象的電話號碼與通話開始與結束時間，就可以依據該通對話是屬於長途或區域通話以及通話所進行的時間而計算出應該向用戶收取的費用。在網路通訊尚未普及的年代，電信法第七條第一項的電信之「有無」即是指通話雙方之電話號碼、通話日期與通話開始與結束時間等不涉及通話內容之用戶使用電信服務的資訊。

隨著網路通訊的普及，通訊紀錄所含括的資料類型將不再僅侷限於用戶識別碼與通訊時間，還包括配發給用戶的 IP 位址、所連線主機或瀏覽網頁的 IP 位址以及連線的時間等資訊[39]。通訊設備本身基於系統管理與資訊安全維護上的需求，亦會記錄設備在運轉過程中相關的運作情形。基於犯罪偵查的需要這些通訊服務提供者所記錄之用戶使用

[36] 電信事業處理有關機關(構)查詢電信使用者資料實施辦法第三條參照。
[37] 電信事業處理有關機關(構)查詢電信使用者資料實施辦法第四條參照。
[38] 電信事業處理有關機關(構)查詢電信使用者資料實施辦法第五條參照。
[39] 謝昆峰，網際網路與刑事偵查，國立台灣大學法律學研究所碩士論文，2002 年，頁 140。

通訊服務的歷程紀錄，成爲瞭解偵查對象以及提供偵查線索的重要來源依據。

實務上查詢電信用戶的通信紀錄必須遵循，依據電信法第七條第二項所授權訂定之「電信事業處理有關機關查詢電信通信紀錄實施辦法」中所規範的要件與程序。就要件要求而言，查詢機關考量必要性、合理性及比例相當原則，並確認符合相關法律程序後，才能依法向電信業者查詢使用者之通信紀錄[40]。第一類電信事業[41]可以提供之通信紀錄範圍包括，以受理查詢日回溯起算最近三個月以內之市內通信紀錄、最近六個月以內之國際、國內長途通信紀錄、以及最近六個月以內之行動通信通信紀錄[42]。

就程序要求而言，查詢機關應提出正式公文或加蓋機關印信之電信通信紀錄查詢單正本記載該辦法第三條所規定之資訊辦理，緊急情況之查詢可以傳真爲之，並於三個工作日內補具正式公文或加蓋印信之電信通信紀錄查詢單正本，若經查詢機關與電信事業雙方事前認證同意，查詢申請的提出得以經加密之電子郵件爲之，該電子郵件並視同正式公文或電信通信紀錄查詢單正本[43]。

實務上查詢網路通訊用戶的通信紀錄必須遵循，依據電信法第十七條第二項所授權訂定之「第二類電信事業管理規則」中所規範的要件。就要件要求而言，該管理規則第二十七條第一項規定基於調查或蒐集證據之需要，並依法律程序查詢電信之「有無」及其「內容」者，經營者應提供之。該條第二項規定對於網路通訊電信內容之監察事項，則應回歸通訊保障及監察法的規範。

該管理規則並未具體規範查詢網路通訊電信紀錄提出申請的程序事項，至於是否應準用「電信事業處理有關機關查詢電信通信紀錄實施辦法」第三條之程序規定亦未提及。本文建議應於該管理規則中規範具體的申請程序事項，以符合法規範明確性之要求。該條第三項規範經營者對於各類網路通訊接取服務紀錄應該保存如以下所列時間：

一、撥接用戶識別帳號、通信日期及上、下網時間等紀錄應保存六個月。

二、非固接式非對稱性數位用戶迴路(ADSL)用戶識別帳號、通信日期及上、下網時間等紀錄應保存三個月。

三、纜線數據機用戶識別帳號、通信日期及上、下網時間等紀錄應保存三個月。

四、張貼於留言版、貼圖區或新聞討論群之內容來源 IP 位址與當時系統時間應保存三個月。

五、免費電子郵件信箱及網頁空間線上申請帳號時之來源 IP 位址及當時系統時間

[40] 電信事業處理有關機關查詢電信通信紀錄實施辦法第三條參照。
[41] 依電信法第十一條之定義，第一類電信事業是指設置電信機線設備，提供電信服務之事業。
[42] 電信事業處理有關機關查詢電信通信紀錄實施辦法第五條參照。
[43] 電信事業處理有關機關查詢電信通信紀錄實施辦法第三條參照。

應保存六個月。

六、電子郵件通信紀錄應保存一個月。

爲了避免有助於犯罪偵查的證據遭到銷毀或遺失，美國儲存通訊法設有緊急保存通訊紀錄的相關規定，執法人員著手偵查網路犯罪的第一件事情就是通知網路服務提供者保存有關特定用戶帳號相關的資料，並同時向法院聲請強制揭露該些資訊的許可。

我國電信法僅就電信管制事項中常見普遍類型的通訊紀錄規範其保存期限，基於刑事偵查作爲的需要且爲因應新型態通訊工具的出現，對於不涉及內容資訊的通訊紀錄且未規範於電信法中應受保存的通訊紀錄類型。本文建議，目前因應的方法爲應賦予執法機關要求通訊服務提供者緊急保存通訊紀錄的權限，而根本解決之道應該在刑事訴訟法或通訊保障及監察法中規範緊急保存與延長緊急保存通訊紀錄的相關規定，以提供通訊服務提供者遵循的法律依據並同時顧及刑事偵查的實務需要。

第三項 提高非通訊內容資訊的保障

非通訊內容泛指通訊過程中伴隨著通訊內容而發生但不涉及實質通訊內容的其他資訊[44]，非內容資訊雖然不會涉及通訊內容，藉由網路服務提供者所記錄的使用者網路活動之相關歷程，可以輕易地拼湊出網路使用者的習性與嗜好[45]，例如都在什麼時間點上網、都造訪什麼類型的網站，由這些片段的資訊可以推知網路使用者的生活習性與個人偏好，平日與他人交往的過程中不曾輕易透露的嗜好，卻在使用網路的過程中毫不防備地徹底顯現，因此這種性質的資訊已經具有某種程度的隱私特質。

對於是否涉及通訊監察法規的適用，我國法制是以是否涉及接觸具有隱私期待之通訊內容爲區分標準，對於非內容資訊之蒐集在電話通信系統上是指蒐集通話雙方的電話號碼，在此應用實例中區分的方式是很清楚並不會有混淆或意外接觸通訊內容的機會。在網路通訊的傳輸過程中，內容與非內容資訊的區分有時並不是如此的明確[46]。

