國立交通大學

管理學院在職專班科技法律組

碩士論文

網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究

A Research on Cybercrime Investigation and the legal system concerning the Assistance of Internet Service Provider for Investigation in ROC

研 究 生：許慈健

指導教授：王明禮　博士

中 華 民 國 九 十 四 年 十 月

網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究

A Research on Cybercrime Investigation and the legal system concerning the Assistance of Internet Service Provider for Investigation in ROC

研 究 生：許慈健　　Student：Tzu-Chien Hsu

指導教授：王明禮　博士　　Advisor：Ming-Li Wang

國 立 交 通 大 學

管理學院在職專班科技法律組

碩 士 論 文

A Thesis

Submitted to Institute of Technology Law

National Chiao Tung University

in Partial Fulfillment of the Requirements

for the Degree of Master of

Technology Law

December 2004

Hsinchu, Taiwan, Republic of China

中華民國九十四年十月

網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究

研究生：許慈健　　指導教授：王明禮　博士

國立交通大學管理學院在職專班科技法律組碩士班

摘　　要

網路犯罪是「網路線上」的犯罪行為，犯罪行為發生時欠缺目擊證人可供查證，亦沒有具體的犯罪發生地與行兇兇器等線索可以蒐集，故不易清查過濾犯罪行為人身分；同時，網路犯罪行為所遺留之證據，均為不可目視的「電磁紀錄」，原本即不易蒐集，再加上近期通訊加密技術與點對點通訊的發展，更使得偵查人員面臨證據蒐集困難的窘境。相較於傳統網路犯罪偵查，二者間不僅偵查思惟截然不同，網路犯罪偵查流程顯然更具高複雜度、專業性與技術性。並且，由於網路行為具有「凡走過必留痕跡」的特性，網路犯罪偵查過程中，包括清查過濾階段之使用者資料或通信紀錄；證據調查階段之實施通訊監察等偵查作為，均須仰賴網路服務提供者提供偵查協助才能繼續後續偵查作為，甚至可以說，網路犯罪偵破與否的關鍵依存於網路服務提供者能否完全配合。

就我國目前法令而言，關於網路服務提供者協助偵查之規定，主要見諸於電信法、通訊保障及監察法與第二類電信管理規則等法規，惟前揭法規之規範對象為電信業者，能否一體適用到網路服務提供者，似有疑慮；另外，第二類電信事業管理規則加諸電信業者儲存及提供使用者資料、儲存及提供網路通信紀錄及建置網路通訊監察設備配合偵查人員實施通訊監察等責任，乃以法規命令規範限制或侵害使用者享有憲法保障之基本權利，更有違反憲法法律保留原則之疑慮，以致網路服務提供者為避免身陷訴訟之囹圄，不願也不能完全配合協助偵查。

因此，本文有鑑於網路服務提供者對於網路犯罪偵查之重要性及解決目前法令網路服務提供者無法完全配合協助偵查之問題，並參酌歐美各國均有相關協助偵查法制之立法例，認為確有制定獨立的網路服務提供者協助偵查法制之需要，以強化網路服務提供者協助偵查之責任，適度擴大偵查人員的偵查權力與偵查能力，解決日益泛濫的網路犯罪問題，還給所有網路使用者一個安全、便捷的網路空間。

關鍵詞：網路犯罪
網路犯罪偵查
網路服務提供者
通信紀錄

A Research on Cybercrime Investigation and the legal system concerning the Assistance of Internet Service Provider for Investigation in ROC

Student：Tzu-Chien Hsu Advisors：Dr. Ming-Li Wang

Institute of Technology Law
National Chiao Tung University

ABSTRACT

The cybercrime is the criminal conduct taking place on the network line. Compared with the traditional crime, cybercrime possesses no eyewitness, concrete criminal occurrence ground and criminal machine as cybercrime happens. Furthermore, due to the cybercrime evidence is the electronic record can't be seen by one's eyes and the rapid development of the communication encryption and peer to peer communication, the investigator even can not collect the useful evidence. Therefore, the process of cybercrime investigation is more difficult to filter the suspect, collect evidence and carry out than traditional crime investigation. In other words, the concept of investigation is entirely different between traditional crime and cybercrime investigation; furthermore, the process of cybercrime investigation is obviously more complicated, professional and technical.

In point of current cybercrime investigation, at first, the investigator has to acquire the user data or the communication record; then may wiretap the suspect's communication or identify the electronic evidence. All above investigative actions in the investigative stage must rely on the assistance of internet service provider; otherwise the investigation can not be continued. Even we can say that whether cybercrime investigation succeeds or not depends on whether internet service provider can offer complete investigative assistance.

Though the current regulation concerning the assistance of the internet service provider for cybercrime investigation in ROC includes Telecommunications Act, the Communication Protection and Interception Act and Administrative Regulations on Type II Telecommunications Business, however, the object of these regulations is confined to telecommunications enterprise. Besides, Administrative Regulations on Type II Telecommunications Business is just an administrative order, it can not request telecommunications enterprise to store and provide the user data and communication record for cybercrime investigation without law authorization; otherwise it will violate the constitution concerning protecting the basic human rights. To sum up, in order not to violate the constitution and avoid the litigation, the internet service provider won't and also can't provide the help to investigate completely.

Therefore, in view of the importance of the assistance of the internet service provider for cybercrime investigation and the problem that internet service provider can't provide complete investigative assistance according to current regulation and consulting along with some related regulation in Euro-American countries, I insist that it is urgent to establish an independent law concerning the assistance of internet service provider for cybercrime investigation. I expect we can increase the liability of internet service provider and expand the staff's investigatory power appropriately by way of this law in order to resolve the increasing cybercrime problem and restore a security and convenient internet space to all internet users.

Keywords: Cybercrime, Cybercrime Investigation,Internet Service Provider, Communication Record.

誌　　謝

本文得以順利完成，首要感謝指導教授王明禮老師不斷在論文架構、實質內容上給予指導與建議，使本文的內容得以更加充實。感謝劉尚志所長、熊愛卿老師、劉宏恩老師、倪貴榮老師多年的教導。另外，林三元兄及趙雯蕙、杜佳蓉等學弟妹們在論文討論時提出的寶貴意見，屢屢激發撰寫靈感，在此一併表達感謝之意。

感謝王敏銓老師、蔡宜芳老師撥冗出任口試委員，提出之寶貴意見，使我受益良多。其中，王敏銓老師指出第五章外國立法例參考部分內容有錯誤之處；蔡宜芳老師提出論文題目應限縮於網路偵查、部分論文架構應調整、緒論部分內容應修正及多處論文本文謬誤之處等寶貴意見，在此予以感謝。除了蔡老師提出應將第五章第三節「合憲性探討」乙節移至第三章之寶貴意見，因考量遷動篇幅過多而未予更動外，已參酌兩位老師之意見加以修正。

撰寫論文期間，感謝父母親不斷地教誨與勉勵；大學同學關維忠、廖大鵬不斷地激勵；法務部調查局新竹縣調查站各長官與同事之鼓勵及同期同學鄧思源、邱舜禾、周士楨提供網路犯罪偵查實務專業知識之協助。最後，感謝內人雪倩的真情相待及全力支持，一肩扛起照顧稚子庭瑄、庭嘉之責任，使本人得以心無旁騖地撰寫論文，實爲本人努力的泉源與精神之支柱。

許慈健

94 年 12 月 13 日于新竹

目錄

頁次

1 緒論

1.1 研究動機

「無遠拂界，天涯若比鄰」是今日網路化社會的最佳寫照。網際網路（Internet）的誕生與迅速發展，爲當今的人類帶來更爲快捷的聯繫方式，在網網綿密相連下，大大縮短彼此的空間距離，全球化「網路社會」（Cyber-society）於焉而生。人們透過「上網」這一個簡單的動作，在網路的虛擬社會中過著「網路生活」（Cyberlife），與真實社會生活並無太大差異。同時爲因應一般大眾對網路強烈地依賴需求需求，ADSL(Asymmetric Digital Subscriber Line，稱之「非對稱數位用戶線路」)[1]、Cable Modem（纜線數據機）[2]、T1 專線[3]等寬頻網路技術急速發展，網路使用者只要憑藉著電腦前，便可輕易地藉由全球資訊網（World Wide Web，簡稱 WWW）快速搜尋全球各種資訊；亦可透過電子郵件（e-mail）、即時通訊軟體（Instant Message，簡稱 IM）[4]、網路電話（Internet Phone 或 Voice over Internet Protocol 簡稱 VoIP）[5]等方式與全世界的網友溝通；甚至，透過網路

---

[1] 參閱吳俊瑩等五人著，電腦、網路、通訊知識百科，二〇〇一年七月十四日初版，第一八〇頁。所謂 ADSL 是利用現有的電話線路，透過其專用數據機之壓縮技術，讓使用者連上網際網路，進行數位資訊傳輸。

[2] 參閱吳俊瑩等五人著，同前註書，第一七八頁。所謂 Cable Modem 是指利用有線電視所架設的纜線與光纖而構成的「混合光纖同軸電纜」（Hybrid Fiber Coaxial,簡稱 HFC），其原理與傳統數據機差不多，都是先將電腦的資訊轉爲類比資料，透過纜線或電話線傳輸，接收端再將類比資料轉爲數位資料讀取。不過，Cable Modem 傳輸速度比電話線快了一百倍左右。

[3] 參閱吳俊瑩等五人著，同前註書，第一八二頁。所謂 T1 專線是指網路服務提供者直接提供專屬的線路，使用者無須進行撥接，即可一直在網際網路上。

[4] 即時通訊軟體原本的功用是提供用戶透過網路作「點對點」的文字交流（即聊天）。不過隨著即時通訊軟體功能和應用方式的改變和不斷完善，漸漸發展成一個綜合型的通訊平臺。並提供包括網路視訊、語音聊天、遊樂場、線上交誼等多樣化之內容。詳細內容請參閱奇摩網站，網址：http://tw.messenger.yahoo.com/。最後瀏覽日期：二〇〇五年七月二十三日。

[5] 參閱王郁琦著，「資訊、電信與法律」，二〇〇四年五月初版，第二五五頁。所謂「網路電話」係指透過網際網路進行分封交換方式，將資料或語音訊號分割成許多封包，從發話端傳送至受信端。目前市面上網路電話服務約有電腦對電腦（PC to PC ）、電腦對電話（PC to Phone）、電話對電腦（Phone to PC）或電話對電話（Phone to Phone）等四種類型。

進行網路購物、網路銀行交易、網路下單等等電子商務（Electronic Commerce）。「網路生活」在二十一世紀的今日，逐漸發展成一個獨立的虛擬空間（Cyberspace），依託於真實的物理空間而存在，甚至有逐漸取代原有真實社會生活的趨勢。

伴隨著「網路生活」益加發展與普及的同時，對於網路管理的相關措施卻寥若晨星，並且由於網路具有強大的資訊流通功能，網路使用者在享有極度自由下，誤以爲網路是沒有法律管理的空間，諸如網路賭博、網路色情、誹謗、詐欺、恐嚇等等脫序的行爲便在虛擬的網路空間中如雨後春筍般顯現，原現實社會之傳統犯罪模式被同步植入虛擬網路世界中；另外與傳統犯罪迥異之新型態犯罪，即必須利用網路方得實現之犯罪行爲，例如網路侵入、散佈病毒等，亦隨之而生，嚴重影響大眾使用網路的便利性，甚至造成網路使用者權益的損害；因此對於網路使用行爲的規範與網路犯罪的防治成爲今日網路生活中不可不重視的焦點議題。

對於這些利用網路之特性做爲犯罪手段或犯罪工具之網路濫用脫序行爲，學者統稱爲「網路犯罪」。面對新興網路犯罪類型，偵查人員起初仍以偵查傳統犯罪案件之思維因應，惟由於網路犯罪本身具有隱匿性、無國界性等特性，偵查過程中往往因「斷點」（所謂斷點係指線索中斷）過多而無法循線追查，以致網路犯罪的破案率不高。另一方面，由於網路犯罪行爲人因遭查獲之機率較低，遂心存僥倖地不斷透過網路進行犯罪行爲，致使網路犯罪如洪流般泛濫。基於人權的保護，世界各國不得不正視網路犯罪猖獗問題，開始探討網路空間的自由開放程度網路行爲管理等等議題，並積極研擬方案，進行相關網路法令的修訂、設置網路偵查專責機構及加強訓練網路偵查人才等等實質作爲。

我國爲解決網路犯罪泛濫問題，曾透過修法方式於民國八十六年及九十一年

兩次進行刑法之修訂；九十二年更增訂電腦犯罪專章[6]，使電腦（網路）犯罪有處置法規之依據，惟因防治網路犯罪偵查與執行成效不張，根本無法抵擋網路犯罪泛濫的洪流。細究網路犯罪泛濫的原因，不僅在於缺乏相關法令規範，網路犯罪的偵破率太低以致無法對犯罪行爲人發揮刑法規範威嚇的作用，亦是另一個造成高網路犯罪率的主要原因。有鑑於此，本研究主張，應積極研究網路規範與管理相關問題，並有效提高網路犯罪的偵破率，使網路使用者不能也不敢在網路世界上進行犯罪行爲，如此才能有效減低網路犯罪事件，並合法保障所有網路使用者之精神與財產之安全。

有句俗語說「凡走過必留痕跡」，這正是網路活動的最佳代名詞，網路上的一切活動，無論是正在進行中或是已完成的網路行爲，在網路服務提供者之主機伺服器內均有紀錄而得以追蹤或蒐集。就目前網路犯罪偵查實務而言，提高偵破率實屬不可能的任務，分析其原因，網路犯罪偵查除了面對網路犯罪本身具有不易追查的特性外、欠缺專責網路犯罪偵查機構與偵查人員能力均有所不足等等原因外，網路服務提供者無法完全配合協助偵查，更是網路犯罪偵破率低迷的主因。按網路犯罪案件一經受理後，偵查的第一個步驟，便是向網路服務提供者調閱客戶登錄資料、通信紀錄等相關資料，以比對過濾犯罪行爲人之身份，然而在實務上卻常發生因取得之客戶登錄資料及通信紀錄不完整或不正確，致無法過濾出行爲人身份。縱使過濾出可疑的行爲人身份，進入蒐集犯罪證據階段之後續蒐證作爲階段，更須仰賴網路服務提供者之協助，其中對於已完成犯罪行爲之案件，偵查人員必須透過網路服務提供者取得通信紀錄或通信內容等違法證據；實施中之案件亦必須仰賴網路服務提供者協助配合實施通訊監察、搜索等強製作爲

---

[6] 刑法於九十二年六月二十五日增訂第三十六章「妨害電腦使用罪」，針對行爲人無故入侵他人之電腦或其相關設備；無故取得、刪除、變更或幹擾他人電腦或其相關設備之電磁紀錄等行爲

方式，以掌握網路犯罪之不法事證。顯見，網路服務提供者之配合協助偵查，乃爲網路犯罪案件能否偵破的關鍵。

不過，在探討防治網路犯罪及建立協助偵查法制之前，我們必須先考量下列幾個問題：

I　網路服務提供者的身份可能爲公家機關或私人機構；亦可能爲營利事業或個人，依現行法令是否均有配合與協助執法單位之義務？

II　網路服務提供者有無經濟能力配合？

III　網路服務提供者與其提供服務的相對人客戶間，視其收費與否各有不同的法律關係，依現行法令未經同意逕自提供執法單位相關資訊及配合網路偵查作爲，會否侵害到客戶的隱私權？

IV　網路服務提供者配合偵查網路犯罪的效益，與可能侵害網路使用人享有隱私權的基本人權之損害間，應如何取得平衡？

綜覽國內關於網路犯罪相關論述，雖然多數學者之見解，認爲網路服務提供者應配合協助網路偵查，但主要的內容多著重於理論面的探討，實際執行面則較少有深入的探討。基於防治網路犯罪泛濫工作之重要性，本研究考量網路服務提供者之協助確能有效協助網路犯罪偵查，卻囿於目前相關法制並不夠完整，致實際網路犯罪偵查執行面陷入困境而無法有效防治網路犯罪；另外，考量在尋求防治網路犯罪的目標，仍應兼顧維護網路使用者的隱私權及減輕業者額外經營負擔等問題下，認爲有必要建立完整的網路服務提供者協助偵查法制。冀望透過本研究，爲目前關於網路服務提供者協助偵查法制投注一份心力，建立更完善的網路

明文處罰規定。

偵查制度，達到使網路犯罪發生率降低，讓所有網民得以自由在網路上暢快奔跑的終極目標。

1.2 研究目的

1.2.1 創造安全與自由的網路空間

網際網路空間的本質是「自由」，即任何網民得以在網路空間內不受管制的過著網路生活，但是網民享有自由的前提乃建立在「安全」的網路空間上，如何建構一個安全且自由的網路空間，成爲現代化生活中一個重要且必要的條件。

網路發展的初期，許多網民認爲任何網路空間都是不可管制的，政府不應介入或干涉。但是隨著網路的發達，網路上脫序的行爲日漸泛濫，網路上的安全性愈來愈低，網民時時刻刻要防範電腦駭客的入侵、注意電腦病毒的侵入及不斷地處理垃圾郵件，甚至還要擔心發送的電子郵件會不會被截取。爲瞭解決網路安全性的問題，各種加密技術、掃毒軟體等不斷精進，但「人外有人、天外有天」，網路犯罪行爲人總是能輕易地破解，繼續在網路空間肆意爲所欲爲。另一方面，網民們倡導「自律」，期能藉由網路倫理觀念的建立維護網路安全，但是成效也有限。

事實上「法律」也是規範網路空間的一種方法[7]，透過政府公權力的介入，加上法律具有事後制裁的威嚇性之優點，對於防範網路犯罪的發生確能發揮較大的功效，雖然這種方式會影響部分網路使用者使用網路的便利性；但是爲維護大多數使用者之權益，以「法律」規範網路使用規則，似乎是較爲可行且有效的網路

[7] 參閱勞倫斯．雷席格（Lawrence Lessig）著，網路自由與法律（CODE and Other Laws of Cyberspace），劉靜怡譯，二〇〇二年七月初版，第二二七頁。在本書中，Lawrence Lessig 認爲規範網際網路空間的力量，包括法律、市場、規範與架構四項限制。

管理方式。然而，單純制定法律仍不足以達到防範網路犯罪的目的，更重要的是取決於執行面能否發揮嚇阻成效。本研究即是基於爲護網路使用者之安全與權益，期望透過對「網路犯罪協助偵查法制」的探討，提昇網路犯罪偵查之能力，強化相關網路法規的威嚇效果，有效降低網路犯罪發生率，進而建構安全與自由的網路空間。

1.2.2 找出防治網路犯罪與侵害隱私權間的平衡

我國憲法第十二條規定「人民有秘密通訊之自由」、第二十二條規定「凡人民之其他自由及權利，不妨害社會秩序公共利益者均受憲法之保障」，均爲我國保障基本人權之規定。世界各民主國家亦莫不以保障基本人權爲第一要務，即使是「網路」上的通訊行爲，亦享有基本人權之保障，偵查機關不得以「防治網路犯罪」爲由，過度擴張偵查權力而恣意侵害使用人的權益。

然而，面對網路犯罪的泛濫，就偵查機關而言，能得到網路服務提供者完全的配合，猶如擁有最鋒利的武器一般，不論是從技術上提供偵查機關截取網路中傳輸的封包或進行監看以蒐集犯罪事證，或是提供所擁有使用個人基本資料及使用通信紀錄，均有助網路犯罪偵查的成功。純粹從偵查犯罪的角度來看，網路服務提供者配合偵查的事項愈多愈好，甚至能讓偵查人員從幕後完全掌控最好。

面對日益氾濫之網路犯罪，如何在維護網路使用者的基本人權與爲有效防治網路犯罪所爲之網路偵查作爲之間尋求平衡點，是個重要且艱巨的難題，本研究試圖透過分析討論找出這個平衡點，並提供有效的解決方案，促使網路犯罪偵查作爲能更有明確依據及有效率，達到防治網路犯罪及維護網路使用者合法權益之目的。

1.2.3 明確網路服務提供者協助偵查之責任

關於要求網路服務提供者協助或配合網路偵查作爲部分，就我國目前法制而言，並沒有單獨針對此一部分進行立法，係散見於各相關法規中。其中，交通部電信總局所制定的第二類電信事業管理規則第二十七條，明定電信事業負有儲存及提供使用者申登人資料、通信紀錄之義務；另外，通訊保障及監察法第十四條則明定電信事業有配合偵查機關實施通訊監察之義務。惟「第二類電信事業管理規則」性質乃法規命令，並非法律位階，電信事業若依該法規命令提供使用者資料及通信紀錄等享有隱私權之資料，可能會有違反憲法或法律之疑義，造成證據取得程式有瑕疵，進而影響法院審判之結果；況且，「第二類電信事業管理規則」及「通訊保障及監察法第十四條」之適用對象均侷限於電信事業，對於非電信事業的公司、個人網站、BBS 版主等網路服務提供者，並不在適用範圍內，造成網路犯罪偵查上的漏洞，使網路犯罪偵查效率大打折扣。

除此之外，在偵查網路犯罪過程中，網路服務提供者能提供之協助事項，不僅是提供使用者申登人資料、通信紀錄與配合偵查機關實施通訊監察而已，在主動過濾、主動舉發、儲存證據、提供證據、協助數位鑑識等方面，亦是網路偵查過程中最強而有力的助手。然而，依現行法令，這些協助事項是否均爲網路服務提供者所應負之責任範圍，仍有疑義。綜上顯見，爲求達到防治網路犯罪之目的，我國目前關於網路服務提供者協助偵查之相關法令仍嫌不足；因此，本研究特針對網路服務提供者協助偵查責任之責任範圍及必要性加以分析研究，以期能提高政府單位對於網路犯罪偵查的重視，並提供偵查人員在進行網路犯罪偵查時，能有更確切的執行依據，提高網路犯罪偵破率，維護網路使用之安全與自由。

1.3 研究方法與範圍

本文研究方法係採取將偵查實務中已臻成熟的傳統犯罪偵查流程，與新興網

路犯罪偵查流程相互比較，藉以說明網路犯罪偵查的困難度與凸顯網路服務提供者在網路犯罪偵查過程中之重要性，進而探討網路服務提供者應如何配合協助偵查、協助事項及目前相關法令有無應興應革等等議題之研究方法，冀能透過建立完善的網路偵查機制方式，有效提昇網路犯罪案件偵破率，達到防治網路犯罪的目的。

而本文研究主題係探討網路犯罪偵查及網路服務提供者協助偵查法制，其研究範圍僅限於在網路犯罪偵查過程中之「偵查階段」，亦即從偵查人員受理案件到調查完畢移送法院審理爲止之階段。因此，雖然從防治網路犯罪的角度而言，網路服務提供者得以提供協助的事項，涵蓋「偵查前」的預防犯罪階段與「偵查後」法院審判階段，例如前階段透過網路服務提供者主動過濾網路內容及主動刪除或阻斷資訊等作爲，可以有效防堵不法網路資訊之流通與傳遞，達到事先預防犯罪的目的；後階段網路服務提供者得以協助作證及協助數位鑑識等作爲，使網路犯罪行爲人得以定罪，達到事後威嚇的效果，惟因均非屬「偵查中」的協助偵查作爲，故非本文之研究範圍。

1.4 論文架構

本研究第一章說明研究動機、研究目的及研究方法與範圍；第二章探討網路犯罪的意義、特性、犯罪手法及泛濫的程度；第三章探討傳統犯罪與網路犯罪之偵查流程，並藉由傳統犯罪偵查與網路犯罪偵查在案件偵查各個階段的偵查之差異性，凸顯網路犯罪偵查的困難與網路服務提供者在網路犯罪偵查角色之重要性；第四章探討我國關於網路服務提供者協助偵查法制的現行規定，嘗試找出我國目前的法制缺失；第五章參考美國、英國及歐盟關於網路服務提供者協助偵查相關法制之規定，嘗試提出網路服務提供者協助偵查法制之立法建議。期能透過網路服務提供者協助偵查法之建置，強化網路服務提供者協助偵查之責任，適度

擴大偵查人員的偵查權力與偵查能力，以解決日益泛濫的網路犯罪問題，還給所有網路使用者一個安全、便捷的網路空間。


E
S
A
1896

2 網路犯罪概論

2.1 網路犯罪之意義

「網路犯罪」一詞並非單一之法定概念或法定犯罪類型，而是犯罪學意義上對一種新型態犯罪之統稱。由於「網路犯罪」相關的研究尚未成熟，學者間對於「網路犯罪」的意義並無統一的定義。尤其「網路犯罪」與「電腦犯罪」二者之概念是否相同，即有迥然不同的討論。其中一派學者認爲「網路犯罪」的定義應從「電腦犯罪」著手，亦即將以往對電腦犯罪的定義「所有侵犯刑法所保障之法益的行爲，且該行爲具有電腦的特性，於事實認定以及偵查上必須使用專業知識之犯罪」中之「電腦」一詞改爲「網路」即可，換言之，「網路犯罪」與「電腦犯罪」是相同的概念[8]。但另一派學者則認爲，就目前網路的發展與利用而言，網際網路之特性與單純之電腦利用行爲迥異，顯見「網路犯罪」與「電腦犯罪」二者之概念迥異，「網路犯罪」應定義爲「利用網際網路之特性作爲犯罪手段或犯罪工具之網路濫用行爲」[9]；另有學者認爲，雖然「網路犯罪」係利用電腦系統之操作進而連結至網路，始能在網路上進行犯罪之行爲，所以目前多數學者認爲「網路犯罪」係於「電腦犯罪」中藉由網路之管道而達成其犯罪目的之謂，係從「電腦犯罪」中逐漸衍生出來的一種犯罪型態，而將「網路犯罪」錯認是「電腦犯罪」的下位概念或將之與「電腦犯罪」混爲一談，惟事實上網路犯罪固屬電腦犯罪的延伸，卻獨具有一種利用網路獨有的特性，而爲犯罪手段或犯罪工具之網路濫用行爲，「網路犯罪」應爲電腦系統與通訊網路相結合之犯罪行爲，其較偏

---

[8] 參閱王銘勇著，網路犯罪相關問題之研究，臺灣新竹地方法院九十年度研究發展項目研究報告，二〇〇一年十一月，第二〇至二一頁。

[9] 參閱馮震宇著，網路法基本問題研究（一），二〇〇〇年九月，第三三六至三三七頁。

重於網路科技的應用，而具有網路性質的犯罪，其與「電腦犯罪」只偏重於電腦或相關設備之使用及破壞之犯罪行為是有區別的[10]。另依國際經濟合作開發理事會（Organization for Economic Co-operation and Development 簡稱 OECD）之定義，「電腦犯罪」係指「利用自動的資料處理系統或資訊通訊系統，以實施違反法律或為論理所非難，所不許之所有犯罪行為」；而「網路犯罪」則主要是「透過電腦所連接的虛擬網路空間區隔，以對某種客體進行資料的處理與輸入、處理與輸出的不正操作行為，或是為有關資料處理的資訊蒐集刺探、資料處理的電腦破壞、對電腦系統的時間竊盜、或是對資料系統侵入等犯罪行為方式」，從以上定義分析，「網路犯罪」之行為模式與「電腦犯罪」二者範圍及犯罪手法亦不相同[11]。

綜上分析，本研究以為「網路犯罪」的發生雖必須藉由電腦的連結，但「網路犯罪」防治的重點在於防堵行為人於網路空間裡，以「網路」為犯罪工具或攻擊對象的嚴重危害社會的行為，強調是維護「網路」空間的自由與安全；與單一利用電腦進行犯罪之行為顯並不相同，因此有獨立其定義之必要，並且為求將任何發生於網路空間的犯罪均納入規範討論，本研究擬採取最廣義的定義，認為網路犯罪係指「行為人以網路為標的、場所或工具，在網路空間裡進行任何致生嚴重危害社會之刑事不法行為」。

2.2 網路犯罪之類型

犯罪行為之類型化，係針對已知之犯罪行為，運用歸納或演繹方式，就相同或相似的犯罪形態歸納為同一類型，藉此瞭解個別犯罪類型之特性或特徵，除了

---

[10]參閱沈榮華著，網路犯罪相關問題之研究，國防管理學院法律研究所碩士論文，九十一學年度，第二十八頁。

[11]參閱王銘勇著，同前註 8 書，第二一頁。

有助於學術理論的研究，更有助於實務偵查作爲的精進，甚至可透過針對各該類型的犯罪行爲分析，進而採取適合的立法政策與防制措施。隨著網路蓬勃的應用及迅速發展，網路上的犯罪行爲態樣眾多，甚至發展出不同於現實社會傳統犯罪的類型(即專屬於網路的犯罪類型)，因此如何完善地將網路犯罪行爲予以分類確是一大困難。

有學者[12]將網路犯罪類型區分爲：一、利用網路服務的傳統犯罪類型的網路犯罪：如網路色情、利用網路發表不當言論、網路詐欺、利用網路煽惑他人犯罪及網路賭博等；二、入侵篡改、破壞資料類型：如利用網路無權侵入他人電腦系統、利用網路入侵而篡改他人資料之行爲、利用網路散佈病毒；三、其他侵害類型：如非法重製電腦程式或檔案、網功能變數名稱稱與商標權之侵害；另有學者[13]則針對「網路」在犯罪中扮演的不同角色，區分爲：一、以網路爲犯罪客體：如入侵型犯罪、攻擊性犯罪、攔截型犯罪及病毒之散佈；二、以網路爲犯罪場所：如網路色情、網路賭博、網路詐欺侵害智慧財產權等；三、以網路爲犯罪工具：如網路恐嚇、網路洗錢、網路洩密等。前述二種分類方式，幾乎已經包含當前所有網路犯罪之類型，而網路犯罪類型化既在探討其行爲模式及特徵，後者以犯罪之主體、客體與工具的區分之分類似更能適切的達到類型化的目的，本研究以下謹參酌各家學者之觀點，就網路犯罪類型中可能包括之類型，依前述分類進行分析，並輔以案例做說明。

2.2.1 以網路爲犯罪客體之犯罪類型

以網路爲犯罪客體之犯罪，係指行爲人利用網路的特性，將「網路」本身或

---

[12]參閱馮震宇著，同前註 9 書，第三三九至三五〇頁。

[13]參閱陳誌銘著，網路犯罪偵查之研究，臺灣臺南地方法院檢察署八十八年度研究發展項目第研究報告，第三六至三九頁。

連結在網路上的電腦系統，做爲實施犯罪對象（標的）之犯罪，是網路犯罪中最典型的一種。其犯罪行爲形態主要可分爲入侵型犯罪、攻擊性犯罪、攔截型犯罪及病毒之散佈等四種類型，其特徵是「行爲的目的在於破壞網路本身及電腦系統」，而此類型犯罪之行爲人通常稱之爲「電腦駭客」（hacker）[14]以下就此四種類型進行說明：

I　入侵型犯罪

i　定義

「入侵型犯罪」之犯罪行爲模式，係行爲人透過網路連結的特性，侵入他人的電腦系統後，再從事各種不法活動，包括單純窺視他人檔案的內容、更改或刪除電腦檔案資料等。

ii　案例說明

九十二年十一月臺北市刑大電腦犯罪專責組，於台中市偵破林○○、曾○○等人不法案，其犯罪手法即是利用網路銀行設置「ＭＭＡ金融交易網」網站，提供存款客戶得以透過身分證字號及語音密碼進入網站，以便查詢帳戶餘額、進行轉帳、證券或基金交易等服務之機會，利用網路「身分證產生器」或汽車公司客戶刷卡資料等方式，取得銀行客戶的身份證、帳號及密碼等資料後，入侵網路銀行系統，將銀行客戶帳戶內之存款，以網路轉帳方式到另一家銀行人頭戶內後，提領現金供自己花用[15]。

---

[14] 所謂電腦駭客，係指行爲人未經授權透過網路逕行進出他人之電腦系統。電腦駭客進出他人的電腦系統，不見得是基於特定犯罪的意圖，多數係爲了好奇或展現個人之能力。其種類可分爲駭客(hacker)、飛客（phreak）、鬼客（cracker）、惡客（abuse）等四種。參閱餘德正著，不法使用網際網路之刑事責任，東海大學法律研究所碩士論文，一九九九年六月，第二十七頁至二十八頁。

[15]參閱陳金章著，「網路銀行破功，客戶遭盜冒貸」，聯合報，社會 A8 版，二○○三年十一月二十七日。

II　攻擊性犯罪

i　定義

「攻擊性犯罪」之犯罪模式，係指行爲人透過網路作爲跳板直接攻擊網路系統，以破壞網路系統或使之陷於癱瘓。

ii　案例說明

微軟公司(Microsoft)、美國線上 (AOL)、雅虎（Yahoo!）及地聯公司(Earthlink)在加州和喬治亞州等地，於九十三年三月十日引用美國同年一月一日實施的「封鎖濫發郵件法」 (Can-Spam Act)，共同對濫發垃圾郵件者提起六件訴訟。濫發垃圾郵件者的犯罪手法即是以僞造回信地址或隱藏原始郵件來源方式，大量寄發垃圾郵件給不特定的用戶，進而癱瘓網路或電腦系統，使網路用戶必須花費大量的時間去刪除。根據反垃圾郵件軟體製造商 Brightmail 公司統計，九十二年三月網路上約有百分之四十五之郵件是垃圾郵件，但是到九十三年二月已增加至百分之六十二。此種犯罪形態儼然成爲數量最多的犯罪類型[16]。

III　攔截型犯罪

i　定義

「攔截型犯罪」之犯罪模式，係行爲人以截取在網路線上傳輸之網路資料方式，進而實施竊聽、阻截、僞變造或幹擾等行爲。

ii　案例

我國法務部調查局於九十三年八月十七日派員至我國駐韓代表處進行偵測，

[16]參閱廖玉玲編譯，「垃圾郵件泛濫，微軟反擊」，經濟日報，國際財經版，第十一版，二〇〇四年三月十二日。

經使用特殊電子儀器偵測館內的電腦及電話線路發現，有數條線路的波長出現異常現象，與正常線路波長頻率有很大差距，疑遭竊聽及盜截機密資料情事。其犯罪手法，係透過電腦傳輸線路，利用網路傳輸的特性，於電子郵件傳輸過程中攔截資料後下載，以取得外交機密[17]。

IV　散佈病毒型犯罪

i　定義

「散佈病毒型犯罪」之犯罪模式，係指行爲人設計電腦病毒[18]，透過網路傳輸至不特定人或特定人之電腦系統，藉由不斷的複製或感染，進行破壞、幹擾網路及電腦系統之行爲。

ii　案例

八十七年初就讀於大同工學院三年級之陳盈豪自行設計名爲「CIH」（或稱車諾比病毒）[19]的電腦病毒，並張貼於網路上供使用者下載，後經由網路的傳送散佈至全世界，結果造成全球約有六千萬台電腦受害。其犯罪手法係以利用網路連結的特性，將設計可能造成電腦系統受害的病毒透過網路傳遞出去，經用戶下載至本身的電腦或只要打開電子郵件，病毒便入侵至電腦系統內，導致電腦檔案滅失，甚至發生當機的結果[20]。

2.2.2 以網路爲犯罪場所之犯罪類型

---

[17]參閱聯合報報導，「駐韓外館機密遭截，電話電腦線路異常，調局偵測被動手腳應是間諜事件」，要聞 A1 版，二〇〇四年八月三十日。

[18]電腦病毒的種類約可區分爲開機磁區病毒、檔案型病毒、複製型病毒、千面人病毒及巨集病毒等等型態。參照資訊安全網，網址：http://www.infosec.gov.hk/chinese/general/virus/type.htm

[19]CIH 爲該陳姓學生英文名字的縮寫，而因該病毒發作日爲四月二十六日，與蘇聯發生之車諾比事件同一日，故國外稱此病毒爲「車諾比病毒」。轉引沈榮華著，同前註 10 論文，第五十頁。

[20]參閱林宜隆著，「網路犯罪之案例分析」，第二四六頁。轉引沈榮華著，同前註 10 論文，第五十頁。

以網路爲犯罪的場所之犯罪，係利用網路之空間特性以進行網路犯罪行爲。所謂網路之空間特性，係指網路連結的結果，形成一不特定多數人，均可同時於網路的虛擬空間裡實施現實社會的犯罪行爲。例如網路色情、網路賭博、網路誹謗、網路恐嚇、網路販售槍毒及網路煽惑犯罪等，以下就幾種主要的犯罪型態，舉例說明之。

I　網路色情

i　定義

「網路色情犯罪」爲我國目前網路犯罪案件影響層面最廣的，由於「色情」[21]本身是一種不確定的法律概念，並且會因國情、社會發展而爲不同的認定，因此實務上並沒有一個明確的定義及判斷標準。依目前實務的案件來看，其犯罪行爲包括在網路上張貼、傳送色情或猥褻性質的圖片或文字等資訊；在網路上媒介色情交易或進行網路援交[22]等形態。

ii　案例

甲、網路援交

臺北市警察局士林分局文林派出所於九十三年一月三日查獲具有碩士學歷的丁姓電腦工程師上網援交，依兒童及少年性交易防制條例罪嫌移送。其犯罪手法，係透過網路聊天室的功能，在網路上張貼期待援交訊息後，尋找援交妹從事性交易[23]。

---

[21]我國刑法規範內並沒有「色情」一字，係以「猥褻」稱之，而依大法官會議第四〇七號解釋文認爲「猥褻」係指一切在客觀上，足以刺激或滿足性慾，並引起普通一般人羞恥或厭惡感而侵害性的道德感情且有礙於社會風化，惟亦強調須依當時之社會一般觀念定之。顯見何謂「猥褻」，會因時、因地而有不同的認定。

[22]「網路援交」係指行爲人透過網路聊天室或電子佈告欄等張貼從事性交易之訊息，並經合意後實際進行性交易之行爲，是新型態的網路色情類型。

[23]參閱張宏業著，「碩士工程師找援交，遇霸王花」，聯合報，綜合新聞 B2 版，二○○四年一月

乙、經營色情網站

色情網站是網路色情類型中最多的形態[24]，根據金車基金會調查，有 5 成的青少年假日使用電腦達到 3 小時以上，其中值得注意的有 23%的青少年上過色情網站，其中男生的比例更遠高於女生，隨著年齡還有逐步攀升的趨勢[25]。刑事局偵查第九隊於九十三年五月二十五日同步查緝全台「戀童癖」網站及網路空間時，一舉查獲顏姓、黃姓六名站主，均爲高中男生，且都有同性戀傾向，被警方依違反兒童及少年性交易防制條例罪嫌函辦。其犯罪手法係行爲人先透過向網路公司申請網域空間成立網站之後，在網上刊登散佈未成年性交、猥褻影片及圖片，使不特定的人可以透過網路觀覽其猥褻之內容，以及提供網路空間供人刊登足以引誘、暗示或促使他人性交易訊息等[26]。