在網路通訊的應用上，通訊內容被分割成較小單位長度的承載資料並加上封包表頭以構成一個完整的封包，接著以封包爲單位傳輸在網際網路的傳輸媒體上，封包表頭記載著發送端與接收端的 IP 位址，以指引傳輸路徑上沿途的路由器將該些封包傳送至接收端，抵達目的接收端之後先將封包表頭丟棄並組合所有接收到的承載資料，以完整呈現發送端所傳送的內容。執法機關欲掌握網路通訊的非內容資訊所執行封包表頭的截取

[44] 李榮耕，論偵查機關對通信紀錄的調取，政大法學評論，115 期，2010 年 6 月，頁 122。

[45] 經由使用者所經常造訪的討論區以及該討論區所張貼的文章內容，即可推知其嗜好取向。

[46] 李震山，挪動通訊保障與通訊監察天平上的法碼—釋字第六三一號解釋評析，台灣本土法學雜誌，98 期，2007 年 9 月，頁 283。

時，無法避免地也會同時截取到承載資料，只能在事後過濾承載資料並加以排除，才不至於構成違法通訊監察[47]。至於是否確實執行過濾排除的動作，目前並無相關的監督機制，只能完全信賴執法人員的自律。

美國電子通訊隱私法中對於用戶個人資料與相關通訊紀錄可以取得的範圍以列舉的方式加以規定，並在程序上要求必須以搜索令狀、法院命令、或依據聯邦或州法律所核發的行政傳票、聯邦或州大陪審團傳票或審判傳票才能取得[48]。

我國有關非通訊內容資訊的保障，在所蒐集的個人資料方面有個人資料保護法用以規範個人資料蒐集、處理與利用的一般規定。另外有電信法第七條第二項授權電信總局訂定查詢用戶個人資料與調閱通訊紀錄的實施辦法，該些辦法雖然以法規命令的形式符合了法律保留的要求，對於相關資料的查詢並沒有一個機關加以控制，也沒有一個比較嚴格的審查標準，電信法本質上是屬於規範電信業務行政管制事項的法律，並不適合同時賦予刑事偵查中節制國家力量並保護相對人基本權利的功能[49]。

學者主張個人資料必然涉及資訊自主權，資訊自主權是屬於資訊隱私權之前哨，每項個人資料之蒐集，不論是否涉及隱私皆應尊重當事人之自主權利，並應依該些資料所涉及隱私敏感程度的高低，考量法規範的強度與密度[50]。

個人資料與網路通訊紀錄的拼湊，可以輕易得知當事人亟欲保持私密不願意他人與聞的習性與嗜好，若僅依據行政命令即可取得這類的資料，顯然存在著較高侵害隱私的可能性，有論者建議，這類資料的取得應該經過法院的審核，爲了避免妨礙犯罪偵查的效率，對於確信程度的要求只需達到比「相當理由」低的審查標準，例如「有合理的懷疑」這樣的門檻，並於刑事訴訟法或通訊保障及監察法中訂定蒐集非內容資訊相關的程序規定，以保障通訊服務使用者的隱私利益[51]。

第四節 電磁紀錄的搜索與扣押

我國對於搜索與扣押的規範，就規範的層次而言與美國不同，美國在憲法第四增修條文中明文規定人民有對抗國家不合理搜索與扣押的權利，我國則是在憲法的列舉基本權清單之後，除了以憲法保留的方式將人身自由的保護規定在憲法第八條之中，其他基

[47] 蘇三榮，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，2008年，頁 74-75。

[48] 謝昆峰，網際網路與刑事偵查，國立台灣大學法律學研究所碩士論文，2002 年，頁 146。

[49] 陳信郎，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，2004 年，頁 101-102。

[50] 李震山，來者猶可追，正視個人資料保護問題—司法院大法官釋字第六０三號解釋評析，台灣本土法學雜誌，76 期，2005 年 11 月，頁 227-228。

[51] 謝昆峰，網際網路與刑事偵查，國立台灣大學法律學研究所碩士論文，2002 年，頁 147。

本權的保護(包括自由權與財產權)則經由法律保留原則的操作，由立法者以法律明定政府可能侵害基本權之公權力行爲的程序與實質規範[52]。

隨著電腦運算能力的提高，逐漸在協助人們處理資料的過程中扮演起重要的角色，也加深人們對於電腦的倚賴，很自然地許多重要的資料都儲存在電腦之中。電腦所擅長的是快速準確地處理資料，資料的處理不再是僅侷限於數字的運算而已，文字、聲音或影像都可以藉由電腦的運算處理之後，而被人們應用於文書、娛樂或通訊目的之達成。電腦是以電能驅動的一種裝置，而其所運算處理的資料信號當儲存於載體[53]之後即是以電磁紀錄[54]的形式存在。犯罪偵查所蒐集的證據是後續刑事程序中認定事實與適用法律的基礎，具有證明犯罪功能之電磁紀錄因此成爲重要的搜索與扣押客體。

我國刑事訴訟法中有關電磁紀錄的規定，首先出現在 2001 年刑事訴訟法修正第一百二十二條將電磁紀錄列爲得搜索的客體，以及修正第一百二十八條將電磁紀錄列爲搜索票應記載事項之一。並於 2003 年刑事訴訟法增訂第一百六十五條之一將電磁紀錄列爲得受調查的新型態證據類型之一。

電磁紀錄本身並不具備有形的形體，亦無法經由人類的感官直接解讀其所承載的資訊內容，而須以一定之科技設備，始能還原成人類五官知覺所能理解之資訊[55]，因此以電磁紀錄爲客體所執行的搜索，亦必須在該些科技設備上爲之，例如在電腦上執行電磁紀錄之搜索。

搜索電腦發現得爲證據之電磁紀錄後，對於該電磁紀錄是否能依據刑事訴訟法第一百三十三條第一項加以扣押則不無疑慮，該條條文所規範的扣押處分只能針對有體物，因此必須將電磁紀錄儲存附著於儲存裝置之類的有體物上，始得符合該條條文對物扣押之規範[56]。

實務上常見的電磁紀錄扣押的方式包括：將儲存有該電磁紀錄的儲存裝置扣押、以科技設備查詢電磁紀錄內之資訊列印後加以扣押、就該儲存裝置內必要之電磁紀錄，複製在執法單位所持有的儲存裝置後加以扣押[57]，或是整部電腦連同其儲存裝置一起扣押。

究竟應採取哪一種扣押方式，應該由電磁紀錄所欲證明的事實以及當時客觀的環境來決定，例如單純爲了證明存在文字資料的內容，則可以將電磁紀錄內之資訊列印後加

[52] 謝昆峰，網際網路與刑事偵查，國立台灣大學法律學研究所碩士論文，2002 年，頁 13。
[53] 何賴傑，錄音、錄影、電磁記錄等之調查(刑事訴訟法第一六五條之一第二項)，全國律師，8 卷 9 期，2004 年 9 月，頁 33。
[54] 刑法第十條第六項參照。
[55] 何賴傑，錄音、錄影、電磁記錄等之調查(刑事訴訟法第一六五條之一第二項)，全國律師，8 卷 9 期，2004 年 9 月，頁 33。
[56] 何賴傑，成大 MP3 搜索事件之法律檢討，台灣本土法學雜誌，23 期，2001 年 6 月，頁 87。
[57] 王銘勇，網路犯罪相關問題之研究，司法院，2002 年 11 月，頁 244。