II 網路賭博

i 定義

「網路賭博」係指行爲人透過網路所提供的虛擬賭場，在網路線上進行賭博的犯罪行爲。

四日。

[24]依據警察機關近年查獲電腦相關案件統計資料分析，色情網站約佔全部案件的百分之三十四；其次爲網路販賣盜版光碟約佔百分之二十；網路詐欺及網路妨害名譽案件約佔百分之十；駭客入侵約佔百分之五。參閱李相巨著，網路科技犯罪專責隊－刑事警察局，透視犯罪問題第四期，九十三年九月，第六十四頁至六十九頁。

[25]參閱朱正庭著，「電腦是最佳玩伴，假日 5 成學子守著它，23%少年郎逛過色情網站」，星報，青春探索 C3 版，二〇〇四年五月二十八日。該調查數據係金車基金會針對全省及外島金門之國小高年級與國、高中二年級的學生所進行調查之結果。依該調查結果顯示百分之二十三之青少年上過色情網站（其中男生占了百分之三十七，比例遠比高於女生之百分之八），而且隨著年齡愈來愈高，比例也越高，到了國中爲百分之四十五；高中職則高達百分之八十上過色情網站，顯示現在網路內容不受限制，讓青少年也過早接觸到不當的內容。其他調查結果包括約百分之三十的青少年平日使用電腦超過三小時，假日使用超過三小時比例約百分之五十成；而超過八成的青少年家中都可以上網；至於青少年透過上網的目的，以舒解壓力之比例爲百分之三十一最高、其次依序爲獲得資訊爲百分之二十五、打發時間爲百分之二十三、認識朋友爲百分之十二。

[26]參閱陳一雄著，「全台掃蕩戀童網，站主全是高中生」，聯合報，北市綜合 B4 版，二〇〇四年五月二十六日。

ii　案例

桃園縣警察局警察分局於九十三年九月七日查獲桃園縣民宋清坤涉嫌經營網路輪盤賭博，依賭博罪嫌移送。其犯罪手法，行爲人係透過架設網路作爲平臺，經營網路輪盤賭博，提供不特定人下注，以押紅、黑、綠三種賭法，若是押紅或黑，賠率一比一；押綠則是一賠三十三，下注從一百元到一萬元，莊家贏的話，收取下注的賭博的資金；如果賭徒贏錢，莊家則要匯款給賭客，但可抽取賭金千分之十二做爲報酬[27]。

III　網路誹謗

i　定義

「網路誹謗」係指行爲人透過網路或電子郵件散佈不實的內容給不特定人，致他人的名譽遭受損害之行爲。

ii　案例

八十六年十一月間國立政治大學某邱姓學生因不滿趙姓教授之教學方法及考試方式，於該校提供網路之電子佈告欄上，以「另一種形式的強暴」爲題，指摘該教授涉嫌抄襲學生所做之報告，作爲其個人之學術論著。其犯罪手法，係利用網路傳遞訊息的功能，故意於網路上將不實的訊息透過電子郵件散佈於不特定人或張貼於網路上供不特定人觀覽，致該特定人名譽受損[28]。

IV　網路恐嚇

i　定義

---

[27]參閱呂開瑞著，「網路賭博，莊家慘賠，債主施暴」，聯合報，桃竹苗綜合新聞 B4 版，二〇〇四年九月八日。

[28]參閱沈榮華著，同前註 10 論文，第六十六頁。

「網路恐嚇」係指行爲人透過網路散佈或以電子郵件傳遞威嚇的言語或文字，使不特定人或特定人心生畏怖之行爲。網路恐嚇依行爲人的主觀目的不同而構成不同的罪，如刑法第一百五十一條之恐嚇公眾罪、第三百零五條之恐嚇危害安全罪及第三百四十六條之恐嚇取財罪等。

ii　案例[29]

甲、恐嚇柯林頓案

民國八十五年間，美國白宮收到一封透過台灣學術網路傳送來的電子郵件，其內容爲「You President, I will kill you when you go out. I see you blood」，即揚言要殺害美國總統柯林頓的恐嚇行爲。嗣經查證後發現發信來源爲國立中山大學。

乙、恐嚇和信集團案

民國八十四年四月十八日，和信集團收到一封未署名的勒索信件，要件於四月二十日交付新台幣九百萬元，否則將炸毀該集團旗下之高雄中信飯店，惟事後並未有人前去取款。

V　網路販售槍毒

i　定義

「網路販售槍毒」，係指行爲人透過網路討論區張貼訊息或利用電子郵件傳遞訊息，在網路上兜售槍枝與毒品之行爲。

ii　案例

刑事警察局偵九隊於九十三年二月十七日查獲現役軍人黃柏仁等三人上網販賣黑槍案，起出國軍四五手槍槍管七枝及一批改造槍彈，依觸犯陸海空軍刑法移

送。其犯罪手法係先在奇摩家族申請成立「槍枝園地」之網站，於網站上刊登販售槍枝之訊息，進而販售槍枝牟利，販售之所得則利用人頭帳戶供購槍者匯款。此案例值得注意的是，該網站屬「封閉型」網路，網友必須先加入會員，經審核同意後才能登入網站瀏覽內容，透過過濾網友身分方式逃避警方查緝，係智慧型的網路犯罪手法[30]。

VI　網路煽惑犯罪

i　定義

「網路煽惑犯罪」係指行爲人利用網路通訊的功能，於網站上張貼或以電子郵件傳遞違法犯罪的訊息，使原未生有犯罪意圖的人心生犯罪的念頭進而進行犯罪行爲。

ii　案例

八十六年九月警方查獲「軍火教父」乙案，即係利用網路張貼詳載槍枝、性能價格之訊息，並透過網站向網友推銷槍枝，甚至歡迎團體購買。因該網站僅係提供一個販售槍枝的媒介管道，尚未真正爲販賣行爲，因此涉及的僅構成刑法第一百五十三條「煽惑他人犯罪」之罪[31]。

2.2.3 以網路爲犯罪工具之犯罪類型

以網路爲犯罪的工具之犯罪類型，係指利用網路之通訊功能所進行之犯罪行爲，其與以網路犯罪犯罪場所之犯罪類型不同處，在於後者係利用網路虛擬空間

---

[29]參閱沈榮華著，同前註 10 論文，第六十八至六十九頁。
[30]參閱陳一雄、盧德允合著，「3 軍人偷槍管，網上賣黑槍」，聯合報，話題 A5 版，二〇〇四年二月十八日。
[31]參閱廖有祿、李相巨著，「電腦犯罪－理論與實務」，五南圖書出版股份有限公司，二〇〇三年九月，第二二八至第二三〇頁。

之特性，直接將犯罪行爲施行於網路上，而前者則是藉由網路爲犯罪工具針對特定目標所進行之犯罪行爲。其犯罪型態包括網路詐欺、網路竊盜、網路洗錢、網路洩密及網路釣魚等。

I　網路詐欺

i　定義

「網路詐欺」係指行爲人透過網路或電子郵件，刊登或傳遞不實的訊息，致不特定人受騙，而從中牟利的犯罪行爲。網路詐欺係發展電子商務所衍生出的犯罪類型，其犯罪手法多樣化，包括網路黑店[32]及網路老鼠會[33]等。

ii　案例

桃園縣警察局楊梅警分局於民國九十三年六月十七日偵破網路購物詐欺集團，逮捕嫌犯楊明瑜、于盛邦二人，依詐欺罪嫌移送。其犯罪手法盜用他人信用卡名義，利用網路購物審查寬鬆的漏洞，向包括中時電子報、智邦、新浪網、番薯藤、柯達、黑橋等著名網路商店進行上網購物，取得商品後變賣獲利[34]。

II　網路竊盜

i　定義

---

[32][網路黑店係指利用網路成立短暫的網站，提供商品廣告於網路上，伺客戶訂單並繳納費用後即關閉網站之犯罪方式。參閱高大宇、王旭正著，駭客入侵網路之偵查模式分析，網址：http://163.25.10.166/lab/project/download/Network-%E5%88%91%E7%A7%91-%E9%A7%AD%E5%AE%A2%E5%85%A5%E4%BE%B5%E5%81%B5%E6%9F%A5%E6%A8%A1%E5%BC%8F%E5%88%86%E6%9E%90.PDF。最後瀏覽日期：二〇〇五年七月二十三日。

[33]網路老鼠會是自國外傳入的犯罪型態，其犯罪手法係透過電子佈告欄及新聞討論群傳送幸運信件，進行類似多層次傳銷之行爲。「網路老鼠會」之特點爲行爲人先以低入會費騙取民眾入會，並宣稱可快速致富，而後再要求繳交加盟金取得經營權方式欺騙民眾從中牟利。參閱陳素玲著，「公平會監控 36 網路老鼠會」，聯合晚報， 經濟生活 6 版，二〇〇四年二月二十七日。

[34]參閱遊文寶著，「刷卡存根外流，用於網路詐財，嫌犯利用卡號購物，騙得百萬元，供稱新光三越員工提供」，聯合報，社會 A8 版，二〇〇四年六月十七日。

「網路竊盜」係指行爲人透過網路通訊的功能從事竊盜之犯罪行爲。網路上之竊盜行爲與一般竊盜行爲之不同處，在於傳統之竊盜行爲係行爲人將他人支配的金錢或是物品等動產，乘其不備的移至自己實力支配之下，網路上因未有所謂「動產」之存在，原不存在竊盜的問題，但是由於網路的盛行，使得網路的「虛擬物品」有其實體的交易價值，致此類的虛擬物品遭竊時亦會造成財產的損失，因此刑法第三百二十三條於民國八十六年十月八日增訂將電磁紀錄列爲動產之一，成爲網路竊盜之法源。

ii　案例

屏東縣警察局潮州警分局於九十三年二月十三日查獲許明倫、蔡瑞文潮州地區竊取網路咖啡店提供之天堂線上遊戲內的寶物及裝備乙案。其犯罪手法係先於網頁中植入木馬程式，遙控竊取玩家密碼後，竊取網路玩家之天堂寶物後販售牟利[35]。

III　網路洗錢

i　定義

「洗錢」的定義依據洗錢防制法第二條之規定爲掩飾或隱匿因自己或他人重大犯罪所得財物或財產上利益者，或收受、搬運、寄藏、故買或牙保他人因重大犯罪所得財物或財產上利益者。而「網路洗錢」係因網路銀行之發展所產生的新型態犯罪行爲，其定義爲「利用網路銀行或各種新支付系統進行交易之機會，從事洗錢犯罪活動」[36]稱之。

---

[35]參閱陳崑福著，「天堂偷寶物，四男一女就逮」，聯合報，高屏綜合新聞 B4 版，二〇〇四年二月十四日。

[36]參閱謝立功著，「電子商務發展之挑戰－網路洗錢相關問題之探討（上）」，資訊法務透析，八十九年十月號。

ii　案例

邱○○於九十年四月間，先僞造洪姓男子之身份證並僞刻其印章，至銀行辦理個人活儲帳戶，嗣進入中國國際商銀、台新銀行、世華銀行、華信商銀等銀行網頁，透過網路多次測試取得客戶使用者代號及密碼後，將客戶帳戶內之存款透過線上轉帳方式，轉帳至前述洪某之人頭銀行帳戶，再以金融卡方式提領現金，使相關行庫陷於錯誤交付如數現金而取得他人財產，並以人頭帳戶方式隱匿自己犯罪所得財物[37]。

IV　網路洩密

i　定義

「網路洩密」是指行爲人利用網路具有便利及快速傳遞之功能，透過網路將機密的資料傳遞給特定人或不特定人，藉以牟利之犯罪行爲，而機密資料的取得除了實體的取得外，亦可透過網路連結他人的電腦系統的方式取得他人機密資料。

ii　案例

九十年七月間聯華電子股份有限公司，以員工利用電子郵件傳送該公司董事長所寄發給員工之電子郵件，不務正業，違反保密規定爲由予以開除[38]；另外，八十九年至九十一年間海軍新江艦之某劉姓上士，藉其工作之便以數位相機拍攝之海軍艦艇的機密，並將拍攝的照片內容利用網路傳送至大國大陸出售牟利[39]。

V　網路釣魚

---

[37]參閱法務部調查局九十一年度洗錢防制工作年報，九十一年四月出版，第七十八頁。
[38]參閱王銘勇著，同前註 8 書，第一四○頁。
[39]參閱沈榮華著，同前註 10 書，第七十八頁。

i　定義

「網路釣魚」（phishing）一詞來自飛客（phreak）及釣魚（fishing）的結合，是新型的犯罪手法，也是目前全世界網路犯罪中最常出現的手法，主要攻擊電子商務。網路釣魚最常見的手法包括偷帳號、偷線上寶物及盜領網路銀行存款，及藉下載修補程式，植入木馬進行遠端遙控，竊取電腦中的資料，窺探隱私。

ii　案例

刑事警察局偵九隊於九十三年九月間查獲十六歲的吳姓專科學生涉嫌利用「網路釣魚」手法，冒用雅虎網站客服中心名義寄發「會員帳號確認信」電子郵件，騙取網友的帳號及密碼，再入侵他人電腦，遭刑事局依僞造文書、詐欺等罪嫌函送法辦。網路釣魚犯罪方式，是由駭客冒充知名公司的名義或網站網頁發出假郵件，騙取使用者輸入名稱、密碼或銀行帳號等資訊；駭客也會誘騙使用者點選垃圾郵件中的網頁，連接到駭客假造的網站，當使用者輸入機密資料，就會被盜取相關帳號及密碼，行爲人再利用取得之帳號及密碼進行網路轉帳至本身或人頭的戶頭牟利[40]。

2.3 網路犯罪之特性

網路犯罪係資訊發展後所產生的新興犯罪型態，其類型包括傳統的犯罪類型及獨特一格的新型態犯罪類型，因此網路犯罪的特性與傳統犯罪的特性並不完全相同，依美國學者 Susan W. Brenner 之見解[41]，傳統犯罪具有以下與網路犯罪四

---

[40]參閱陳一雄著，「新聞辭典飛客+釣魚=網路釣魚」，聯合報，焦點 A3 版，二〇〇四年九月二十三日。

[41]See Susan W. Brenner, *TOWARD A CRIMINAL LAW FOR CYBERSPACE：A NEW MODEL OF LAW ENFORCEMENT*, Rutgers Computer and Technology Law Journal, 2004。Available in WESTLAW。

項截然不同的特性：一、行爲人與受害人有身體的接觸（physical proximity of victim and victimizer）；二、一對一的犯罪（one to one crime）；三、行爲人會受到實體的拘束（physical constraints）；四、犯罪模式容易預測（crime pattern）。本節以下探討網路犯罪的特性，分類方式與 Susan W. Brenner 之分類方式不盡相同，但亦係相對於傳統犯罪類型之差異所歸納之特性。一般而言，網路犯罪應具有以下之特質[42]：

I　犯罪手段的智慧性、技術性

與傳統的一般犯罪比較，網路犯罪需要更多的智慧而非體力。因爲網路系統管理者，爲了提供更安全的網路空間，不斷地精進其安全防範措施，因此要進入網路空間實施犯罪，行爲人必須具備相當程度的專業知識和熟練的操作技術，以逃避網路安全的稽核防護，達到侵入或破壞網路系統的目的。因此利用網路犯罪之犯罪手法具有相當地智慧性及技術性。

II　犯罪的隨機性、瞬間性

傳統的一般犯罪在某種程度上必須受到時間之限制，但是網路犯罪時間，幾乎在一天二十四小時任何一個時間都可進行。同時由於網際網路寬頻的發展，傳輸速度極爲快速，犯案時間可以短至以「秒」計算即可完成，與傳統犯罪係以「時日」爲計算單位截然不同。

III　犯罪的無國界性

網路犯罪係在網路的虛擬空間進行，由於網路空間裡沒有國境的分隔線，亦沒有任何地理空間上的限制，行爲人只要透過電腦終端機連結上網際網路，即可

[42]參閱馮震宇著，同前註 9 書，第三三七至三三九頁。

超越省界、國界，針對連結在網路線另一頭的電腦或網路系統進行犯罪行爲。

IV　犯罪之隱匿性

網路犯罪的隱匿性可分爲真實身分、犯罪行爲過程兩種不同的形態：

i　真實身分的隱匿性

網路犯罪行爲人在網路上使用的名稱均爲暱稱或代號，並不使用真實的姓名，即使透過查詢清查出使用者的 IP 位址，進而查出申登人之真實姓名，亦不能斷然認定爲犯罪行爲人。更何況提供上網的場所眾多，包括網路咖啡店、學校、圖書館等，縱使清查到 IP 位址，也無法得知犯罪行爲人爲何人。

ii　犯罪行爲過程的隱匿性

網路犯罪的實施方式，主要係透過程式數據等各種無形訊息的操作進行，此類相關的犯罪證據易被刪除或更改，致犯罪行爲完全不留任何痕跡，而不易被查覺與偵破。

V　犯罪低成本（低風險性）

網路犯罪成本係從經濟學的角度來探討，其意義係指行爲人在實施網路犯罪行爲時所可能付出的代價，而此代價包括物質上或精神上的成本。由於網路犯罪行爲在極短的時間內即可完成，並且網路犯罪行爲人從事犯罪行爲出於好奇的心態居多，不認爲自己是實施一種危害社會的行爲，再加上網路犯罪極具隱匿性及偵破網路犯罪極爲不易，因此在行爲人在精神上的成本很低。同時網路犯罪行爲人在實施犯罪行爲時，往往只要輕輕地按下鍵盤即完成犯罪行爲，根本不用負擔任何物質上的成本。

VI　犯罪結果之嚴重社會危害性

由於網路資訊傳遞技術不斷發展，不但人類的生活、工作與網路相連結在一

起，就連國家的相關設施包括電力、電信等，甚至國防與國家安全都與網路息息相關。再加上網網相連之網路無國界特性，任何連結網路的電腦系統都可能受害，因此網路犯罪所可能造成經濟上的損害、國家危害均是傳統犯罪所無法比擬。以今年五月肆虐全球之電腦病毒「殺手（Sasser）」爲例，短短幾秒鐘內擴散到整個網路，不到三天時間便已經有五十萬部電腦受害，企業也超過數萬家受害，造成的損害無法估計[43]。

VII 犯罪黑數高

「犯罪黑數」（dark figure of crime） 係指實際上已經發生，可是卻未出現在官方犯罪統計的案件數之現象[44]。根據美國聯邦調查局電腦犯罪特勤組的統計，約有百分之八十五至九十五左右的網路入侵犯罪未被發現，而在發現的網路犯罪案件中，亦只有百分之一左右的案件爲偵查機關偵辦[45]，顯示網路犯罪之犯罪黑數非常嚴重。分析其原因，除了網路犯罪本身具有隱匿性不易查覺外；另外網路犯罪被害人爲保護名譽、保守秘密或認爲偵查機關也無法解決之故，而不願意加以追究。

VIII 犯罪客體多樣化

「網路犯罪」一詞並非單一之法定概念或法定犯罪類型，而是犯罪學意義上對一種新型態犯罪之統稱，因此犯罪形態多樣化，如前所述包括網路入侵、網路

---

[43]參閱李若松著，「殺手攻擊百萬台電腦－史上變種最快，傳播速度驚人，歐美災情嚴重，亞太感染趨緩，可能影響三億台電腦」，聯合報，生活 A6 版、二〇〇四年五月五日。

[44]犯罪黑數發生的原因，有學者臚列主要七種原因：一、行爲人與被害人根本不知有犯罪的發生；二、當事人爲了庇護犯罪人或是出於投鼠忌器的心理，而不願提出告訴；三、被害人可能擔心遭到報復或難堪，而不敢提出告訴；四、被害人可能對司法機關缺乏信心，而不願提出告訴；五、社會大眾缺乏正義感，而不會舉發；六、警察機關的吃案；七、警察機關不能破案，而使犯罪案件成爲懸案。參照林山田、林東茂合著，「犯罪學」，八十八年八月增訂三版，第一六七至一六八頁。

[45]參閱馮震宇著，同前註 9 書，第三三八頁。

散佈病毒、網路色情、網路誹謗、網路恐嚇等等不同態樣，相對地，犯罪客體（受害人）亦因而多樣化。

IX　網路犯罪偵查困難

網路上傳遞的訊息是由數字 0 或 1 組成，必須經過特定演算法轉換後，才能以肉眼辨識內容；而且網路犯罪行爲人多是以「代號」在網路上實施犯罪，使用密碼又不斷變更，偵查人員不易過濾出行爲人身份。再加上網路犯罪通常須經過一段時間後才能既遂其犯罪目的，致行爲與結果存在時間差，相關犯罪證據蒐證困難；更何況網路犯罪偵查過程中，原本即存在可能涉及多國偵查管轄的棘手問題以及檢、警 調人員缺乏電腦或網路的專業知識與不熟悉網路偵查相關要領的窘境，致使網路犯罪偵查作爲盲點重重，偵破率始終無法提升。

2.4 網路犯罪行爲人的特性[46]

在犯罪學的研究，除了針對各種不同的犯罪類型所顯現的不同犯罪現象進行統計及分析，以探討犯罪行爲發生的原因外；對於犯罪行爲人本身所具有的特性分析，也是非常重要的分析指標。因爲要先瞭解犯罪的行爲人，才能分析行爲人爲何犯罪的整個因果關係，進而達到犯罪預測或預防的目的。前節已針對網路犯罪的各種態樣及網路犯罪本身的獨有的特性進行探討，雖可大略窺知網路犯罪發生與泛濫的原因，但因未探討網路犯罪行爲人本身的特性，遂始終無法盡窺網路犯罪發生成因之全貌，相關研究的成果縱使運用在網路犯罪偵查與預防上亦有所不足，因此有必要再就網路犯罪行爲人的特性進行探討。而網路犯罪行爲人的特性，隨著網路日漸發達也有部分調整，本文以下主要區分爲犯罪主體多樣化、犯

[46]參閱**冯卫国，张立宇合着，网络空间的犯罪与刑法面临的挑战**，網路法律評論（Internet Law Review），二〇〇二年七月，第二一八至二一九頁。

罪行爲人動機複雜化、犯罪行爲人罪惡感趨漠化、犯罪行爲人年齡層下降化等特質，分別討論之。

I　犯罪行爲主體多樣化

在網路發展初期並不普及，有能力使用網路的人不多，因此網路犯罪行爲人的分析，學者多認爲是具有高智商、高學歷，且擁有豐富的電腦及網路專業知識之人，甚至認爲網路犯罪具備白領犯罪所具備的特徵，而視爲白領犯罪的一種[47]。然而，隨著網路的發達及流行，網路使用者不斷地增加，網路不再只是白領階層的專屬權利，包括各種年齡層、各種不同的職業、各種不同身份、性別的人，均能輕易地駕馭網路，自然都有可能成爲實施網路犯罪的行爲人。

II　犯罪行爲人動機複雜化

網路犯罪行爲人的動機隨著不同的犯罪型態而有不同，以網路入侵類型而言，行爲人犯罪的動機包括出於好奇、展現個人的專業能力、滿足個人的心理等；網路詐欺、網路販售槍毒等類型犯罪，則是基於獲取不法財物；網路誹謗類型，則是出於發洩個人不滿情緒之動機。

III　犯罪行爲人罪惡感淡漠化

與真實社會的犯罪最大的不同，網路犯罪是在「虛擬空間」裡進行，實施行爲的「犯罪現場」通常是在上網的所在地，可能是家中、學校或辦公室等，與犯罪被害人不會有直接接觸的機會，而是透過網路線做爲連結的媒介，因此多不會認爲是在從事犯罪行爲。同時大多數的網路使用者，都認爲網路是新時代的產物，應享有絕對的自由，政府法律不應當加以管制，因此對於網路犯罪的感受遠不及於一般傳統類型的犯罪，導致犯罪行爲人在實施犯罪行爲人根本不覺得有罪

惡感。

IV　犯罪行爲人年齡層下降

由於網路的蓬勃發展，網路使用者的年齡層快速下降，再加上實施網路犯罪的成本低，不同年齡層的人都可以實施網路犯罪，尤其相對於成年人而言，年輕使用者對於相關法令並不熟諳、行爲控制能力亦不如成年人，往往在好奇心驅使下，便不小心地實施網路犯罪行爲，因此網路犯罪年齡層[48]遠比傳統犯罪類型的年齡層還要再下降幾歲。

2.5 網路犯罪被害人的特性

犯罪被害人特性，在犯罪學研究上也是重要的一環，因爲透過分析被害人的特性的共同點，或許可以找出防範的方式，減少同一類型犯罪的發生。特別是網路犯罪，其本身已具備隱匿不易偵查的特性，如果犯罪被害人又不願意舉發並與偵查機關合作，偵破網路犯罪案件機率更顯渺茫，網路犯罪將更加泛濫猖獗。不過，網路犯罪類型中之網路賭博、網路色情等形態的犯罪，由於並沒有直接的被害人，其侵害的法益爲社會法益，因此侵害的對象可說是「社會純樸風氣」，而無法針對被害人的特性進行分析外，其餘形態的網路犯罪，包括網路入侵、網路誹謗等的被害人，其特性約略可歸納如下：

I　被害人根本不知有網路犯罪的發生

從網路犯罪被害的原因分析，相當多的被害人本身缺乏安全的概念，因此才會被害。再加上網路犯罪類型的隱匿性高，特別是網路入侵類型的網路犯罪，行爲人可能只是侵入後進行瀏覽或植入木馬程式進行竊看等行爲，不一定會造成被

---

[47]參閱林山田、林東茂合著，犯罪學，八十八年八月增訂三版，第四六三頁。

[48]參閱林宜隆、邱士娟合著，我國網路犯罪現況分析，網址：http://jitas.im.cpu.edu.tw/2003-2/6.pdf。最後瀏覽日期：二〇〇五年七月二十三日。

害人任何實質上可感受到的損害，行爲人完成犯罪後又會技術性地將進入的資料（或稱痕跡）刪除，所以通常被害人對於網路犯罪行爲的發生根本未發現。

II　被害人多不願意舉發網路犯罪

網路犯罪的受害人中，多數可能因擔心遭到報復或難堪、對司法機關追訴犯罪缺乏信心並不願意出面舉發。最實務上最特殊的，應是從事網路銀行、網路證券等類型的公司，縱使遭到網路入侵而致損害，爲了維護公司名譽或商業秘密，也多選擇不出面舉發，而自行吸收損失。

2.6 網路犯罪手法介紹

傳統犯罪案件偵查實務中，最重要的觀念就是「知已知彼」，亦即偵查人員必須處於犯罪行爲之立場，嘗試分析犯罪行爲人之犯罪手法，以瞭解犯罪行爲人爲何及如何進行犯罪行爲，進而清查出可疑之犯罪行爲人，達到順利偵破案件之目的。

所謂「犯罪手法」，係指犯罪行爲人在從事犯罪行爲之際，多會以自已之能力、知識、習慣、便利性、成功機率等因素，做爲從事犯罪行爲之考量，並在可以完成犯罪行爲之多種途徑或方法之間，譬如犯罪的準備工作、犯案時間、地點、被害者、犯罪工具、脫逃路線等等，選擇其中一種特定犯罪方法稱之[49]。通常，一個人選擇的犯罪手法雖然可能會有所調整，但改變幅度不大，而具有犯罪的慣性；且不同的犯罪行爲人，由於其身分背景、邏輯思考方式及心理因素均有所不同，因此選擇完成犯罪行爲的途徑或方法也各有不同，換言之，每個犯罪行爲人各自擁有一種獨特之犯罪手法。特別是智慧型犯罪或是連續犯罪之案件，偵查人員可藉由分析不同案件間之犯罪手法方式，從「犯罪慣用手法」（modus

operandi）[50]確認行爲人的身分，以判斷是否爲同一特定犯罪行爲人所爲，進而鎖定該犯罪行爲之身分進行清查蒐證，甚至可預測其下一次犯罪的模式。

網路犯罪經過類型化後，亦可歸納出其犯罪手法。由於網路犯罪係發生在網路虛擬空間之行爲，在分析網路犯罪之犯罪手法時，反而會發現不同案件間有著固定模式之犯罪手法，例如犯罪行爲人一定要選擇連結上網方式，才能實施網路犯罪行爲。相對於傳統犯罪案件而言，網路犯罪行爲人可選擇之犯罪手法反而比較少，使得偵查人員更易於分析出各類型網路犯罪之犯罪手法，而能迅速偵破網路犯罪案件。本研究爲說明網路犯罪之犯罪手法，並比較不同類型網路犯罪間犯罪手法之異同，謹區分「以網路爲犯罪之客體」、「以網路爲犯罪之場所」及「以網路爲犯罪之工具」三種不同類型，輔以實例剖析其犯罪手法如後：

2.6.1 以網路爲犯罪客體之犯罪手法

I　案例摘要

九十年四月間，邱○○基於爲自己不法所有之意圖，多次利用網路咖啡廳提供之連線服務，連結至「臺灣網路認證股份有限公司」之網頁，取得申請金融 EDI 憑證之公司及個人帳戶之安全代碼及身分證字號、數位金融憑證等資料後，連結至中國國際商業銀行所網路銀行之網頁，並使用前述取得之公司名稱、營利事業統一編號、個人姓名、身分證字號等資料，逐一測試使用者代號及密碼方式，再取得該帳戶之使用者代號、身分證字號、相關開戶資料及存款餘額等資料，接著以先前取得之自然人及法人帳號、營利事業登記證號碼、國民身分證字

[49]參閱林燦璋、林信雄合著，偵查管理－以重大刑案爲例，二○○四年三月初版，第一八六頁。
[50]布萊恩．隱內（Brian Innes）著，犯罪心理剖繪檔案（Profile of a Criminal Mind），吳懿婷譯，二○○五年七月六日初版，第二十四頁。

號、銀行通行密碼等資料，登入該網路銀行之帳戶，藉由網路銀行轉帳之方式將銀行帳戶之存款，轉移至個人之人頭帳戶內，再以金融卡提領現金[51]。本案係屬以網路爲犯罪客體之犯罪類型中之入侵型犯罪類型。

II　犯罪手法

i　連結上網

網路犯罪係在虛擬的網路空間內從事犯罪行爲，其實行犯罪的前提就是必須連結上網路。連結上網路必須具備相關連線設備，包括電腦、數據機等等，並向網路連線服務提供申請取得連線上網的帳號，始能連結網路從事犯罪行爲。分析偵查實務案例，行爲人從事網路犯罪行爲時，爲避免遭偵查人員循線查獲，通常不會選擇需要提出身分證明及聯絡電話等個人資料之月繳型撥接或固接帳號方式連結網路，而選擇不用提供真實身份及聯絡電話之上網儲值卡方式連線；連結網路場所也多不會選擇在自己家中，而係選擇不易被查獲之網路咖啡店。前述實例，行爲人即係利用網路咖啡店提供網路連線服務連結網路從事網路犯罪行爲。

ii　取得被害公司或個人之基本資料

本案行爲人係利用「臺灣網路認證股份有限公司」之網頁提供認證服務的漏洞，取得申請金融 EDI 憑證之公司及個人帳戶之安全代碼及身分證字號、數位金融憑證等資料。

iii　登入網路銀行竊取被害公司或個人銀行帳戶之使用者代號及密碼

本案行爲人利用所取得之被害人帳戶之安全代碼及身份證字號，數位金融憑證等資料，登入中國國際商業銀行所網路銀行之網頁方式，使用取得之公司名

[51]參閱台灣臺北地方法院九十年度訴字第六九三號判決。

稱、營利事業統一編號、個人姓名、身分證字號等資料，並以〇〇〇〇至九九九九逐一測試方式，再取得使用者代號及密碼。

iv　將被害公司或個人之帳戶銀行存款轉出

本案行爲人取得網路銀行客戶之使用者代號及密碼後，利用網路銀行只認代號及密碼而無法稽查使用者真實身分之漏洞，透過網路銀行轉帳之方式將銀行帳戶之存款，轉移至預備之人頭帳戶內。

v　取款

前述款項轉帳至人頭帳戶後，行爲人再持事先申請之金融卡，將轉入人頭帳戶之款項，以提領現金方式取用。

2.6.2 以網路爲犯罪場所之犯罪手法

I　案例摘要

陳〇〇基於意圖銷售營利之概括犯意，於八十九年四、六月間，在未取得科藝百代股份有限公司、魔岩唱片股份有限公司等錄音著作權人之同意或授權下，於臺北縣板橋市八德路二段一九七巷五十九號六樓住處，以其父親名義向「中華電信數據通信分公司」購買定額撥接帳號 S 七三二七撥接上網後，至電腦家庭文化事業股份有限公司申請架設個人虛擬空間網站〔設定網址爲 http：//home.pchome.com.tw/boy/cdplays/left.htm；轉址網站爲 http：//playcd.cjb.net 及 http：//server11.hypermart.net/ffddf/cgi-bin/dbt/movie1/movie1.cgi〕，大量張貼擬以每片新台幣八十元至二百五十元不等之價格販售盜版光碟片（俗稱大補帖）之訊息，供他人上網閱覽。陳〇〇並利用向至易達網股份有限公司所申請之免費電子郵件信箱 faith@ms13.url.com.tw 及 playcd@playcd.cib.net 號等作爲交易聯繫之用。陳〇〇接獲客戶電子郵件訂單後，即依訂購品名，連續擅自燒錄重製該等錄

音著作之盜版光碟片，並利用郵局代收貨款郵寄交貨之方式，於客戶將款項匯入其所申請之郵局局號０二六一０二－六、帳號０一五０四三－九號帳戶後，郵寄前述盜版光碟片交付予買受人[52]。本案係屬以網路爲犯罪場所之犯罪類型中網路違反著作權類型。

II　犯罪手法

i　連結上網

本案行爲人係以其父親名義向「中華電信數據通信分公司」購買儲值定額之撥接帳號Ｓ七三二七，於其住所連結上網。

ii　申請免費電子郵件信箱

行爲人連結網路後，犯罪訊息必須透過電子郵件傳送，因此必須申請電子郵件信箱做爲傳送及接收站，特別是有相對人之犯罪類型，例如網路拍賣詐欺、網路販售大補帖等，都必須透過電子郵件彼此聯絡才能完成之犯罪類型。一般而言，向網路連線服務提供者申請月繳型撥接或固接帳號，業者即會提供一免費電子信箱供客戶使用，惟行爲人考量申請帳號必須留下個人資料方式，容易遭偵查人員循線查獲，故多不選擇使用前述電子郵件信箱做爲聯絡站，而選擇向提供免費電子信箱的網站申請免費的電子郵件信箱，做爲傳送及接收訊息之聯絡站。雖然申請前述免費電子郵件信箱申請，業者也會要求登錄個人基本資料，惟因不用提供個人身份證或駕照等資料，而無法對申請人鍵入之個人資料與其真實身份進行任何查核比對，行爲人只要係填具不實的身份資料充數，便可輕易申請到免費之電子郵件信箱，進而逃避偵查人員之查緝。本案行爲人便係向易達網股份有限

[52]參閱臺灣臺北地方法院八十九年度第一六〇六號判決。

公司所申請之免費電子郵件信箱 faith@ms13.url.com.tw 及 playcd@playcd.cib.net 號等，以散發廣告信、提供客戶下訂單及作爲交易聯繫之用。

iii 申請免費網頁空間散佈廣告訊息

行爲人除了透過免費電子郵件信箱傳遞廣告信外，亦可能向網站業者申請免費的網頁空間，張貼交易目錄、商品介紹和訂購方法等網頁內容供網友瀏覽。如同前述申請免費電子郵件信箱一樣，在申請免費網頁空間時，業者亦應要求會員填寫個人基本資料，惟因無法查核比對真實身分，且行爲人爲避免遭查緝，多係填具不實的身份資料，致偵查人員不易清查出行爲人之真實身分。本案行爲人便係向電腦家庭文化事業股份有限公司，申請架設個人之虛擬空間網站以散佈廣告訊息。

iv 轉址服務

行爲人考量申請之網頁遭提供免費網頁空間的公司刪除，導致原有客戶無法搜尋到其所製作之網頁，或基於網頁名稱便於記憶，多會向提供「免費轉址服務」的公司申請轉址服務。透過轉址服務，網友或客戶只要點選該轉址之網址，亦可連上行爲人原來製作之網頁。縱使原網頁之位址更改，只要在轉址位址更改爲新的網頁網址，即可連到原網頁。由於申請免費轉址服務時，無法查核比對個人真實身分，故也有避免遭偵查人員查緝之作用。本案行爲人所設定販售大補帖之網頁網址爲 http：//home.pchome.com.tw/boy/cdplays/left.htm，而轉址網站則設爲 http：//playcd.cjb.net 及 http：//server11.hypermart.net/ffddf/cgi-bin/dbt/movie1/movie1.cgi 等，提供客戶連結所架設之販售大補帖網頁。

v 等待客戶訂單

行爲人完成前置作業後，開始透過電子郵件或網頁散佈訊息，客戶或受害人

則透過電子郵件方式進行下單，行爲人則可再透過電子郵件回覆客戶，已接受下單之訊息。本案行爲人係向易達網股份有限公司所申請之免費電子郵件信箱 faith@ms13.url.com.tw 及 playcd@playcd.cib.net 提供給客戶訂單之用，並等待客戶下訂單。

vi 製作大補帖

本案行爲人接獲客戶訂單後，依照客戶所下訂單內容，開始自行燒錄重製未取得科藝百代股份有限公司、魔岩唱片股份有限公司等錄音著作權人之同意或授權下之錄音著作。

vii 以代收貨價方式取款

偵查實務中，行爲人爲躲避查緝，重製之大補帖多是利用郵局所提供的代收貨價服務，由郵局人員將大補帖送至客戶手中並代爲收取貨款後，轉入行爲人指定之帳戶。本案行爲人即係採取利用郵局代收貨款方式，由郵局人員交付大補帖予買受人並收受貨款後，將款項匯入其所申請之郵局局號０二六一０二－六、帳號０一五０四三－九號帳戶，以完成販售大補帖之犯罪行爲。

2.6.3 以網路爲犯罪工具之犯罪手法

I 案例摘要

九十年八、九月間，孫○○基於自己不法所有之常業詐欺犯意，依報紙分類廣告欄上所刊登廣告之電話號碼，以每件新台幣三千元之代價購買他人已開戶之銀行存摺及金融卡等物，隨即至網路咖啡廳上網連線，並向瑞典雅虎網站申請 porsche928s42002@yahoo.se、jagdaimler2002@yahoo.se 等數個免費電子郵件信箱；及向奇摩拍賣網站申請登錄 mysweetlord2002、lotusesprit2200 等帳號後，明知自己並沒有任何商品，卻在網站上公開競標拍賣Ｖ６合唱團演唱會門票、古董

郵票、古董錶等物品，並謊稱先付款再交貨，致得標者陷於錯誤匯款至孫○○之人頭帳戶後，卻未取得任何標得之商品[53]。本案係屬於網路爲犯罪工具之犯罪類型網路詐欺類型。

II　犯罪手法

i　連結網路

本案行爲人係利用網路咖啡店提供網路連線服務連結網路。

ii　申請免費電子郵件信箱

本案行爲人係向瑞典雅虎網站申請 porsche928s42002@yahoo.se 、jagdaimler2002@yahoo.se 等數個免費電子郵件信箱，以傳送及接收訊息。

iii　透過網站散佈廣告訊息

本案行爲人係向奇摩拍賣網站申請登錄 mysweetlord2002、lotusesprit2200 等帳號取得會員資格後，於該網站上散佈公開競標拍賣Ｖ６合唱團演唱會門票、古董郵票、古董錶等物品之訊息。

iv　辦理競標後接受被害人訂單

本案經被害人出價最高而取得下單資格後，向行爲人進行購買Ｖ６合唱團演唱會門票、古董郵票、古董錶等物品之下單作爲。

v　取款

本案行爲人與被害人完成交易後，由被害人匯款至行爲人之人頭帳戶，行爲人再以金融卡提領現金方式取款。惟行爲人取得款項後，並未交付競標商品給被

[53]參閱臺灣臺北地方法院九十一年度訴字第六九號判決。

害人。

2.6.4 小結

本文前揭區分「以網路爲犯罪之客體」、「以網路爲犯罪之場所」及「以網路爲犯罪之工具」三種不同網路犯罪類型，加以剖析其犯罪手法後，發現網路犯罪之犯罪手法，與傳統犯罪案件最大的不同點，在於各類型的網路犯罪或不同的網路犯罪行爲人之犯罪手法間係具有一定之共同點，使得偵查人員易於掌握偵查的方向，而這些共同點如後：

I　網路犯罪行爲人必須連結網路才能實施網路犯罪行爲

網路犯罪係於虛擬的網路空間從事犯罪行爲，行爲人必須連結網路，才能在網路的空間裡實施犯罪。對於偵查人員而言，如果能稽查行爲人從何處、使用何種方式連結網路等資料，便能順利清查過濾出行爲人身分。

II　網路犯罪行爲人會透過免費申請之電子郵件信箱或網頁空間散佈犯罪訊息或通訊以完成犯罪行爲

網路犯罪行爲人必須藉由電子郵件或網頁，才能在網路上傳遞或散佈犯罪資訊，進而完成犯罪行爲。但是行爲人爲避免身分曝光，只能選擇申請免費的電子郵件及網頁空間方式做爲犯罪的工具。

III　利用人頭帳戶現金取款

網路犯罪行爲人實施犯罪之目的雖不一定爲牟個人之利益，惟大多數的犯罪行爲人實施犯罪的目的都是爲了「錢」。爲掩飾個人的真實身分，在犯罪行爲的最後階段，多會利用他人或不實的身分申請人頭帳戶，並要求被害人將所得之不法款項匯入人頭帳戶後，以提款卡提領現金。

2.7 網路犯罪泛濫現況

我國目前網路犯罪泛濫現況，本研究擬以法務部、內政部警政署所做之統計數據說明：

I　根據內政部警政署於九十二年三月十九日公佈第九十二年第十二號警政統計通報[54]，針對九十一年台閩地區查獲網路犯罪案件進行統計資料，顯示：

i　查獲案件數量方面

九十一年查獲網路犯罪案件三千五百五十三件，較九十年一年四百四十六件增加了二千一百零七件，成長率爲百分之一百四十五點七一。

ii　查獲人數方面

九十一年共計移送法辦三年九百八十三人；較九十年移送法辦一千六百八十二人增加二千三百零一人，成長率爲百分之一百三十六點八。

iii　案件類型方面

九十一年網路犯罪類型以網路散佈性交易訊息查獲一千三百十五件、占百分之三十七點一，移送法辦一千三百五十六人，占百分之三十四點四最多；其次爲網路詐欺共計查獲三百七十一件，占百分之十點四四，移送法辦四百六十九人，占百分之十一點七八次之；第三爲網路色情查獲二百三十件，占百分之六點四七、移送法辦二七二人，占百分之六點八三。以上三案類約占五成三。

iv　以場所區別部分

---

[54]參閱內政部警政署全球資訊網，網址：http://www.npa.gov.tw/stats.php?page=content06_1&id=72&tr_id=73&pages=5。最後瀏覽日期：二〇〇五年七月二十三日。

九十一年網路犯罪利用網路咖啡店犯罪查獲件數九百三十九件，占百分之二十六點四二；較九十年查獲二百四十二件件，占百分之十六點七四，共增加六百九十七件，成長了近十個百分點。而九十一年年移送法辦人數一千零四十三人，占百分之二十六點一九，較九十年年二八六人，占百分之十七，增加七五七人，亦約成長十個百分點。顯示利用網路咖啡店實施網路犯罪有明顯增加的現象。

II 根據法務部於九十四年一月十一日針對「電腦犯罪案件」公佈各地方法院檢察署偵查終結之統計分析數據[55]顯示：

i 案件數量方面

九十二年度爲一千八百八十三件，然而九十三年一月至十一月間，網路犯罪案件數量即高達二千六百五十件，其犯罪案件數量之成長率爲百分之四十點五。

ii 涉案人數方面

九十二年度爲涉案人數爲二千一百五十九人，然而九十三年一月至十一月間，涉案人數即高達三千二百六十七人。

iii 網路犯罪類型

網路犯罪類型中以線上遊戲竊取虛擬實務之竊盜行爲最數量多；其次依序爲利用網路散佈性交易訊息、網路色情或網路援交之違反兒童及少年性交易條例之行爲。

III 根據內政部刑事警察局統計，九十二年一至至十月間各類網路犯罪案件發生數即已達五千二百一十三件[56]。

---

[55]參閱法務部全球資訊網法務統計，網址：http://www.moj.gov.tw/tpms/statanal2.aspx。最後瀏覽日期：二〇〇五年七月二十三日。

[56]參閱李相巨著，網路科技犯罪專責隊－刑事局偵九隊，透視犯罪問題第四期，二〇〇四年九月，第六十四至六十九頁。

IV　小結

從前述統計數據來看，網路犯罪案件發生數量及涉案行爲人數均逐年呈大幅度的成長現象，惟由於網路犯罪具有不易被發覺或不被舉發之比例（即犯罪黑數）甚高，前述數據可能僅是冰山一角，更顯示網路犯罪泛濫之嚴重性。分析網路犯罪泛濫之原因，除了使用者欠缺倫理觀念及業者自律功能不彰外，最主要的原因在網路犯罪案件偵破率不到百分之十[57]之故，不過，有關網路犯罪偵破率爲何始終無法提昇及網路犯罪偵查過程中所面臨的瓶頸，在此先不贅述，留待下一章再詳述。

[57]參閱卜繁裕，「網路詐欺，防範重於破案」，九十三年九月三日，財團法人中華民國消費者文教基金會全球資訊網，網址：http://www.consumers.org.tw/unit422.aspx?id=96。最後瀏覽日期：二〇〇五年七月二十三日。

3 網路犯罪偵查概論

犯罪偵查是門專門的學問，案件偵查絕非一蹴可幾，偵查人員從受理案件，經判定有偵辦之價值，開始著手清查過濾可疑的涉嫌人，蒐集有證據價值之證物，及統合所蒐獲之證物加以初步研判後，擬定偵查方向及人員配置計畫，進而執行偵查作爲，均有一定之步驟。尤其是在講究科學辦案的今日，如何達到避免人力的耗費及儘速偵破案件的目的，成爲各辦案單位所極力追尋的目標。

傳統犯罪案件偵查，由於已累積長期的偵查經驗，除已建立犯罪類型之偵查模式外，相關犯罪資料庫也有一定之規模，因此偵查人員在偵辦傳統犯罪案件顯得容易許多。然而網路犯罪偵查係新興的一門學問，雖然同屬犯罪偵查之一環，多少可以援引傳統犯罪偵查之模式，惟礙於網路犯罪偵查有其獨特之處，因此偵查人員無法全然援引傳統犯罪偵查之思惟模式，而必須重新學習、建立新的偵查模式。不過，傳統犯罪偵查既已建立一定之流程，對於建立網路犯罪偵查流程仍有參考之價值，因此本研究在探討網路犯罪偵查流程及網路犯罪偵查之困難度前，擬先說明傳統犯罪偵查相關實務運作的情形後，再探討網路犯罪偵查流程相關議題，冀能透過網路犯罪偵查與傳統犯罪偵查的比較，瞭解網路犯罪偵查的現況及所面臨的困難，進而探討網路服務提供者在網路偵查中得以協助的事項及扮演角色之重要性。

3.1 傳統犯罪案件偵查流程

傳統犯罪案件，包括殺人、竊盜、毒品等一般刑事案件；詐欺、背信、洗錢等經濟犯罪案件及公務員貪瀆案件等等。犯罪行爲一旦發生，如何破案對於偵查人員是沈重的責任，姑且不論案件數量的多寡，縱使僅專注於一個案件，其偵破亦非一蹴可幾，就算偵破後，犯罪行爲人能否伏首認罪、會否被起訴、判刑都是

未定之天，刑事訴訟法修訂後對於『證據』的要求更趨嚴格，因此各偵查機關為求達到科學辦案及提升定罪率的目的，對於案件偵辦均已建立嚴謹的偵查流程。一般而言，案件偵查流程大致可區分為線索立案、清查過濾、證據調查、案件執行、案件偵結等五個階段[58]，以下謹就各該階段的查證內容加以說明。

3.1.1 線索立案階段

線索立案階段是偵查犯罪的第一個階段，因為沒有線索即不可能啓動後續的偵查作為。司法警察受理案件線索後，為避免偵查人力及時間之浪費，會對案件線索進行初步過濾，過濾結果若認為有不法行為或具有偵查必要時，便會製作案件受理表格並啓動偵查作為；若判斷並沒有任何不法行為與不具偵辦必要時則不予處理，例如某甲檢舉某乙涉嫌犯詐欺罪乙案，惟經初步過濾後，判斷甲乙二人間係借錢不還之民事借貸法律關係，並不涉及任何刑事詐欺罪情事，而不屬於司法警察職掌範圍，遂不予受理。通常在偵查實務上，依據案件線索來源的不同，可以區分為下列幾種類型。

3.1.1.1 主動發掘

主動發掘又可稱為主動偵查，其意係指案件偵查的啓動是由檢警調人員自行立案偵查（即線索來源為檢警調人員本身），而其線索來源可能是檢警調人員從個人之人際關係取得、可能是透過過濾或分析各類媒體的報導內容、可能係由實施通訊監察中或從已偵辦的案件中追查出之其他案件線索。

---

[58]本研究將傳統案件偵查流程區分線索立案、清查過濾、證據調查、案件執行、案件偵結等五個階段等五個階段之名詞，係參考法務部調查局關於偵查案件流程之內部作業規定。至於各偵查階段偵查作為之偵查目的、偵查要領等內容，為著者歸納整理自己及同事多年實務經驗所得之心得。

3.1.1.2 民眾報案檢舉

民眾報案檢舉，係指民眾以電話、信函或親至各地檢署、警察局、調查站等偵查單位提出檢舉事項，其檢舉內容包括犯罪事實、涉嫌行爲人等等。而民眾提出檢舉方式可分爲「具名」與「匿名」兩種，前者係檢舉人以本人之真實身份出面提出檢舉；後者係以假名或不具名的方式，直接向偵查人員提出檢舉或寄發匿名信函給偵查機關。

實務上，偵查人員辦理受理檢舉時，由於檢舉人往往會考量與被檢舉人有親戚、朋友關係而不願曝光或是擔心身份曝光而遭到報復（特別是檢舉黑道流氓案件）等等問題，爲保護檢舉人的人身安全，並提高檢舉人出面提出檢舉之意願，偵查人員多會以製作「化名」之檢舉筆錄方式處理。而「化名」筆錄之製作方式，係先製作檢舉人真實姓名對照表或筆錄後予以彌封；再另製作乙份非檢舉人真實身份（例如張三、李四等代號）之筆錄。一旦案件偵破，爲避免檢舉人曝光，原則上只隨案移送化名之舉筆錄，至於經彌封之真實姓名對照表或筆錄則不隨案移送法院[59]。

對於偵查人員而言，具名檢舉之案件因有檢舉人可以進行初步查證，比較容易判斷有無偵查之價值；並且由於偵查中可以獲得檢舉人的協助，偵破的機率比較高；至於匿名檢舉之案件，尤其是匿名檢舉信函，因無法對於檢舉人進行初步的查證作爲，除非違法事證非常明確，否則多無偵辦之價值，更遑論有偵破的機會。

[59]經彌封之真實姓名對照表或筆錄只有以下兩種情形會拆封：一、核發檢舉獎金；二、法院正式行文要求提供。

3.1.1.3 犯罪嫌疑人自首

自首係指犯罪嫌疑人實施犯罪行爲後，在其犯罪行爲尚未被偵查機關發覺[60]之前，主動向偵查機關申告其犯罪行爲，並表明願意接受裁判之意思表示。至於犯罪嫌疑人實施犯罪後自首的原因，可能其基於內心自責、愧疚、反悔、擔心被查獲或是期望能有減刑之機會等等。

3.1.2 清查過濾階段

線索資料經初步過濾，認有進一步偵查之必要而予立案後，首要步驟即須先針對犯罪事實之相關人、時、地、物進行清查過濾，其目的在於蒐集可能之蛛絲馬跡，以做爲擬定案件偵辦方向之依據，甚至可做爲呈堂證據之用。本文爲方便說明案件清查過濾階段之重要性，以下謹以「台中市民顧○○遭斷頭分屍」之殺人案件爲例做說明。

案情摘要

九十三年十二月十七日上午七時許，台中市清潔隊員在收集垃圾時發現某男姓死者被切下的頭顱裝在垃圾袋中，遂報警處理；台中市警方接獲報案後立刻封鎖現場蒐證，並地毯式搜索其餘屍塊，約同日九時復於距離棄置頭顱地點約三百公尺處發現用紅色毛毯包裹的男屍。警方經比對指紋及查訪附近裏長後，查出死者爲五十三歲男子顧○○，除立即通知家屬趕來指認，並根據頭顱、屍塊棄置地點及現場血跡等事證之地緣關係，研判棄屍地點附近已人去樓空之汽車美容公司最爲可疑，嗣警方入內執行搜索，果然發現該公司一樓之電話線和沙發墊均染有大片血跡，而確定該汽車美容公司一樓乃本案之第一現場。嗣警方偵訊該汽車美

[60]「所謂犯罪未發覺係指刑事追訴機關尚未知悉犯罪事實或犯罪行爲人其中之一，均屬之」。參閱林山田著，刑法通論，一九九三年八月增訂四版，第五八三頁。

容公司劉姓老闆，發現該公司出租房客陳○○經濟狀況欠佳，已積欠三個月房租未繳，並經常與顧○○及該公司已離職的楊姓員工打麻將，警方經綜合事證初步判斷本件殺人案應是一起因賭博糾紛而起之殺人案。且由於陳○○在案發後行蹤不明，而認爲其涉有重嫌，並加強追緝陳○○到案[61]。

3.1.2.1 人

本文所指之「人」包括「被害人」與「行爲人」二者，因爲從犯罪偵查角度而言，「被害人」與「行爲人」既爲犯罪事件的兩方，對於案件之偵查自有相當的影響，因此如何查明「被害人」與「行爲人」的身份，便成爲案件偵查中最重要的課題，茲分述如後：

I 被害人

i 被害人爲唯一之線索

犯罪行爲發生後，行爲人除了自首或投案外，爲脫免責任多是逃之夭夭，偵查單位根本無法在第一時間確認其身份。因此，在有被害人之犯罪類型中，例如殺人罪、傷害罪等，被害人便成爲案件偵查中第一且唯一能掌握的線索，此時案件清查過濾的第一作爲就是「確定被害人之身份」，惟有先確定被害人的身份，才能進行後續查證作爲。

ii 被害人與行爲人間具有關聯性

從犯罪統計發現，犯罪案件（尤其是殺人案件）之行爲人與被害人間多具有一定之關聯性，例如美國聯邦調查局曾於一九九二年間針對殺人犯與被害人間之

[61]參閱廖福本、賴孟科，「中市驚傳斷頭命案，男子顧炎成遇害，警方鎖定兩人」東森新聞網，重點新聞，二○○四年十二月十七日。網址：http://www.ettoday.com/2004/12/18/545-1729166.htm。最後瀏覽日期：二○○五年七月二十三日。

關聯性做一項統計，發現行爲人與被害人認識者佔百分之五十二，其中行爲人爲家庭中成員者佔百分之二十六，而陌生者僅占百分之二十二[62]；另外，英國學者伊斯特在一九五〇年針對二百名精神正常之殺人犯爲對象分析與被害人的關係，亦發現與被害人關係爲陌生人的比例僅爲百分之十六點五；而彼此相識者占百分之六十八點一（其中朋友爲百分之二十點四；戀人爲百分之三十一點二；妻子爲百分之十六點五）[63]。因此，從確定被害人身份著手，是查明可能行爲人的最有效手段。

iii　清查過濾被害人之背景資料及週遭關係

被害人身份一旦確定，偵查單位必須立即針對被害人的家屬或親友等進行訪查，進一步清查過濾其背景資料及週遭關係。換言之，必須針對被害人之就學或就業、職業（一般行業或特種行業的工作）、人際關係（複雜或單純的往來關係）及生活作息等等事項進行瞭解，其主要目的在於透過過濾被害人的週遭關係，以瞭解有無導致犯罪行爲發生之可能原因或疑點，進而推斷可能的行爲人之身份與案件發生原因。一般而言，受害人的職業、人際關係及生活作息愈單純，愈容易從其週遭關係過濾出可能的行爲人與受害原因。

iv　案例分析

前述分屍殺人案件中，警方在偵查初期，所掌握的線索只有遭分解的頭顱、軀體等屍塊外，沒有其他有用的線索，因此查明死者身份便成爲首重要的工作。在本案中警方係採取指紋比對、查訪附近裏長及請死者家屬指認等方式後，確定死者爲五十三歲男子顧○○。而死者身份確定後，警方接著查訪家屬及附近裏長

[62]參閱楊士隆主編，暴力犯罪－原因、類型與對策，二○○四年五月初版，第二八三頁。
[63]參閱林山田、林東茂合著，同前註 47 揭書，第二○五至二○六頁。

以瞭解受害人之背景資料及週遭關係，進而發現死者沒有工作、生活單純，惟經常與金○○專業汽車美容公司已離職的楊姓員工及陳姓房客打麻將等資料，復因楊姓員工及陳姓房客不見蹤跡，遂推斷該二人爲可能之嫌疑人，並研判犯罪動機可能係因賭博糾紛而起之殺機。

II　行爲人

i　確定行爲人身份

案件偵查的最終目標是將犯罪行爲人繩之以法，犯罪行爲既爲行爲人所實施，因此清查過濾行爲人的部分，自是案件偵查流程中不得不進行的部分。一旦行爲人身份可以確定後，偵查人員即可針對鎖定之犯罪涉嫌人進行證據之蒐集或實施通訊監察、搜索、扣押、逮捕、拘提等強制作爲。而清查過濾行爲人的重點[64]，包括必須研判該案件係單純犯罪或是共同犯罪之型態？行爲人之性別（共同犯罪則研判其中有無女性參與）？行爲人之年齡（成年人或是未成年人）？甚至慣用手爲右手或左手？等等項目。一般而言，共犯成員愈多，由於可能遺留的跡證愈多，所以通常會較容易偵破。

ii　清查過濾行爲人之背景資料及週遭關係

偵查人員確定行爲人的身份，通常是採取訪談受害人或現場目擊證人之方式，惟若案件之受害人死亡或欠缺現場目擊證人時，則不易過濾出行爲人之身份。就算初步判斷出行爲人的身份後，爲求避免發生誤判情形，必須查核其背景資料及清查週遭關係，而查核的方式包括查詢基本資料、前科資料、出入境資料、出入監資料及通聯紀錄等相關資料，茲分述如後：

---

[64]參閱林燦璋、林信雄合著，同前註 49 揭書，第一八八頁。

(i)　基本資料

確定可能之行爲人身份後，可透過戶政機關或是各縣市警察局戶口通報台方式查詢該人包括個人姓名、出生別、年籍、出生地、身分證統一編號、戶籍、父母親姓名、配偶姓名、教育程度等基本資料，其目的在於透過資料的比對判斷所推斷結果的正確性，例如目擊證人供述之行爲人爲中年男子，若資料顯示爲女性，代表推斷結果有誤差而必須重新進行清查過濾；反之，則代表推斷結果正確，偵查人員則而依據查得之相關基本資料繼續追查行爲人之所在。

(ii)　前科資料

前科資料係指偵查單位將行爲人所違犯之犯罪案件，按移送、起訴、判決（裁定）不同順序時之資料輸入電腦建檔，以便日後偵查案件查詢之用。一般而言，犯罪行爲人可能再犯之機率甚高[65]（特別是從事毒品製造、販售或僞造貨幣等罪），因此在清查過程中常會發現同一人多次違犯相同類型之案件之情形。偵查人員調閱前科資料後，若經初步過濾之行爲人曾犯過類此案件之前科時，則表示推斷結果應爲正確。

(iii)　出入境資料及出入監資料

清查出入境資料及出入監資料之目的，在於比對確定可能之行爲人有無在案件發生時間點出國或在監執行，一旦發現案件發生時，該對象出國或在監中則可排除其涉案可能，而無須再針對該對象進行任何蒐證。

(iv)　通聯（信）紀錄

---

[65]參閱法務部資訊網針對「我國與日本刑事案件偵查、執行及矯正統計之比較」法務統計，網址：http://www.moj.gov.tw/tpms/a90-1.aspx。根據該統計資料顯示日本一九九二年受刑人出獄後截至一九九九年再入監資料中，出獄受刑人於出獄後七年間，再犯罪而入監比率百分之四九點九；我國一九九二年出獄截至一九九九年再犯率爲百分之三二點三。最後瀏覽日期：二〇〇五

前述資料的查詢多係在有目擊證人或已查訪出特定的行爲人時所做的查核作爲。犯罪案件發生時若欠缺目擊證人，並無法立即確定行爲人之身份時，清查過濾的作爲將更加困難。本文前述在說明清查受害人身份時，曾提及受害人與行爲人多具有一定之關聯，再加上電話通訊的發達，因此偵查實務上常發現受害人與行爲人間會有通話情形。因此，在無法特定行爲人身份的情形下，偵查人員可以採取先向電信事業調閱受害人電話通聯（信）紀錄[66]資料方式，以初步過濾行爲人身份。由於目前電信事業所提供的通聯紀錄內容中，包括發話方之電話號碼、受話者之電話號碼、通話起迄時間及基地臺地位元等資料，偵查人員遂可利用取得之通聯紀錄，比對案件發生前後時間受害人的通話紀錄有無異常及有無重複性等情形，先行過濾可疑之通聯對象後，再向電信事業調閱該可疑通聯對象之使用者登記基本資料[67]，進而循線查明可疑對象之身份。偵查人員甚至可再調閱該可疑通聯對象之通聯紀錄，除可確定案發當時該可疑對象之所在地是否與案發地點相同或相近，亦可藉以清查過濾有無可能涉嫌之共犯。不過，依目前偵查實務而言，市內電話的申請由於必須有裝機地點才能裝設，較容易從電話申請之登記資料來過濾出行爲人；至於行動電話部分，因犯罪行爲人爲避免偵查人員追查，行動電話部分均多以申請『預付卡』及『外勞卡』[68]爲主，再加上電信事業在辦理

年七月二十三日。

[66]目前調閱通聯紀錄係依據電信法第七條第二項之規定及交通部電信總局公佈之「電信事業處理有關機關查詢電信通信紀錄實施辦法」第三條之規定辦理，依該辦法第二條之規定，所謂「通信紀錄」，係指電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼、通信日期、通信起迄時間等紀錄。

[67]目前調閱使用者資料係依據電信法第七條第二項之規定及交通部電信總局公佈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筋三條之規定辦理，依該辦法第四條規定，所謂「使用者資料」，指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爲限。

[68]外勞卡係指專供外勞使用的預付卡，其申請方式只要提供護照或居留證等證件，即可辦理申請。參閱許國禎，「冒辦外勞卡，賣出 20 萬張」，自由新聞網，網址：http://www.libertytimes.com.tw/2004/new/dec/2/today-so3.htm。最後瀏覽日期：二〇〇五年七月二十三日。

申請人資料登記程式並不嚴謹，致使偵查人員難以從電話使用者之申請資料來追查辨識行爲人。

iii　案例分析

前述顧○○斷頭分屍案中，警方在偵查中係先以現場採證方式，發現在第一現場金○○專業汽車美容公司內有三個可疑鞋印，並經大小比對後，認爲應有女性共犯，而判斷有兩人以上之共犯。再經實地訪查該公司負責人劉○○而推斷該公司已離職的楊姓員工及陳姓房客爲可能之嫌疑人。

3.1.2.2 時

I　確定案件發生時間點

所謂「時」係指案件發生的時間。確定案件發生時間的目的，在於使偵查人員得以儘速蒐集正確的事證，避免浪費不必要之人力及時間。案件確定發生時間後，可查詢出入境資料及出入監資料，先行排除與案件無關的人員。就殺人案而言，對於有民眾現場目擊的案件，偵查人員多是採取查訪案件現場目擊民眾方式，瞭解案件發生時間點；然而多數發生的案件，均缺乏任何現場目擊者，並不易清查出案件發生的時間。因此，目前偵查實務亦運用科學技術方式以確定案件發生時間點，以殺人罪爲例，只要透過醫學鑑識受害人的屍體方式，包括屍體的體溫狀況、腐爛與否及殘留於胃裡的食物分解情形等來推測其死亡時間，進而判斷案件發生的時間。

案件發生時間點一旦確定，偵查人員可以調閱案件發生時相關道路及商店的監視錄影帶或查訪案件發生時的現場民眾，以迅速清查出可疑的人、事、物、地等資料，進而準確的掌握偵查對象及方向，達到迅速偵破的目的。以爭議不斷的「總統槍擊案」爲例，該槍擊案發生後，因總統車隊迅速駛離現場，偵查人員直到總統車隊開至奇美醫院後始知悉該案件發生，故無法掌握案件發生（開槍）的

確切時間點，以致迄今無法清查出犯罪行爲人的開槍地點，過濾出可疑的開槍行爲人，本案偵查作爲因而陷入嚴重的瓶頸，由此可見，判斷案件發生時間點的重要性。

II　案例分析

前述顧○○斷頭分屍案，警方確定案發時間點之方式，即是運用醫學鑑識之技術，判斷血液凝結成血塊情形、屍體溫度等事證，以推斷顧○○死亡時間應該是在用完餐後半小時內遭殺案，即距屍體發現的時間約三個小時左右。

3.1.2.3 地

I　確定案件發生地點

所謂「地」係指案件最初發生地（又稱案件的第一現場或原始現場）。就殺人罪案件而言，兇案的第一現場往往存有較多值得蒐證的資料，例如現場可能遺留行爲人的毛髮、行兇兇器、指紋、腳印、血跡或是現場有無打鬥痕跡等對於案件偵查有助益的物證。前述物證經偵查人員採集分析後，往往得以過濾可疑的涉案對象及犯罪動機，甚至能推斷案件究係事先預謀或是臨時起意，一般而言，事先預謀的案件，行爲人會擬定計畫，甚至進行沙盤推演，以預謀殺人案件爲例，行爲人事前即會擬妥棄屍的地點，例如選擇棄置至人煙罕至、較不易在短時間被發現的偏僻山地，致偵查人員不易循線追查到案件發生之第一現場。

案件發生地點一旦確定後，偵查人員可透過第一現場的所在位置，判斷受害人與行爲人間有無地緣關係，亦可調閱附近商店之錄影帶或訪查附近民眾，進而過濾可疑的行爲人。由上分析可知，確定案件發生地是能否偵破案件的關鍵，惟由於行爲人爲了湮滅證據及避免遭偵查人員查獲，均會將受害人移離第一現場，致案件發現的地點不一定是犯罪實施的第一現場，而增加犯罪偵查的困難度。

II　案例分析

前述顧○○斷頭分屍案，警方係根據頭顱、屍塊棄置地點及現場血跡等事證之地緣關係，研判已人去樓空之汽車美容公司最可疑，經警方入內搜查，於該公司一樓之電話線和沙發墊均染有大片血跡，進而確定該汽車美容公司一樓乃第一現場，警方接著訪查該公司之負責人劉○○，才能推斷該公司已離職的楊姓員工及陳姓房客爲可能之嫌疑人。本案警方短時間即稽查出第一現場，且犯罪現場仍遺留大量的血漬等事證，可推斷本案並非預謀之案件，才會遺留許多事證爲警方追查。

3.1.2.4 物

I　確定行兇兇器

「物」係指案件發生時所遺留可能做爲日後呈堂供證的事證。犯罪案件遺留現場的物證，最重要的是「行兇兇器」。以殺人案而言，殺人的方式很多種，可能是槍殺、刀殺、毒殺或是勒斃等等，而其行兇兇器則可能是槍枝、刀、毒藥或是繩索[69]等等，這些都是案件偵查中不可遺漏的部分。案件發生現場若能蒐獲疑似兇器，即可直接採集其上之血液、指紋等資料來過濾行爲人，對案件之偵查作爲有極大的助益。惟若未能發現係行兇兇器時，則只能經由比對受害人身上的痕跡或現場遺留的痕跡方式判斷行兇兇器種類及犯罪形態。例如受害人身上是槍傷，而現場亦留有彈頭、彈殼、彈孔等痕跡，則可推斷係槍殺案。

另外，藉由行兇兇器的確定，還可以判斷行爲人的性別（例如女性力量小，

[69]依據內政部警政署刑事警察局針對九十一年故意殺人案件嫌疑人犯罪工具之統計分析顯示，使用刀類佔百分之四十三點六；槍械類佔百分之十三點一九；竹木及繩索類佔百分之九點九三；徒手佔百分之十一點三七；鐵具類佔百分之八點一七；化學物佔百分之二點零四。參閱內政部警政署刑事警察局資訊網，網址：http://www.cib.gov.tw/crime/crime01_4_a.aspx。最後瀏覽日期：二○○五年七月二十三日。

通常無法以繩索勒斃男性）、行爲人與受害人之關係（例如彼此熟識的人，才有可能以下毒方式實施毒殺行爲）；甚至採集、檢驗、鑑定行兇兇器上的指紋、血跡來清查過濾可疑行爲人。

II　蒐集現場遺留之證物

案件發生現場可能殘留的物品包括血跡、毛髮、衣服褲子碎屑纖維、地板痕跡、鞋印、指紋、彈殼或彈頭等等，均是重要的物證，因爲現場遺留之物品可能是行爲人所遺留。並且，在犯罪過程中，被害人可能會與犯罪嫌疑人搏鬥掙紮，而發生彼此血液、毛髮、衣服纖維轉移的情形。因此，偵查人員只要採集前述微量證物並送請鑑定，日後若查獲犯罪嫌疑人，即可以所採集的物證及鑑定報告內容，建立被害人與犯罪嫌疑人之關聯，甚至做爲使犯罪行爲人不得不伏首認罪的最佳武器[70]。

III　案例分析

前述顧○○斷頭分屍案，警方發現屍體兩腿彎屈，身體蜷曲，除了頭部，其他地方未遭支解，其餘並無明顯外傷，頸部切口並不平整，遂認爲係件刀殺案，且行兇兇器應該是大型有重量的刀。警方在案件現場並蒐集可疑的煙蒂、檳榔渣、綑綁死者之電話線、染有血跡的沙發墊等等物品，以做爲呈堂證物之用。。

3.1.2.5 事

I　確定案件發生的原因

所謂「事」係指案件發生的原因或行爲人的犯罪動機。犯罪的發生必有其原因，而行爲人對受害人實施犯罪之原因，可能基於報仇心態、貪婪心理、糾紛；

[70]參閱駱宜安著，刑事鑑識學，二○○三年八月二版，第二十一頁。

或犯罪傾向等等不同的原因。以殺人罪爲例，殺人的原因可能是感情因素、金錢因素、報仇等等[71]。由於被害人與行爲人多具有一定之關聯性，因此分析犯罪原因的目的，在於勾稽出可能的行爲人。例如若判斷爲情殺案件，被害人與行爲人間必定有感情的糾紛，所以偵查對象可鎖定與被害人有感情往來者；若判斷爲仇殺案件，則被害人與行爲人間必定有利益糾葛，所以偵查對象可以鎖定與被害人有衝突者。

至於犯罪動機爲何？則可以透過研判犯罪型態（臨時起意或是事先預謀）；犯罪的手法（例如一槍朝致命點擊斃或是全身刀傷流血過多致死）及現場特徵（例如抽屜有無被撬開、金錢有無損失）[72]等等相關線索來推斷，進行清查過濾出可能之行爲人。惟隨著社會的演變，突發案件或是被害人與行爲人間毫無任何關聯性的案件日漸增多，例如青少年飆車族之殺人案件頻增，其殺人動機只是好玩或是一時興起，以致不易從判斷犯罪行爲人的動機方式，來推斷出可能之行爲人身份。

II　案件分析

前述顧○○斷頭分屍案，警方經訪查後發現死者顧○○經常與金○○專業汽車美容公司已離職的員工楊○○及分租房間獨居的男子陳○○，於汽車美容店二樓打麻將，並且附近住戶表示於案發前一日曾聽到爭吵聲，因此研判該案可能係因賭博金錢糾紛所引起之殺人案。

---

[71]依據內政部警政署刑事警察局針對九十一年故意殺人案件嫌疑人犯罪原因之統計分析顯示，犯罪原因包括投機、好奇、口角、糾紛、一時衝動、自衛、幫助犯罪、憤怒、替人討債、肇事逃逸、施用毒品等等，其中口角比例佔百分之三十五點九八；其次爲仇恨佔百分十五點二三；一時衝動佔百分之十二點三一。其餘數據請參閱內政部警政署刑事警察局資訊網，網址：http://www.cib.gov.tw/tw/crime/crime01_4_a.aspx。最後瀏覽日期：二○○五年七月二十三日。

[72]參閱林燦璋、林信雄合著，同前註 49 揭書，第一八六頁。

3.1.3 證據調查階段

案件偵查經初步清查過濾人、時、地、物、事等資料，對於案件的類型、犯罪的原因及可能的嫌疑人應有初步的輪廓，爲有效掌控案件偵查流程及時程，達到速偵速結的目標，偵查人員必須迅速比對分析所蒐集的資料後，擬定偵查計畫，開始著手蒐集與調查相關之證據。偵查實務上，經常運用的具體調查作爲包括調卷、查證、會勘、行動蒐證、通訊監察、鑑定等等，其各個偵查作爲之目的及操作方式分述如後。

3.1.3.1 調卷

「調卷」係指偵查單位在有理由相信所要調閱之資料與調查事項有關時，以正式行文方式向各機關或私人機構調借相關卷宗資料之偵查作爲，其目的在於從取得之書面文件，瞭解案件全貌及蒐集書面之證據。案件偵查實務中，愈複雜的案件包括貪瀆案件、重大經濟犯罪（如超貸、掏空公司資產等），愈須透過調卷方式取得相關書面文件。因爲愈複雜的案件，其卷宗數量及內容愈繁雜，往往非經長時間研閱無法瞭解全貌及發現其中不法之處；並且偵查人員在未研閱相關卷宗前，尚難以認定有任何不法情事，若冒然採取搜索、扣押等強製作爲並不妥當，因此只能選擇不具強制力的調卷作爲，取得所需之資料。

調閱作爲在偵辦銀行超貸案件時最能發揮其功效[73]，因爲此類型的案件之犯罪手法是以虛灌公司或個人所提供擔保品價值或虛報個人或公司資產、公司營業

---

[73]參閱曹敏吉著，「土銀超貸案前經理求刑九年」，聯合報，高屏澎綜合新聞 C4 版，二〇〇四年十一月十一日。本案高雄地方法院地檢署於民國九十三年十月間偵辦土地銀行高雄市博愛分行人員超貸新台幣五億八千萬元案爲例，該案犯罪手法便是以僞造土地買賣契約書之買賣金額，將實際買賣金額從新台幣六千多萬元虛灌爲新台幣一億一千九百多萬元，而貸得超額之款項。偵查人員便是採取調卷作爲先行向銀行取得申請貸款時所檢附之土地買賣契約書等相關證明文件，經判斷確認爲不實之交易證明及契約書，與認定銀行行員有包庇圖利之行爲後，始執行後續偵查作爲。

收入或盈餘等方式，提高貸款的額度，因此在申請貸款過程中，必須提供相關證明文件，包括會計師查核報告書、營運計畫書、資產負債表、清償計畫或是足以證明有償債能力之書面資料。另外，各家銀行爲防止所屬行員有不法之情事，避免造成呆帳致公司損失之情形發生，對於貸款申請到核撥款項的流程均有詳細作業規定，承辦人員必須製作貸款申請書、鑑價報告、審核報告等等文書，由下逐層簽奉核准；高額貸款甚至必須召開董事會核定後才能撥款。對於案件偵查而言，前揭文書資料均是相當重要的線索及證據，偵查人員如能順利取得將有利於案件之偵查。

3.1.3.2 查證

「查證」係指偵查單位通知證人（包括被害人、檢舉人、告訴人、告發人、關係人）等人到場製作筆錄。其目的主要有二：一、將證人的供述做爲證據之用；二、以證人的供述內容做爲日後偵訊涉嫌人的利器。至於通知查證的方式則不限任何形式，不論是書面、口頭或電話通知均可。

案件偵查流程中，最重要的觀念就是「由外而內、由遠而近」，換言之，偵查人員必須先從愈外圍（指沒有利害關係者）的人進行查證，再逐漸縮小範圍，鎖定查證對象。因爲，一旦通知證人製作筆錄，必定要將已蒐集的物證或已分析之事證提示給證人，此時若證人與涉嫌人間有利害關係，可能會發生將偵查作爲及內容私自通知涉嫌人之情形，而對於案件後續偵查造成無法想像的影響，例如原本秘密進行的偵查作爲可能曝光、涉嫌人事先知悉偵查方向及偵查人員所掌握的事證、使得涉嫌人得以事先進行模擬演練或串供之作爲。

在各類型案件中，以偵辦賄選案件最容易發生前述副作用，因爲賄選案件通常犯罪行爲及偵查作爲時程短，所能掌握的證據有限，通常在進行查證時並沒有足夠的物證諸如蒐證錄影帶或賄款流向等可以提示；另外，行賄者與受賄者多具