以扣押。若所欲取得的電磁紀錄係儲存於網路系統的儲存裝置中且僅占極小的資料量，扣押整個網路系統的儲存裝置將不符合比例原則，則可以採取將必要之電磁紀錄，複製在執法單位所持有的儲存裝置後加以扣押之方式。倘若所欲取得的電磁紀錄是具有系統檔案的特性，無法以瀏覽列印的方式加以顯現，則應將整部電腦連同其儲存裝置一起扣押，再以電腦鑑識的方式取得證據，例如要證明該電腦被用於網路攻擊的犯罪，或是要證明犯罪嫌疑人聲稱該電腦被當成網路犯罪的跳板，係純屬狡辯脫罪之詞。

學者將扣押定義爲「爲保全證據物件爲目的，以取得物之占有而實施之強制處分。」[58]，該定義呈現出扣押處分係以移轉占有之方式對於持有利益造成干預。電磁紀錄的特性之一是可以輕易地複製，以複製的方式扣押電磁紀錄並不會造成支配權的侵奪，因此對於電磁紀錄的扣押並不符合傳統上對於扣押的定義。

在電磁紀錄的扣押相關法條文字的使用上，有論者建議應將「扣押」改爲「取得」，才不至於破壞傳統上對於扣押的定義[59]。沒收是我國刑法第三十四條所規定從刑的種類之一，扣押是暫時對於支配權的干預，沒收則是永久地剝奪其支配權。對於具有犯罪性質的電磁紀錄我國刑法亦定有相關的沒收規定[60]，考量電磁紀錄的無實體特性，在法條文字的使用上應將「沒收」改爲「刪除」方爲妥適。

第一項 有令狀的搜索

搜索是對於人民基本權利的侵犯，實施這類國家行爲的聲請要件與程序之訂定，必須要符合法律保留原則，執法機關執行搜索必須踐行向法院聲請搜索票核發的程序，法院審核聲請書上所記載的發動要件，認爲存在發動搜索的「必要」或「相當理由」時，簽發搜索票並記載必要之資訊，交由執行人員收執並適時向相關人員提示，以提供執行搜索時遵循的依據。

我國有關電磁紀錄的搜索，始於刑事訴訟法第一百二十二條將電磁紀錄列爲得搜索的客體，該條進一步將搜索被告或犯罪嫌疑人以及第三人，發動的門檻區分爲「必要時」與「相當理由」兩個要件。

「必要時」要件之滿足，須有合理之根據認爲被告或犯罪嫌疑人之身體、物件、居住處所或電磁紀錄存在有得作爲犯罪證據或與之相關之證據的可能性，而「相當理由」要件之滿足，並非以搜索者主觀標準判斷，尚須有客觀之事實爲依據，兩者之間搜索權

[58] 蔡墩銘，刑事訴訟法論，五南，2001 年 2 月，頁 197。
[59] 謝昆峰，網際網路與刑事偵查，國立台灣大學法律學研究所碩士論文，2002 年，頁 150。
[60] 刑法第二百零五條參照。

發動的差別在於「相當理由」之標準要比「必要時」高，此二要件均應由搜索票之聲請人於聲請書上釋明以供法官審酌[61]。

依據「法院辦理刑事訴訟案件應行注意事項」第六十三點所確立的指導原則，在網路犯罪的偵查過程中，當犯罪嫌疑人的身分一經確定，偵查機關即可依其主觀上的判斷，認爲存在搜索之必要性時，得向法院聲請搜索犯罪嫌疑人的電磁紀錄。以電子郵件散佈惡意程式爲例，經由發信電子郵件位址查出寄件者的身分後，可以主觀上合理地認定該含有惡意程式的電子郵件依然以寄件備份的形式存放在該寄件者的電腦中，而可以發動對該電腦搜索電磁紀錄。將對被告或犯罪嫌疑人執行搜索所需滿足的「必要性」門檻，與美國的搜索要件加以相互比較，美國並不刻意區分搜索對象是第三人而是統一適用「相當理由」這個標準，顯然我國對被告或犯罪嫌疑人的搜索要件較寬鬆。

令狀原則的效用之一爲將執行搜索的過程中，執行者與搜索對象所有的權利與義務均詳實地記載於搜索票上，我國刑事訴訟法第一百二十八條將電磁紀錄列爲搜索票應記載事項之一，亦即當搜索客體涉及電磁紀錄時，必須明確記載於搜索票之上，否則即構成違法搜索。

規範搜索票的應記載事項之用意，在於確定欲搜索與扣押之客體係爲電腦主機、硬體、外部儲存裝置抑或是電磁紀錄，並盡可能爲個別具體之記載，以確定執行搜索人員強制處分之權限範圍，並使受處分之人對於其負有相應之忍受義務範圍得以明確[62]。

倘若搜索票僅記載對電腦之儲存裝置實體之搜索與扣押，其效力應不及於儲存在該儲存裝置內之電磁紀錄，必須在搜索票上同時記載「電腦之儲存裝置」及「儲存在該儲存裝置內之電磁紀錄」，始得同時扣押[63]。

在搜索票聲請書中載明電磁紀錄爲搜索與扣押的客體，可以達到讓法院審查是否存在搜索電腦的相當理由，並藉由令狀的特定性以達成避免執行搜索人員的釣魚式搜索等功能，例如所要找尋的證據是實體證物，自然不存在搜索與扣押電腦與電磁紀錄的相當理由，而所要找尋的是文字文件，即不能任意打開圖檔加以瀏覽檢視[64]。

以找尋電磁紀錄爲標的之搜索，應明確將該些電磁紀錄的性質記載於搜索票之應扣押物品欄之上，不宜僅概括記載爲「電磁紀錄」，以毒品案件之偵查爲例，合宜的記載方式爲「有記載關於販賣毒品案件，有關之帳冊、顧客名冊之電磁紀錄」以符合令狀明確性之要求[65]。

---

[61] 法院辦理刑事訴訟案件應行注意事項，第六十三點(搜索之要件與釋明)參照。
[62] 黃佩倫，入侵電腦行爲之研究，國立交通大學科技法律研究所碩士論文，2004 年，頁 91。
[63] 王銘勇，網路犯罪相關問題之研究，司法院，2002 年 11 月，頁 243。
[64] 謝昆峰，網際網路與刑事偵查，國立台灣大學法律學研究所碩士論文，2002 年，頁 149。
[65] 王銘勇，網路犯罪相關問題之研究，司法院，2002 年 11 月，頁 245。