有一定之利害或身份關係，受賄人經查證後通知行賄者機會甚高，使行賄者與受賄者得以事前進行串證或湮滅證據之動作，徒增案件偵破之困難度。

3.1.3.3 會勘

「會勘」係指偵查人員會同行政機關人員或行爲人至犯罪現場進行勘查作爲。其目的在於透過現場勘查作爲，確認並紀錄行爲人違法之情事，會勘紀錄則可做爲日後證據之用。而會勘紀錄應記載之內容，以偵查盜採土石案件爲例，應詳實記載行爲人之行爲係未經申請核准、遭盜挖土地之長度、寬度及深度及已否造成水土流失等內容，以利後續偵查作爲。在各類型案件中，偵辦違反水土保持法、山坡地保育利用條例、區域計畫法等破壞國土案件，會勘作爲係偵查流程中不可缺少之步驟，因爲依據目前對於破壞國土案件之規範，均係採取「先行政後司法」立法方式，易言之，行爲人破壞國土之行爲，必須先經行政機關予以行政罰鍰之處分，並於改善期限屆至日，經檢查仍認定行爲人未能達到「停止一切違法開挖行爲」或「恢復原狀」之要求，始能該當前述法令關於刑責之構成要件。綜上可知，前揭類型案件夜偵查作爲能否繼續進行完全取決於會勘之結果，假設會勘結果認定並沒有違法情事，則偵查作爲即告結束；縱使認定有違法情事，偵查人員仍須俟行政處分之期限屆至，經再次會勘後仍認定未有改善時，才有進行後續偵查作爲之必要。

3.1.3.4 行動蒐證

「行動蒐證」即係俗稱的「埋伏跟監」，其意係指偵查人員依據情報或調查事項，對特定之對象或目標，進行連續之秘密觀察與跟蹤之蒐證行動，以便蒐集與犯罪有關之各種不法活動資料、線索及證據[74]。實施行動蒐證之目的，依實施

[74]參閱林燦璋、林信雄合著，同前註 49 揭書，第二〇四頁。

當時偵查人員所能掌握的資料多寡而有所不同，若案件掌握的事證已充足而將近可以執行的階段時，實施行動蒐證的目的在於將所得之資料做爲日後案件執行之重要依據。例如偵辦毒品案件，偵查人員經實施通訊監察後，雖已確認行爲人販毒之情事，惟對於毒品之來源、置放處及共犯結構並無法完全掌控，爲避免徒勞無功，偵查人員必須先實施行動蒐證查明正確的執行地點，以利後續執行作爲；相對地，若案件仍處在摸索或欠缺事證的階段，實施行動蒐證的目的則是爲了蒐集犯罪不法之證據，以做爲日後提示行爲人或呈堂證據之用。以偵辦違反廢棄物清理法案件爲例，行爲人之犯罪手法係以砂石車載運廢棄物至偏僻地區傾倒方式牟利，然而單純從廢棄物傾倒地並無法過濾出行爲人，縱使過濾出嫌疑人身分，嫌疑人亦不會承認犯行。因此，爲證明行爲人之犯罪事實，偵查人員唯有實施行動蒐證全程錄影，才能迫使行爲人不得不承認。目前偵查人員實施行動蒐證作爲時，爲正確掌握對象之行蹤，均會搭配通訊監察之現譯，以達到最大的功效。

從偵查實務來看，行動蒐證的重要性與日俱增，歸納其因如後：一、物證是「死」的，不若人證會有翻供之機會；二、刑事訴訟法修正後，對於案件證據的要求愈趨嚴格，只有人證卻欠缺物證的案件，判刑定罪的機率愈來愈低；三、有物證可以提示，行爲人比較無法否認犯行；縱使否認一切犯行，法院也不會採信。以桃園地方法院檢察署偵辦曾盛琪任意棄置有毒廢棄物案爲例，本案原接獲檢舉之內容，對於行爲人、遭棄置廢棄物數量、載運路線及傾倒地點等線索均不清楚，於是偵查人員採取行動蒐證作爲，經數日跟監後始發現行爲人曾盛琪涉嫌將東漢邦股份有限公司廠房內（位於桃園縣縣大溪鎮）所貯存之有害事業廢棄物傾倒至桃園縣農田水利會位於桃園縣楊梅鎮之溜池；及發現曾盛琪爲計算載運數量均至同一地磅站進行秤重等情事，於是偵查人員嗣後傳訊曾盛琪時，即以行動蒐證所監錄之錄影帶及地磅單等等證據，迫使曾盛琪無法否認犯行，最後遭法院

判刑定罪[75]。

3.1.3.5 通訊監察

「通訊監察」即俗稱的「監聽」，其意係指偵查人員截收受監察對象的通訊內容，實施通訊監察之目的有三：一、監控對象即時動態；二、紀錄犯罪通訊內容；三、確定行爲人身份。而得以實施通訊監察之通訊內容範圍依通訊保障監察法第三條之規定，包括：一、利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他資訊之有線及無線電信；二、郵件及書信；三、言論及談話。其中透過電信事業提供之監察線路對於受監察對象使用之電話通訊內容進行截聽的方式爲偵查人員最常用的偵查手段。

目前偵查人員實施通訊監察之方式主要有「代錄」及「現譯」兩種，前者係由各監察機房截錄受監察對象之電話通訊內容後，先轉錄成錄音帶或光碟，交由聲請實施通訊監察之偵查人員進行破譯作爲；後者係指由偵查單位指派人員至監察機房提供之現譯台進行破譯作爲，一旦對象電話有通訊情形，即可同步進行截聽。

以往實施通訊監察是偵查人員犯罪偵查之利器，因爲截聽到行爲人犯罪行爲之通訊內容機率很高，惟近年來犯罪行爲人逐漸知悉偵查人員的偵查模式，因此在使用電話通訊中極爲謹慎，以偵辦毒品案爲例，在通訊時對於毒品均以代號稱之，例如搖頭丸之代號爲「衣服」；K 他命的代號爲「褲子」；大麻的代號爲「便當」。甚至在通訊時，犯罪嫌疑人並不談論犯罪事實，只約定聯絡地點，致使偵查過程過於依賴實施通訊監察之偵辦方式逐漸陷入窘境，尤其偵辦賄選案件，候選人或椿腳經過幾次查賄的洗禮，對於偵查人員實施通訊監察作爲早有防範，根

[75]參閱臺灣高等法院刑事判決九十二年度上訴字第二七三號判決。

本無法透過通訊監察蒐集到任何犯罪資料。最糟糕的是，前述「代錄」的方式，由於「下帶」與「送達」均須耗費時間，偵查人員實際進行破譯時間與錄音帶通訊時間往往會有數天的差距，而無法即時掌握犯罪行爲人的動態，失去執行案件的契機。由上可知，偵查人員以往實施通訊監察的偵查模式及心態必須有所調整，對於可疑之對象，必須同步進行「現譯」及「行動蒐證」作爲，才能有效全程掌握對象的動態[76]。不過，由於現譯台的數量及各單位偵查人力的不足，目前採取前述偵查作爲多在偵辦毒品案件時才會使用。

3.1.3.6 鑑識

「鑑識」係指偵查人員應用自然科學的知識和方法，對於證物予以鑑定（Identification）、個化(Individualization)和評估（evaluation），其目的在於透過鑑識程式重建犯罪現場、提供偵查方向、鑑定證物供法院判刑之參考[77]。鑑識的項目包括體液、血液、槍枝、指紋、文書、毛髮、毒品等等。目前我國從事刑事證物鑑識工作單位包括法務部調查局第六處，內政部警政署刑事警察局鑑識科、指紋室及法醫室，臺北市政府與高雄市政府所屬警察局刑事警察大隊鑑識組等等。在各類型案件中，偵辦毒品案件在移送地檢署前一定要進行鑑定程式，因爲依毒品危害防制條例毒品共分爲四級，刑責各有不同；且毒品種類繁多，偵查人員不易辨識（目前有簡易檢驗包提供給第一線偵查人員，惟種類僅包括海洛英、安非他命等常見之毒品）；再加上毒犯爲牟高利，經常以假的毒品或摻雜添加物的方式販售，致成分難以確認。因此偵查單位在移送案件前，除必須先對於行爲人進行尿液鑑定，先查明有無吸食毒品情形外，對於查獲之毒品必須先送請鑑定機構進行鑑定確定毒品之等級，並做成正式鑑定報告書，以做爲日後論罪之基礎。

---

[76]採取「現譯作爲」，即使沒有任何通訊內容，只要處於開機狀態，仍可掌握對象所在的基地台位元址資料，而監控對象的動態位置。

3.1.4 案件執行階段

案件經清查過濾人、時、地、物、事，勾勒出犯罪事實的概況及犯罪嫌疑人的身份後，經過證據調查程式，初步認定犯罪嫌疑人犯行事證明確後，偵查人員應整理查獲之證據，著手擬定執行計畫，規畫人力、時間，以進行案件收尾階段之執行作爲，其項目包括偵訊、搜索、扣押、逮捕、拘提等等，茲分述如後：

3.1.4.1 偵訊

「偵訊」係指偵查人員對於犯罪嫌疑人所做的詢問，目前對於犯罪嫌疑人均係以制式樣式之通知書方式，通知犯罪嫌疑人到場接受詢問。詢問犯罪嫌疑人的目的，在於透過筆錄的製作，將原本在證據調查階段所蒐集的證據，包括通訊監察譯文、行動蒐證之錄影帶、調卷所取得之書面資料或其他證人之供述，提示給犯罪嫌疑人，迫使行爲人承認犯行。另外，偵訊作爲亦具有讓行爲人澄清說明的功能，因爲偵查人員可透過犯罪嫌疑人之供述，發現原擬定之偵查方向錯誤、涉嫌人對象有錯誤或不足認定犯罪之情形，而修正偵查方向或將案件結案，還嫌疑人清白。

一般而言，偵訊要能達到預期效果，使犯罪嫌疑人能伏首認罪，事前準備工作極爲重要。首先偵查人員必須詳研案卷資料、整理過濾應提示給犯罪嫌疑人的證物、擬定詢問要點，更重要的爲增加犯罪嫌疑人之心理壓力，避免讓犯罪嫌疑人認爲事證不足而堅不吐實，還必須先研析犯罪嫌疑人之特性（包括基本資料、家庭背景、心理狀況、弱點及社會關係等）與可能之辯解，以便透過詢問的技巧突破犯罪嫌疑人之心防，順利偵破案件。前述曾盛琪任意棄置有害事業廢棄物案，偵查人員實際製作筆錄之初，曾盛琪並沒有預想到其犯罪行爲已遭偵查人員

---

[77]參閱駱宜安著，同前註 69 揭書，第三頁。

全程監錄，遂完全否認犯行；事實上偵查人員事前準備時，亦已預料到曾某可能之辯解，因此詢問過程中先讓曾某全盤否認後，再提示實施行動蒐證時所錄影之內容攻其不備，使其心理錯愕，方能順利突破其心防，最後曾盛琪只能選擇自白認罪並供出其他共犯，全案始能順利偵破。

3.1.4.2 搜索扣押

「搜索扣押」係偵查人員至犯罪嫌疑人或第三人住所實施搜查之偵查作爲，具有高度的強制力，是案件偵查作爲中蒐集證據與保全證據之最有效手段。以偵辦賄選案件的搜索爲例，搜索的重點在於蒐集選民名冊、文宣品、賄款等等物品，以做爲日後證據之用。執行搜索要能竟其功，偵查人員必須做好事前準備，除了事先準備相關搜索扣押文書外，最重要的，偵查人員必須先行勘察現場，其目的在於查明擬執行搜索地點之確實地址有無錯誤及有無人員居住等線索，避免發生無法執行的情形；另外，爲了防止行爲人乘機脫逃或湮滅證據，尚須瞭解現場之環境、位置、大小、聯外道路等，以規畫部署適當的人力。

偵查人員一旦蒐獲應扣押之物，必須立即將應扣押之物編號、列冊，製作成扣押筆錄，交由受搜索扣押人簽名，才算完成整個搜索扣押作爲。以往偵查人員執行扣押作爲，爲求能順利儘快離開現場，多採取將證物裝箱後帶回偵查機關，再進行啓封及造冊扣押之方式處理，惟此種作法易造成受搜索人極大之不便及不必要的爭議，因此目前偵查人員均改採取現場製作扣押物清單，當場給予收據方式以茲證明，避免日後發生爭議致執行案件程式發生瑕疵。

至於執行搜索的型態，依刑事訴訟法之規定，包括持票搜索、逕行（緊急）搜索、同意搜索及附帶搜索四種（後三者又稱無票搜索）。其中在持票搜索部分，偵查人員在實施搜索前向法院聲請核發搜索票後始得爲之，然而刑事訴訟法修正後，法官對於聲請搜索票的審核愈趨嚴格，偵查人員並不易順利聲請到搜索

票，加上聲請時間與審核聲請時間冗長，往往會牽制到偵查的時效性，甚至影響案件能否偵破。雖然，偵查人員爲爭取偵查時效，可採取同意搜索、逕行搜索及附帶搜索等無票搜索方式執行搜索，惟在同意搜索部分，偵查人員必須考量如何取得受搜索人同意及事後容易發生爭執搜索無效之問題；逕行搜索部分，須判斷是否符合法令規定之要件與執行完畢報經檢察官或法院審核的問題；附帶搜索部分，其搜索範圍僅限於搜查其身體、隨身攜帶之物件、使用之交通工具等等問題。綜上可知，對於偵查人員而言，搜索扣押雖然是偵查作爲中主動出擊的利器，惟囿於前揭問題，使得偵查人員選擇以搜索扣押方式蒐集證據的數量日漸減少，再加上犯罪行爲人的警覺性日漸提高，搜索扣押之成效不若以往，而嚴重影響案件之偵破率。

3.1.4.3 逮捕拘提

「逮捕拘提」是偵查人員主動出擊的的偵查作爲，逮捕的對象爲現行犯或通緝犯，拘提的對象則爲經合法傳喚不到或有逃亡、湮滅證據或串供之犯罪嫌疑人。對於偵查人員而言，執行逮捕拘提作爲前，必須先清查對象的住所地、出入地點、往來情形，並研析對象之心理狀況、性格及瞭解有無火力等事項，事先擬定計畫、部署人力及地點，甚至進行沙盤推演，對可能的情形事先模擬。如此一來，除可避免執行時，因對象的抗拒造成人員的傷害，亦可發生執行作爲失敗致對象脫逃，徒增案件偵查困難之情形。一般而言，執行逮捕拘提作爲，如能搭配實施通訊監察中之現譯作爲，因可確實掌握對象的動態，執行成功率最高。同時愈是重要的對象，其警覺性愈高，對於週遭些許的異常均十分敏銳，因此在執行拘捕作爲時，應適時依據現場之環境，以僞裝方式融於其中，避免造成對象及現場不相關民眾之驚擾，使其失去戒心，方能趁其不備順利拘捕對象到案。以桃園地方法院檢察署偵辦藍○○大陸女子涉嫌偷渡案，偵查人員經清查過濾藍女之居

住地點後，因無法確切掌握藍女之動態，無法逕自針對該居住地實施搜索，遂採取守候於該居住地的外圍，並利用週遭環境僞裝，致藍女及其雇主古○○失去警覺，趁其返回居住地之瞬間，迅速順利拘捕藍女到案。

3.1.4.4 測謊

「測謊」（又稱謊言偵查測驗）係指利用電子儀器設備對於被試者之脈搏、血壓、呼吸及膚電反應等生理指標同時描記之測驗方式，並經由所記錄之生理指標的改變，判斷被試人是否說謊之一種客觀的科學方法[78]。使用測謊的目的主要有二：一、增加受偵訊者之心理壓力：受偵訊者如果有說謊之情形，由於經過測謊測驗後，其結果應會呈現說謊反應之結果，因此受偵訊者之心理壓力加大，坦白供述之機率增加；二、測謊結果可以做爲輔助證據之用：測謊鑑定結果若呈現說謊反應，則檢察官或法官可依據測謊結果及所掌握的其他事證搭配做爲論罪之依據。

實施測謊的原理係依據受測試者之生理指標的變化，判斷有無說謊之現象，然而由於每個受測試人之生理反應不同，因此測試者必須針對不同個案及不同對象擬定不同之測試問題。目前測謊實務之流程包括測試前的面試及正式測試兩個階段。前階段，測試者會向受測試者解釋測試的目的及方法，以解除受測試者不必要的緊張情緒；另測試者還必須瞭解受測試者之心理狀況及身體狀況，判斷受測試者身體沒有任何異常或會影響結果之情形，決定是否進行測試。後階段，測試者必須先行擬定問題，包括無關問題及考驗問題兩種類型，無關問題係指對於受測試人而言是絕對不會也不能說謊的問題，例如對於男性受試者提出「是否爲男性」之問題，用以確定受測試者在沒有說謊時之生理反應；考驗問題則是與案

[78]參閱沈政主編，「法律心理學」，一九九二年二月初版，第七十一頁至八十六頁。

件有關之問題，而爲便於判斷有無說謊情形，考驗問題的設計必須是直接可以回答，而不得有模擬兩可之問題。例如偵查人員想瞭解受試人與乙間收受賄款情事，其題目必須設計爲「你有沒有收受賄款」及「你有沒有收受乙交付賄款」，才有可能測試出受測試者之說謊反應；反之，題目若設計成「是何人交付給你賄款」，因問題的題意不明，受測試者無法明確回答，則無法測試出任何結果。至於提問的方式，一般而言，無關問題與考驗問題會交互順序的提問，再透過生理指標的不同反應來判斷有無說謊，簡單的說，受測試者回答無關問題的生理反應比較不強烈；受測試者回答考驗問題時如果說謊，其生理反應會比較強烈，而測試者即是依不同的生理反應判讀受試人有無說謊。依目前測謊實務，在同一測試中均會重覆測試兩次，以增加判讀之正確性，而第二次測試的整體生理反應，其強度雖然均會較第一次來的低，但是其指數變化的圖形不會有太多的改變，仍是呈現受測試者回答無關問題受試者之生理反應比較不強烈，回答考驗問題時如果說謊，其生理反應比較強烈之情形。

以往偵查實務中，偵查人員仰賴測謊的案件非常多，特別是在物證很少，人證又相互推諉的案件，爲判斷何人的證言比較可信，只能採取測謊方式爲之。惟目前實施測謊的方式頻率逐漸減少，其主要原因有三：一、現行法令對於測謊的結果能否做爲證據並未有任何規定，而且部分法官對於測謊結果之正確性仍有疑義，甚至對於實施測試的人員資格諸多質疑，以致測謊的功用大大減低[79]。二、必須取得受試人之同意；三、受試人故意造成身體的不適，使之不能測試的情形增加，例如受測前日不睡覺或晚睡致血壓增高而不宜受測。

3.1.5 案件偵結階段

[79]參閱臺灣新竹地方法院刑事判決九十年度訴字第六四號判決。

案件從受理線索經判斷有偵查價值而予立案偵查開始，經清查過濾人、時、地、物、事，勾勒出犯罪事實的概況及犯罪嫌疑人的身份，透過查證、調卷、行動蒐證、通訊監察等證據調查程式，初步認定犯罪嫌疑人犯行事證明確後，再擬定案件執行計畫，實施偵訊、搜索、扣押、逮捕、拘提等偵查作爲後，整個案件偵查沈重則進入最後之偵結階段。在這個階段偵查人員應將所有的人證、物證全部彙整，綜合判斷已掌握行爲人違法之事證，若偵查人員認定所掌握的犯罪事證充足，應即製作移送書類將全案卷證移送地檢署偵查；若認定事證不足，則應續行蒐證作爲；若認定並無任何犯罪嫌疑或偵辦之價值時，則應停止偵查作爲，將全案終結。

3.2 網路犯罪案件偵查流程

本文前節針對傳統犯罪案件偵查流程，從線索立案、清查過濾、證據調查、案件執行及案件偵結等不同階段加以分析各該階段的偵查作爲及目前偵查實務的實際運作情形，爲傳統案件偵查流程建立大概之輪廓。本節將繼續探討網路犯罪案件之偵查流程及目前實務運作的情形，從案件偵查的角度而言，網路犯罪案件偵查流程與傳統案件偵查流程大致相同，所採取之偵查作爲也相去不遠，惟由於傳統犯罪與網路犯罪有幾項截然不同的特性：一、行爲人與受害人有身體的接觸；二、一對一的犯罪；三、行爲人會受到實體的拘束；四、犯罪模式容易預測下一次犯罪。前述特性導致網路犯罪偵查與傳統犯罪案件偵查在各階段流程中所進行查證作爲內容及所面臨的問題顯不相同，因此無法將偵查傳統犯罪案件的思惟及模式完全移植到網路犯罪偵查概念中，使得偵查人員在從事網路犯罪偵查過程中必須重新摸索及建立新辦案思惟，以應付日益泛濫的網路犯罪。爲凸顯出網路犯罪偵查之特殊及詳細分析其個別偵查作爲，與傳統犯罪案件偵查相互比較，本研究以下仍區分爲線索立案、清查過濾、證據調查、案件執行、案件偵結等五

個階段，依各該階段之查證作爲加以說明，惟爲避免與前節探討傳統案件偵查流程之內容重覆，謹就其特殊的部分加以論述。

3.2.1 線索立案階段

網路犯罪案件線索來源與傳統犯罪案件線索來源大致相同，包括偵查人員主動發掘線索、民眾報案檢舉及犯罪行爲人自首，並且必須經過初步判斷，認有偵查價值之線索始立案著手偵查作爲。惟由於網路犯罪具有高度的隱匿性之特性，犯罪行爲人亦多不知道有網路犯罪之發生與不願提出檢舉，因此檢舉之數量與實際案件發生之數量往往有極大之差距。另外由於網路使用者對於網路犯罪的認知不足及罪惡感淡漠等原因，主動自首的情形亦不常見。因此，目前網路犯罪案件之線索來源，主要是以偵查人員主動發掘的比例較高，而其發掘線索的方式，係由偵查人員在網路上自行蒐集不法之資訊，包括主動巡邏（即透過瀏覽）方式發現不法的線索，或以設定特定程式過濾關鍵字方式蒐集犯罪之線索。

3.2.2 清查過濾階段

網路犯罪線索資料經初步過濾，認有進一步偵查之必要而予立案後，與傳統案件偵查之思惟流程相同，爲避免耗費不必要的時間，必須先針對各種不同類型的犯罪手法進行分析，例如本文前章探討網路犯罪之犯罪手法時，即歸納出幾項共同點：一、網路犯罪必須連結網路才能實施；二、行爲人會透過免費申請之電子郵件信箱或之網頁空間散佈犯罪訊息或通訊以完成犯罪行爲；三、利用人頭帳戶取款。其目的即在藉由歸納各種不同類型網路犯罪犯罪手法之共同點，提供偵查人員在執行偵查時參考，進而使之發覺可以追查的蛛絲馬跡。接著開始針對犯罪事實之相關人、時、地、事、物開始進行清查過濾，以蒐集可能之蛛絲馬跡，做爲擬定案件偵辦方向之依據，甚至可做爲呈堂證據之用。惟由於網路犯罪具有

隱匿性、隨機性、無國界性、智慧性等特性，因此清查過濾網路犯罪之人、時、地、物、事等事項，其實際運用之方法與傳統犯罪偵查方法截然不同，且難度提高許多。實務上有不少網路犯罪案件，往往由於在此一階段無法過濾出可疑之人、事、物等線索而告全案終結。以下謹說明現行實務所採行之清查過濾方式如後：

3.2.2.1 人

網路犯罪實施地點係在網路虛擬的線路空間裡，因此不會有目擊證人可以查訪；同時網路犯罪的完成，加害人與受害人彼此並不需要面對面，網路犯罪行爲人實施網路犯罪通常又沒有特定的對象，就像是『姜太公釣魚』是願者上釣一般，加害人與受害人間的關係極爲薄弱。縱使偵查人員查訪被害人，亦無法清查過濾出犯罪行爲人之真實身份，頂多只能從留存的電腦檔案中知道犯罪行爲人之「代號」或「暱稱」而已，因此在清查過濾可疑行爲人階段，不能採取像傳統案件偵查模式先從清查被害人的身份及週遭關係著手，而必須採取截然不同的偵查思惟及方法。幸而，網路行爲具有「凡走過必留痕跡」之特性，使得偵查人員得以有追查方向。對於偵查人員而言，電腦中留存的紀錄有時遠比證人的查證效用更高，因爲證人的記憶不見得清晰明確，而且隨時間而逐漸模糊，而電腦留存的紀錄一旦取得，因不易發生更改或記憶模糊之情形，故比較不會發生偵查方向遭誤導或誤判的情形，日後提示法庭之證據能力亦比較高。依目前偵查實務，清查過濾行爲人身份之方法，依其實施犯罪方式不同而有如下三種不同的方法，茲分述如後[80]：

I 網頁內容（有電子郵件回覆）偵查涉嫌人方法

[80]本研究清查過濾犯罪行爲人身分之步驟，係參酌法務部調查局辦理內部員工網路犯罪偵查訓練課程內容。

犯罪行爲人利用申請免費之個人網頁或透過網路服務提供者提供之網頁散佈犯罪資訊以實施犯罪行爲，例如網路販賣大補帖、網路販售槍毒等。此種犯罪型態由於必須有受害人之行爲才能完成犯罪行爲，行爲人必然會提供聯絡之方式，包括聯絡電話或信箱地址等等資料。因此清查行爲人身分的第一步，便是先從網頁內容裡去尋找是否有行爲人的電子郵件信箱及姓名、連絡電話等資料，藉以過濾行爲人身份。惟通常不會有任何令人振奮的發現，因爲網路犯罪行爲人爲躲避偵查人員追查到其身份，根本不會將前述個人資料等線索張貼在網頁內容中。此時，偵查人員追查此種型態之網路犯罪行爲人身份之方法如後：

ⅰ　清查行爲人之電子郵件信箱帳號

網路犯罪類型中，行爲人與被害人間的通訊多是透過電子郵件方式傳輸，特別是在涉及交易之網路犯罪類型，以前述網路販售大補帖案爲例，縱使在網頁內容沒有任何聯絡方式之內容，行爲人亦勢必要提供連結方式，例如在網頁上設置「訂購」或「確定寄出」之框框，以方便客戶下訂單。此時，偵查人員可以按下前述框框，將訂購之內容發送給犯罪行爲人，然後透過瀏覽網頁的原始碼方式，查明訂購單的流向，取得收信的電子郵件信箱帳號。

ⅱ　清查提供行爲人電子信箱主機伺服器之 IP address

從電子郵件傳輸的原理分析，電子郵件需要硬碟空間來儲存，因此在收信人下載至個人電腦前，均需要放在郵件伺服器上。而在網際網路空間裡，每個伺服器都有專屬 IP address 做爲識別的代碼，猶如每個人有屬於自己的身份證一般。因此偵查人員取得行爲人使用之電子郵件信箱帳號後，必須先清查電子信箱主機伺服器伺服器的 IP address，進而查出該電子伺服器之申登人，才能透過向該 IP address 申登人調閱郵件伺服器上使用人的資料。目前偵查實務所採取清查郵件伺服器申登人，多係選擇在 MS-DOS 系統下，利用 ping 指令查詢得到網功能變數

名稱稱及 IP address 之申登資料，並加以比對確定電子郵件伺服器之 IP address。

iii　查詢行爲人電子信箱主機伺服器之 IP address 之申登人

確定電子郵件伺服器之 IP address 後，偵查人員必須進一步查詢該 IP address 之申登人，目前實務係透過財團法人台灣網路資訊中心81(TAIWAN NETWORK INFORMATION CENTER，簡稱 TWNIC)經由 TWNIC 的 WHOIS 系統查詢郵件伺服器 IP address 之申登人資料。

iv　調閱該電子信箱之使用者申登資料

清查出電子郵件伺服器之申登人後，由於使用者在申請免費電子郵件時，爲方便管理，伺服器之業者會要求申請者填寫個人基本資料，因此偵查人員可採取向電子信箱伺服器之業者調閱申請者之申登資料，以查明可能行爲人之身份。

v　調閱存取記錄檔(log file)

雖然經向電子郵件伺服器之業者調閱信箱使用者之申登資料，應可以過濾出行爲人之身份。惟由於使用者申請免費電子郵件信箱時，多數不用真實姓名和基本資料，而不易直接清查出行爲人之身份。幸而，經偵查實務的累積發現，部分業者會將該帳號產生之初次連線 IP address 及時間記錄下來；或將該帳號於伺服器上所作的全部動作予以記錄之情形，這些資料對於清查行爲人身份而言，有相當大之助益。因此偵查人員可透過向電子信箱伺服器之業者調閱存取記錄檔，藉由彙整比對行爲人利用電子信箱伺服器之連線時間與連線 IP address 之方式，查明使用者所利用那一個網路服務提供者所提供之上線 IP address，進而查明使用者係透過那一個網路服務提供者所提供的上網帳號與相關網站相連結。

---

[81]參閱財團法人台灣網路資訊中心網站，網址：http://www.twnic.net.tw。最後瀏覽日期：二〇〇五年七月二十三日。

vi　向網路服務提供業者調閱使用者之申登資料與存取記錄

經查明行爲人係以那一個網路服務提供者之連線帳號上網後，偵查人員必須向該網路服務提供者調閱前述存取記錄檔中各個 IP address 在特定時段係由那一個客戶使用之紀錄，接著再調閱該使用人之基本資料，以清查行爲人之身份。惟行爲人若係使用上網儲值卡連線，由於無需登錄客戶基本資料，網路服務提供者並無法提供客戶資料；因此，偵查人員必須再調閱行爲人所使用連線帳號之存取記錄檔案循線反覆繼續清查，一般而言，如能追查到行爲人上網連線使用之市內電話，由於市內電話均連接固定之地址內，便容易清查出行爲人的身份。

vii　清查前科、戶籍及電話申登資料

經前述步驟逐步清查出特定對象後，偵查人員仍必須再清查該特定對象之基本資料，包括清查前科以瞭解有無從事過相關類型案件之犯罪；清查戶籍資料以比對電話申登地址及人員之關聯，以確保清查出之對象身份即是犯罪行爲人。

II　網頁內容（沒電子郵件回覆）偵查涉嫌人方法

犯罪行爲人雖係利用申請免費之個人網頁或透過網路服務提供者提供之網頁散佈犯罪資訊以實施犯罪行爲，惟在不需要被害人之行爲即可完成犯罪行爲之類型，例如網路誹謗、網路色情等，行爲人並不會提供聯絡之方式，致偵查人員無法從行爲人留下的聯絡電話或信箱地址進行，藉以過濾行爲人身份。因此，此種型態之網路犯罪，其追查犯罪行爲人身份之方法如後：

i　清查網頁空間伺服器之 IP address

網頁空間與電子郵件一樣，都需要放在伺服器上，同樣地在網際網路上每個伺服器都有專屬 IP address。而其清查方法，與前述清查電子郵件伺服器 IP address，亦係在 MS-DOS 系統下，利用 ping 指令查詢得到網功能變數名稱稱及

IP address 對照情形，以確定網頁內容係置於前述 IP address 之伺服器上。

ii　查詢網頁空間伺服器之 IP address 之申登人

確定網頁內容係置於前述 IP address 之伺服器上，偵查人員接著須查詢網頁空間伺服器 IP address 之申登人，此時亦係透過財團法人台灣網路資訊中心[82](TAIWAN NETWORK INFORMATION CENTER，簡稱 TWNIC)經由 TWNIC 的 WHOIS 系統查詢 IP address 之申登人資料。

iii　調閱該網頁空間之使用者申登資料

查出網頁空間伺服器 IP address 之申登人後，由於使用者在向伺服器業者申請免費網頁空間時，必須先填寫個人基本資料，因此偵查人員可透過向網頁空間伺服器之業者調閱申請者之申登資料，來查明行爲人之身份。

iv　調閱存取記錄檔

由於使用者申請免費網頁空間時，多數不用真實姓名和基本資料，因此偵查人員調閱申請者之申登資料不見得能得知行爲人之身份。此時，可再向業者調閱相關存取記錄檔，利用彙整比對存取記錄檔中關於行爲人利用網頁空間伺服器之連線時間與連線 IP address 之情形，來查明爲那一個網路服務提供者所提供之上線 IP address。

v　向網路服務提供業者調閱使用者之申登資料與存取記錄

清查出行爲人係以那一個網路服務提供者之連線帳號上網後，偵查人員仍須彙整比對存取紀錄檔中各個 IP address 在特定時段係由那一個客戶使用之紀錄，然而調閱該使用人之基本資料，以查明行爲人之身份。如果無法查明，則必須再

[82]同前註。

一次調閱行爲人使用帳號之存取記錄檔案循線繼續清查。

vi　清查前科、戶籍及電話申登資料

經前述步驟逐步清查出特定之對象之後，仍必須再清查該對象之前科、戶籍等基本資料，以確定行爲人之身份。

III　從電子郵件內容偵查涉嫌人

犯罪行爲人若係利用申請免費之電子郵件傳送犯罪資訊，以實施犯罪行爲，例如網路販賣大補帖、網路販售槍毒等，此種犯罪型態，爲完成犯罪行爲，行爲人亦可能會提供聯絡之方式，包括聯絡電話或信箱地址等，因此清查的第一步，便是先從電子郵件內容裡尋找是否有行爲人的電子郵件信箱位址及姓名、連絡電話等資料，藉以過濾行爲人身份。惟網路犯罪行爲人通常不會將前述線索記載在電子郵件內容中，偵查人員不易從電子郵件內容輕易追查到其身份。因此，此種型態之網路犯罪，其追查犯罪行爲人身份之方法如後：

i　清查電子郵件標頭

電子郵件傳輸的原理，並不是將信件傳送到收信人之電腦內，而是傳送至收信人之電子郵件伺服器（Mail Server）裡，等待收信人來收信；而收信人取信的動作，是到指定的電子郵件伺服器，下載信件至自己的電腦，至此完成電子郵件傳送接收之動作。而整個信件的傳遞過程都記錄在電子郵件標頭裡，因此清查電子郵件標頭之目的在於瞭解其內包含了郵件寄信人與收信人的電子郵件地址、寄出的 IP 位址、郵件經過的路徑、轉信路徑、到達各 Mail Server 時間和寄送資料格式、大小等等資料，換言之，電子郵件標頭往往是網路偵查的重要線索來源，因此偵查人員在清查過濾電子郵件之發送人時，必須先查閱電子郵件之標頭紀錄。

ii　清查提供行爲人電子信箱主機伺服器之 IP address

從電子郵件標頭查明行爲人使用電子郵件帳號及伺服器之 IP address 後，仍須進一步清查電子郵件伺服器 IP address，此時須在 MS-DOS 系統下，利用 ping 指令查詢得到網功能變數名稱稱及 IP address 對照情形，以確定行爲人電子郵件伺服器 IP address。

iii　查詢行爲人電子信箱主機伺服器之 IP address 之申登人

確定行爲人電子郵件伺服器 IP address 後，則再透過 TWNIC 的 WHOIS 系統查詢 IP address 之申登人資料。

iv　調閱該電子信箱之使用者申登資料

確認電子郵件伺服器 IP address 申登人後，偵查人員須向該電子信箱伺服器之業者調閱使用者之申登資料以查明行爲人身份。

v　調閱存取記錄檔(log file)

若無法從電子信箱之使用者申登資料查出行爲人時，則必須再向電子信箱伺服器之業者調閱存取記錄檔，並彙整比對郵件標頭中所記載之發送電子郵件時間與連線 IP address 之情形，查明使用者係透過那一個網路服務提供者所提供的上網帳號連結網路。

vi　向網路服務提供業者調閱使用者之申登資料與存取記錄

查明使用者上網帳號連結網路之網路服務提供者後，再透過網路服務提供者調閱該使用人之基本資料或該帳號之存取記錄檔案循線繼續清查。

vii　清查前科、戶籍及電話申登資料

清查出特定之對象之後，爲確定行爲人真實身份，仍必須清查該對象之前

科、戶籍等基本資料加以比對。

IV 小結

前揭偵查犯罪嫌疑人身份之方法，是偵查人員在屢次偵查中所逐漸累積的偵查方法，並且主要係針對網路犯罪類型中偵辦包括網路色情、網路詐欺、網路販售槍毒等等形態的網路犯罪。然而，偵查實務上清查過濾行爲人身分所面臨的瓶頸非常多。以偵查網路病毒散佈及網路駭客入侵等類型之網路犯罪行爲爲例，犯罪行爲人往往會隱匿使用之 IP address，例如行爲人可以選擇設定 proxy 代理伺服器、僞造連線來源地（Connection Initiation）由侵入者假扮成其他使用者的情形或以軟體隱藏 IP address 等等方式來爲躲避追查，致偵查人員無法單純透過網路服務提供者提供之通信紀錄，透過行爲人使用之 IP address，追蹤犯罪對象的身分。

縱使偵查人員費盡心力突破前隱匿來源及路徑之技術而追查到行爲人使用之 IP address，也可能會因爲提供免費電子郵件信箱或網頁之業者，因未留存申請者真正之個人基本資料，致無法清查過濾出行爲人之真實身份。甚至，若行爲人所使用之電子郵件或網頁係向國外網路服務提供者申請，換言之，清查出之 IP address 或網站乃設置於國外之情形，例如行爲人以設定 PROXY 代理伺服器或隱匿ＩＰ等技術從事網路犯罪，經追查 IP address 係在美國某一州情形。對目前實務而言，偵查人員除可發文台灣微軟公司提供協助調閱 hotmail、msn 等電子信箱記錄嘗試取得相關資料外，由於欠缺國際合作偵辦的平臺，偵查人員根本完全無法取得任何有用的資料，而成爲偵辦網路犯罪案件最大之盲點。

3.2.2.2 時

網路犯罪案件所謂「時」之涵義，與傳統犯罪案件之「時」係案件發時間點有所不同，因爲網路犯罪行爲人與被害人不會有身體上的接觸，且實施犯罪行爲

之時間點與案件發生之時間點往往會有時間差距，因此網路犯罪所指之「時」係指「行爲人實施犯罪行爲之時間點」。前章分析網路犯罪手法時，曾提及行爲人實施犯罪行爲前必須先連結網路，因此，行爲人連結網路的時間即可能是網路犯罪行爲實施時間點。

清查過濾連結網路時間點之目的，主要在於透過「犯罪行爲時間點」與「犯罪行爲地」的交互研判，以釐清行爲人之身份。至於，清查網路犯罪行爲實施時間的原理，亦是基於網路具有「凡走過，必留痕跡」之特性，因爲網路上傳遞的訊息，除了記錄 IP address、電子郵件信箱位址外，亦會記載傳送及接收之時間點，以及行爲人連結網路之時間點，因此偵查人員可以藉由過濾網路上留存之記錄內容即可得知連結之時間點。實際執行清查方法與清查涉嫌人身份之方法大致相同，如前述電子郵件發送時間，偵查人員可以從電子郵件標頭的內容查知，前項均已詳述，在此不多贅述。