第二項 無令狀的搜索

搜索依其程式，可區分爲要式搜索與非要式搜索，其中非要式搜索亦即無令狀搜索又區分爲同意搜索、緊急搜索與附帶搜索，分別規範於刑事訴訟法第一百三十一條之一、第一百三十一條、第一百三十條[66]，以下僅就電磁紀錄之無令狀搜索與扣押加以說明。

第一款 同意搜索

我國刑事訴訟法第一百三十一條之一規定：「搜索，經受搜索人出於自願性同意者，得不使用搜索票。但執行人員應出示證件，並將其同意之意旨記載於筆錄。」亦即取得受搜索人有效之同意，即可執行無令狀搜索。

實務上，對於同意之有效性判斷，必須審酌同意搜索是否係出於受搜索人之自願性決定，「自願性」係指同意必須出於同意人之自願，非出自於明示、暗示之強暴、脅迫；法院對於證據取得係出於同意搜索時，首先應審查同意之人是否具同意權限，有無將同意意旨記載於筆錄由受搜索人簽名或出具書面表明同意之旨，並應綜合一切情狀包括徵求同意之地點、徵求同意之方式是否自然而非具威脅性、同意者主觀意識之強弱、教育程度、智商、自主之意志是否已爲執行搜索之人所屈服等情況加以整體考量，遇有被告抗辯其同意搜索非出於自願性同意時，更應於理由詳述審查之結果，否則即有判決理由不備之違法[67]。受搜索人倘若因不知法律且執法人員未告知有拒絕之權利或經執法人員誘導而誤認有配合偵查之義務，基於上述情狀而同意搜索時，則不能認爲是有效的同意[68]。

偵查實務上經常藉由第三人之同意而取得搜索之權限，法條的文字以「受搜索人」爲同意權行使的主體，呈現出容許第三人同意搜索的可能性，而審判實務上也明確地承認第三人之同意搜索[69]。美國聯邦最高法院所建立第三人同意搜索的基礎，必須同時具備「共同權限」與「風險承擔」此二個要件[70]。我國實務的見解，只重視「共同權限」這個要件是否存在，至於被告是否主客觀上承擔了共同權限之人可能會同意執法人員搜

[66] 94 年度台上字第 1361 號判決參照。
[67] 94 年度台上字第 1361 號判決參照。
[68] 何賴傑，成大 MP3 搜索事件之法律檢討，台灣本土法學雜誌，23 期，2001 年 6 月，頁 88。
[69] 蔡榮耕，Yes, I do! —同意搜索與第三人同意搜索，月旦法學雜誌，第 157 期，2008 年 6 月，頁 113。
[70] 請參照本文第三章第三節第二項第一款同意搜索。

索的風險，則不是判決關注的重點[71]。

就同意權限的行使，必須先確定該人是否具有行使同意的權限，以及同意權所及的範圍爲何。第三人對於儲存在電腦中的電磁紀錄有共同的存取權限，則被認爲具有行使同意搜索的權限，對於電腦系統中特定儲存區域經設定區分使用者存取權限或施以密碼保護，則該第三人就該特定儲存區域不應視爲具有同意之權限[72]。同意所授與執法人員的權限，僅在同意的範圍內發生效力，因此同意場所的搜索所發現的電腦，該同意範圍並不自動及於搜索該電腦內的電磁紀錄，受搜索人並同時保有隨時撤回同意的權限以終止執法人員的搜索。

電腦網路的系統管理者，是擁有該系統最高權限之人，可以越過使用者存取權限區分或密碼保護的障礙，系統管理者是否因此而取得行使第三人同意搜索之權限，實務研究指出，如果存在使用者可以預期系統管理者將存取其存放在該系統中之檔案的情況，例如電腦系統藉由登入畫面或電腦網路使用規則告知使用者，則該系統管理者將被認爲具有行使同意搜索的權限[73]。

第二款 緊急搜索

我國刑事訴訟法第一百三十一條第二項規定：「檢察官於偵查中確有相當理由認爲情況急迫，非迅速搜索，二十四小時內證據有僞造、變造、湮滅或隱匿之虞者，得逕行搜索，或指揮檢查事務官、司法警察官或司法警察執行搜索，並層報檢察長。」此即爲我國偵查實務當面臨緊急情狀不及聲請搜索票，必須藉由緊急搜索之執行以達到證據保全目的之法律依據。

由該條文所規範的要件分析，實施的主體爲檢察官，或受檢察官指揮之輔助偵查主體，依當時情況判斷存在急迫情況且不及聲請搜索票，若不迅速執行搜索以保全證據，證據將有可能會遭到僞造、變造、湮滅或隱匿。實務上，搜索的執行大多由輔助偵查主體實施，因此當面臨需要緊急搜索的情狀，又爲了符合刑事訴訟法第一百三十一條第二項的規範，學者認爲應以向檢察官報備取得核可的方式，視爲檢察官之處分[74]。

在涉及搜索電磁紀錄的情況急迫之判定，硬體及其內之電磁紀錄應分開考量，如發現電腦硬體正在遭受破壞或電磁紀錄正在遭受刪除，非立即將該電腦加以扣押並切斷對外之網路連線，使其隔離於行爲人實力支配之外，該證據將有遭湮滅之可能，此即符合

[71] 蔡榮耕，Yes, I do! —同意搜索與第三人同意搜索，月旦法學雜誌，第 157 期，2008 年 6 月，頁 115。
[72] 黃佩倫，入侵電腦行爲之研究，國立交通大學科技法律研究所碩士論文，2004 年，頁 99。
[73] 王銘勇，網路犯罪相關問題之研究，司法院，2002 年 11 月，頁 254。
[74] 林鈺雄，刑事訴訟法(上)，元照，2004 年 9 月，頁 361。

以證據保全爲目的之緊急搜索扣押要件，該些裝置一經緊急扣押隔離之後此急迫情況即已消失，此時欲搜索電磁紀錄則應該先取得搜索票方爲適法[75]。

倘若急迫情狀無法藉由緊急扣押加以排除，則仍應允許當場執行緊急搜索，例如電磁紀錄所處之電腦網路系統過於龐大且儲存資料之主機分散各地，若執意對該些裝置加以扣押不僅耗費太多資源且不符比例原則，此時則應立即搜索電磁紀錄並以複製或列印的方式加以扣押。