3.2.2.3 地

網路犯罪案件所謂「地」之涵義，與傳統犯罪案件之「地」係案件發生地有所不同，此時所指之「地」應該是指連結網路的地點。從前述分析網路犯罪手法時，已知行爲人必須先連結網路，才能實施犯罪行爲，因此連結網路的地點便是網路犯罪行爲人實施犯罪行爲實施之所在地。而清查連結網路地點之方法，與前述清查「人」、「時」之方法，均係透過比對過濾留存之紀錄內容，以稽查出連結網路地點。至於偵查人員清查行爲人連結網路地點，其目的主要在於確認行爲人之身份，因爲從前述清查過濾「人」的階段，所能蒐集到的資料僅爲書面申請之資料中所記載之身份，惟實際行爲人究竟是否即爲申請資料中記載之人仍無法確認。因此，偵查人員縱使清查出行爲人之使用帳號、或上網連線之電話，而循線追查到申請登記之使用人，惟該使用人仍無法直接認定即行爲人，份必須從連結

網路地點進行蒐證以查明行爲人之身份。例如追查到上網連線帳號若爲網路咖啡店，然而進入網路咖啡店使用之客戶眾多，偵查人員如何能認定行爲人身份，其透過留存記錄清查出之連結地點，至多只能代表行爲人係使用前述地點提供之連線服務連結網路從事犯罪行爲。此時偵查人員仍必須到該網路咖啡店進行查訪，瞭解在犯罪行爲發生時間之使用者爲何人，甚至可以調閱錄影帶資料加以比對，以清查行爲人之身份，或者採取在現場埋伏蒐證守株待兔的方法，等待犯罪行爲人下一次的行動，進而予以追捕。惟目前由於使用網路咖啡店連線上網的客戶眾多，再加上業者欠缺製作使用者登記及使用紀錄等資料，致無法追查出行爲人身份，因此，行爲人若透過網路咖啡廳內之連線設備連結上網以從事犯罪行爲，除非行爲人已有使用慣性，否則並不易清查出行爲人身份，致使網路咖啡店成爲網路犯罪行爲人從事網路犯罪行爲之最佳掩護處所。

3.2.2.4 物

網路犯罪與傳統犯罪關於「犯罪物」不同之處，在於網路犯罪係屬於純智慧型犯罪，行爲人根本無需使用兇刀、兇槍等兇器即可完成犯罪行爲，若強要剖析網路犯罪行爲所使用的行兇兇器爲何？或許只能勉強說是「電腦」或「連線設備」等等物品，然而這些所謂的兇器並不會遺留在犯罪現場，因此偵查人員無法蒐集到行兇兇器；同時網路犯罪係在網路虛擬的空間裡進行，沒有現實具體之第一現場，且行爲人與被害人間並未有任何身體上的接觸，因此無法從犯罪現場及行爲人的身上採集到血液、指紋等微量證物。在「物」的探討部分，最重要的觀念，是充分利用犯罪行爲所可能遺留的證物，均可能保存在網路中之特性，偵查人員在受理網路犯罪時，必須儘速將網路上之犯罪資訊保留或列印下來做爲證物，以免超過保留時效而消失。

3.2.2.5 事

網路犯罪案件與傳統犯罪案件發生原因大致相同，行爲人犯罪的原因可能係基於感情因素、金錢因素、報仇因素等等，二者最大不同處在於網路犯罪行爲人的年齡層較低，加上網路犯罪的罪惡感淡漠等因素，因此犯罪行爲人基於「好奇」原因實施犯罪行爲的比率遠比傳統犯罪案件高。而此一結果，對於網路偵查而言，將使偵查人員不易從行爲人犯罪之主觀意圖出發去瞭解其犯罪動機，進而清查過濾可能的行爲人。

3.2.3 證據調查階段

網路犯罪案件經初步清查過濾人、時、地、物、事，對於案件有了初步的輪廓後，必須彙整所蒐集的資料加以比對分析並擬定偵查計畫後，開始著手蒐集與調查相關之證據，其偵查流程與前述傳統案件偵查流程大致相同，惟具體調查作爲與傳統案件偵查內容卻不盡相同。其中會勘作爲在偵辦網路犯罪偵查並無實施之必要；另外，查證及行動蒐證作爲與傳統犯罪案件偵查方式及內容並無太大差異，故不予贅述。本文以下僅就包括調卷、通訊監察、鑑定等項與傳統犯罪案件偵查概念、偵查內容有明顯不同之偵查作爲部分進行說明如後：

3.2.3.1 調卷

調卷作爲對於傳統犯罪偵查而言，主要目的在於從取得之書面文件瞭解案件全貌及蒐集書面之證據，惟並非所有傳統犯罪類型之案件均須採取調卷作爲才能瞭解全案案情，例如殺人、傷害等刑事案件，偵查過程中根本無須向相關單位調閱任何卷宗資料。然而，調卷作爲對於網路犯罪案件偵查而言，是不得不也不能少的作爲，特別對於已經完成犯罪行爲之案件（又稱「死案」），其偵查手段只有調卷乙途。其主要原因在於網路犯罪係在虛擬的網路空間實施，且其與傳統網路犯罪最大的不同點，在於網路犯罪行爲具有「凡走過，必留痕跡」之特性，亦即

所有的犯罪證據（包括歷史使用紀錄、內容），不論係以電子郵件或張貼網頁方式從事犯罪行爲，在一定期間內均會保存在提供網路服務者之伺服器主機內。因此，偵查人員經過前述清查過濾人、時、事、地、物後，針對清查所得行爲人之 IP address、連線時間、可疑帳號、傳遞路徑等等資料[83]，偵查人員尚必須以發公文方式向各類型之網路服務提供者調閱相關之歷史使用記錄檔或犯罪內容，才有繼續偵查作爲之可能。

不過，依我國目前相關法令，網路服務提供者並無提供犯罪內容等資訊之義務，另外，網路服務提供者主動提供犯罪內容之資訊亦有侵害隱私權之疑慮，因此偵查實務中尚未有以正式公文調閱前述犯罪內容資料之情形。目前偵查人員均係採取勸導方式，促使網路服務提供者主動提供犯罪內容資料予偵查人員辦案參考。例如 BBS 站張貼不法的訊息內容，若偵查人員受理案件時，未能及時下載或列印作爲證據，此時只能透過 BBS 站版主主動將犯罪不法內容提供給偵查人員。然而，BBS 站版主是否有權提供前揭犯罪證據之權利及會否侵害使用者之隱私權而發生所取得證據產生瑕疵之問題，均值得商榷。

3.2.3.2 通訊監察

實施通訊監察係對於尚在進行中之犯罪案件（又稱「活案」），所做之偵查作爲。目前偵查實務實施之方式，主要包括監看電子郵件及監看瀏覽紀錄兩種，茲分述如後：

I 監看電子郵件

對於傳輸中之電子郵件，偵查人員可以透過網路服務提供者之協助進行監看，目前的做法亦分爲三種：一、偵查人員提供截錄之機器予業者，於監察之機

[83]參閱周士楨著，網路犯罪偵查參考資料，法務部調查局內部員工訓練課程資料。

房裝設上網及通信紀錄器協助進行節點封包之截錄後，交由偵查人員透過解讀之機器，將電子郵件內容解讀出來；二、透過業者設定於郵件伺服器收信後轉寄至指定之電子郵件信箱，直接轉寄傳輸到偵查人員指定之電子郵件信箱內，以同時收受郵件；三、偵查人員直接進入業者之機房同步截收、解讀涉嫌人之電子郵件。由於電子郵件之傳輸路徑不一定，若單純鎖定在發送方節點進行截錄，不但無法達到截收到對象所傳送資訊之目的，並且易截收到與案情無關聯之資訊而有侵害不特定人通訊隱私權之疑慮；因此目前均係採取鎖定在接收方之伺服器進行截收、側錄後交由偵查人員判讀，換言之，就目前監看電子郵件實務而言，只能截收到犯罪行爲人所接收之電子郵件，卻無法截收到其發送之電子郵件，以致無法完全發揮實施電子郵件通訊監察之功能。

縱使截收到犯罪行爲人所接收之電子郵件，亦不代表偵查人員能夠從截收到的電子郵件取得任何對於案情有利之證據，因爲業者爲避免電子郵件在傳輸過程爲他人截收而知悉通訊內容，均提供使用者得以採取「加密」的方式傳遞，並且，只有取得「解密」金鑰之接收者才能讀取電子郵件內容，未取得「解密」金鑰之截收者只能看到一堆亂碼代號，根本無法瞭解其內容。目前，由於網路服務提供者並無提供解密金鑰或協助解讀之義務，因此偵查人員一旦取得經加密之電子郵件，根本無法判讀其內容，使得實施通訊監察電子郵件之目的無法達成。

II　監看瀏覽紀錄

目前網路通訊監察實務中，除了採取對於電子郵件進行監看外，另一種實施網路通訊監察方式，係透過網路服務提供者協助監看截錄犯罪行爲人所有上網瀏覽網頁之行爲。此種監察方式係透過網路服務提供者將截錄之機器裝置於受監察

對象上網線路之節點上，紀錄犯罪行爲人所有之瀏覽行爲，並加以側錄後交由偵查人員後，利用解讀機器將所有瀏覽之紀錄予以判讀。換言之，偵查人員使用此種通訊監察方式，必須先查明犯罪行爲人使用上網連線之市內電話，經向地檢署聲請針對該線電話實施通訊監察取得許可後，才能透過業者裝設上網及通信紀錄器於受監察對象最近之電話機房，藉以攔截行爲人之郵件及儲存其上網之瀏覽紀錄，再透過解譯機器將該紀錄解碼還原行爲人所有上線及使用過程。

對於網路犯罪偵查而言，此種網路通訊監察方式似乎能有效地掌握犯罪行爲人的一切上網行爲，惟實際上其功效不如想像中的大，因爲此種監看瀏覽紀錄之方式，除了會受限於電信業者本身使用之系統，不一定能裝設機器與解碼外，最大的問題在於此種方式只能鎖定特定電話線路進行截錄，即只能在犯罪行爲人係聲請固定線路（例如寬頻網路）之上網連線方式才能實施，假設行爲人係使用移動式之上網方式，例如採取撥接帳號連線方式或利用網路咖啡廳提供之網路連線方式連結網路等形態，因無法確定犯罪行爲人上網連線之地點，故並無法對之實施通訊監察。另外，截錄之瀏覽紀錄同樣存在著「解讀密碼」的難題，一旦行爲人必須使用密碼才能進入之網頁，例如進行必須加入會員之聊天室，偵查人員也會因爲無法取得該行爲人之「使用者代碼」及「通行密碼」而無法順利進入取得相關之證據。

3.2.3.3 電腦鑑識（鑑定）

電腦鑑識[84](Computer Forensics)，又稱數位證據鑑識，一九九一年波特蘭的電腦國際專家協會（International Association of Computer Investigative Specialists）中首次提出「電腦鑑識科學」之名詞，其意係指針對網路犯罪案件或與電腦有關

[84]參閱賴左罕著，「高科技犯罪及電腦鑑識」，二〇〇四年一月二十七日，刊載於資安人全球資訊網－網路安全專題聚焦，網址：http://www.isecutech.com.tw/feature/view.asp?fid=155。最後瀏

的犯罪案件所產生之現場證據，進行數位證據的採證之研究。實施電腦鑑識的目的，在於處理電腦有關的數位證據之保留（Preservation）、識別(Identification) 、粹取（Extraction）、文件化(Documentation), 以確保犯罪現場電腦物證、數位證據之原貌，與鑑定結果之完整性，使數位證據具備證據能力，提高證明力，作爲法院審理網路犯罪案件之參考依據。目前電腦鑑識的項目主要包括：

I　辨識行爲人之身份

網路犯罪行爲人爲了躲避追查，往往利用跳板或是以他人的身份來掩飾自己的行蹤，此時遭網路犯罪行爲人利用之跳板或身份遭竄用之人，在形式上看起來是行爲人，實際上卻非其所爲，此時惟有先透過電腦鑑識的方式，過濾出真正的行爲人後，才能進行後續偵查作爲。

II　確認電腦存取紀錄之內容

網路犯罪行爲人所使用的電腦中之所有資料，均係人們無法目視之電磁紀錄，並無法直接提示做爲法庭上之證據，因此必須透過電腦鑑識手段予以判讀並做出鑑識報告後，以該鑑識報告確認電腦內之存取紀錄內容，以做爲法庭證據。以臺灣彰化地方法院審理陳聰宜涉嫌僞造貨幣案件[85]爲例，法院爲確認電腦內存取之資料，便委託法務部調查局進行鑑識扣案之電腦主機，經鑑識後發現被告陳聰宜所有之扣案電腦主機內，所儲存之新臺幣紙幣圖像檔案高達四十幀，同時判讀出不同時日之掃描儲存時間，並做出鑑識報告提供予院方，承審法官則依據該鑑識報告認定被告陳聰宜所供述之內容均不實在而判決有罪。

III　確認數位證據之原貌

覽日期：二〇〇五年七月二十三日。

[85]參閱臺灣彰化地方法院刑事判決九十二年度訴字第一四五九號判決。

電腦鑑識最重要的工作爲確認偵查人員所取得之數位證據未被竄改，因爲犯罪行爲人一旦對於偵查人員所引用之數位證據提出質疑，法院勢必針對該等證據進行勘驗，此時只能透過電腦鑑識之方式，針對該數位證據內包括存取紀錄、內容等等之資料進行比對，惟有經確認未經竄改或修正之數位證據才會爲法院所採用。目前偵查實務中，偵查人員對於刪除後之檔案係使用回復軟體而取得相關證據；執行搜索扣押時亦多係採用直接操作電腦取得相關證據，而這些取證之操作作爲均會變更原有之存取紀錄而易遭質疑，因此必須藉由電腦鑑識程式確認取得之數位證據未被竄改，否則其取證程式易遭認定有瑕疵，致取得之數位證據遭排除其證據力。

事實上，電腦鑑識也屬於傳統刑事鑑識的一環，不過其鑑識程式顯然困難許多，因爲電腦鑑識除了專業人員及人力匱乏外，最大的困難點在於不易保存相關證據。按傳統刑事鑑識之標的物係人們可以目視或實際接觸的具體物，偵查過程中或蒐集證據過程中不易遭到偵查人員或其他人破壞證據的原貌；然而，電腦鑑識之標的物是人們無法實際觸摸到的「電子紀錄」，從外觀上來看均是一台「電腦」，進行取證的過程中，往往會因不經意的一個操作動作，便破壞了數位證據之完整性，進而影響其證據能力。甚至執行電腦鑑識的過程中，亦容易因爲鑑識人員的不注意而變更到其原有之紀錄。綜上可知，數位證據的取證過程及電腦鑑識進行過程，均需要更爲完善及可驗證的數位元證物保護方式，以保護鑑識前後的數位證據不被竄改，才能使得經鑑識分析後的證據更具可信度及法律地位。

然而，縱使經嚴格的程式取得數位元證據並經鑑識完成，究竟能否做爲法庭證據，雖然臺灣彰化地方法院刑事判決九十二年度訴字第一四五九號判決，採用法務部調查局之鑑識報告做爲判決之基礎，但該判決畢竟僅是個案，國內對於數位證據在法庭上有無證據能力仍欠缺具體的定論。另外，鑑識數位證據過程應符

合何種程式，其做出之鑑識報告才能採用爲證據，國內亦未有任何規定，以上均是國內電腦鑑識面臨的瓶頸。反觀美國、美國及部分國家司法系統即已經將數位證據做爲有效的法庭證據[86]，並且紛紛成立國家級的電腦鑑識實驗室及高科技犯罪的研究中心，並加強偵查人員的專業訓練；英國警察協會（Association of Chief Police Officers）甚至提出電腦物證（數位證據）指導原則（The Good Practice Guide for Computer Based Electronic Evidence）做爲數位元證據處理程式，使偵查人員在蒐證時能有所依循，並且惟有符合該指導原則中所提出四項處理原則之數位證據在法庭上才具有證據能力[87]。該四項原則分別爲：

I 處理刑事案件之警察人員或後其委託之人員，必須確保電腦或數位證據爲犯罪現場原始之狀態，即不得遭受任何內容之修改。（No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in cour）

II 在例外情況下，偵查人員如果需要存取原始數位元證據的資料，必須由有能力處理之人員進行，且對其處理之動作應予說明及與過當解釋證據的意義。（In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions）

[86]同前註 83。

[87]參閱網址http://www.4law.co.il/Lea92.htm。轉引至劉嘉明著，電腦鑑識實務，法務部調查局內部員工訓練課程資料。最後瀏覽日期：二〇〇五年七月二十三日。

III　對於電腦物證的任何稽核資料或其他記錄的處理過程，應建立處理方法與保留結果。如係委由公正的第三者進行相同的處理程式，其所得結果應相同。（An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved。An independent third party should be able to examine those processes and achieve the same result）

IV　案件承辦人必須確保遵守法律的規範及前述處理原則。（The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to）

反觀我國目前對於電腦鑑識實務，不但欠缺專責的鑑識機構、欠缺蒐證數位證據之取證準則，甚至連數位證據能否做爲法庭上的有放證據均未有明文，顯見國內電腦鑑識課題之發展仍屬落後。然而，爲了因應日趨嚴重的網路犯罪問題，使偵查人員取得的數位證據具有證據能力與證明力，進而降低網路犯罪率，實應仿效國外成立國家級之電腦鑑識單位、制定完整的數位元證據處理程式及積極加強專業人員之訓練，才能使電腦鑑識在網路犯罪偵查發揮功效。

3.2.4 案件執行階段

網路犯罪案件與傳統犯罪案件相同，偵查人員清查過濾人、時、地、物、事，勾勒出犯罪事實的概況及犯罪嫌疑人的身份，經證據調查程式而初步認定事證明確後，即應擬定執行計畫，進入案件執行階段。本階段之執行作爲亦包括偵訊、搜索、扣押、逮捕、拘提等，其中在執行搜索扣押部分[88]與傳統犯罪案件執

[88]參閱宋美雲著，電腦犯罪想像力之搜索、蒐證及詢問等事項，法務部調查局內部員工訓練課程資料。

行搜索扣押部分有所不同，其餘執行作爲並無相異，因此本文不擬重覆贅述，僅針對搜索扣押部分說明如後：

3.2.4.1 搜索

網路犯罪案件偵查之搜索與傳統案件偵查之搜索，雖然執行目的均係爲了蒐集與保全證據。然而，搜索的標的及方式卻截然不同，網路犯罪案件搜索之標的爲「無法爲人目視之電磁紀錄」，從執行面分析，遠比傳統案件之搜索係面對具體的事物來得困難許多。而執行網路犯罪搜索的對象大致可區分爲對犯罪涉嫌人所有電腦之搜索及對網路服務提供者之搜索兩種類型。前者之搜索標的爲犯罪涉嫌人所有電腦內儲存與犯罪有關之資料，包括瀏覽紀錄、電子郵件及存取紀錄等等資料，此種搜索方式爲目前偵查人員實施最多之偵查手段，惟搜索成效並不如預期，因爲實際執行搜索時往往會面臨幾項問題：一、行爲人所使用之電腦設定有「使用者代號」及「通行密碼」，致偵查人員無法進入；二、行爲人所使用之電腦內設定自動刪除程式，偵查人員執行時若沒有正確的密碼時，所儲存之資料會自動刪除。實務案例曾發生在執行搜索時，因啓動原本的警戒系統，致海外的母公司發現遭下載，而自動刪除該檔案之情形；三、行爲人在偵查人員執行搜索之際，將原有之檔案全部刪除，致無法發現任何相關之證據。

後者係指搜索網路服務提供者之伺服器，因爲網路行爲具有「凡走過必留痕跡」之特性，理論上相關犯罪證據在網路服務提供者之伺服器均可留存，偵查人員執行搜索應會有相當之收獲。然而實務上卻並非如此，其原因約略有下列幾點：一、搜索網路服務提供者係屬於對第三人之搜索類型，法院對偵查人員所提出搜索聲請之審核，會嚴格限縮其要件符合刑事訴訟法第一二二條第二項「有相當理由可係爲被告或犯罪嫌疑人或應扣押之物或電磁紀錄存在爲限」之規定，因此偵查人員聲請搜索時必須提出相關之證明或查證報告，然而對於偵查人員而言

如何提出證明著實是一大困難。更何況，網路服務提供者技術上雖可能會留存相關之電磁紀錄，但網路服務提供者服務的客戶眾多，若是動輒可以實施搜索，對於網路服務提供者是經營的嚴重負擔，甚至會影響其經營之意願，而不宜動輒對之實施搜索，因此法院同意核發搜索票的機率相對降低。偵查實務中，迄今尚無任何對網路服務提供者執行第三人搜索之案例；二、偵查人員縱使取得搜索票，然而網路服務提供者之伺服器內儲存紀錄成千上萬，實際執行上亦不易搜獲應扣押之犯罪證據。況且，網路服務提供者依目前法令並無儲存犯罪證據相關紀錄之義務，爲了節省成本及儲存空間，網路服務提供者（尤其是使用個人電腦爲主機之網路服務提供者）可能早已刪除相關使用之紀錄及內容，而遑論有搜獲任何相關證物之機會。

3.2.4.2 扣押

傳統案件執行扣押時，由於應扣押之物如帳簿、存摺等均爲具體之物件，執行扣押只須將應扣押之物原封不動地以封條封緘，再予以編號載明扣押筆錄後帶回即可。惟網路犯罪案件執行扣押時，應扣押之物乃儲存於電腦主體中之電磁紀錄，若逕自將該電腦主機封緘查扣，恐會造成日後無法逕自利用該電磁紀錄做爲證據，偵查人員必須在受扣押人之面前重新進行啓封，之後再重新查扣等重覆之動作，非常不具經濟效益。於是，偵查人員改採先將應扣押之檔案內容加以列印與燒錄成光碟方式併行後，將所列印之檔案及燒錄之光碟予以封緘查扣，電腦主機硬碟部分則不封緘扣押，惟此種執行方式耗時甚久，亦不具經濟效益；並且容易發生扣押時因未能將所有需要檔案全部列印、燒錄，事後涉嫌人卻將電腦主機硬碟內之犯罪資訊全部刪除，而全盤否認擁有相關犯罪證據之情形。綜上，前述執行扣押之方式均有瑕疵，因此新近偵查人員執行扣押時，已改採取先使用特定程式將電腦資料全部複製至預先準備之硬碟，再將原電腦主機硬碟予以查扣之執

行方式，其優點如下；一：不會發生遺漏未予查扣之情形；二：偵查人員可以運用該複製之硬碟內之資料反覆查核比對，並適時予以列印做爲日後法庭之證據；三：犯罪嫌疑人否認犯罪行爲或質疑扣押證據時，可以查扣之原主機硬碟內的檔案內容做爲偵查人員反駁之利器。

除上述問題外，在執行扣押時尚有幾個值得探討的問題：

I　遭刪除檔案內容之扣押

以往偵查人員執行搜索時，面對檔案設定自動刪除程式與涉嫌人爲逃避追查事前將原有資料刪除等情形均束手無策，惟隨著科技的進步，依現行技術偵查人員只要運用 Final Data、R-mail、O&O Un Erase 等相關之軟體即可將遭刪除資料予以回復[89]，然而扣押經回復之已遭刪除的犯罪資訊，其取得證據程式可能會遭受到嚴重質疑，因爲比較具體之信件，縱使該信件內容爲重要之證據，惟一經銷毀則無法再回復，故無法再做爲證據之用；然而刪除之電子郵件或檔案卻可利用程式回復，甚至引爲證據，孰有商榷之處。惟目前偵查實務，偵查人員執行扣押時仍係將刪除之資料予以查扣做爲法庭證據之用。

II　經加密檔案內容之扣押

加密的檔案內容，在沒有解密前是一堆亂碼，縱使查扣亦無法判讀而做爲證據，然而偵查人員亦可使用 O&O blue con、Password Recovery 解密軟體予以破解密碼[90]，然而扣押時究竟應扣押該加密檔案或是已經解譯之檔案、解譯後之檔案如何證明爲原有之檔案內容及解密後的檔案內容在法庭之證據力等等，均係執行查扣時所會面臨的問題。惟目前偵查實務，偵查人員並未考量如上所提之問題，

[89]同前註。
[90]同前註 87。

而係逕自將經解密之檔案資料予以查扣做爲法庭證據之用。

3.2.5 案件偵結階段

在案件偵結階段，網路犯罪案件與傳統犯罪案件偵查流程大致相同，一個案件歷經線索立案、清查過濾、證據調查、擬定計畫及執行偵查作爲等步驟後，偵查人員必須對案件做收尾執行作爲。在案件偵結階段，偵查人員必須將所蒐集之事證彙整並研判，一旦認爲足以證明犯罪行爲人之違法行爲，則應製作移送書類將全案卷證移送地檢署偵查及法院審理；若認爲所蒐獲之事證仍不足以認定犯罪行爲人之犯罪行爲，應持續進行補強蒐證；若認定犯罪嫌疑人並不構成犯罪行爲時，偵查人員即應停止一切偵查作爲，將全案終結，並還犯罪嫌疑人一個清白。

3.3 網路犯罪偵查困難原因分析

本章第一節探討傳統犯罪案件之偵查流程，第二節探討網路犯罪案件之偵查流程，從分析兩種不同犯罪類型之偵查流程，可知網路犯罪案件偵查並無法依循既有傳統犯罪案件偵查之思惟來處理；同時網路犯罪案件偵查之困難度，顯然遠比傳統犯罪案件偵查高了許多，所面臨的偵查瓶頸亦比較多。至於網路犯罪案件偵查困難的原因，本研究認爲有以下幾點，茲分述如後：

3.3.1 網路犯罪偵查機關專責偵查人力不足

目前國內偵查網路犯罪之機關約有臺灣高等法院檢察署「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三個主要機構，該三個機構成立目的及組織略述如後：

I　臺灣高等法院檢察署「電腦犯罪防治中心」

臺灣高等法院檢察署爲因應網路犯罪日漸泛濫之情形，並有效遏止電腦網路犯罪的蔓延及擴大，於民國八十六年四月十六日成立「電腦犯罪防治中心」，統

籌協調、整合各相關單位資源，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：一、研擬防治電腦犯罪及網路犯罪的政策；二、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，給于辦案支援，以落實查緝成效；三、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；四、強化國內外電腦犯罪及網路犯罪的研究，並對國內辦理電腦犯罪及網路犯罪案件加以列管、追蹤，建立研究資料庫；五、加強教育宣導，以建立適用電腦及網路社會的倫理及秩序，以減少網路犯罪的發生。

II　法務部調查局資訊室第四科

法務部調查局爲因應日趨泛濫的網路犯罪，於民國八十九年元月一日成立資訊室第四科，統籌全局網路犯罪案件的偵辦。目前該科成員共九人，專責防制電腦犯罪規劃支援偵辦案件時有關數位證據之取得、分析及鑑識提昇偵查電腦犯罪技能及執行情形辦理有關電腦犯罪偵查及鑑識教育訓練等工作。所屬臺北市調查處及高雄市調查處，並成立查緝電腦犯罪機動專組，專責網路犯罪案件的偵辦。

III　刑事警察局偵查第九隊[91]

刑事警察局偵查第九隊，爲刑事警察局爲因應網路犯罪而成立的單位，專責資訊、網路、科技犯罪之偵查。刑事警察局於民國八十五年九月首先在資訊室下成立電腦犯罪組，嗣於民國八十八年七月將電腦犯罪組擴編爲偵查第九隊，該隊目前成員約三十人，共分四組負責偵辦高科技犯罪案件。其主要工作內容包括「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」二項，前者係

指偵辦電腦惡意程式、網路入侵、網路詐欺、網路色情及網路販售盜版光碟等案件；後者則包括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；蒐集網路不法犯罪資料，建置電腦犯罪資料庫；規畫成立電腦鑑識單位，建置數位證據鑑識標準作業程式等等工作。

IV　小結

依據內政部警政署之統計資料顯示，九十年查獲網路犯罪案件一千四百四十六件；九十一年查獲網路犯罪案件三千五百五十三件；九十二年一至至十月間查獲網路犯罪案件即已達五千二百一十三件；法務部於九十四年一月十一日針對「電腦犯罪案件」所做之統計分析數據，亦顯示各地方法院檢察署偵查終結之網路犯罪案件數量，在九十二年度爲一千八百八十三件；九十三年一月至十一月間，網路犯罪案件數量即高達二千六百五十件。綜上顯見，網路犯罪案件發生數量與日俱增，發生成長率乃呈現倍數之成長，然而國內目前專責網路犯罪偵查單位雖有法務部調查局資訊室第四科及內政部警政署刑事警察局偵九隊等機構，惟其專責人力相對於網路犯罪案件發生數量顯然十分不足。以法務部調查局爲例，全局約有二千三百餘成員，而專責網路犯罪偵查之成員不過十餘人，其比例這麼低，如何能勝任網路犯罪偵查之重任。

3.3.2 偵查人員專業能力不足

網路犯罪偵查流程中，無論在清查過濾涉嫌人身份、案件發生時間、比對通信紀錄或執行搜索扣押電腦內之資料，偵查人員均須具有電腦專業知識，否則不

---

[91]同前註 55。

僅會導致追查與蒐證的遲延，甚至可能會破壞得做爲證據之資料。由於網路犯罪係屬於新興之犯罪型態，案件發生數量亦超乎預期地驟增，爲各偵查單位始料未及，因此無法適時補充具有相關專業之人員，亦來不及對原有人員進行相關專業訓練。況且，網路犯罪偵查係橫跨法律與資訊科學兩種截然不同的學科，偵查過程中主導偵查方向之人員必須兼具相當專業電腦於網路知識技術、法律概念、犯罪偵查及蒐證技巧等等不同領域之學識，換言之，網路犯罪偵防人員需要集專業的鑑識工作與實際偵查工作於一體，對於人員之訓練更顯困難，以致目前第一線偵查人員仍有多數不具相關電腦專業能力，因而許多網路犯罪案件無法順利進行偵查。

3.3.3 網路犯罪行爲人身份不易確認

網路犯罪偵查中，偵查人員無法確認行爲人身份的原因，主要有如下幾點：

I　從受害人方面無法清查出行爲人身份

網路犯罪與傳統犯罪本質上不同點，在於行爲人與受害人並沒有身體的接觸，因此受害人根本無法知悉或提供任何關於行爲人身份之資料。

II　受害人與行爲人間欠缺關聯

傳統犯罪案件之統計資料顯示，行爲人與受害人間多具有一定之關聯，且行爲人選擇受害人做爲實施犯罪的對象均有一定之動機，惟網路犯罪案件之行爲人與受害人唯一的關係就是透過傳輸線連結，且由於網路犯罪動機多樣化，無法從受害人週遭的關係確定行爲人身份。

III　欠缺目擊證人

傳統犯罪案件，特別是殺人罪、傷害罪等類型案件，在犯罪實施過程中可能會有目擊證人存在，偵查人員可對之進行查訪。然而，網路犯罪係發生網路虛擬

的空間國度內，所有的犯罪行爲均係在網路傳輸線上完成，因此不會任何目擊證人可以進行初步查訪。

IV　網路行爲匿名的特性

民眾在網路上之活動所使用的名稱多爲「暱稱」或「代號」，並不使用真實的姓名，因此偵查人員不易從表面證據直接獲得行爲人之身份資料，縱使從查詢使用者的 IP 位址，進而清查出申登人之姓名，惟申登人是否即爲實際使用人仍有疑義，故仍不能斷然認定爲犯罪行爲人。

V　犯罪行爲人刻意隱藏身份

網路犯罪行爲人爲逃避查緝，多會隱藏自己使用之 IP 位址或是採取跳板方式從事網路犯罪，例如行爲人可以選擇設定 proxy 代理伺服器、僞造連線來源地（Connection Initiation）由侵入者假扮成其他使用者的情形或以軟體隱藏 IP address 等等方式來爲躲避追查，因此不易清查其身份。

VI　提供連結上網的場所眾多

隨著新興科技的發展，民眾連結網路已成爲日常生活的必需品，包括提供休閒營利的網路咖啡店及免費提供服務之學校、圖書館等機構，均提供使用者便捷連結網路的服務。由於透過這些提供場所連結網路，其所留存之紀錄均爲該場所申登之資料，因此犯罪行爲人若選擇至前述提供連線服務之場所從事犯罪行爲，縱使偵查人員循線清查到 IP 位址，也只能過濾出提供場所服務者之資料，而無法直接得知犯罪行爲人爲何人。

VII　網路服務提供者管理之缺漏

網路服務提供者爲了擴充市場佔有率、增加利潤及同業競爭的壓力下，除了提供使用者無須填具申請資料之預付儲值型連線服務外；縱使要求客戶填具個人

資料，也不會硬性要求客戶提供對照證件正本或查核真實身分，以致偵查人員即使清查出行爲人使用之連線帳號或及使用者登記資料，最後亦可能是個假名字，而造成追查中斷，徒然浪費辦案時間。

3.3.4 物證有限

從物的方面分析，由於網路犯罪的第一現場係在虛擬的網路空間裡，能留下的證據僅有數位化之電磁紀錄外，並無其他之證據可以蒐集。反觀傳統犯罪，在犯罪的第一現場，偵查人員不僅可以蒐集到現場遺留之物品，包括兇刀、血跡、槍彈、血衣、指紋、地板痕跡等等實體的跡證；另外，行爲人與受害人間多會有身體接觸，偵查人員可以在受害人身上採集到毛髮、衣服纖維等等微量證物。尤其，指紋、ＤＮＡ等證物均具有其獨特性、個別性，除可做爲偵查過程之判斷行爲人身份之依據外，亦可做爲日後法庭上之證據。然而，這些有用的物證在網路犯罪案件都不存在。

3.3.5 毀滅證據容易

網路犯罪的實施方式，係透過無形的程式數據等各種訊息進行，因此相關的犯罪證據容易被刪除或更改，致犯罪行爲完全不留任何痕跡，而不易被查覺與偵破網路犯罪。例如電腦駭客程式、不法取得之數據資料，只要輕輕按下刪除鍵或執行格式化指令，即能於瞬間銷毀證據。反觀，傳統犯罪案件則比較難以毀滅證據，例如殺人案，縱使行爲人爲湮滅證據而採取將死者屍體分解的手段，不僅分屍的過程必須大費周章，事後仍會殘留屍塊、血跡等物件，使得偵查人員仍可能取得相關跡證進行後續偵查作爲。

3.3.6 利用國外網路服務的犯罪行爲

網路犯罪行爲人若使用國外網路服務提供者之網路連線服務或利用國外網站、登記國外網址及向國外業者申請電子郵件信箱從事犯罪行爲，由於目前網路犯罪國際合作制度尚且闕如，使得偵查人員即使循線清查出源頭，亦會因爲無法向國外查詢、調閱相關資料，致案件偵查過程中發生「斷點」，無法繼續偵查之情形。

3.3.7 留存紀錄不完整

網路犯罪行爲人必須連結網路後始能實施犯罪行爲，再加上網路具有「凡走過必留痕跡」之特性，網路犯罪案件偵破的關鍵資料往往留存於網路服務提供者之伺服器裡。因此，網路服務提供者若能竭力協助偵查人員辦案，將儲存於伺服器之證據或所擁有的資料，包括使用者資料、帳戶資料、通信紀錄等等，提供予偵查人員，對於網路犯罪案件之偵查有絕對的助益。反之，若網路服務提供者留存之紀錄不完整或提供不充足之紀錄，案件則無法繼續進行偵查。惟因現行法令對於網路服務提供者協助偵查之規定並不完整，網路服務提供者是否有協助之義務、協助之事項等等均未明確，特別是屬於個人性質或非營利性質之網路服務提供者，由於使用主機之硬碟容量不夠或是考量成本問題，根本無法留存相關通信紀錄來配合偵查，以致在偵查過程中困難重重。

3.3.8 網路犯罪內容無法保存

網路犯罪偵查過程中，偵查人員雖得以向網路服務提供者調閱包括使用之路徑、時間、位址等等通信資料，惟這些資料仍屬於表面證據，只能做爲偵查時之參考依據。至於實質犯罪內容則無法以調閱方式取得，其主要原因並非技術上不可行，而係依據現行法令，網路服務提供者根本不能保存該通訊內容，否則恐有侵害隱私權之問題。以電子郵件爲例，一旦經收信人下載至所有之個人電腦後，

網路服務提供者應隨即刪除原留存在信箱伺服器之信件，而不能留存任何之郵件內容，否則網路服務提供者可能會侵害到使用人之隱私。因此，除非偵查人員已事先實施通訊監察而截收到傳輸中之電子郵件或通訊，否則根本沒有取得該犯罪內容之機會。更何況，隨著新科技的發展，通訊方式從原本必須透過伺服器傳輸，已發展到利用網路電話及即時通訊等 P2P 通訊方式，此種通訊方式之傳輸過程並不用透過伺服器，因而不會留存任何紀錄，更遑論得以保存相關犯罪內容。

3.3.9 偵查時程冗長

網路犯罪偵查在清查過濾階段往往比傳統案件偵查所需耗費的時程冗長。從偵查人員受理網路犯罪案件開始，無論是清查過濾行爲人身份、調閱相關之通信紀錄或使用者申登資料、逐筆過濾所取得網路服務提供者提供之通信紀錄、甚至可能必須再調閱已過濾之申登資料或是通信紀錄加以比對等過程，均須花費相當大的心力及時間。並且案件愈複雜，愈須反覆調閱相關資料，若再加上公文反覆往返耗費的時間，在清查過濾行爲人身份的階段，偵查人員便不知要耗費多少時間，然而網路通信紀錄的保存期間有期限限制，一旦超過保存期間，縱使查出了源頭，卻也可能因無法再取得任何資料，而無法繼續偵查。

3.4 網路服務提供者協助網路偵查之事項

網路犯罪的第一個步驟，就是要連結上網，而行爲人連結上網必定要透過網路服務提供者之連線網路設備；連結網路後，行爲人可能會向網路服務提供者申請免費之電子郵件信箱、網頁空間或轉址服務等服務，以傳遞網路犯罪之訊息；在需要受害人之行爲始能完成之犯罪型態，尚須透過網路服務提供者接收受害人傳遞之訊息；如此一來整個網路犯罪行爲才算是完成，綜上顯見，網路服務提供者提供之服務對於行爲人實施網路犯罪之重要性；相對地，對於網路犯罪偵查而