第三款 附帶搜索、扣押與另案扣押

刑事訴訟法第一百三十條賦予執行逮捕時，執法人員得在無令狀的情形下附帶搜索受逮捕人之身體、隨身攜帶之物件、所使用之交通工具以及其立即可觸及之處所。其用意是要找尋可能被用於攻擊執法人員的武器或可能遭到毀損的證據[76]。

在電腦網路犯罪的偵查中，附帶搜索的發動不是以找尋可能被當成武器攻擊執法人員的電腦或電磁紀錄爲目的，而是藉以找尋可能存在儲存有犯罪證據之電磁紀錄的儲存裝置，例如小型的 USB 隨身碟，以防止證據遭到毀損或湮滅。搜索過程中發現與本案可能相關的證據，即可以依據刑事訴訟法第一百三十七條執行附帶扣押。經附帶扣押的儲存裝置已經不存在緊急的情狀，必須先取得搜索票才能搜索在該儲存裝置中的電磁紀錄，以進一步釐清是否存在涉案證據。

電磁紀錄的另一種無令狀扣押情形是出現在，基於一個合法的搜索過程中發現另案得扣押的犯罪證據，該另案證據是以使執行搜索人員處於一目瞭然的方式，出現在執行搜索人員的眼前，此時執法人員可以依據刑事訴訟法第一百五十二條之規定對該另案證據加以扣押，例如搜索票的核發是以找尋販賣毒品相關的電磁紀錄，卻意外在搜索電磁紀錄的過程中發現槍械買賣的交易名單。執行搜索人員不能立即轉向該另案證據的搜索，必須取得另一張核准找尋該另案犯罪證據的搜索票，所執行的搜索方屬適法。

第三項 專家在場的協助

執行有體物的搜索與扣押遭遇阻礙時，刑事訴訟法第一百四十四條第一項賦予執行人員得開啓鎖扃、封緘或爲其他必要處分之權限。執行電磁紀錄之搜索與扣押最常遇到的情況爲無法取得登入系統的帳號與密碼，或是所尋得的檔案是受有密碼之保護而無法

[75] 王銘勇，網路犯罪相關問題之研究，司法院，2002 年 11 月，頁 255。
[76] 何賴傑，逮捕、搜索與扣押，台灣本土法學雜誌，25 期，2001 年 8 月，頁 119-120。

解除加密措施以進一步閱讀檔案內容[77]，此時倘若以非專業的方式貿然行動將有可能導致證據資料的毀損與滅失。

刑事訴訟法第一百二十八條之二規定搜索實施的主體以及必要時得請求司法警察官或司法警察的輔助。面對搜索電磁紀錄可能遭遇的障礙，該條文中並未賦予執行搜索人員請求相關專家到場協助的權限或是課以具備協助搜索順利進行之特定專業知識之人的協助義務，例如課以受搜索電腦系統之系統管理者，協助搜索執行的義務。

今日的電腦通常非以單機的狀態獨立運作，而是藉由網路的連結相互分享資源，網路的架構與電腦互連的情況存在著許多種的可能方式，藉由一些簡單的技巧即可以掩飾重要電腦主機的存在，例如將後端資料庫主機置於無線傳輸的另一端。沒有專家的在場協助，將無法清楚瞭解整個電腦網路系統的架構，縱使貿然採取行動扣押取得前端的電腦設備，還是無法有效掌握儲存在後端資料庫中能證明犯罪的電磁紀錄。

對於電腦單機的扣押也要同時考量後續電腦鑑識的成功實施可能性，應以符合鑑識要求的標準步驟進行扣押程序，不至於因爲急於扣押證據導致電磁紀錄的變更，例如當場藉由檔案總管翻動資料夾瀏覽檔案，導致檔案最後存取時間的更動[78]，或是沒有遵循標準作業程序的要求[79]，以拔除電源插頭的方式切斷電源供應，反而是以正常程序關機，或是任意將處於關機狀態中的電腦開啓電源執行開機程序，這些標準程序的違反將導致作業系統執行關機、開機程序的過程中重新設定部分系統檔案，而使可能成爲證明犯罪的電磁紀錄因此滅失。

另一個經常發生的情況，即當犯罪嫌疑人預知或正面臨搜索與扣押之執行時，會將儲存犯罪證據的儲存裝置加以實體毀損或下達刪除指令以企圖湮滅其中之電磁紀錄，儲存裝置中的電磁紀錄能夠順利的取得完全倚賴該儲存裝置的實體層與邏輯資料層能正常的發揮功能[80]，有專家的在場協助可以即時防止災害的繼續擴大，例如執法人員抵達現場發現電腦正快速地刪除資料中，卻不知如何下達終止刪除的電腦指令，並藉由提供適當扣押方式的建議，以提高後續電腦鑑識回復資料成功的機會。

電磁紀錄的證據能力經常成爲法庭上攻防的重點，欲針對所扣押的儲存裝置讀取其內容資料時，爲了確保證據本身的安全性以及不至因後續的搜索行爲更改到電磁紀錄，藉由映像檔複製或磁碟一對一複製的方法，對該扣押取得的證據加以保護，並於複製的過程或完畢後針對所複製的儲存裝置內容資料產生必要的摘要(Digest)，即 SHA/MD5

[77] 黃佩倫，入侵電腦行爲之研究，國立交通大學科技法律研究所碩士論文，2004 年，頁 95。
[78] 黃敬博、莊明霓，數位鑑識之資料回復技術探討，資訊安全通訊，17 卷 2 期，2011 年 4 月，頁 93。
[79] Best Practices for Seizing Electronic Evidence, available at http://www.forwardedge2.com/pdf/bestPractices.pdf (last visited June 13, 2012)。
[80] 黃敬博、莊明霓，數位鑑識之資料回復技術探討，資訊安全通訊，17 卷 2 期，頁 88。

之雜湊值，藉以比對供執行搜索的複製資料內容與扣押的資料內容是否完全一致，以防禦未來法庭審理過程中可能來自被告的挑戰[81]。

專家在場的好處爲可以真實評估搜索與扣押所應執行的幅度，提供現場執法人員技術專業上的建議，幫助執法人員所爲之處分將不至逾越所欲達成之目的與所採行之手段相權衡之比例原則規範，此外並應考量修正刑事訴訟法第一百二十八條之二相關規定，賦予執行搜索人員請求相關專家到場協助的權限或是課以具備協助搜索順利進行之特定專業知識之人的協助義務。

第五節 小結

我國憲法本文或增修條文之中，並沒有針對隱私權的明文規定，但是從司法院大法官會議第二九三號解釋開始，隱私權的概念與相關原則開始被援引爲說理與論證的依據，並藉由個案爭議的決議過程中，逐漸勾勒出隱私權的面向與保障的範圍。綜觀大法官的解釋文可以得知，隱私權所呈現的面向至少包括限制個人資訊傳播、個人自我決定權限、以及個人私密空間不受侵擾等具體內容。該些基本權的確立過程是以人性尊嚴爲核心，依序向外擴展至一般人格權、個別人格權之隱私權、隱私權中之資訊隱私權、以及涉及個人資料之資訊自主權。有關控制個人資料流向的資訊自主權則蘊含著資訊隱私權、個人資料保護權、秘密通訊自由等內容，分別對應至搜索電磁紀錄、調閱個人資料、通訊監察等強制處分實施時所將涉及的基本權侵害。隱私權並不是一個絕對的權利，在符合憲法第二十二條與第二十三條的情形時，國家可以對這個權利加以限制。

對於具有隱私期待之即時通訊內容截取即有我國通訊保障及監察法的適用。網路通訊是屬於受通訊保障及監察法規範之受保障的通訊類型。受限於網路犯罪的特性，必須倚賴通訊監察才能有效的蒐集犯罪證據，卻礙於未能通過重罪列舉原則的檢驗，而無法以通訊監察的方式執行犯罪證據蒐集的強制處分，有學者建議應可考慮適度放寬得進行通訊監察的網路犯罪案件類型。

該法規定通訊監察的執行「不得逾越所欲達成目的之必要限度」且「應以侵害最少之適當方法爲之」呈現出該法的「比例原則」與「最小侵害原則」內涵。該法並未明文規定，執行人員第一次截取到足以證明犯罪的通訊內容後應立即停止通訊監察，而必須經由檢察官或法官判斷是否有繼續監察的必要，才會做出停止監察的決定，從第一次截取到足以證明犯罪的通訊內容到檢察官或法官做出停止通訊監察決定的這段期間，將會接觸更多監察對象的通訊內容，此與該法所揭示的「最小侵害原則」相悖。

[81] 黃敬博、莊明霓，數位鑑識之資料回復技術探討，資訊安全通訊，17 卷 2 期，頁 90。

除了執行機關向檢察官或法官的報告義務之外，該法並課以執行完畢後對監察對象的通知義務。事後的通知雖然不如事前通知能有效且即時防止侵害的擴大，事後的通知使監察對象有機會知悉並檢視其是否已遭受違法通訊監察或其受通訊監察內容是否遭到洩漏或濫用，該法並賦予受有損害之人損害賠償求償的權利。

該法對於執行機關不存在不通知的例外情形，卻未能確實履行事後通知的義務時，並未規範任何的法律效果，應考慮對於沒有正當理由卻未能確實履行該義務者課以罰則，以促進事後通知義務的落實。該法亦未如美國聯邦監聽法一般，要求執法機關對於每年通訊監察的聲請與核發資料加以記錄，並經過彙整後呈報立法機關備查，因而沒有公開的統計資料可以評估通訊監察的實施成效，進而提供未來修訂相關法律時的參考依據。

對於通訊內容以外之非內容資訊保護則適用個人資料保護法、電信法與刑事訴訟法等相關法律之規定。在網路犯罪偵查的過程中經常必須倚賴通訊服務提供者提供其所掌管的個人資訊，與偵查機關所掌握的電話號碼、IP 位址、電子郵件帳號或是網頁位址等資訊加以比對，以便確認犯罪嫌疑人之身分。

爲了避免有助於犯罪偵查的證據遭到銷毀或遺失，美國儲存通訊法設有緊急保存通訊紀錄的相關規定。我國電信法僅就電信管制事項中常見普遍類型的通訊紀錄規範其保存期限，基於刑事偵查作爲的需要且爲因應新型態通訊工具的出現，對於不涉及內容資訊的通訊紀錄且未規範於電信法中應受保存的通訊紀錄類型。應考慮在刑事訴訟法或通訊保障及監察法中規範緊急保存與延長緊急保存通訊紀錄的相關規定，以提供通訊服務提供者遵循的法律依據並同時顧及刑事偵查的實務需要。

非內容資訊雖然不會涉及通訊內容，藉由網路服務提供者所記錄的使用者網路活動之相關歷程，這些片段的資訊可以推知網路使用者的生活習性與個人偏好，平日與他人交往的過程中不曾輕易透露的嗜好，卻在使用網路的過程中毫不防備地徹底顯現，因此這種性質的資訊已經具有某種程度的隱私特質。

美國電子通訊隱私法中對於用戶個人資料與相關通訊紀錄可以取得的範圍以列舉的方式加以規定，並在程序上要求必須以搜索令狀、法院命令、或依據聯邦或州法律所核發的行政傳票、聯邦或州大陪審團傳票或審判傳票才能取得。

我國有關非通訊內容資訊的保障，在所蒐集的個人資料方面有個人資料保護法的一般規定。另外有電信法授權電信總局訂定查詢用戶個人資料與調閱通訊紀錄的實施辦法，該些辦法雖然以法規命令的形式符合了法律保留的要求，對於相關資料的查詢並沒有一個機關加以控制，也沒有一個比較嚴格的審查標準，電信法本質上是屬於規範電信

業務行政管制事項的法律，並不適合同時賦予刑事偵查中節制國家力量並保護相對人基本權利的功能。學者主張個人資料必然涉及資訊自主權，資訊自主權是屬於資訊隱私權之前哨，每項個人資料之蒐集，不論是否涉及隱私皆應尊重當事人之自主權利，並應依該些資料所涉及隱私敏感程度的高低，考量法規範的強度與密度。

隨著電腦逐漸在協助人們處理資料的過程中扮演起重要的角色，電腦中具有證明犯罪功能之電磁紀錄因此成爲重要的搜索與扣押客體。電磁紀錄本身並不具備有形的形體，亦無法經由人類的感官直接解讀其所承載的資訊內容，因此對其所爲之搜索與扣押必須藉由一定之科技設備或是儲存載體才能達成。

我國有關電磁紀錄搜索的發動門檻，依被告或犯罪嫌疑人以及第三人之不同，刑事訴訟法區分爲「必要時」與「相當理由」兩個要件。將對被告或犯罪嫌疑人執行搜索所需滿足的「必要性」門檻，與美國的搜索要件加以相互比較，美國並不刻意區分搜索對象是第三人而是統一適用「相當理由」這個標準，顯然我國對被告或犯罪嫌疑人的搜索要件較寬鬆。

執行電磁紀錄之搜索與扣押最常遇到的情況爲無法取得登入系統的帳號與密碼，或是所尋得的檔案是受有密碼之保護而無法解除加密措施以進一步閱讀檔案內容，此時倘若以非專業的方式貿然行動將有可能導致證據資料的毀損與滅失。專家在場的好處爲可以真實評估搜索與扣押所應執行的幅度，提供現場執法人員技術專業上的建議，幫助執法人員所爲之強制處分將不至逾越所欲達成之目的與所採行之手段相權衡之比例原則規範，應考慮修正刑事訴訟法相關規定，賦予執行搜索人員請求相關專家到場協助的權限或是課以具備協助搜索順利進行之特定專業知識之人的協助義務。