言，無論是線索立案階段、清查過濾階段、證據調查階段，乃至案件執行階段，均須網路服務提供者提供一定之協助。另外，前述探討網路偵查所面臨瓶頸之原因，除了專業人員及偵查人力不足外，其餘各項原因皆與網路服務提供者之配合程度息息相關，假設網路服務提供者能全力提供協助，相信對於網路偵查作爲能有極大的幫助。而實際網路偵查過程中，網路服務提供者可以提供協助偵查之事項，茲分別說明如後。

3.4.1 主動過濾

案件偵查是重要的觀念是「預防重於治療」。對於偵查人員而言，偵辦案件的目的在於預防犯罪之發生，以刑罰處置行爲人只是最後不得已之手段。因爲，犯罪行爲不發生，便不會有任何法益受到損害，自然偵查人員也無須之介入，更無須藉刑罰之方式去處罰犯罪行爲人。而由於網路資訊的傳輸原理，是使用者將訊息透過網路服務提供者之伺服器傳遞予特定人或不特定人接收，亦即網路犯罪行爲人必須透過網路服務提供者所提供之服務才有可能實現犯罪行爲，例如網路販售大補帖違反著作權之行爲或在網路上散佈援交之訊息等等，無論是張貼在網頁或是以電子郵件傳遞，均須經由網路服務提供者伺服器，因此唯一能攔截犯罪訊息者就是網路服務提供者。從預防網路犯罪發生之角度而言，網路服務提供者若能採取主動過濾方式，不定時對於上載或傳輸之資料進行檢查，並在發現任何犯罪訊息時，立即加以攔阻，從源頭阻絕犯罪資訊之散佈或張貼，將可有效降低網路犯罪發生率。

3.4.2 主動刪除或阻斷資訊

網路服務提供者主動過濾犯罪資訊，雖可阻絕犯罪資訊之散佈或張貼，惟由於網路服務提供者實際執行時不見得能過濾出網路犯罪資訊而事先予以阻絕，因

此對於未能事先過濾的不法資訊，只能採取事後防範的手段，以降低或減少犯罪之發生可能性。例如網頁上已張貼販售大補帖之訊息，此時網路服務提供者雖未事先過濾出該犯罪訊息，惟事後自行發現或經第三人通知使用者張貼訊息涉有違法情事，如能主動刪除或阻斷違法之資訊，對於防止網路犯罪案件發生，亦可產生極大的功用。

3.4.3 主動舉報

網路服務提供者主動過濾、刪除或阻斷網路上之犯罪資訊，其目的係在網路犯罪訊息尚未造成任何法益損害時，即予以攔阻之作為。惟犯罪訊息一旦已經傳遞出去，並已造成相當之損害時，則必須透過公權力介入給予事後的處罰。然而，網路犯罪本身具有隱匿性、犯罪黑數高等特性，不但行為人身份不易確定，相關犯罪證據之取得與保留才是困難之處。例如網路拍賣詐欺案件，受害人發現遭受騙之時間點通常都是在完成交易後，並且往往不會保留原來取得之訊息，也不知悉犯罪行為人之身份。受害人到偵查單位提出舉發，有可能會無法提出相當之事證，致偵查人員無法受理；縱使偵查人員受理案件，亦可能因欠缺查證路線而無法進行偵查作為。相對地，為了提供使用者最好的服務及便於管理之目的，網路服務提供者均會不定時地檢查網路資訊內容及維護網路系統，成為最容易發掘及掌握網路犯罪行為之人，因此若網路服務提供者能主動保留該犯罪訊息並主動向偵查單位舉報，可有效掌握偵查時程，提高網路犯罪偵破率。

3.4.4 儲存提供使用者資料、通信紀錄

網路服務提供者提供服務予使用者，不論是提供連線、電子郵件信箱或網頁空間之服務，均會給予使用者一組帳號與密碼，換言之，使用者進入網路世界，需要一個網路上的帳號及密碼，以便網路管理者核對使用者的身分，設定使用權

限，避免系統遭到無意或惡意的破壞。而網路服務提供者核發帳號與密碼前，使用者必須先填具個人基本資料，以供網路服務提供者認證身份或收取費用之用。另外，網路服務提供者與傳統電話業者之紀錄電話通聯相同，亦會保留使用者之 IP address、連線時間、傳遞路徑等通信資料，做爲計算費用及提供供使用者查核帳單之用。對於網路犯罪偵查而言，前揭使用者申登資料，使得偵查人員得以清查過濾行爲人或可疑帳號之身份；前揭通信紀錄則便於偵查人員勾稽行爲人之犯罪流向，以查明犯罪的人、時、地、物等線索，進而清查出犯罪的源頭（即行爲人），甚至可做爲偵訊時迫使行爲人坦承之利器及法庭上之有利證據。因此，若網路服務提供者無法儲存並提供使用者資料及通聯紀錄，或是提供不正確之使用資料及不完整的通聯紀錄的話，縱使偵查人員再厲害、投入更多人力及心血也是枉然，根本沒有偵破案件之機會。

3.4.5 自動保存、主動提供證據（儲存犯罪內容）

網路資訊的傳輸原理，是使用者將訊息透過網路服務提供者之伺服器傳遞予特定人或不特定人接收，而網路服務提供者除了保留使用者資料及通聯紀錄外，網路通訊內容亦可能會保存於網路服務提供者之伺服器中，例如 BBS 站之張貼內容，即使已經過期，在容量允許的情形下，往往仍會儲存在版主之主機伺服器內，以便提供使用者在一定期間內得以查詢以往之張貼資訊。另外，網路服務提供者爲確保服務品質，亦會自動儲存通訊內容備份，尤其是傳送電子郵件，爲避免因網路服務提供者本身之過失造成傳輸失敗，發生遭使用者請求賠償之情形，網路服務提供者會採取備份的做法以確保服務品質。顯見在技術上，網路服務提供者有保存資訊內容之能力。

網路服務提供者提供使用者資料、通聯紀錄等資料，雖能提供相當的助益，但前述資料的功用仍侷限於提供偵查人員清查過濾行爲人身份及研擬偵查作爲之

用；對於案件偵查而言，能否取得犯罪的直接證據（亦即網路上的犯罪資訊），例如張貼網路色情或網路援交等訊息之內容，才是案件能否偵破的關鍵。然而，網路犯罪案件受理時間與實際發生之時間往往有差距，偵查人員受理案件後，若無法在第一時間取得該違法內容，除非行爲人係連續或持續進行犯罪行爲，偵查人員有第二次之蒐證之機會，否則日後可能因無法再取得該犯罪內容，而無法續行偵查。因此，網路服務提供者如能自動保存該違法證據，並主動提供給偵查人員辦案參考，將可減少偵查時程，有效提昇偵破率。

3.4.6 協助實施通訊監察

犯罪案件偵查過程中，實際蒐證作爲會因受理案件時，案件本身是否已經完成或仍持續進行有所不同，通常對於已經完成犯罪行爲之案件（稱之「死案」）類型，因爲沒有對之實施任何蒐證行爲之需要，偵查人員只要向網路服務提供者調閱通聯紀錄、犯罪內容等等資料，即足以進行後續偵查作爲。相反地，仍持續進行之案件（稱之「活案」），偵查人員必須實施積極的偵查作爲，以蒐集其他犯罪之證據。而各種偵查作爲中，最有效的手段便是利用實施網路通訊監察取得犯罪行爲人之犯罪證據，然而無論是截取電子郵件或是監錄瀏覽紀錄，偵查人員均須透過網路服務提供者之協助，才能鎖定受監察對象使用網路之節點或電子郵件帳號進行截錄，蒐集犯罪行爲人犯罪之證據。另外，實施通訊監察過程若截錄到經「加密」之電子郵件或通訊內容，偵查人員無法自行解密及判讀時，更是需要透過網路服務提供者協助提供解密金鑰或協助解讀，才能達到實施通訊監察的目的。

3.4.7 協助執行搜索、扣押

偵查人員執行網路犯罪之搜索扣押作爲時，在執行搜索涉嫌人之電腦部分，

由於會涉及行爲人之刑事責任，涉嫌人自然不會與偵查人員配合，因此偵查人員必須靠自己的本事去執行搜索。至於在搜索網路服務提供者部份，其性質係屬於第三人搜索，雖然偵查人員執行搜索時依法具有強制力，網路服務提供者不得拒絕，然而其所有伺服器內之資料多如牛毛；況且爲避免資料發生外洩情形，網路服務提供者通常會設定通行密碼或管理權限，此時若欠缺網路服務提供者配合，面對龐大的資料庫，偵查人員根本無從執行搜索作爲。縱使經執行搜索發現應扣押之物，偵查人員要如何進行查扣也是一大難題。因此若網路服務提供者能協助偵查人員過濾、搜尋，列印或儲存所擬搜索查扣之資料，偵查人員即可迅速順利完成執行搜索扣押作爲。

3.4.8 協助作證

對於網路案件偵查而言，網路服務提供者本身是最好的證人，因爲無論是取得之使用者資料、通聯紀錄，乃至實施通訊監察、搜索扣押等作爲，均須透過網路服務提供者之協助。因此，偵查人員取得前揭資料之過程是否係依法取得，取證過程有無任何違法情形，一旦被告或辯護人有所質疑，甚至對於所提供之資料正確與否、有無遭到刪除或更改，甚至行爲人是否確係透過網路服務者提供之服務從事犯罪行爲等實質事項，網路服務提供者在法庭上均可做爲偵查人員最有利之證人，使行爲人無法狡辯而只能伏首認罪。

3.4.9 協助數位鑑識的工作

網路服務提供者爲提供最好的服務品質、維護系統的穩定，會隨時進行系統之檢測及維護，因此擁有的豐富的網路人才。而從目前法院實際運作實務，行爲人及辯護人均會先針對程式問題提出質疑，例如主張偵查人員取得證據過程有瑕疵、取得之犯罪內容遭竄改或取得回復已刪除之資料並非文件原貌等程式問題，而程式問題一旦遭到質疑，法院通常會依職權或聲請針對相關犯罪之證據進行勘

驗或檢送鑑定機構進行鑑識，然而由於國內欠缺專門職司數位鑑識之政府機構，專業鑑識人才又明顯不足，因此網路服務提供者若能提供協助數位資料鑑識之工作，既可解決鑑識機構及人力不足之問題，亦可順利完成數位鑑識，做爲法庭證據之目的。

4 我國法制關於網路服務提供者協助偵查責任規定

4.1 現行法制介紹

前章探討網路服務提供者協助網路偵查之事項，已約略說明網路服務提供者可以協助之事項，包括主動過濾、主動刪除或阻斷資訊、主動舉報、儲存提供使用者資料及通信紀錄、自動保存及主動提供證據、協助實施通訊監察、協助執行搜索扣押、協助作證及協助數位鑑識的工作等九項協助內容。然而，由於我國有關網路服務提供者是否有協助偵查的責任或義務，協助事項及範圍爲何等等，尚未有統一之法規，而係散見在電信法、通訊保障及監察法等不同法規，而不易依法規內容逐一說明。因此，本研究爲求能完整說明現行法制關於網路服務提供者協助偵查之規定，以下謹以各協助偵查事項爲標題，探討所涉及之相關法規規範。

4.1.1 主動過濾

網路資訊的傳輸原理，是使用者將訊息透過網路服務提供者之伺服器傳遞出去予特定人或不特定人接收，因此網路犯罪行爲人實施犯罪行爲必須透過網路服務提供者所提供之服務才有可能實現犯罪。例如網路販售大補帖違反著作權之行爲或在網路上散佈援交之訊息等等，無論是張貼在網頁或是以電子郵件傳遞，均須經由網路服務提供者伺服器。因此，若網路服務提供者若能採取主動過濾方式，不定時對於上載或傳輸之資料進行檢查，一旦發現任何犯罪訊息，立即從源頭阻絕犯罪資訊之散佈或張貼，將可有效的降低網路犯罪發生率。惟我國現行法規並無任何要求網路服務提供者應主動過濾網路上違法內容之規定。

不過，由於商業電子郵件濫發的問題日益嚴重，除了導致收信人必須付出相當時間刪除不當的電子郵件及阻礙重要郵件之接收；另外，由於大量商業電子郵件之濫發，容易造成網路容量之壅塞，使得電子郵件服務提供者必須耗費龐大人力、物力處理。因此，爲解決濫發商業電子郵件嚴重妨礙正常之通信服務及破壞社會大眾網路使用的環境，交通部電信總局遂草擬「濫發商業電子郵件管理條例草案」[92]送立法院審議，企圖以法律規定抑制商業電子郵件濫發之現象。同時，爲督促電子郵件服務提供者配合達到有效管制的目的，該法第六條規定「主管機關得促使電子郵件服務提供者採行必要措施，防止濫發商業電子郵件之行爲」。所謂「必要措施」依該條立法說明係指「相關防制濫發之技術與過濾機制」，換言之，電子郵件服務提供者依該規定負有過濾及防止濫發商業電子郵件之責任。

另外，行政院新聞局爲解決網際網路不妥內容對青少年身心造成不良影響之問題，期透過網路業者自律，落實網站內容過濾、分級及標示制度，依兒童及少年福利法第二十七條第三項之規定[93]，於民國九十三年四月二十六日公佈「電腦網路內容分級處理辦法」，要求網路服務提供者擔負過濾內容並分級之責任。前揭辦法將網路服務提供者區分爲網際網路連線服務提供者、網際網路平臺提供者及網際網路內容提供者三種，並加諸不同的過濾、分級之義務。惟由於電腦網路分級之相關準備措施，尚需民間推動委員會之成立及推動，相關硬體之設置與軟體之配合開發等，亦需一段籌備時間，因此該辦法第十條規定「電腦網路服務提供者應自本辦法施行之日起十八個月內，完成電腦網路分級之相關準備措施，並

---

[92]參閱交通部電信總局全球資訊網，網址：http://www.dgt.gov.tw/chinese/ncc/mail-requlation/ncc-mail-requlation.htm。最後瀏覽日期：二〇〇五年七月二十三日。

[93]兒童及少年福利法第二十七條規定：「出版品、電腦軟體、電腦網路應予分級；其他有害兒童及少年身心健康之物品經目的事業主管機關認定應予分級者，亦同。前項物品列爲限制級者，禁止對兒童及少年爲租售、散佈、播送或公然陳列。第一項物品之分級辦法，由目的事業主管機關定之」。

進行分級。期限屆至前，應依台灣網際網路協會訂定之網際網路服務業者自律公約。」換言之，目前網路服務提供者係依台灣網際網路協會訂定之網際網路服務業者自律公約[94]之規定，採用內容過濾或身分認證等措施機制，防制兒童或少年接取不良之資訊。

4.1.2 刪除或阻斷資訊

網路服務提供者目前依現行法令，雖尚未負有主動過濾之義務，惟若網路服務提供者主動發現或經第三人（包括主管機關、偵查單位）通知使用者張貼或傳遞之意見、資訊涉有違法情事時，如能迅速予以刪除或阻斷該違法之資訊，對於防止網路犯罪案件發生，亦可產生極大的功用。我國現行法令規定網路服務提供者負有刪除或阻斷資訊之義務，主要爲電信法第八條及第二十二條之規定，分述如後：

4.1.2.1 阻斷資訊（停止用戶網路服務）

我國目前要求網路服務提供者知悉使用者傳遞違法資訊，主動停止或經第三人要求停止用戶之網路服務，係依據我國電信法第八條第二項規定，該條規定「以提供妨害公共秩序及善良風俗之電信內容爲營業者，電信事業得停止其使用」，此條文賦予電信業者得以停止提供以妨害公共秩序及善良風俗內容爲營業之用戶（例如提供色情資訊營利的用戶）之虛擬主機租用、連線等網路服務之權利。另外，電信法第二十二條規定「電信事業非依法律不得拒絕電信之接受與傳遞。但對電信之內容顯有危害國家安全或妨礙治安者，得拒絕或停止其傳遞。」，亦賦予電信業者對於有危害國家安全或從事販售槍毒違禁品等妨礙治安

[94]參閱台灣網際網路協會全球資訊網，網址：http://www.twia.org.tw/p02-self-policing.htm。最後瀏覽日期：二〇〇五年七月二十三日。

之違法內容，有停止並拒絕對該用戶繼續提供網路連線、e-mail 等服務之權利[95]。

惟無論是依電信法第八條第二項或是第二十二條之規定，均係賦予電信業者「得」停止服務之權利，而非「應」停止提供之義務[96]。再加上前述條文適用前提，均須符合「以提供妨害公共秩序及善良風俗內容爲營業」或「顯有危害國家安全或妨礙治安」之要件，然而前述要件均屬於「不確定的法律概念」，電信業者是否有能力認定，實有疑問。更何況，若發生認定有誤而善意停止用戶網路服務，致違反與用戶間之網路服務契約義務，依前述條文均未有任何免責之規定，以致業者欠缺配合執行阻斷違法資訊傳遞之意願。目前網路服務提供者均是透過與用戶簽訂網路服務契約方式，約定網路服務提供者得片面停止服務之契約條款[97]，惟一旦發生爭議，該契約所約定之免責條款，能否做爲網路服務提供者主張免責之依據，仍值得商榷。

4.1.2.2 刪除違法資訊

I 「主動」刪除違法資訊

網路服務提供者知悉用戶透過其提供服務傳遞違法訊息時，是否負有「主動」刪除或移除該資訊之義務，依目前法令並無任何明文規定。換言之，網路服務提供者，依現行法令並不負有主動刪除或移除違法資料之義務。更何況，網路

---

[95]參閱張雅雯著，網際網路連線服務提供者就網路內容之法律責任（下），資訊法務透析，一九九八年六月，第二十二頁。

[96]參閱周慧蓮著，「電信法中關於網際網路服務提供者權義規範簡析」，科技法律透析，二〇〇四年八月期，第十二至十四頁。

[97]依數位聯合電信股份有限公司網際網路連線服務租用契約條款 〈個人 ADSL〉第十條規定「用戶應遵守網際網路國際使用慣例，不得有入侵網際網路上其他系統之意圖與行爲；不得破壞網路上各項服務亦不得在網際網路上以任何方式發送大量郵件造成本公司系統之障礙或從事違反公共秩序、善良風俗、及法律所禁止之行爲。如有違反，除須自行負責外，本公司爲維護服務品質，依網際網路國際應用慣例，得終止用戶之租用，任何後果及可能損失概由用戶自行承擔・・・・・」。網址：http://service.seed.net.tw/adslrule.shtml。最後瀏覽日期：二〇〇五年七月

上傳遞之資訊違法與否，非網路服務提供者所能認定，且貿然刪除用戶之資訊又恐有侵害使用者言論自由與違反網路服務契約義務之賠償等等問題[98]，使得網路服務提供者更無法配合之意願。目前電信業者係透過網路服務契約與用戶約定方式，一方面達到刪除違法資訊之目的，另一方面排除其可能應負之損害賠償責任[99]。惟一旦發生爭議，該契約所約定之免責條款，能否做爲網路服務提供者主張免責之依據，仍值得商榷。

II 「被動」刪除違法資訊

網路服務提供者是否負有「被動」刪除違法內容之義務，依前揭行政院新聞局九十三年四月二十六日公佈「電腦網路內容分級處理辦法」第八條之規定「電腦網路服務提供者經政府機關或其委託之機構告知電腦網路內容違法或違反本辦法規定者，應爲其他限制兒童及少年接取、瀏覽之措施，或先行移除」，依從該規定，網路服務提供者經政府機關或其委託之機構告知電腦網路內容違法或違反該辦法規定之情形下，負有「被動」將該違法資訊移除之義務。惟本條文未有任何免責之規定，且本辦法之位階僅爲法規命令，網路服務提供者一旦接受告知而移除使用者所傳輸之資訊，仍有可能會侵害到使用者之隱私權或負擔違反契約之賠償等問題。

4.1.3 儲存、提供使用者資料及通信紀錄

網路服務提供者儲存、提供使用者資料及通信紀錄之法律依據，係依據電信

二十三日。

[98]參閱張雅雯著，同前註 94 揭書，第二十三頁。

[99]依 Yahoo!奇摩服務條款第十六條規定「‧‧Yahoo!奇摩並未針對「會員內容」事先加以審查，但 Yahoo!奇摩有權（但無義務）依其自行之考量，拒絕或移除經由本服務提供之任何「會員內容」。在不限制前開規定之前提下，Yahoo!奇摩及其指定人有權將違反本服務條款和令人厭惡之任何「會員內容」加以移除‧‧」，網址：http://tw.yahoo.com/info/utos.html。

法第七條之規定「電信事業或其服務人員對於電信之有無及其內容，應嚴守秘密，退職人員，亦同。前項依法律規定查詢者不適用之；電信事業處理有關機關(構) 查詢通信紀錄及使用者資料之作業程式，由電信總局訂定之・・・・・・」及第二類電信事業管理規則第二十七條第一項之規定「經營者對於調查或蒐集證據，並依法律程式查詢電信之有無及其內容者，應提供之」。惟前揭條文適用前提均必須符合電腦處理個人資料保護法第二十三條第一款「爲增進公共利益者」及第三款「爲防止他人權益之重大危害而有必要者」，且在有必要之情況下，電信業者始可提供偵查人員用戶之個人資料及通信紀錄。至於具體的查詢辦法及儲存及提供的事項茲分述如後。

4.1.3.1 儲存及提供使用者資料

電信業者儲存使用者資料之規定，爲第二類電信事業管理規則第二十七條第四項及第五項規定，該條第四項規定「經營者應核對及登錄其用戶之資料，且虛擬行動網路服務經營者應於二日內載入經營者之系統資料檔存查，並至少保存至服務契約終止後一年；有關機關依法查詢時，經營者應提供之；以預付卡或期他預付資費方式經營虛擬行動網路服務者，亦同。」第五項則規定「前項用戶之資料包括使用者姓名、身分證統一編號及住址等資料，且虛擬行動網路服務經營者另應包括所指配號碼。」

至於調閱使用者資料之具體作業程式，則依據交通部電信總局公佈之「電信事業處理有關機關 (構) 查詢電信使用者資料實施辦法」，依該辦法第四條規定「使用者資料，係指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爲限。前項所稱電信號碼，係指電話號碼或用戶識別碼」。調閱的條件依該辦法第三條第一項規定「下列情形得依法向電信事業查詢使用者資料：只有在下列情形得依法向電信事業查詢使用

者資料：一、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。二、其他政府機關因執行公權力所需者。三、與公眾生命安全有關之機關（構）爲緊急救助所需者。」實際調閱的方式則依該辦法第五條規定，偵查人員應備正式公文或電信使用者資料查詢單，載明需查詢之電信號碼或姓名及其身分證統一編號、電信服務種類、法律依據、案由說明、查詢案號、資料用途、查詢機關(構)、機關（構）主管、連絡人、連絡電話或傳真機號碼、機關（構）加蓋印信及其首長署名、職章等，送該電信使用者所屬電信事業指定之受理單位辦理。

4.1.3.2 儲存及提供國內通信紀錄

電信業者負有儲存及提供通信紀錄責任，係依第二類電信事業管理規則第二十七條第三項規定，依該項規定區分不同類型經營者課以不同保存通信紀錄之保存期間如下：

I 語音單純轉售服務通信紀錄應保存六個月。

II 網路電話服務通信紀錄應保存六個月。

III 網際網路接取服務：

i 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。

ii 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。

iii 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。

iv 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。

v 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應保存六個月。

vi 電子郵件通信紀錄應保存一個月。

vii 虛擬行動網路服務通信紀錄應保存六個月。

至於調閱通信紀錄之具體作業程式，則依「電信事業處理有關機關(構)查詢電信通信紀錄實施辦法」之相關規定，依該辦法第三條規定偵查人員調閱通信紀錄，亦必須備正式公文或附上電信通信紀錄查詢單，載明需查詢之電信號碼、通信紀錄種類、起迄時間、查詢依據或案號、資料用途、連絡人、連絡電話或傳真機號碼、及指定之列帳相關資料等，送該電話用戶所屬電信事業指定之受理單位辦理。

4.1.3.3 儲存及提供跨境連線通信紀錄

美國九一一事件後，我國為防範遭到恐怖份子侵襲，建構相關反恐怖作為及完備法律制度，以與世界各國建立反恐怖合作關係，法務部曾擬定「反恐怖行動法草案」[100]。該草案為防範恐怖份子對我國網路之攻擊、破壞、幹擾、入侵等作為，以及利用本國網路作為攻擊他國網路之跳板，於第七條規定為防範恐怖份子利用網際網路從事恐怖行動之目的，要求電信事業應使其通信系統之軟、硬體設備具有保存及提供網際網路跨境連線紀錄之功能；保存期限為九十日，必要時得延長一次等內容。惟該條規定要求電信事業保存及提供網路跨境連線通信紀錄，並非自動保存所有的通信紀錄，必須係經由治安機關通知有事實疑為恐怖份子利用網際網路從事恐怖行為之要件下，始就特定範圍之網際網路位址，保存網路跨

[100]「反恐怖行動法草案」相關條文參閱法務部主管法規資料庫查詢系統－法規草案，網址：http://mojlaw.moj.gov.tw/ShowScript.asp?id=2898。最後瀏覽日期：二〇〇五年七月二十三日。

境連線通信紀錄[101]，與前述第二類電信事業管理規則第二十七條係要求電信事業主動保存所有通信紀錄之方式不同。

另外，該草案第十七條並規定電信事業不配合之罰責，該條規定「電信事業無正當理由違反第七條第一項、第三項至第五項規定之一者，由交通部處新台幣五十萬元以上二百五十萬元以下之罰鍰；經通知改善而屆期仍不改善者，按日連續處罰，並得廢止其特許或許可。」該草案並對於保存及提供跨境連線通信紀錄，將電信業者建置及維護成本、建置的時程及罰責等事項均有明文規定，堪稱不錯之立法方式，惟迄今並未通過立法。

4.1.4 協助實施通訊監察

偵查人員實施網路通訊監察，無論是對於截錄電子郵件或是監看瀏覽紀錄，均須網路服務提供者之協助，目前要求網路服務提供者配合偵查人員實施通訊監察，係依據通訊保障及監察法第十四條之規定，依該條規定「電信事業及郵政機關（構）有協助執行通訊監察之義務，其通訊系統應具有配合執行監察之功能。協助執行通訊監察之電信事業、郵政機關（構）於執行後，得請求執行機關支付必要之費用。其費額由交通部會同內政部、國防部及法務部定之。」至於電信業者具體配合之義務，則是依據通訊保障及監察法施行細則第二十一條之規定，該條規定本法第十四條第二項之規定，包括應使其通訊系統之軟硬體設備具有配合

[101]該法草案第七條全文：「一、爲防制恐怖份子利用網際網路從事恐怖行動，電信事業應使其通信系統之軟、硬體設備具有保存及提供網際網路跨境連線紀錄之功能。二、前項所稱網際網路跨境連線通信紀錄，指網際網路資訊發送點至目的點之國際連線紀錄。三、第一項電信事業，應依法務部調查局所提網際網路連線通信紀錄之需求，擬訂所需軟、更體設備與該等設備建置時程、建置及維護費用之計畫，與該局協商確定後辦理建置；必要時，由交通部電信總局協助之。四、若有事實疑爲恐怖份子利用網際網路從事恐怖行爲時，電信事業應依治安機關之要求，就特定範圍之網際網路位址，保存及提供網際網路跨境連線通信紀錄。五、前項通信紀錄之保存期限爲九十日，必要時，得延長之，其延長期間不得逾九十日，並以一次爲限。六、電信事業爲執行第一項業務所需軟、硬體設備建置及維護費用，應由法務部調查局編列預算支應。」

執行通訊監察時所需之功能，並於執行機關執行通訊監察時予以協助，必要時並應提供場地、電力及相關介接設備等等配合事項。

交通部電信總局爲因應網路科技的發展及配合網路犯罪偵查之需要，並於九十三年七月二十二日另增加下列幾項通訊監察之項目[102]：

I　網路電話服務

網路電話服務中提供 PC to Phone 或 Phone to PC 服務者（即除 PC to PC 服務者外），需能自業者設備端（如 TDM Switch 或 VoIP Gateway），將依通訊監察法特定之監察對象於通訊監察書許可期間內通話內容、時間及傳送路徑紀錄儲錄或轉送至通訊監察機關[103]。

II　語音單純轉售服務

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

III　電子郵件服務

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

雖然依前揭函文，要求網路服務提供者配合實施通訊監察之項目已經包括網路電話、語音單純轉售服務及電子郵件收、送內容等等，惟實務上網路服務提供

---

[102]參閱交通部電信總局九十三年七月二十二日電信公字第 09305065320 號函。

[103]交通部電信總局公告應配合辦理通訊監察之業別後，警調單位已開始與相關業者進行洽談通訊監察設備建置事宜。惟由於通訊監察技術多掌握於國外科技先進國家，部分規模較小之網路電話業者因技術取得困難且無足夠人力、財力因應通訊監察規劃工作，於是網路電話互聯互通聯盟應業者反映，決定主動發起網路電話通訊監察機制之研發，並計畫由台灣網路資訊中心擔任計畫之執行單位，期以研擬提出一通訊監察需求統籌處理之集中式因應方案，供警調單位作爲通訊監察設備建置事宜之參考。參閱交通部電信總局全球資訊網，網址：http://www.dgt.gov.tw/chinese/News-press/94/press-dgtnews-940429.shtml。最後瀏覽日期：二〇〇五年七月二十三日。

者實際配合實施通訊監察的項目，仍僅侷限於協助監看電子郵件及上網瀏覽之紀錄，對於日益盛行的即時通訊、網路電話等屬於點對點的通訊方式，業者並無法協助實施通訊監察。

4.1.5 協助執行搜索、扣押

I　協助執行搜索

偵查人員執行搜索的對象若爲涉嫌人所有之電腦時，因涉嫌人享有「不自證已罪原則」[104]之權利，有權及當然拒絕配合偵查人員之搜索扣押作爲。因此此處探討協助執行搜索之內容，係指當網路服務提供者並非涉嫌人，但偵查人員有執行搜索網路服務提供者所有網路伺服器必要時，網路服務提供者是否負有配合偵查人員之義務。依我國目前法令，偵查人員執行搜索作爲之法律依據爲刑事訴訟法第一百二十二條至第一百三十二條之一等規定，同法第一百三十二條並賦予偵查人員於執行搜索時具有其強制力，使受搜索人不得抗拒偵查人員之執行搜索作爲。惟偵查人員執行搜索雖具有其強制力，但是由於網路服務提供者所有之伺服器內之資料繁多，包括執行對象及非執行對象之資料，以致偵查人員實際執行搜索時，不僅難以蒐尋到執行的標的，反而容易侵害到非執行對象的隱私權。更何況業者爲避免所擁有之資料外洩或遭竊取，通常會有設定通行密碼或管理權限等等措施，此時若無網路服務提供者的配合，偵查人員根本無法進入系統中，更遑論能順利完成搜索作爲及查扣應扣押之證據。惟依目前法令，並無要求網路服務提供者協助偵查人員搜索之義務。

---

[104]所謂「不自證已罪原則」，依美國聯邦憲法第五增修條文之規定，係指「不得強制任何人在刑事案件中爲不利已之證人」，違反該條款所取得之證據，應適用證據排除法則予以排除。參閱林輝煌著，「論證據排除－美國法之理論與實務」，九十三年九月初版，第一〇二頁。

在執行網路搜索作爲中，最具爭議性的問題應屬「網路服務提供者能否同意搜索的問題」，因爲偵查人員執行搜索的對象雖然係網路服務提供者所有之伺服器，然而該伺服器內儲存的資料卻爲用戶所有，因此網路服務提供者是否有權同意偵查人員執行搜索，猶如房東對於房客之房間有無同意搜索之權利一般是有疑義。有學者[105]認爲對大眾提供服務之電腦網路系統，依我國電信法第六條之規定，電信事業應採取適當及必要措施，以保障其處理通訊秘密，因此無權就用戶使用該網路系統之電子檔爲同意搜索，亦即該電腦系統網路管理者不能就用戶之「電子郵件」爲同意搜索。

然而，網路服務提供者若不享有同意搜索之權利，若偵查人員採取聲請搜索票之程式，向法院聲請搜索票執行有票搜索方式，又恐所擬執行的標的（電子檔案）於執行有票搜索前遭涉嫌人刪除之危險，例如用戶在執行搜索前刪除原儲存於郵件伺服器之電子郵件，導致執行搜索作爲徒勞無功。爲解決此一問題，美國司法部所訂定「關於電腦之搜索、扣押之聯邦準則」(FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS ）[106]中關於同意搜索（CONSENT SEARCHES ）之規定中，即建議偵查機關在選擇申請搜索票方式時，爲避免執行搜索前執行對象會刪除相關犯罪資訊，偵查機關應該考慮要求網路系統操作者就系爭檔案製作備份並加以保留，以保全相關之證據，便於取得搜索票時得以順利取得該電子郵件[107]。

II 協助執行扣押

偵查人員執行扣押作爲，係依據刑事訴訟法第一百三十三條之規定，該條規

---

[105]參閱王銘勇著，同前註 8 揭書，第二五三至二五四頁

[106]參閱網址http://www.usdoj.gov/criminal/cybercrime/search_docs/sect2.htm#E.2.e。最後瀏覽日期：二〇〇五年七月二十三日。

定「對於可爲證據或得沒收之物，亦得扣押之。對於應扣押的所有人、持有人或保管人，得命其提出提出或交付。」因此，偵查人員執行搜索時若蒐獲可爲證據之搜索標的，可逕自扣押之，不容網路服務提供者有置喙餘地。惟偵查人員若無法蒐獲，卻確信網路服務提供者所有伺服器內有保留可爲證據之資料時，亦可依該條第二項規定要求網路服務提供者配合提出或交付該等證據；另外，同法第一百三十八條規定，網路服務提供者無正當理由而拒絕提供或交付時，偵查人員也可用強制力扣押之。從前揭條文之文義解釋來看，立法者似乎有意加諸網路服務提供者協助執行扣押之義務，然而前揭條文之適用前提，必須在偵查人員擁有相關事證足以證明網路服務提供者所有伺服器內確有可爲證據之資料，而無正當理由拒絕提供之情形，否則網路服務提供者縱使不配合提出或交付時，本研究認爲並不違反前述條文之規定，偵查人員不宜貿然施以強制力強行執行扣押。

4.1.6 協助作證

網路服務提供者本身對於網路案件偵查而言，不論是程式或是實質方面均是偵查單位最有利的證人，因爲網路服務提供者可以在法庭上證明偵查人員取得證據之合法性，亦可提昇法庭引用證據之證據能力及證明力。目前網路服務提供者負協助作證的義務，係依刑事訴訟法第一百七十六條之一規定，該條規定「除法律另有規定外，不問何人，於他人之案件，有爲證人之義務。」，因此除非網路服務提供者與網路犯罪嫌疑人間具有一定的身份或關係，得依同法第一八〇條[108]

---

[107]同前註 104。

[108]刑事訴訟法第一百八十條規定：「證人有下列情形之一者，得拒絕證言：一、現爲或曾爲被告或自訴人之配偶、直系血親、三親等內之旁系血親、二親等內之姻親或家長、家屬者。二、與被告或自訴人訂有婚約者。三、現爲或曾爲被告或自訴人之法定代理人或現由或曾由被告或自訴人爲其法定代理人者。對於共同被告或自訴人中一人或數人有前項關係，而就僅關於他共同被告或他共同自訴人之事項爲證人者，不得拒絕證言。」

及第一八一條[109]規定選擇拒絕證言之情形外，網路服務提供者負有作證之義務。

4.1.7 協助數位鑑識

網路服務提供者爲提供使用者完善的服務品質及維護系統的穩定與安全，均會延攬眾多網路相關專業的人才。這些擁有網路專業知識之人才，如能協助法院進行數位資料鑑定工作，例如協助鑑定引爲證據之電磁紀錄有無遭到更改及協助電磁紀錄的內容判讀，進而提供鑑定報告予法院，有助於法官認定數位證據之證據能力及證明力，該鑑定報告本身並可做爲法院裁判之依據。然而，依我國現行法令，網路服務提供者並未負有協助鑑定之義務，因爲刑事訴訟法第一百九十七條至二百十一條雖規定鑑定人的資格應係「就鑑定事項有特別知識經驗」或「經政府機關委任有鑑定職務」之機構、機關或個人，惟並未規定具有資格之鑑定人一經法院選任即負有鑑定之義務，因此網路服務提供者雖擁有充足的專業人才，具有數位證據鑑定之資格，依現行法令仍不能認爲負有協助數位鑑識之責任。

4.2 現行法制檢視

前節已說明網路服務提供者可提供協助的事項包括主動過濾、主動刪除或阻斷資訊、主動舉報、儲存提供使用者資料及通信紀錄、自動保存及主動提供證據、協助實施通訊監察、協助執行搜索、扣押、協助作證、協助數位鑑識的工作等，然而檢視我國現行法令，雖然關於主動刪除或阻斷資訊、儲存提供使用者資料及通信紀錄、協助實施通訊監察、協助作證等事項已有相關規定，卻有規範對象狹隘、侵害隱私權等等缺失；另外，關於主動過濾、主動舉報、自動保存及主

[109]刑事訴訟法第一百八十條規定：「證人恐因陳述致自己或與其有前條第一項關係之人受刑事追訴或處罰者，得拒絕證言。」

動提供證據等協助事項，以及協助偵查所涉及之成本補助、責任免除、行政檢查、罰責、保密規定等均未有任何規定，均爲現行法制所不足之處。

4.2.1 規範對象過於狹隘

4.2.1.1 第二類電信事業管理規則之規範對象

我國目前法令關於網路服務提供者爲配合偵查人員偵查網路犯罪，負有儲存或提供使用者資料、通聯紀錄等義務，係依據第二類電信事業管理規則第二十七條之規定，惟該條規範對象爲「經營者」，而「經營者」之定義，同辦法第二條規定「係指經交通部電信總局許可並發給執照經營第二類電信事業者」。至於第二類電信事業之意義，由於第二類電信事業管理規則係依據電信法第十七條第二項授權訂定，因而必須回歸電信法的規定加以探討。根據電信法第二條之規定，「電信事業」是指經營電信服務供公眾使用之事業；而電信事業之分類依電信法第十一條規定，採取電信事業設置電信相關設備之有無之標準，區分爲第一類電信事業及第二類電信事業[110]。前者之設立要件，依據電信法第十二條規定，必須先依公司法設立之股份有限公司，且應經交通部特許並發給執照後，始得營業；後者之設立要件，依電信法第十七條規定，應向交通部電信總局申請許可，經依法辦理公司或商業登記並發給許可執照，始得營業。換言之，電信法所稱之「電信事業」，共可區分爲兩種類型：第一類電信事業，必定是「股份有限公司」。二、第二類電信事業，必定是「已辦理公司或商業登記的單位」。綜上分析，第二類電信事業管理規則第二十七條規定所指之「經營者」，僅侷限於「已辦理公