第五章 結論

一、物理入侵、合理隱私期待

搜索是對人民基本權利的侵犯，這個誡命首先見諸於美國憲法第四增修條文賦予人民有免於政府不合理搜索與扣押的權利。在當時對於搜索行爲的判斷原則，是以是否有物理入侵「人身、住所、文件及財產」等受憲法所保障的區域所劃設的界線。因此，在住宅外的街道上所進行的電話監聽行爲，將不構成憲法第四增修條文意義下的搜索行爲。

Katz 案所建立的「合理隱私期待」原則，將受憲法第四增修條文所保障的範圍，由「人身、住所、文件及財產」等有形的區域擴展到無形的隱私期待所界定的領域，通訊監察於是成爲搜索行爲態樣的一種，對於人民主觀上呈現隱私的期待，以及社會上也認爲這樣的隱私期待是合理的的侵犯行爲，將有憲法第四增修條文的適用。

由於通訊監察所可能侵害的人民隱私，遠較搜索爲大且無法預期，因此於憲法第四增修條文之外，另外訂定較嚴格的聯邦監聽法，並與撥號記錄器與追蹤裝置法及儲存裝置法，共同構成電子通訊隱私法，希望能對科技時代人民的通訊隱私有進一步的保障。

二、高科技對隱私所帶來的挑戰

Brandeis 大法官在 Olmstead 案的不同意見書中，已經清楚的預告科技的進步將會對政府刺探人民的隱私提供更多的協助，也將對憲法所保障的人民基本權利帶來衝擊。聯邦最高法院過去在個案所建立的原理原則，將在這些科技設備出現的過程中再度受到檢驗。在地面上有圍籬阻隔的隱私期待，經由飛行器的協助所呈現的三度空間下，該隱私期待將不再成爲可能，經由掃瞄房屋所發散出來的熱能，可以清楚地窺知屋內人員的活動狀態與生活上的細節，以及以往必須耗費大量人力的跟尖行爲，如今只需貼附一個衛星定位系統追蹤器，就可以在電腦前輕易的接收被追蹤對象的行蹤。

當人們享受著科學技術的進步爲生活所帶來的便利之時，也面臨著隱私領域正逐漸受到高科技的侵蝕，今日我們所面對的問題是如何對科技的力量施以適當地限制，以減少受憲法保障的隱私領域的縮小。

三、網路通訊監察列舉重罪

通訊監察係對現在正在進行或未來即將發生通訊內容的截取，對於可能蒐集到的通訊內容難以事先加以預測，並可能觸及與本案無關第三人之通訊內容，因此存在著極大的侵害可能性。

在我國的通訊保障及監察法設有「重罪原則」、「相當性原則」、「必要性原則」三個要件，必須同時符合三個要件要求才能實施通訊監察。網路犯罪基於其犯罪的特性，必須倚賴通訊監察的執行才能有效的掌握犯罪證據。

相較於同樣是採取重罪原則的美國法制，其能夠執行通訊監察的案件範圍遠較我國爲大，倘若存在法院能確實審查通訊監察書核發的前提下，應可考慮適度放寬我國通訊保障及監察法得進行通訊監察的案件類型。

四、提高非通訊內容的保護

我國法制是以是否涉及內容與非內容資訊的接觸，以區分不同法律規範的適用。對於非內容資訊的蒐集，實務上是以電信法所授權之「電信事業處理有關機關(構)查詢電信使用者資料實施辦法」與「電信事業處理有關機關查詢電信通信紀錄實施辦法」規範通訊服務用戶個人資料與通訊紀錄之蒐集行爲。

在今日網路通訊普及的年代，非內容資訊雖然不會涉及通訊內容，藉由網路服務提供者所記錄的使用者網路活動之相關歷程，由這些片段的資訊可以拼湊出網路使用者的生活習性與個人偏好，平日與他人交往的過程中不曾輕易透露的嗜好，卻在使用網路的過程中毫不防備地徹底顯現，因此這種性質的資訊已經具有某種程度的隱私特質。

美國電子通訊隱私法中對於用戶個人資料與相關通訊記錄可以取得的範圍以列舉的方式加以規定，並在程序上要求必須以搜索令狀、法院命令、或依據聯邦或州法律所核發的行政傳票、聯邦或州大陪審團傳票或審判傳票才能取得。

在我國僅依據行政命令即可取得這類的資料，顯然存在著較高侵害隱私的可能性，應考慮規定這類資料的取得應該經過法院的審核，並於刑事訴訟法或通訊保障及監察法中訂定蒐集非內容資訊相關的程序規定，以保障通訊服務使用者的隱私利益。

五、專家在場的協助

電腦網路犯罪的證據保全將是以電磁紀錄爲中心，對電磁紀錄的搜索與扣押方式將影響著後續電腦鑑識的成敗，所取得的電磁紀錄的證據能力也經常成爲法庭上攻防的重點。

面對日益複雜的電腦網路系統，基於專業分工的考量，確實存在專家在場協助的必要性，專家在場的好處爲可以真實評估搜索與扣押所應執行的幅度，提供現場執法人員技術專業上的建議，幫助執法人員所爲之處分將不至逾越所欲達成之目的與所採行之手段相權衡之比例原則規範。

此外並應考慮修正刑事訴訟法第一百二十八條之二相關規定，賦予執行搜索人員請求相關專家到場協助的權限或是課以具備協助搜索順利進行之特定專業知識之人的協助義務。

不同的犯罪機制將會產生不同型態的證據，也影響著不同的偵查步驟，而產生不同於傳統犯罪的法規範需求。刑事程序法是有機的法律，其緊緊依附在它所規範的犯罪偵查事實上，事實的改變，將會導致對現行法規範的改變帶來壓力。必須能真實瞭解事實改變所帶來的差異，才能確實衡量現行的法規範是否能適用至新的事實，或需進一步調整法規範。