[110]電信法第十一條規定「電信事業分爲第一類電信事業與第二類電信事業。第一類電信事業指設置電信機線設備，提供電信服務之事業。前項電信機線設備指連接發信端與受信端之網路傳輸設備、與網路傳輸設備形成一體而設置之交換設備、以及二者之附屬設備。第二類電信事業指第一類電信事業以外之電信事業。」

司或商業登記」之第二類電信事業[111]。

4.2.1.2 通訊保障及監察法之規範對象

網路服務提供者協助偵查人員實施網路通訊監察，對於犯罪證據之蒐集有極大的幫助，至於其法律依據係依通訊監察保障及監察法第十四條之規定，該條規定「電信事業及郵政機關 (構) 有協助執行通訊監察之義務，其通訊系統應具有配合執行監察之功能。」同法第三十一條並規定不予配合之行政罰責，該條規定「有協助執行通訊監察義務之電信事業及郵政機關 (構) ，違反第十四條第二項之規定者，由交通部處以新台幣五十萬元以上二百五十萬元以下罰鍰；經通知限期遵行而仍不遵行者，按日連續處罰，並得撤銷其特許或許可。」從前揭條文之文義分析，負有協助實施通訊監察之對象限於「電信事業」或「郵政機關」。

由於通訊保障及監察法本身對於電信事業並未給予任何定義，因此應回歸電信法之相關規定，亦即通訊保障及監察法適用對象根據電信法第二條之規定，包括第一類電信事業及第二類電信事業，而前者設立要件，依據電信法第十二條規定，必須先依公司法設立之股份有限公司，且應經交通部特許並發給執照後，始得營業；後者之設立要件，則依電信法第十七條規定，應向交通部電信總局申請許可，經依法辦理公司或商業登記並發給許可執照，始得營業。換言之，通訊保障及監察法所稱之「電信事業」，如歸屬於第一類電信事業，必定是「股份有限公司」；如歸屬於第二類電信事業，必定是「已辦理公司或商業登記的單位」。

4.2.1.3 「電信事業」定義無法涵蓋網路服務提供者

電信法、第二類電信事業管理規則或通訊保障及監察法所規範的對象「電信事業」，其地位不是「股份有限公司」，就是「已辦理公司或商業登記之單位」。

---

[111]參閱蔡美智著，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，一九九九年十二月，第四十三至第四十五頁。

惟觀察我國偵查單位實際進行網路犯罪偵查之現況，無論是調閱使用者資料、通聯紀錄或是實施通訊監察，均需要各類網路服務提供者之協助。這些提供協助偵查之網路服務提供者，包括學校、圖書館、私人網站站主、網路咖啡店及非屬電信事業的機構等，由於這些網路服務提供者的規模有大有小，不一定都會辦理公司或商業登記，而不符合前揭電信事業之定義。更遑論學校、圖書館等公益機構，均係提供免費的網路服務，不會也不能辦理公司或商業登記，更是無法歸屬於電信事業的範疇。縱使是有公司或商業登記的機構，包括紡織公司、塑膠公司、網路銀行等，其營業項目並非「經營電信服務供公眾使用之事業」，亦無法認定新爲電信法所稱之電信事業。

有學者甚至明確指出，最嚴重的問題是出現在我國三大網路之一的台灣學術網路（Taiwan Academic Network；簡稱 TANET），按網路犯罪行爲人可能會透過台灣學術網路提供之服務進行網路犯罪，惟偵查單位若基於偵查犯罪之需要，向台灣學術網路調閱相關之通信紀錄或於網路上進行網路監聽時，礙於現階段台灣學術網路之地位屬於教育部所有之實驗網路，而不屬於電信法所稱的電信事業。並且，教育部本身是一個機關，但從電信法對於電信事業的定義來看，電信事業絕對不可以是「機關」，而必須是「股份有限公司」，因此即使台灣學術網路向交通部電信總局申請，也不可能拿到電信事業的執照。對於網路偵查而言，在台灣學術網路的網路犯罪有可能成爲日後偵查最大的盲點所在[112]。

4.2.1.4 規範對象狹隘之影響

I　非「電信事業」者不負有協助偵查之義務

私人網站、學校、網路咖啡店、圖書館及非電信事業機構，雖具有提供網路

[112]同前註。

服務的地位，均有提供網路相關之服務，對於網路偵查亦能提供相當的協助，但是因欠缺公司或商業登記或係非經營電信服務供公眾使用之事業，而不符合電信法與通訊保障及監察法對於「電信事業」的定義，自然無須根據前揭條文負有協助偵查之義務。因此，就目前相關法令而言，該等網路服務提供者無須負儲存及提供使用者資料、通訊紀錄等資料之義務，對於偵查單位在偵查網路犯罪時所提出協助實施通訊監察之要求，亦因無配合之義務而可拒絕提供協助。

II　非「電信事業」者無法適用免責規定

人民享有秘密通訊自由不受非法侵害之權利，依通訊保障監察法第二十四條規定違法監察他人通訊者，可處五年以下有期徒刑。由於「電信事業」協助偵查人員實施通訊監察，其性質上屬於監察他人的秘密通訊，而有侵害隱私權及違反通訊保障及監察法之情形，因此為使電信事業能放心配合協助偵查，通訊保障及監察法特於第二十九條規定幾項免責之事由，該條規定「監察他人之通訊，而有下列情形之一者，不罰：一、依法律規定而為者。二、電信事業或郵政機關 (構) 人員基於提供公共電信或郵政服務之目的，而依有關法令執行者。三、監察者為通訊之一方或已得通訊之一方事先同意，而非出於不法目的者。」惟本條適用前提係指「電信事業」配合協助偵查人員實施通訊監察之情形，非屬電信事業之其他各類網路服務提供者並無適用本條免責規定之餘地，致使其等懼於動輒觸法及避免事後遭致賠償等問題而欠缺配合意願。

4.2.2 侵害隱私權

4.2.2.1 隱私權的意義

隱私權的概念係源自於英美法系之侵權行為法，其主要涵義係指個人有決定其想法、感覺以及情緒如何表達之自由。揭露他人之隱私者，縱無惡意或揭露之

事爲事實，也無法作爲免責之抗辯。顯見隱私權與自我尊嚴及自主決定有密切的關聯[113]。在美國法院在判決中，對於隱私權引用最多的定義是：「隱私權，個人人格上之利益，不受不法之僭用或侵害，其與公眾無合法關聯之私事，不得妄予發布公開，而其私人之活動，不得以可能造成一般人精神痛苦或感覺羞辱之方式非法入侵之權利也。」簡言之，就是「不受幹擾」、「保持孤獨之權利（the right to be let alone」[114]。而隱私權的分類，美國賓州 (Pennsylvania)大學法學院學者 Anita Allen 則將之歸納爲下列四類；一、資訊隱私權(information privacy)；指一個人可以自行決定何時、以怎樣的方式，將有關個人資訊公開的權利；二、身體隱私權(physical privacy)；指一個人有排除他人接近個人身體或侵入個人生活空間的權利；三、自主決定隱私權(decisional privacy)；指一個人有不受政府或第三人干涉個人抉擇的權利；四、具財產價值之隱私權(proprietary privacy)；指個人對於隱私權中人格權利益的經濟利用及所有權[115]。

4.2.2.2 資訊隱私權的意義

所謂「資訊隱私權」，有學者認爲係指「非侷限於不讓他人取得我們的個人資訊，而是應該擴張到由我們自己控制個人資訊的使用與流向」[116]；有學者認爲其意義係指「在沒有通知當事人並獲得其書面同意之前，資料持有者不可以將當事人爲某特定目的所提供的資料用在另一個目的上」[117]；另有學者則認爲資訊隱

---

[113]參閱江國慶著，「由電子郵件隱私權探討隱私權與科技監視」，美國資訊通信法案例評析 1991~2002 案例精選，第三〇一頁。

[114]參閱蔡碧玉著，「從偷拍事件談隱私權保護之刑事立法」，法令月刊，第四十九卷第四期，八十七年四月，第二十頁以下。轉引自許文義著，「個人資料保護法論」，九十年一月初版，第五十三頁。

[115]參閱謝穎青著，「建構新世代網路交易安全之新規範－人性尊嚴與商業利益孰終擅場」，二〇〇三年十二月十六日，太穎國際法律事務所全球資訊網，網址；http://www.elitelaw.com。最後瀏覽日期：二〇〇五年七月二十三日。

[116]參閱劉靜怡著，「資訊科技與隱私權焦慮」，當代雜誌第一二四期，第八十頁。

[117]參閱王鬱琦著，「網路上的隱私權問題」，資訊法務透析，八十八年十月，第三十九頁。

私權具有積極性，有別於古典隱私權僅具消極防禦性質者，資訊隱私權具有「免於資料不當公開之自由」或「對自己之資料之蒐集、輸入、累積、流通、使用，有完全決定及控制之權利」[118]。綜上定義可知，資訊隱私權比隱私權更具有積極性，至於在實際網路通訊上上，資訊隱私權保護的客體約略可分爲四個面向[119]：

I　個人屬性的隱私權 (Privacy of a Person's Persona)

個人屬性的隱私權內容，係指包括一個人的姓名、身份、肖像、聲音等直接涉及個人領域之第一層次，而可謂「直接」之個人屬性，爲隱私權保護之首要對象。

II　個人資料的隱私權 (Privacy of Data about a Person)

當個人屬性被抽離成文字之描述或記錄，如個人的消費習慣、病歷、宗教信仰、財務資料、工作、前科等紀錄，若其指涉之客體爲獨一且個人化(unique and personal)，則此等資料即含有高度之個人特性而常能辨識該個人之本體，此可謂「間接」之個人屬性而亦應以隱私權加以保護。

III　通訊內容的隱私權(Privacy of a Person's Communications)

個人之思想與感情，原本存於其內心之中，不易爲人所辯識；惟當與外界藉由電子通訊媒介（如網路）溝通時，即易於暴露於他人之窺探之下，故此通訊內容亦應加以保護，以助成個人人格之完整發展。

IV　匿名之隱私權 (Anonymity)

匿名發表在歷史上一直都扮演著重要的角色，這種方式常可以保障讓人願意

---

[118]參閱許文義著，「個人資料保護法論」，九十年一月初版，第五十三至五十四頁。
[119]參閱 Thomas F. Smedinghoff（editor）,ONLINE LAW，第二六九至二七〇頁，轉引自前註書第五十五至五十六頁。

對於社會制度提出一些批評。畢竟，群體生活中，集體之價值未必與個人之想法相符，此種落差常易引發個人以匿名方式表達其意見之需求。此種匿名權利之適度容許，常能鼓勵個人之參與感，並保護其自由之創造力空間；而就群體而言，亦常能藉之收真知直諫之效，而得進步之動力。

4.2.2.3 我國資訊隱私權之法律保障

I 憲法層次

憲法第十二條規定「人民有秘密通訊之自由」，賦予人民享有以秘密方式傳達訊息，而不受公權力或私人之侵犯之基本人權，傳遞訊息的方式則包括傳統的郵件、電話、傳真及電子郵件各種類型。此處所指的秘密通訊自由應包含『保障通訊的自由』及『秘密的自由』兩種涵義，前者係指不受國家公權力及經營通訊業者的任何妨害；後者則指享有隱密通訊內容的權利[120]，換言之，不論誰和誰間有無通訊、通訊起迄、通訊時間長短及通訊內容均屬受保障之隱私。

II 法律層次

在法律層次關於保障使用者秘密通訊自由之主要規定如後：

i 電信法第二十二條

電信法第二十二條規定，依該條規定「電信事業非依法律，不得拒絕電信之接受及傳遞。但對於電信之內容顯有危害國家安全或妨害治安者，得拒絕或停止其傳遞」。

ii 電信法第六條

電信法第六條規定「電信事業及專用電信處理之通信，他人不得盜接、盜錄

[120]參閱謝瑞智著，「憲法新論」，二〇〇〇年二月增訂版，第二六三至二六四頁。

或以其他非法之方法侵犯其秘密。電信事業應採適當並必要之措施，以保障其處理通信之秘密」。

iii 電信法第七條

電信法第七條規定「電信事業或其服務人員對於電信之有無及其內容，應嚴守秘密，退職人員，亦同。前項依法律規定查詢者不適用之；電信事業處理有關機關 (構) 查詢通信紀錄及使用者資料之作業程式，由電信總局訂定之」。

iv 通訊保障及監察法第一條

通訊保障及監察法第一條開宗明義規定「爲保障人民秘密通訊自由不受非法侵害，並確保國家安全，維護社會秩序，特制定本法」。

v 電腦處理個人資料保護法第十八條

電腦處理個人資料保護法第十八條規定「非公務機關對個人資料之蒐集或電腦處理，非有特定目的，並符合左列情形之一者，不得爲之：一、經當事人書面同意者。二、與當事人有契約或類似契約之關係而對當事人權益無侵害之虞者。三、已公開之資料且無害於當事人之重大利益者。四、爲學術研究而有必要且無害於當事人之重大利益者。五、依本法第三條第七款第二目有關之法規及其他法律有特別規定者。」

4.2.2.4 現行法規侵害隱私權之處

關於隱私權的保障範圍，在消極面係保障個人通訊不受幹擾；在積極面則係保障個人通訊得以完全控制及決定之權利；隱私權保障客體則包括個人屬性的隱私權、個人資料的隱私權、通訊內容的隱私權及匿名之隱私權。換言之，使用者之基本資料、通訊之有無及通訊之內容，均屬於資訊隱私權所保障之內容，因而受到憲法層次的保障，除非符合憲法第二十三條對於基本人權的限制之規定，即

基於「防止妨礙他人自由、避免緊急危難、維持社會秩序或增進公共利益所必要」等條件，並且符合法律保留原則，否則不容政府或任何人恣意侵害及限制。然而，我國現行關於網路網路服務提供者協助偵查之法制，不是欠缺相關法令規定，便是訂定屬於法規命令位階之辦法或規則予以規範而不符合法律保留原則，導致網路服務提供者協助偵查之行為陷入違憲及侵害隱私權之疑慮，茲分述如後：

I　主動過濾犯罪資訊

網路服務提供者主動過濾使用者在網路上從事犯罪之訊息，若過濾的資訊屬於公開的資訊，例如張貼在網路論壇或網頁空間上，因不享有隱私權之保護，故不會發生隱私權受到侵害之問題。反之，過濾的資訊屬於私密的通訊內容，例如以電子郵件發送給特定人之情形，因為我國欠缺關於網路服務提供者主動過濾使用者通訊內容之法律，因此網路服務提供者自行過濾使用者傳遞之網路資訊，將會侵害使用者之隱私權。另外，行政院新聞局雖然依據兒童及少年福利法授權訂定公佈「電腦網路內容分級處理辦法」，做為網路服務提供者過濾網路上資訊內容之依據，惟該辦法仍僅為法規命令的位階，並不符合前述法律保留之原則，依據前述辦法實施過濾網路內容之作為，仍有侵害隱私權之問題。

II　儲存或提供偵查單位使用者資料及通信紀錄

電信事業負有儲存或提供偵查單位使用者資料及通信紀錄之責任，目前係依據第二類電信事業管理規則第二十七條之規定。至於詳細之查詢程式，則依交通部電信總局係依據電信法第十七條第二項之規定授權訂定頒布之「電信事業處理有關機關(構)查詢電信使用者資料實施辦法」及「電信事業處理有關機關查詢電信通信紀錄實施辦法」辦理。惟前述辦法之位階均屬法規命令層次，與前述取得或限制秘密通訊必須符合法律保留之原則顯有衝突，致網路服務提供者縱使依前

述辦法之規定儲存或提供客戶使用者資料及通信紀錄，仍有侵害使用者隱私權之疑慮。

III　協助實施通訊監察

網路服務提供者依據通訊保障及監察法第十四條規定，提供協助偵查人員實施通訊監察，雖有侵害使用者隱私權之實質作爲，惟網路服務提供者協助實施通訊監察係基於偵查犯罪之公益需要，符合憲法第二十三條所規定之四個條件；並且通訊保障及監察法係屬於法律位階，亦符合法律保留原則之要求，因而無須擔心遭到認定有違憲之情形。不過，有學者[121]認爲網路服務提供者配合偵查人員實施通訊監察作爲，雖係依據通訊保障及監察法第十四條之規定，形式上符合憲法法律保留原則之規定。惟前揭條文僅空泛規定電信業者有協助執行通訊監察之義務，其他包括電信業者所需配合建置之通訊監察設備內容、電信業者如何建置相關配合通訊監察設備、電信業者配合建置相關設備之費用等等，均會對於人民之隱私權保護及網路服務業者之營業權與財產權產生重大影響之事項，並未於通訊保障及監察法有所規定，卻是僅以法規命令位階之通訊保障及監察法施行細則予以規範，這種規範方式仍可能有侵害到使用者隱私權之問題。

4.2.3 使用者資料範圍過狹

網路服務提供者依第二類電信事業管理規則第二十七條第五項之規定，「前項用戶之資料包括使用者姓名、身分證統一編號及住址等資料，且虛擬行動網路服務經營者另應包括所指配號碼」，其應記載事項之範圍仍有不足。因爲申請時

[121]參閱劉靜怡著，資訊社會的規範困境：台灣網際網路法律發展的歷史考察，網址：http://140.109.196.10/pages/seminar/infotec4/4-3.doc。最後瀏覽日期：二〇〇五年七月二十三日。

所填具的姓名、身分證統一編號及住址容易僞造，而不具有任何參考價值，在偵查實務中最具參考價值的資料，多數爲涉及金錢有關之資料，因此使用者應記載之事項，如能擴張紀錄使用者付款的方式（以現金、轉帳、匯款或信用卡等方式）及來源（轉帳帳號或信用卡帳號等金融資料），將有助於提高偵查人員清查過濾行爲人身份之正確性，以便進行後續偵查作爲。

4.2.4 通聯紀錄儲存期間過短

網路服務提供者依第二類電信事業管理規則第二十七條之規定，對於相關資料之保存項目及期間均有明文規定：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、ADSL 及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；三、對於張貼於留言版、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；四、對於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應保存六個月；五、電子郵件通信紀錄應保存一個月。保存期間過後，網路服務提供者便不能再加以保存，惟偵查實務上，網路案件發生時間與受理時間往往有一定之差距，偵查流程從案件立案、清查過濾、調查證據、案件執行到移送，亦必須耗費相當之時間，以清查過濾行爲人階段做說明，偵查人員與網路服務提供者之公文往返須耗費時間；研閱比對向網路服務提供者調閱之資料以過濾出行爲人亦須耗費時間，更遑論類比之的偵查作爲往往要重覆幾次，因此在時間的耗費是無法估計的。特別是電子郵件通聯紀錄之保存期間僅短短的一個月，根本無法滿足偵查實務之需求。

4.2.5 現行法制欠缺之規定

4.2.5.1 強制主動過濾之規定

網路資訊的傳輸原理，是使用者將訊息透過網路服務提供者之伺服器傳遞出去予特定人或不特定人接收，因此網路犯罪行爲人實施犯罪行爲必須透過網路服務提供者所提供之服務才有可能實現犯罪。因此，若網路服務提供者若能採取主動過濾方式，不定時對於上載或傳輸之資料進行檢查，一旦發現任何犯罪訊息，則不讓該犯罪訊息張貼在網頁上或透過電子郵件傳輸，如此從源頭阻絕犯罪資訊之散佈或張貼，可有效的降低網路犯罪發生率。惟對於網路服務提供者而言，依我國法令並未負有監督及強制過濾網路上違法資訊之義務，而係採取自律的方式進行過濾違法資訊，因此實務上真正有進行過濾傳遞訊息者，只有台灣學術網路的連線學校及單位（如附屬圖書館）等，安置過濾機制阻擋使用者去讀取不當資訊等的網站，其餘網路服務提供者，基於考量主動過濾網路上的資訊，可能會陷入侵害隱私權及使用者請求損害賠償之雙重麻煩中，根本不願意積極配合。因此，爲促使網路服務提供者能積極配合過濾違法資訊，進而降低網路犯罪之發生率，以及避免網路服務提供者因配合偵查而致遭受可能損害責任，應以法律規定強制其主動過濾不法資訊之責任。

4.2.5.2 主動舉發之規定

網路服務提供者爲提供用戶最好的服務，會不定時的檢查內容及維護系統，因此網路服務提供者對於用戶使用其網路服務從事犯罪行爲乙事是最容易發掘之人，因此若能經由網路服務提供者主動向偵查單位舉報，在偵查時效最能掌握。並且網路服務提供者如能進而將相關之違法證據蒐集完整，並主動提供給偵查單位，可以減少偵查人員蒐證的時間，對於網路犯罪偵查而言助益甚大。然惟依我國目前法令，網路服務提供者並未負有檢查監督及主動舉報之義務，致網路服務提供者若逕自提供使用者之違法通訊內容給偵查人員，有可能因侵害到使用者隱

私權及違反契約而可能面臨遭請求賠償之問題，因而配合協助的意願不高，導致網路犯罪案件偵查可能無法掌握偵查的契機及即時取得相關之事證，而無法繼續偵查下去。

4.2.5.3 主動提供證據之規定

案件受理與實際偵查之時間往往會有差距，再加上偵查人員實際進行查證作爲時，可能因爲公文的往返或是偵查其他案件等等因素，造成偵查時程延宕，若偵查人員未能將相關違法證據（例如網路上張貼猥褻圖片之網路色情行爲）即時加以列印或留存，一旦證據發生消失或湮滅的情形，偵查人員因無法蒐集到任何違法證據，只能將全案予以偵結。因此，爲解決此一問題，除了要求偵查人員加快偵查時程外，本研究認爲如能使網路服務提供者負有自動保存證據並主動提供予偵查人員之義務，既可避免因偵查時程遲延造成違法證據消失的風險，網路服務提供者適時提供之相關證據，更能使偵查人員正確地研判案件全貌及迅速執行偵查作爲，，提昇偵破率。。不過，我國目前法令並未有任何類此之規定。

4.2.5.4 強制停止傳遞違法資訊服務之規定

電信法第八條第二項「以提供妨害公共秩序及善良風俗之電信內容爲營業者，電信事業得停止其使用。」同法第二十二條但書規定「對於電信之內容顯有危害國家安全或妨害治安者，得拒絕或停止其傳遞」，均爲電信業者停止服務之依據。惟前揭二條文乃賦予電信業者有「得」停止服務之權利，而非負「應」停止提供之義務[122]，其適用前提均須符合「以提供妨害公共秩序及善良風俗內容爲營業」或「顯有危害國家安全或妨礙治安」之要件，然而該等要件均屬於「不確定的法律概念」，電信業者並不一定有能力認定，一旦發生認定錯誤，逕自停止

[122]同前註 95。

用戶網路服務之作爲，將違反與用戶間之網路服務契約義務，而遭到請求賠償，因此，網路服務提供者考量本身之利益及目前欠缺強制義務之規定雙重因素下，根本無法期待網路服務提供者會徹底執行前揭條文之規定。爲解決此一執行盲點，本研究認爲必須強制業者有停止傳遞違法資訊之責任，才能達到有效防堵犯罪資訊傳遞之目的，然而我國目前法令並未有任何類此之規定。

4.2.5.5 成本補助之規定

I 儲存或提供使用者資料及通信紀錄成本

關於電信事業儲存及提供使用者資料及通信紀錄等資料，並沒有任何補助業者成本之規定，目前係採取「使用者付費」原則，依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九條規定「電信事業處理有關機關 (構) 查詢使用者資料時，得以每號新臺幣五元計收，按月結算之。法官、檢察官或監察院依法查詢電信使用者資料者，查詢費用得予減收或免收・・・」；另依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七條、，查詢費用依下列方式計收：一、單向發信通信紀錄：以每頁新臺幣十元計收。二、雙向通信紀錄：以每號每日新臺幣一百二十元計收，查詢期間不滿一日以一日計收・・・」；第八條則規定「法官、軍事審判官、檢察官、軍事檢察官或監察院、審計部及所屬審計機關依法查詢電信通信紀錄者，查詢費用得予減收或免收。」事實上，偵查單位中各地檢察署查詢使用者資料或通聯紀錄無須支付查詢費用外，警察、調查機關基於案件之需要查詢而支付查詢費用相當可觀[123]，惟這些查詢費用只能支應協助個案調閱相關資料的費用，尚無法彌補業者爲儲存及提供使用者資料及通聯紀錄所建置之設備及維護設備之成本。尤其隨著網路使用普及化，網路上的通信行

[123]參閱苗君平，「調閱通聯免費，警方促比照同是辦案，地檢署有優待，中警一年支出逾三百萬，吃不消」，聯合報，中部綜合新聞，B4 版，二００四年五月六日。

爲愈趨頻繁，所要保存的通信紀錄容量與日俱增，電信事業所需負擔的經營成本更高，基於成本因素，自然不會全力配合協助偵查。

II　協助通訊監察之成本

網路服務提供者依通訊保障及監察法依第十四條第二項規定負有協助執行通訊監察之義務。而其具體應配合事項則依據通訊保障及監察法施行細則第二十一條之規定，該條規定「本法第十四條第二項所稱協助執行通訊監察之義務，指電信事業及郵政機關（構）應使其通訊系統之軟硬體設備具有配合執行通訊監察時所需之功能，並於執行機關執行通訊監察時予以協助，必要時並應提供場地、電力及相關介接設備及本施行細則所定之其他配合事項。應使其通訊系統之軟硬體設備具有配合執行通訊監察時所需之功能。而其並於執行機關執行通訊監察時予以協助，必要時並應提供場地、電力及相關介接設備及本施行細則所定之其他配合事項。交通部電信總局應將本細則施行前經特許或許可設置完成之第一類電信事業之通訊系統及通訊網路等相關資料，提供予法務部調查局或內政部警政署評估其所需之通訊監察功能後，由法務部調查局或內政部警政署依第一類電信事業之業務及設備設置情形，向第一類電信事業提出需求；第一類電信事業應即依該需求，擬定所需軟硬體設備、建置時程及費用之建置計畫，與法務部調查局或內政部警政署協商確定後辦理建置。必要時，由交通部電信總局協助之。第一類電信事業於本細則施行前已經同意籌設或許可之新設、新增或擴充通訊系統，於本細則施行時尚未完成籌設或建置者，於其通訊系統開始運作前，應依前項之規定擬定配合執行通訊監察所需軟硬體設備、建置時程及費用之建置計畫及辦理建置，並於其通訊系統開始運作時同時協助執行通訊監察。本細則施行前交通部已公告受理特許經營之第一類電信業務，其經核可籌設者，亦同。第一類電信事業於本細則施行後新設、新增或擴充通訊系統者，其通訊監察相關設備應先與法務

部調查局或內政部警政署協商；依法務部調查局或內政部警政署提出之監察需求，擬定配合執行通訊監察所需軟硬體設備、建置時程及費用之建置計畫，與法務部調查局或內政部警政署協調確定後，由交通部或交通部電信總局核發建 (架) 設許可證 (函) 後辦理建置，並經交通部電信總局與法務部調查局或內政部警政署確認符合通訊監察功能後，於其通訊系統開始運作時同時協助執行通訊監察。前三項建置計畫是否具有配合通訊監察所需之功能發生爭執時，由交通部認定並裁決之。第一類電信事業應即依裁決結果辦理。第二類電信事業須設置通訊監察設備之業務種類，由交通部電信總局邀集法務部調查局或內政部警政署協調定之，並準用前四項規定辦理。」綜上述條文規定，網路服務提供者協助執行通訊監察必須自行建置硬體、軟體等設備，並應隨時配合偵查單位之需求擴充設備，除此之外，依通訊保障及監察法施行細則第二十一條規定，電信事業還負有指派技術人員協助執行實施通訊監察之義務，電信事業不配合時，依同細則第三十一條規定尚必須擔負行政責任。

然而，通訊保障及監察法第十四條基於偵查犯罪之需要，強制電信事業有協助實施通訊監察之義務，但是履行義務所需負擔額外的經營成本（包括硬體、軟體建置與維護費用及人事成本），對於電信事業而言是非常沈重，然而對於業者協助執行通訊監察所支應之費用，該法卻只規定電信事業在「執行協助執行通訊監察後」得以請求執行機關支付實際使用之設施及人力成本等「必要費用」，至於電信業者爲配合協助實施通訊監察所建置設備、維護設備及人事管理等等所支應之費用則完全沒有任何補助之規定。因此，電信事業（特別是規模小的第二類電信事業）基於在成本的考量，配合意願當然不高，甚至是欠缺負擔協助實施通訊監察之能力，而無法配合，顯見欠缺成本補助規定也是國內實施網路通訊監察

難以落實的重要原因[124]。

4.2.5.6 協助偵查之免責規定

網路服務提供者配合偵查人員，協助犯罪偵查，可能會發生造成用戶損害或違反契約義務而須負擔賠償責任之情形，目前除了依通訊保障及監察法第二十九條有規定電信事業協助偵查單位實施通訊監察有免責之事由外，其餘無論是依電信法第八條第二項或是第二十二條停止提供用戶網路服務；或依電腦網路內容分級處理辦法第八條移除違法內容；或依第二類電信事業管理規則第二十七條儲存及提供使用者資料及通信紀錄等協助偵查作爲，均未訂定任何免責之規定。一旦造成用戶有損害時，電信業者仍必須負擔賠償責任。以電信法第八條第二項或是第二十二條停止提供用戶網路服務爲例，該二條文中「以提供妨害公共秩序及善良風俗內容爲營業」或「顯有危害國家安全或妨礙治安」之要件，均屬於「不確定的法律概念」，電信業者並無有能力認定，一旦發生認定有誤而善意停止用戶網路服務，致違反與用戶間之網路服務契約義務，並無任何免責規定可以主張，雖然目前電信業者係以透過網路服務契約與用戶約定方式，排除其可能應負之損害賠償責任，畢竟是不得已的作法，如果能訂定協助配合偵查人員進行案件偵查之免責規定，電信業者才不會因心有忌憚而無法完全配合。

4.2.5.7 不配合之罰責規定

網路服務提供者不配合偵查人員偵查時，依現行法令僅通訊保障及監察法第三十一條訂有電信業者不配合時相關行政罰責規定，依該條規定可處罰電信業者新台幣五十萬元以上二百五十萬元以下罰鍰，甚至得撤銷其特許或許可。至於，第二類電信事業規則第二十七條規定，雖然規定電信事業負儲存使用者資料及通

[124]同前註 120。

信紀錄，惟電信法及前揭規則對於未配合之網路服務提供者並未訂有任何處罰規定，因此縱使不配合或儲存、提供之使用者資料與通信紀錄內容發生重大瑕疵情事，也不會受到任何處罰；另外，依電腦網路內容分級處理辦法第八條之規定，亦要求網路服務提供者負有移除違法內容之義務，但也沒有任何處罰規定。因此，在沒有任何罰責的規定下，網路服務提供者考量自身利益及可能面臨的賠償責任雙重因素下，配合意願當然不會高。

4.2.5.8 強制協助解密之規定

對於電子郵件實施通訊監察雖可以有效監控犯罪行爲人，但由於加密的技術進步，爲防止通訊內容爲他人所知悉，利用電子郵件加密的情形愈來愈多，致使偵查人員縱使截收到已加密之電子郵件，因偵查人員無法加以解密，所看到的內容只顯示一堆亂碼而無法判讀，對於案件之偵查毫無實益。由於目前電子郵件進行加解密的金鑰，多係業者提供給電子郵件寄信者與收信者，因此如能強制負擔將截收到已經加密的電子郵件，明文呈現給偵查人員判讀之義務，才能達到實施通訊監察之目的。惟依我國目前法令，並沒有要求業者協助解密之規定。

4.2.5.9 行政檢查之規定

雖然電信法、第二類電信事業管理規則要求電信業者負有儲存及提供使用者資料、通信紀錄之義務；通訊保障及監察法要求電信事業負有建置通訊系統之軟、硬體設備，使之具有配合協助偵查人員執行通訊監察時所需的功能，然而該等負有協助義務之電信事業，是否均有依相關法令規定之內容、時程完成建置相關之設備及儲存相關資訊內容。對於偵查人員而言，網路服務提供者徹底執行前揭規定之事項，是案件偵查成敗的關鍵。然而現行法令並未訂有任何行政檢查之規定，使執行機關或主管機關無法針對負有協助義務之業者進行任何行政檢查，瞭解業者實際執行進度及內容，進而督促業者履行相關協助偵查之義務。

4.2.5.10 保密規定

網路服務提供者協助網路犯罪偵查，所提供協助的資料，包括使用者資料、通信紀錄及監察所得的內容等，均屬於用戶享有高度隱私權的資料，雖然基於防治網路犯罪之公益需要，可選擇以採取立法方式剝奪用戶的隱私權，但取得前揭資料的偵查人員，只能限定在偵查犯罪的時候才能運用，並且應負有保密的義務，以免用戶因資料外洩，造成其隱私權第二次遭到侵害，因此本文建議應制定保密規定並輔以刑責規定，讓偵查人員警惕及防止發生資料外洩之情事。

4.2.5.11 取得儲存及提供通訊內容之規定

依第二類電信事業管理規則第二十七條之規定，網際網路接取服務者負有保存用戶識別帳號、通信日期及上、下網時間；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；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；及電子郵件通信紀錄等資料一至六個月不等之義務。不過，前述保存資料的作用，對於偵查犯罪而言，只能作爲研判案情、擬定執行計畫之用，就算做爲呈堂證據，亦屬於補強證據的性質。事實上，網路傳輸之內容本身才是最有效的證據。以偵查網路色情犯罪爲例，行爲人透過電子郵件發送或在網頁上張貼猥褻之圖片本身，才是最有力犯罪證據。因此，若偵查人員能取得該電子郵件或網頁留存之內容，定能順利迅速偵破案件。然而，該等網路違法內容除了由受害人主動提供外，偵查人員可否透過網路服務提供者取得？應透過何種偵查作爲取得才不會侵害到客戶之隱私權？，前揭問題均值得去思考。本研究爲方便說明，不擬針對所有網路內容的部分，僅針對保存電子郵件內容部分加以說明如後：

I　保存電子郵件內容

發送電子郵件的原理，是從發信方將電子郵件傳送至收方之郵件伺服器內，

郵件伺服器接收後會暫時將電子郵件儲存於信箱中，俟收信方進入郵件信箱進入打開電子郵件或先將電子郵件下載至個人電腦之信箱中再打開。一般而言，郵件伺服器原暫存之電子郵件，俟用戶下載即不再儲存，否則可能會違反與用戶之間的契約，甚至可能侵害到用戶隱私權。不過，使用 Web mail 收發信件方式，用戶之電子郵件進入郵件伺服器，用戶可直接打開瀏覽，並選擇是否刪除，經刪除的電子郵件仍會保存在垃圾筒，除非用戶選擇清理垃圾筒，才不會再保存；用戶若打開郵件瀏覽後，並未選擇刪除時，則該郵件仍儲存郵件伺服器內。此時，電子郵件保存在郵件伺服器內，係用戶自己自主決定的結果，因此不生侵害隱私權之問題。

另一種可能儲存的原因，係電子郵件伺服器業者爲了防止傳輸過程發生郵件遺失而必須擔負賠償責任的問題，會以建立兩套平行、互不幹擾的系統設備收取電子郵件，以做爲備份檔案，因此用戶縱使選擇刪除或下載儲存在郵件伺服器之信件，電子郵件備份仍有可能留存。而前揭業者爲避免傳輸上發生瑕疵，運用新科技保留電子郵件備份之行爲，其出發點係爲提供用戶更好的服務品質，並非專爲侵害用戶之隱私權，本研究認爲不能逕自認定有侵害到用戶之隱私權。

II　取得電子郵件內容

依我國目前法令，對於偵查人員能否及如何取得保存於郵件伺服器之電子郵件方式並未有任何規定，因此在學者間有不同之意見，茲分述如後：

iii　採取單純公文調閱的方式

依據電信法第七條第一項、第二項之規定「電信事業或其服務人員對於電信之有無及其內容，應嚴守秘密，退職人員，亦同。前項依法律規定查詢者不適用之；電信事業處理有關機關 (構) 查詢通信紀錄及使用者資料之作業程式，由電信總局訂定之。」從法條文義解釋上，偵查人員依法應可調閱電信之內容，惟實

際上因爲交通部電信總局只訂定公告調閱通信紀錄之作業辦法，而未訂定公告關於調閱電信內容之相關作業規定，因此偵查人員無法以公文調卷的非強行偵查作爲，向電信業者調閱儲存於郵件伺服器之電子郵件。

iv　採取聲請通訊監察方式

偵查人員依據通訊保障及監察法向法院聲請實施通訊監察，係針對「活」的案件，即尚在進行中的案件實施通訊監察加以監控，因此係針對行爲人現在或未來的通訊行爲所作之事前掌控。至於行爲人過去發生的通訊行爲，不得對之實施通訊監察[125]，因此縱使電子郵件尚保存在郵件伺服器裡，因爲屬於已經過去發生之通訊行爲，故偵查人員亦不可以實施通訊監察方式取得該電子郵件內容。

v　採取搜索扣押方式

對於尚保存在郵件伺服器的電子郵件，有學者[126]認爲電子郵件之內容爲秘密通訊之核心，郵件伺服器業者不得任意將該電子郵件內容提供給偵查單位。此時應區分該電子郵件是否已經收信人閱讀，若該電子郵件已經收信人閱讀，雖然存檔於網路服務提供業者之伺服器，就該電子郵件而言，均屬於電磁紀錄，因此可依刑事訴訟法關於搜索、扣押電磁紀錄之方式爲之；若係未經閱讀之電子郵件，則經搜索網路服務業者後，得依刑事訴訟法第一百三十五條第一項之規定，扣押該電磁紀錄。

vi　小結

本研究認爲儲存在郵件伺服器之電子郵件無論打開與否，均係置放於用戶所申請之郵件信箱中，並且必須輸入正確的使用者代號及密碼始能進入該信箱中閱

[125]參閱蔡美智著，同前註 110 揭書，第三十九至第四十頁
[126]參閱王銘勇著，同前註 8 揭書，第二六一至二六三頁。

讀郵件，因此應認爲該電子郵件信箱屬於用戶之私密空間，而享有隱私權之保障，不容他人肆意侵犯。

反之，對於網路偵查而言，該保存於郵件伺服器的電子郵件內容，是相當重要的證據，偵查人員如能取得相關電子郵件內容，對於偵破案件有極大的幫助。至於應採取何種方式取得該保存之電子郵件，才能兼顧偵查網路犯罪之需要及保障人民隱私權之目的，本研究認爲實施通訊監察係針對現在及未來之通訊所做之偵查作爲，而儲存於電子郵件信箱之電子郵件並非即時之通訊內容，因此不宜以實施通訊監察方式取得；至於，以出具正式公文向網路服務提供者調閱儲存在郵件伺服器之電子郵件的方式，對於偵查人員而言是最簡單、最便利的手段，但這種方式賦予偵查人員過多的權力，使得偵查人員在無任何規制或監督下，得以漫無限制地調閱儲存在電子郵件信箱中之電子郵件內容，恐有過度侵害人民之隱私權之虞，因此亦不適宜以公文調閱方式取得；本研究認爲採取搜索扣押取得儲存中電子郵件之方式，既有法律的依據，又有法院審核搜索票之監督，可避免爲偵查犯罪過度侵害人權，有效保障人民的隱私權，是最爲可行的方式。