參考文獻

(一) 中文書籍：

- Corwin, Edward S. & Peltason, J. W.，美國憲法釋義(Understand the Constitution)，廖天美編譯，結構群，1992 年 3 月。
- Corwin, Edward S.，美國憲法(The Constitution and What It Means Today)，Chase, Harold W. & Ducat, Craig R.修訂，王震南譯，陽明管理發展中心，1992 年 5 月。
- 王銘勇，網路犯罪相關問題之研究，司法院，2002 年 11 月。
- 史慶璞，美國憲法與政府權力，三民，2001 年。
- 林俊益，刑事訴訟法概論(上)，新學林，2008 年 9 月。
- 林俊益，刑事訴訟法概論(下)，新學林，2009 年 2 月。
- 林鈺雄，刑事訴訟法(上)，元照，2004 年 9 月。
- 張承瑞，科技犯罪偵查暨數位鑑識出國參訪報告書，台中市警察局，2010 年 11 月。
- 陸潤康，美國聯邦憲法論，文笙，增訂再版，1993 年 5 月。
- 蔡墩銘，刑事訴訟法論，五南，2001 年 2 月。
- 謝名冠，網路行爲規範之研究，臺灣臺北地方法院檢察署，2001 年。

(二) 英文書籍：

- Balkin, Jack M. et al., Cybercrime: Digital Cops in a Networked Environment, New York University Press, 2007.
- Brenner, Susan W., Cybercrime : Criminal Threats from Cyberspace. Santa Barbara, CA: Praeger, 2010.
- Dunham, Ken and Melnick, Jim, Malicious Bots, An Inside Look into the Cyber-Criminal Underground of the Internet, Taylor & Francis Group, 2009.

(三) 中文期刊：

- 王兆鵬，重新定義高科技時代下的搜索，月旦法學雜誌，93 期，2003 年 2 月。
- 何賴傑，成大 MP3 搜索事件之法律檢討，台灣本土法學雜誌，23 期，2001 年 6 月。

- 何賴傑，逮捕、搜索與扣押，台灣本土法學雜誌，25 期，2001 年 8 月。
- 何賴傑，錄音、錄影、電磁紀錄等之調查(刑事訴訟法第一六五條之一第二項)，全國律師，8 卷 9 期，2004 年 9 月。
- 李相臣，網路科技犯罪專責隊-刑事局偵九隊，透視犯罪問題，4 期，2004 年 9 月。
- 李榮耕，論偵查機關對通信紀錄的調取，政大法學評論，115 期，2010 年 6 月。
- 李震山，來者猶可追，正視個人資料保護問題—司法院大法官釋字第六０三號解釋評析，台灣本土法學雜誌，76 期，2005 年 11 月。
- 李震山，挪動通訊保障與通訊監察天平上的法碼—釋字第六三一號解釋評析，台灣本土法學雜誌，98 期，2007 年 9 月。
- 法思齊，美國法上數位證據之取得與保存，東吳法律學報 ，22 卷 3 期，2011 年 1 月。
- 陳起行，資訊隱私權法理探討—以美國法爲中心，政大法學評論，64 期，2000 年 12 月。
- 黃敬博、莊明霓，數位鑑識之資料回復技術探討，資訊安全通訊，17 卷 2 期，2011 年 4 月。
- 楊竹生，論美國憲法第四修正案所述搜索與扣押，中原財經法學，第 1 期，1995 年 6 月。
- 楊雲驊，證據保全的規定與實務—以偵查階段爲中心，月旦法學雜誌，114 期，2004 年 11 月。
- 廖元豪，多少罪惡假「國家安全」之名而行？—簡介美國反恐措施對人權之侵蝕，月旦法學雜誌，131 期，2006 年 4 月。
- 劉靜怡，不算進步的立法：「個人資料保護法」初步評析，月旦法學雜誌，183 期，2010 年 8 月。
- 蔡美智，「通訊保障及監察法」關於網路監聽的相關爭議，資訊法務透析，1999 年 12 月。
- 蔡美智，美國重要之網路犯罪防制相關單位組織簡介，資訊法務透析，2000 年 3 月。
- 蔡榮耕，I Am Listening to You（上）－釋字第六三一號解釋、令狀原則及修正後通訊保障及監察法，台灣本土法學雜誌，104 期，2008 年 3 月。
- 蔡榮耕，Yes, I do! —同意搜索與第三人同意搜索，月旦法學雜誌，157 期，2008

年 6 月。

(四) 英文期刊：

- Hill, D. Garrison "Gary", United States v. Jones and the Search for Fourth Amendment Coherence, 23 S. Carolina Lawyer 28, 31 (2012).
- Kerr, Orin S., An Equilibrium-Adjustment Theory of the Fourth Amendment, 125 Harv. L. Rev. 476 (2011).
- Kerr, Orin S., Are We Overprotecting Code? Thoughts on First-Generation Internet Law, 57 Wash & Lee L. Rev. 1287 (2000).
- Kerr, Orin S., Digital Evidence and the New Criminal Procedure, 105 Colum. L. Rev. 279 (2005).
- Kerr, Orin S., Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531 (2005).
- Millcarek, Lauren, Eighteenth Century Law, Twenty-First Century Problems: Jones, GPS Tracking, and the Future of Privacy, 64 Fla. L. Rev. 1045, 1109 (2012).
- Volokh, Eugene, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You, 52 Stan. L. Rev. 1049 (2000).
- Warren, Samuel D. & Brandeis, Louis D., The Right to Privacy, 4 Harv. L. Rev. 193 (1980).

(五) 學位論文：

- 林孟瑤，網際網路色情犯罪與刑事偵查之研究，中國文化大學法律學研究所碩士論文，2006 年。
- 林建中，隱私權概念之再思考—關於概念範圍、定義及權利形成方法，國立台灣大學法律研究所碩士論文，1999 年。
- 陳信郎，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，2004 年。
- 黃佩倫，入侵電腦行爲之研究，國立交通大學科技法律研究所碩士論文，2004 年。
- 葉昭熙，以開放始碼爲基礎的蜜罐系統設計與實現，國立高雄師範大學資訊教育研究所碩士論文，2007 年。

- 謝昆峰，網際網路與刑事偵查，國立台灣大學法律學研究所碩士論文，2002 年。
- 蘇三榮，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，2008 年。

(六) 網路參考文獻：

- 李美雯，北區 A-SOC 建置與管理，available at http://tais2011.ntu.edu.tw/docs/2-7-3.pdf (last visited June 19, 2012)
- Best Practices for Seizing Electronic Evidence, available at http://www.forwardedge2.com/pdf/bestPractices.pdf (last visited June 13, 2012)
- SOC 參考指引，九十五年度國家資通安全技術服務與防護管理計畫，available at http://www.rdec.gov.tw/public/Data/74217484571.pdf (last visited June 19, 2012)
- USDOJ, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (2009 年版), available at http://www.cybercrime.gov/ssmanual/index.html (last visited Aug. 28, 2011)
- Wuslich, Julie P., An Overview of Electronic Surveillance in the United States; Law, Policy, and Procedure, available at http://www.unafei.or.jp/english/pdf/PDF_rms/no59/ch26.pdf (last visited May 1, 2012)