5 法制建議

5.1 立法建議

本研究第三章已說明網路犯罪偵查的困難度及網路服務提供者協助偵查的重要性及得以提供協助之偵查事項；第四章臚列我國現行關於網路服務提供者協助偵查法制之規定，並指摘現行規定之缺失及不足。事實上，本研究認爲網路服務提供者無法完全配合協助偵查的重要原因，在於欠缺一套完善的協助偵查法制，以致網路犯罪偵查始終無法跳脫瓶頸。因此，本研究認爲有必要制定網路服務提供者協助偵查法，並提出個人立法建議，期能透過立法程序促使網路服務提供者完全配合偵查，以有效強化偵查人員偵查網路犯罪之能力，提高網路犯罪偵破率，進而降低網路犯罪發生率。

5.1.1 立法方向

5.1.1.1 制定協助偵查專法取代修法

我國關於網路服務提供者協助偵查責任之規定，並沒有統一之法律加以規範，而係散見於電信法、通訊保障及監察法、第二類電信事業管理規則、反恐怖行爲法草案等相關法規，分別針對電信業者應配合提供使用者資料、通聯紀錄、及配合實施通訊監察等內容加以規定。不過，前揭法規之規範對象均僅侷限於電信業者。事實上，面對網路的多元化發展及網路使用者對於網路的多樣化需求，業者所提供服務內容不再只提供使用者連線上網之服務，並且提供收發電子郵件、電子報與網頁資訊、檢索功能、線上遊戲、即時通訊、網路電話、線上購物等等各種不同類型的服務項目；同時，經營前述網路服務的業者，可能爲非電信業者或個人，根本無法適用電信法相關法規，更遑論依電信法相關法規擔負協助偵查之責任，因此，縱使修改目前電信相關法規內容，仍無法適用於非電信事業

之網路服務提供者。

事實上，爲瞭解決網路多元化所帶來各類型網路犯罪之副作用，政府相關單位均已著手研擬相關法規嘗試解決，以目前刻在立法院審議中的法案，其中「濫發商業電子郵件管理條例」係針對「垃圾郵件」泛濫的問題所制定，依該條例郵件伺服器業者負有過濾及防止電子郵件泛濫之責任[127]；另外，「資訊休閒業管理條例草案」則針對網路犯罪行爲人利用「網路咖啡店」進行網路犯罪之問題所制定，依該條例草案要求網路咖啡店之業者，負有建置防止賭博及色情網路內容篩選過濾設備、現場錄影監視器及警民連線裝置、使用者登錄之歷史紀錄檔等設施[128]。前揭二法案雖係針對非電信事業之業者應負協助偵查責任加以規定，惟其規範對象僅針對「郵件伺服器業者」或「網路咖啡店業者」兩者，非屬前揭二者類型之非電信事業則不包括在內。

綜上，有鑒於網路服務內容的多元化，非電信事業的網路服務提供業者及提供服務項目及內容愈來愈多，修改電信法相關條文納入業者協助偵查責任等內容，因其規範對象侷限於電信事業，無法適用於非電信事業，因此並非可行的方式；另外，採取「一個蘿蔔一個坑」的立法方式，雖然可以解決非屬電信事業之網路服務提供者協助偵查之問題，但因欠缺全盤的考量，無法徹底解決業者協助偵查網路犯罪的問題，隨著網路服務多元化發展，所需制定的法規數量恐將不斷增加以應付新的服務類型所可能帶來的問題，如此一來，不僅耗時又無法達到立法之功效。因此，本研究以爲針對網路服務提供者協助偵查法制議題，採取修改電信法相關法規及針對特定類型業者單獨訂定規範之立法方式均非可行之方案，

---

[127]參閱交通部電信總局全球資訊網，網址：http://www.dgt.gov.tw/chinese/ncc/mail-requlation/ncc-mail-requlation.shtml。最後瀏覽日期：二〇〇五年七月二十三日。

[128]參閱經濟部全球資訊網，焦點新聞，網址：http://w2kdmz1.moea.gov.tw/user/news/detail-1.asp?kind=1&id=8946。最後瀏覽日期：二〇〇五年七月二十三日。

必須採取全盤檢討現行相關法規及考量日益新穎的網路服務內容，制定專法（網路服務提供者協助偵查法），將所有網路服務提供者類型及應協助內容均納入規範的方式最爲適宜。

5.1.1.2 制定協助偵查專法取代網路內容管理法

隨著網路的發達，網路上犯罪行爲日漸泛濫，網路上的安全性愈來愈低，對於網際網路之脫序行爲，應如何處理，國內外學者均有所爭議且尚未有定論。世界各國中，主張以法律嚴格管制網路內容的國家主要有新加坡[129]與大陸[130]兩個國家；而相對於新加坡與大陸的嚴格管制手段，歐美各國則傾向以較自由的態度看待網路內容的管理[131]。我國對於網路行爲的管理，目前係採取較寬鬆的管制態度，尚未訂定任何網路內容管理法規，不過在我國司法實務判決，已有認定網路服務提供者應對其傳遞內容負相關刑事責任之情形[132]；我國國內學者多數見解，則基於維護網路科技的發展，多主張以業者自律的爲主的管理方式，具體建議包括透過業者自律限制犯罪資訊的提供、採行內容分級及強化資訊安全等方式來減少網路犯罪的發生[133]。另外由交通部電信總局委託資策會科技法律中心研究之

---

[129]新加坡於一九九六年七月十五日通過了「網際網路管理辦法」，該辦法中規定網路上活動必須遵守新加坡廣播局所頒發的「網路內容指導原則」（Internet Content Guidelines），而該指導原則第四條禁止網路傳遞有害公共安全與國家安全的內容；第五條則禁止透過網路傳遞有害種族與宗教和諧的內容；第六條則禁止網路宣揚傳遞與新加坡道德標準相違的內容，包括色情、性、裸露、暴力、恐怖與同性戀等內容。凡是違反上述規定傳遞禁止內容的網路業者將被廣播局吊銷執照，網友也會受到嚴格的處分。

[130]中華人民共和國於一九九六年二月一日公佈了「中華人民共和國計算機資訊網絡國際聯網管理暫行規定」。該法第十三條規定:「從事國際聯網業務的單位和個人，應當遵守國家有關法律、行政法規 ，嚴格執行安全保密制度，不得利用國際聯網從事危害國家安全、洩露國家秘密等違法犯罪活動，不得製作、查閱、複製和傳播妨礙社會治安的資訊和淫穢色情等資訊。」；同法第五條則授權「國務院經濟資訊化領導小組」得對網路通訊內容進行檢查監督。

[131]參閱範傑臣著，各國網路內容管制政策之比較研究，網址：http://www.ccu.edu.tw/TANET2001/scheduel/paper_abs/T103.html。最後瀏覽日期：二○○五年七月二十三日。

[132]參閱台灣臺北地方法院八十八年度少連易字第八號刑事判決。該案於於八十八年十二月九日宣判，承審法官認定 ISP 業者彭某明知柯某經營色情網站，竟基於幫助之故意而提供虛擬主機與網路頻寬服務，故以幫助犯論處，處有期徒刑參月，緩刑貳年。

[133]參閱馮震宇著，同前註 9 揭書，第三六六至三六七頁。

「網際網路管理辦法建議草案之訂定」之研究計劃，其研究成果亦建議對於網路管理宜由電信總局輔導網際網路服務提供業者成立同業公會，並制訂自律規約規範之，以民間自律之力量來提昇網路內容與服務之品質[134]。

然而，從本研究第二章探討網路犯罪案件數量之數據分析，網路犯罪行為隨著網路的發達日益泛濫，雖然歐美各國主張業者自律及使用者自製及教育宣導的方式，但是面對網路犯罪，仍是積極研擬相關防治的措施及法規，顯見光是藉由業者自律或是教育宣導的方式並不足以達到防治網路犯罪的目的；另外，新加坡及中國大陸採取嚴格控管網路內容的手段，制定相關網路內容管理法規，加諸網路服務提供者過多的民事、刑事責任，雖然可以達到防治網路犯罪目的，卻恐將造成網路服務提供者退卻，不願繼續提供網路服務，甚至對於網路的發展將造成嚴重阻礙之副作用，故亦非適合的管理手段。綜上，本研究以為制定網路協助偵查法制，是採取低度管制網路，以取代制訂網路內容管理法嚴格管制手段，並可彌補業者自律無法達到防治網路犯罪之目的，是侵害最小又能達到防治網路犯罪的最佳手段。

5.1.2 立法目的

從第三章及第四章的探討得知網路服務提供者對於網路犯罪偵查中實扮演相關關鍵的角色，不論是從清查過濾階段起迄案件執行階段，均需要網路服務提供者之協助。另外，網路犯罪偵破率無法提高的原因，除了偵查人員本身人力、能力的問題外，無法獲得網路服務提供者完全配合協助更是最大原因，顯見網路服

[134]參閱張雅雯著，「網際網路管理辦法建議草案」出爐建議以業界自律為管理主軸，資訊法務透析，一九九八年八月。該研究報告並提出六項管理之原則：一、尊重國際趨勢；二、保障網路言論自由；三、保障隱私權；四、尊重市場機能；五、政府盡量減少介入與幹預，採取最低度的管理；六、賦予使用者選擇權。

務提供者之協助對於網路偵查的重要性。因此，採取立法方式建置網路服務提供者協助偵查法制，加諸網路服務提供者額外協助偵查責任，使得偵查人員有更多的利器去面對日益泛濫的網路犯罪，其立法目的茲分述如後。

5.1.2.1 防治網路犯罪泛濫

目前網路犯罪的破案率不到百分之十[135]，分析其原因，包括偵查人員面對新興之網路犯罪類型，其偵查方法無法遵循既有傳統犯罪案件偵查之思惟；偵查過程無法引用已建置犯罪資料庫之資料；網路犯罪本身具有隱匿性、無國界性、不易追查、證據不易蒐集、證據毀滅容易等特性，致偵查過程中「斷點」甚多；以及專責網路犯罪偵查人員與偵查能力均有所不足等等原因外，本研究認爲最重要的原因在於欠缺網路服務提供者之完全配合協助偵查。因爲，偵查人員受理網路犯罪案件後，實務偵查的第一個步驟，是向網路服務提供者調閱客戶登錄資料，以清查過濾犯罪行爲人之身份；過濾出可疑的行爲人身份之後，向網路服務提供者調閱相關通聯紀錄，以比對時間點、帳號、地點等相關資料，進而研擬偵查計畫；案件進入蒐集犯罪證據階段，對於已完成犯罪行爲之案件，必須透過網路服務提供者取得通信紀錄或通信內容等違法證據；正在實施中之案件，必須仰賴網路服務提供者協助實施通訊監察、搜索等強製作爲，以蒐集網路犯罪行爲人之不法事證；案件進入法庭審理階段，網路服務提供者更可做爲偵查方有利的證人，甚至可以協助實施鑑定數位證據之證明力。顯見，網路服務提供者若能全力配合協助偵查，自能有效掌控網路犯罪案件之事證，提昇網路犯罪偵破率，達到防治網路犯罪的目的。

---

[135]同註 56。

5.1.2.2 符合憲法法律保留原則[136]

在網路通訊中，包括使用者之基本資料、通訊之有無及通訊之內容，均屬於資訊隱私權所保障之內容，受到憲法保障而不容咨意侵害或限制。依我國憲法規定，除非符合第二十三條對於基本人權的限制之規定，即基於「防止妨礙他人自由、避免緊急危難、維持社會秩序或增進公共利益所必要」等條件，並且符合法律保留原則，才能予以限制，否則即有違憲之疑慮。雖然基於犯罪防治的立場，在網路犯罪偵查中，需要網路服務提供者之協助，但是網路服務提供者所可以提供的協助，包括提供使用者資料、提供通信紀錄、協助實施通訊監察、保存證據等等項目，均屬於侵害使用者隱私權及言論自由等憲法賦予的基本權利之行爲，若網路服務提供者在沒有任何法律依據，即逕自提供相關資料給偵查人員，是嚴重侵害到用戶的基本人權，而有違憲之虞，因此本研究認爲惟有必要以制定法律方式，明定網路服務提供者協助偵查之責任，才能符合憲法法律保留原則。

5.1.2.3 保障人民隱私權

雖然偵查機關基於調查犯罪的理由，可以透過法律的方式，享受更多的權力以調查網路犯罪，並可要求網路服務提供者負有協助偵查的責任，然而在偵查機關取得更多的調查權力的同時，正代表使用者享有隱私權等憲法賦予的基本人權可能因此遭受到極大的影響。因此，法規爲保障因逐漸擴增的調查權力所可能帶來對隱私權侵害的影響部分必須加以規範，以平衡保障隱私權及防治犯罪兩種不同的目的。例如法律應禁止偵查人員將從網路服務提供者處取得的個人資料外洩或規定網路服務提供者在提供協助後通知用戶等等規定，以保障人民隱私權。

---

[136]「法律保留原則」係指沒有法律授權行政機關即不能合法的作成行政作爲，蓋憲法已將某些事項保留予立法機關，須由立法機關以法律加以規定。參閱吳庚著，行政法之理論與實用，增訂七版，第八十四頁。

5.1.2.4 促進網路使用的目的

制定網路偵查法制的目的並非在限制網路之使用，而是希望透過法制的建立，讓偵查人員得以順利偵查網路犯罪，進而產生威嚇效果，致使網路上脫序的行爲減少，創造安全與自由的網路空間，使得網民能更加放心的在使用網路，進行促進網路的使用。

5.1.2.5 免除法律責任

從第三章及第四章的探討得知在網路犯罪偵查中，網路服務提供者所可以提供的偵查協助，包括主動過濾不法的資訊、提供使用者資料、提供通信紀錄、協助實施通訊監察、保存證據等等項目，無一不會涉及使用者的隱私權及言論自由的權利，因此若業者在沒有法律規定的情形下，以自律的方式提供偵查人員協助，除會侵害到憲法保障的基本人權外，更因爲欠缺法律賦予的免責規定的保護，而可能會遭受到民事賠償及刑事責任等法律責任。致網路服務提供者縱使有心協助偵查機關，亦會因協助之作爲動輒侵害到使用者的隱私權及言論自由，進而遭致損害賠償的責任，而不願意提供協助。

5.1.3 立法原則

雖然建制協助偵查法制足以達到防治網路犯罪、符合憲法法律保留原則、保障人民隱私權及免除網路服務提供者協助偵查的責任等目的。然而協助網路偵查的事項眾多，包括主動過濾不法的資訊、提供使用者資料、提供通信紀錄、協助實施通訊監察、保存證據等等項目，各種不同類型的協助事項對於用戶隱私權可能造成之侵害程度不同；再加上各種不同類型的網路犯罪提供者所應負擔及能負擔的責任內容亦不相同，因此實際制定加諸網路服務提供者協助責任內涵之細部規定時，仍應秉持下列幾個原則。

5.1.3.1 比例原則

以立法方式強制網路服務提供者負有協助偵查責任，將會影響網路服務提供者的營業自由，也會增加網路服務提供者之營業成本，甚至會侵害到使用者的隱私權。雖然，本研究以爲網路犯罪可能造成的損害大小無法預測性、可能造成個人、社會，甚至是國家損害嚴重性，遠高於保障網路服務提供者之營業損失及人民隱私權遭侵害之私益。因此基於考量防治網路犯罪、維護社會秩序、甚至維護國家安全等公共利益及網路服務提供者提供協助對於網路犯罪偵查之重要性，主張應制定網路協助偵查法制，惟實際訂定之相關法律條文，仍應個別檢視法規內容是否符合「比例原則」[137]，茲分述如後。

I　適當性原則

適當性原則係指行爲應適合於目的之達成[138]，因此在制訂法規強制網路服務提供者擔負協助偵查責任，其內容必須能夠達到防治網路犯罪泛濫、保障人民隱私及維護網路使用安全的目的。

II　「必要性原則」

必要性原則係指行爲不超越實現目的之必要程度，亦即達成目的須採取影響最輕微的手段[139]。因此，制訂法規時，必須考量不同偵查階段、不同類型的犯罪類型，加諸網路服務提供者不同的協助偵查責任。例如對於已經完成的案件，透過調閱通聯紀錄、使用者資料即可達到偵查目的之情形，偵查人員不得實施通訊監察，換言之，實施通訊監察只能限於針對進行中之案件。

---

[137]「比例性原則」有廣狹兩義之分，廣義之比例原則包括「適當性原則」、「必要性原則」、「衡量性原則（又稱狹義比例性原則）。參閱吳庚著，行政法之理論與實用，增訂七版，第五十七頁至第五十八頁。

[138]同前註。

[139]同前註 136。

III 「衡量性原則」

「衡量性原則，又稱狹義比例性原則，係指手段應按目的加以衡判，即任何干涉措施所造成之損害應輕於達成目的所獲致之利益，始具有合法性[140]。因此，制訂條文時必須考量個別協助偵查責任之內容，其能達到的目的必須輕於可能造成之損害，以兼顧防治網路犯罪及維護人民隱私間公益與私益之平衡。以實施通訊監察爲例，由於實施通訊監察對於使用者之通訊隱私侵害性最大，若網路犯罪類型中屬於輕微案件之類型，例如網路誹謗、網路援交等，偵查人員均可對之實施通訊監察，相對於遭侵害的隱私權而言，顯然是以「大砲打小鳥」，並非可行之方案。因此本研究以爲得實施通訊監察之案件類型，必須嚴格限縮於重大犯罪類型或具有跨國性、集團性犯罪類型；並且必須事先經嚴格審核其必要性後，才能實施通訊監察。

5.1.3.2 明確性原則

所謂「明確性原則」係從憲法上之法治國原則所導出，爲依法行政原則之主要成分，其意義乃指在法律保留原則支配下，法律及法規命令之規定，內容應明確。[141]其目的在於使人民得以預見及考量何種事項爲法律所許可，何種事項屬於禁止之事項，而有遵循之可能。而網路服務提供者的類型眾多且提供的服務多元化，因此各種網路服務提供者應負擔之協助的事項均不相同，對於何種網路服務提供者應負擔何種協助偵查事項，專法在制定時必須明確其協助偵查之責任，使之有規可循。

5.1.3.3 平等原則

所謂「平等原則」係指相同事實應爲相同處理，非有正當理由，不得爲差別

---

[140]同前註 136。
[141]參閱吳庚著，同前註 136 揭書，第六十五頁

待遇。[142]而所謂「正當理由」，依司法院大法官會議釋字第二二一號解釋，乃指「爲保障人民在法律上地位之實質平等，並不限制法律授權主管機關，斟酌具體案件上之差異及立法目的而爲合理之不同處置」，因此如係基於事物本質上的不同，而爲合理之差別待遇，亦與平等原則無異[143]。換言之，平等原則具有另一個概念，即「不同之事件應爲不同之處理」。由於本文所稱網路服務提供者係指「任何提供網路相關服務之個人或機構」，但實際上網路服務提供者的類型眾多，經營的模式包括營利及非營利；經營的規模大小不同，有個人性質、公司性質；提供服務的內容多元化，若一味要求負擔相同的協助責任，顯然違反「平等原則」，因此在探討網路服務提供者協助責任之課題，仍應秉持「平等原則」，區分不同形態、經營規模之網路服務提供者，以決定各自應負擔的協助偵查責任之高低及應協助偵查之事項之多寡。至於其區分之方式，本研究認爲得區分以下各種類型：

I　是否爲電信事業

網路服務提供者應先區分爲電信事業（第二類電信事業）及非電信事業兩類。所謂電信事業，依據電信法之規定係指電信服務：指利用電信所用之機械、器具、線路及其他相關設備，提供之通信服務予公眾使用之事業。而其設立的方式，必定爲指具有公司性質，且經交通部電信總局許可並發給執照經營第二類電信事業者。反之則屬非電信事業之網路服務提供者。

II　是否爲營利單位

電信事業是以提供電信服務獲取利潤爲目的，因此不用再做細分。而非電信

[142]參閱蔡茂寅等四人合著，「行政程序法實用」，二〇〇一年十一月一版，第二十五至二十六頁。
[143]參閱吳庚著，同前註 136 揭書，第六十六頁。

事業則可以其區分爲營利及非營利之單位，前者係指利用提供之網路服務獲取利潤，後者則係免費提供網路服務。

III　是否爲公司或個人

前述營利事業的部分，有屬於公司性質，例如網路銀行；亦有屬於個人性質，例如個人拍賣網站；而非營利單位可亦區分爲個人或公家或公益機構，前者爲個人網站者，後者爲圖書館、學校等。

IV　區分的目的

依照經營模式區分不同經營模式及規模的網路服務提供者，其目的在於決定其應負擔協助偵查義務的高低，其中應負擔最高的義務者爲，具有電信事業地位的網路服務提供者，因爲電信事業係利用公共的電信資源經營獲利，且經營規模最大，故應負有最高的協助責任。至於其他類型之網路服務提供者應負擔的協助責任大小，依序爲以營利爲目的之非電信事業公司性質、以營利爲目的之個人網站、非營利事業及公家及公益機構、最後爲非營利目的之個人。

5.1.4 立法參考

我國現行關於網路服務提供者協助偵查法制之不足處，如前所述包括規範主體範圍過於狹隘、有侵害用戶隱私權之疑慮、應提供協助偵查事項及相關配套之行政規定不是付之闕如，就是不夠完善等等缺失，以致偵查人員無法透過網路服務提供者提供之協助，達到有效提昇網路犯罪偵破率，降低網路犯罪發生率的目的。因此，本研究基於防治網路犯罪的目的，認爲現行法制確有修正或補強之處，並擬嘗試提供相關法制之建議，期能做爲建立一部完善的網路服務提供者協助偵查法制之參考。所謂「他山之石，可以攻錯」，由於網路服務提供者協助偵查法制在美國、英國及歐盟等國家早已有相關之規定，因此，以下將先介紹美

國、英國及歐盟等國家協助偵查法制之相關規定，並嘗試歸納各國關於規範主體、協助偵查事項範疇之具體規定，以做爲本研究提出具體法制建議之參考依據。

5.1.4.1 美國

美國爲網路之發源地，亦是網路使用最頻繁的國家，因此爲因應網路科技造成的網路泛濫情形及對於偵查機關在進行網路犯罪偵查的衝擊，早就針對相關法制進行研究及修訂，其中關於協助網路偵查法制部分，主要有電子通訊隱私法、愛國者法、犯罪偵查通訊協助法等相關法規，茲分述如後：

I　電子通訊隱私法

美國國會於一九三四年訂立聯邦通訊法（Federal Communication Act）來限制政府對於電話通訊之不當監聽。一九六八年制定犯罪控制及街道安全法第三篇（Omnibus Crime Control and Safe Street Act of 1968 Title III），該法內容主要是限制政府對於電話通訊及面對面談話內容的監聽，亦即擴大保護秘密通訊的範圍至有線通訊及口頭對話。一九八〇年美國國會於爲因應電信通訊科技快速進步，人與人之間的溝通已不限於使用有線網路通訊，制定電子通訊隱私法（Electronic Communications Privacy Act ，簡稱 ECPA）[144][145]。一九八六年晚期美國國會爲因應迅速發展的數位通訊時代的來臨，及近年來快速增加的駭客攻擊、電腦間諜等行爲，遂再次修正擴張 ECPA 之適用範圍，因而成爲美國第一部能保護人民在「電子通訊」的傳輸過程及儲存時，免於未經授權的截取、竊聽和洩露等行爲之

[144]See Electronic Communications Privacy Act of 1986,Pub.L.No 99-508,100 Stat. 1848.

[145]參閱謝穎青，通訊科技與法律的對話，太穎國際法律事務所資訊網，網址：http://www.elitelaw.com/05Publications/03promotion/%B2%C4%A4Q%A4G%B3%B9%A8%D3%B9q%C5%E3%A5%DC%AA%BA%C1%F4%A8p%C5v%C4%B3%C3D.pdf。。

聯邦法規[146]。而所謂「電子通訊」，依據本法係指「全部或一部經由有線、無線、電磁波、光電、光學之系統所傳送任何足以影響州際或外國商業之記號、信號、文書、影像、聲音、資料或任何性質之傳送」[147]。而本法所謂的電子通訊服務，係指提供用戶有能力傳送及接收電子通訊之服務[148]。

綜觀 ECPA 全文，關於協助偵查之規定，主要區分爲三章，茲分述如後：

i 電子通訊之截取及相關議題（Interception of Communications and Related Matters）

本章規定口頭或有線通訊服務提供者、地主、管理者或其他可以提供申請者所有資料、設備及必要的技術協助者（A provider of wire or electronic communication service, landlord, custodian or other persona provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary）負有協助執法單位實施截取傳輸中的通訊內容及相關紀錄之責任[149]。

ii 有線、電子通訊儲存與交易紀錄之進入（Stored Wire Electronic Communications and Transactional Record Access）

本章規定提供公眾有線或電子通訊服務之個人或機構（a person or entity providing an electronic communication service to the public）或「提供公眾電腦遠距服務之個人或機構（a person or entity providing remote computing service to the public），不得任意揭露使用者之通訊內容，除非在符合法律授權等特定條件下，

[146]參閱王邦琦著，同前註 5 揭書，第九十五頁。
[147]See 18 U.S.C. §2510.
[148]See 18 U.S.C. §2510.
[149]See 18 U.S.C. §2518.

才能例外地揭露使用者儲存之通訊內容[150]。

iii Pen Register and Trap and Trace 裝置（Pen Register and Trap and Trace Device）[151]。

本章規定口頭或有線通訊服務提供者、地主、管理者或其他可以提供調查或執行法律人員所有資料、設備及必要的技術協助者（a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary），負有協助裝置 Pen Register and Trap and Trace Device 等設備之責任[152]。

II 愛國者法

美國發生九一一恐怖攻擊事件後，凸顯出美國情報單位對於恐怖活動情報蒐集的漏洞，爲解決這一問題，美國國會於二〇〇一年十月二十五日通過美國愛國者法(Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001，又稱 USA PATRIOT ACT，簡稱 USAPA)，並由美國總統布希於隔（二十六）日簽署通過，該法案總計修正通訊監察法（Wiretap Statute Title III）、電子通訊隱私法（Electronic Communications Privacy Act）、電腦詐欺及濫用法（Computer Fraud and Abuse Act）、外國情報調查法（Foreign Intelligence Surveillance Act）、Pen Register and Trap and Trace Statute、洗錢法Money Laundering Act、移民法（Immigration and Nationality Act）

---

[150]See 18 U.S.C. §2702.
[151]參閱錢世傑著，網路通訊監察法制與相關問題研究，中原大學財經法律學系碩士論文，九十一年七月，第四十四頁。
[152]See 18 U.S.C. §3124.

等超過十五個不同的法案[153]，其中與網路犯罪偵查有關的部分主要是規定在第二章「調查程式之提升」（ENHANCED SURVEILLANCE PROCEDURES），主要內容如下：

i 擴大 Pen Register 位址紀錄器 and Trap and Trace 設備能截取之內容範圍至網路通訊內容[154]。

ii 擴張形式審查的證人傳票(subpoena)所能取得的資料範圍至用戶之信用卡資料及帳戶資料[155]。

iii 擴張可扣押的的電子通訊範圍至語音電子郵件（voice mail message）[156]。

iv 秘密搜索(sneak and peak search)明文化及擴大適用範圍[157]。

v 建立機動性監聽制度（Roving Wiretaps）[158]。

vi 緊急狀況下電子通訊內容強制揭露[159]。

vii 擴張適用範圍至有線電視經營網路業務者[160]。

對於網路犯罪偵查而言，美國愛國者法提供偵查機關更大的偵查權限，本法所規定的負有協助義務的適用主體，係指「任何提供有線或電子通訊服務之個人或機構及其他可以提供設備或科技協助之人」（a provider of a wire or electronic

---

[153]參閱網址：http://www.epic.org/privacy/terrorism/usapatriot/#analysis。最後瀏覽日期：二〇〇五年七月二十三日。
[154]See USA Patriot Act of 2001 §216.
[155]See USA Patriot Act of 2001 §210.
[156]See USA Patriot Act of 2001 §209.
[157]See USA Patriot Act of 2001 §213.
[158]See USA Patriot Act of 2001 §206.
[159]See USA Patriot Act of 2001 §212.
[160]See USA Patriot Act of 2001 §211.

communication service or other person to furnish facilities or technical assistance）[161]。

III　犯罪偵查通訊協助法

一九九四年十月美國國會，基於保護人民安全及國土安全，及偵查機關在面對快速進步的通訊科技的時代，仍能保存執行電子調查的法律的能力等等考量，通過犯罪偵查通訊協助法案（有學者譯爲協助法律執行通訊法）（Communication Assistance for Law Enforcement Act，簡稱 CALEA）[162]。依據該法案，「電信業者」（telecommunications carrier）負有協助執行法律的責任及要求電信業者設計或修改系統以確保合法授權的電子調查得以達到其目的。換言之，依該法案，電信業者在有法院命令（court order）或合法授權實施通訊監察的情形下，必須具備確保其裝置、設備或服務有具有如下之能力[163][164]：

i　迅速使政府有能力截取電信業者提供給用戶之服務範圍內之有線及電子通訊內容。

ii　迅速使政府有能力取得在電子通訊傳輸期間所合理取得之電話識別資料（call-identifying information ），或者是從屬於通訊之電話識別資料。不過，透過 pen registers and trap and trace devices 所取得的資料，則不包括得以顯示用戶所在地點的電話識別資料。

iii　傳送已截取的電子通訊內容及電話識別資料給政府。

---

[161]See USA Patriot Act of 2001 §222.
[162]See Communications Assistance for Law Enforcement Act of 1994 (CALEA), Pub. L. No. 103-414, 108 Stat. 4279.
[163]See 47 U.S.C. §1002.
[164]參閱錢世傑著，同前註 147 揭書，第六十八頁。

iv　在最小侵害用戶之電信服務之條件下，協助執行已授權之截取通訊及取得電話識別資料，並且在一定程度上，保護未經授權截取之通訊及電話識別資料與已經政府截取之通訊內容及已取得之電話識別資料之隱私及安全。

依據本法，其規範對象爲「電信業者」，至於「資訊服務業者」（information services）[165]、「私人網路業者」（private networks）、「長途網路通信業者」（interconnection services）等類型之業者，本法則免除像電信業者一般負擔必須使其設備可供執法機關進行合法監聽之義務[166]。

IV　小結

美國電子通訊隱私法與愛國者法所適用的主體並不限於電信事業，而包括所有電子通訊服務，其加諸電子通訊提供者協助偵查之責任，包括配合實施通訊監察、提供通信紀錄等等之責，但不包括建置相關通訊監察設備之義務。而犯罪偵查協助通訊法要求應建置相關通訊監察設備之義務所規範的對象則限定於電信業者，而資訊服務業者、私人網路業者、長途網路通信業者等類型之業者，則不用負擔必須使其設備可供執法機關進行合法監聽義務，但仍負有提供包括姓名與地址在內的詳細的客戶資料[167]。

5.1.4.2 英國（調查權力規制法）

英國於二千年七月通過「調查權力規制法」（Regulation of Investigatory Powers Act 2000，簡稱 RIPA）做爲網路偵查的利器，該法允許政府在較低的標準

---

[165]See 47 U.S.C. §1001(6) ，所謂「資訊服務業」，其定義係指「經由電信而產生、取得、儲存、轉換、處理、擷取、利用或製造可取得資訊之功能」。
[166]See 47 U.S.C. §1001(8) .
[167]參閱王郁琦著，同前註 5 揭書，第九十九頁。

下可以取得個人的電子通訊內容，依本法規定，業者負擔之協助偵查內容爲[168]：

I　負有協助實施通訊監察之義務[169]。

II　負責提供適合的設置使政府得以順利實施通訊監察：本法規定偵查機關基於偵辦網路犯罪之需要，得以要求 ISP 裝置後門程式，達到監視的目的[170]。

III　負有協助政府取得網路通聯紀錄之義務：本法規定基於國家安全或防止犯罪或偵查犯罪等理由，政府可以蒐集例如瀏覽紀錄、電子郵件收發紀錄、下載紀錄及登入紀錄等等[171]。

IV　擁有解密金鑰業者負有提供解密方法之義務[172]：本法規定負有提供解密金鑰責任的對象[173]爲擁有保護資料之金鑰之人，在偵查機關基於維護國家安全利益、預防或偵查犯罪之目的、英國經濟利益等目的[174]，以書面通知或其他能提供給予通訊紀錄之通知下，負有揭露解密方法之責任。

綜上，英國「調查權力規制法」之規範對象有二：一、郵政服務；二、公眾電信事業。而對於公眾電信事業的定義，係指「任何在英國一地或多地提供給公眾之電信服務」[175]，而此定義非常廣泛，因此可能適用於網路服務提供者、電話公司，甚而經營個人網站者[176]。

---

[168]See James Hammerton ，Regulation of Investigatory Powers Act (2000) －commentary，網址：http://www.magnacartaplus.org/bills/rip/#interception.
[169]See RIPA sections 1 to 11.
[170]See RIPA sections 12.
[171]See RIPA sections 22.
[172]See RIPA sections 49 to 56.
[173]See 錢世傑著，同前註 147 揭書，第一五一頁。
[174]同前註。
[175]See RIPA section 2(1).
[176]See James Hammerton ，Regulation of Investigatory Powers Act (2000) －commentary，網址：http://www.magnacartaplus.org/bills/rip/#interception.

5.1.4.3 歐盟網路犯罪公約

由於網路技術迅速發展並得到廣泛應用，爲全球經濟與社會發展帶來巨大變化，與此同時網路犯罪也滋生起來。雖然各國皆意識到網路犯罪泛濫的問題，並積極修改或訂定刑事法規，對於網路犯罪加強規範，但是由於網路無國界的特性，以及各國主權所繫之管轄權的影響，各國所訂立之內國法對於具有跨國性格的網路犯罪而言，並無根本防制的可能。因此各國在考慮到網路犯罪跨國性追訴之困難後，體認到唯有國際合作方能對利用網路從事犯罪之行爲人有實質的規範與警惕，再加上體認到各國國情及法制文化背景不一，亦唯有全球一致的立法才能提供網路使用者具體明確之指標，不至因跨越國界而受到兩種內容迥異系統之規範。是故各國乃企圖藉由協調國家立法及國際合作之方式，以達到保障安全生活的刑事政策目標[177]。因此面對網路犯罪在世界各國迅速發展，嚴重危害著各國和國際社會秩序的現象，爲有效遏制網路犯罪及針對網路犯罪對司法實務引發的衝擊，歐洲議會（Council of Europe，簡稱 CEO）自一九九六年開始組成電腦專家委員會（European Committee on Crime problem），著手進行相關立法工作，並於二〇〇一年十一月二十三日，由二十六個會員國和四個非會員國（美國、加拿大、日本與南非）在布達佩斯簽署成立了網路犯罪公約（Convention on Cybercrime）[178]。目前已簽署的國家超過四十個[179]。

依「網路犯罪公約」之規定，與協助網路犯罪偵查之部分主要係規定於第二

---

[177]參閱馮震宇著，網路犯罪與網路犯罪條約（上），財團法人亞太智慧財產權發展基金會智權情報網，網址：http://www.apipa.org.tw/Search/Article-ViewADA.asp?strSearch=網路犯罪與網路犯罪條約&intADAArticleID=89。最後瀏覽日期：二〇〇五年七月二十三日。

[178]參閱網址：http://stlc.iii.org.tw/tlnews/net9306.htm#n4。最後瀏覽日期：二〇〇五年七月二十三日。

[179]參閱章光明著，「莫讓網路成爲犯罪天堂路」，台灣年鑑，二〇〇五年。資料來源，我的 E 政府全球資訊網，網址：http://www.gov.tw/EBOOKS/TWANNUAL/show_book.php?path=3_011_001。最後瀏覽日期：二〇〇五年七月二十三日。

章（Section 2），其中要求服務提供者(service provider)應配合協助的事項如後：

I　應迅速保存儲存及提供電腦中之相關資料[180]。

II　應迅速儲存及部分揭露通信紀錄[181]。

III　協助實施搜索及扣押[182]。

IV　協助即時收集通信紀錄[183]。

V　協助截取內容資料[184]。

依「網路犯罪公約」之規定，其適用的規範主體爲「服務提供者」(service provider)，而所謂的服務提供者之定義，係指「提供用戶有能力經由電腦系統進行通訊的任何公眾或私人機構」(any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and any other entity that processes or stores computer data on behalf of such communication service or users of such service)[185]，因此包括任何提供網路服務提供者，而不限於電信業者。

5.2 立法重點

5.2.1 擴大規範對象

5.2.1.1 專法之規範對象定義

我國關於協助網路犯罪偵查的規定，主要係依據電信法、通訊保障及監察

[180]See Convention on Cybercrime Article 16.
[181]See Convention on Cybercrime Article 17.
[182]See Convention on Cybercrime Article 19.
[183]See Convention on Cybercrime Article 20.
[184]See Convention on Cybercrime Article 21.
[185]See Convention on Cybercrime Article 1.

法、第二類電信事業管理規則第二十七條等規定，所規範的對象僅限於「電信事業」，即指具有「股份有限公司」，就是「已辦理公司或商業登記之單位」，並經交通部許可核發執照經營第二類電信事業者。而不包括非電信事業的網路服務提供者，包括學校、圖書館、私人網站站主、網路咖啡店及非屬電信事業的機構等在內。換言之，非電信事業的提供者並不負有協助偵查的義務。然而，我國偵查單位實際進行網路犯罪偵查之現況，無論是調閱使用者資料、通聯紀錄或是實施通訊監察，不僅需要具有第二類電信事業資格之網路服務提供者之協助，亦需要非電信事業之網路服務提供者之協助。顯見，前揭法規之規範對象範疇過狹，無法涵蓋所有的網路服務提供者。

事實上，行政院新聞局於民國九十三年四月二十六日公佈之「電腦網路內容分級處理辦法」曾嘗試賦予網路服務提供者定義，依該辦法第二條第一項該規定網路服務提供者係指「網際網路接取提供者、網際網路平臺提供者及網際網路內容提供者」[186]，並分別予以定義[187]。

前述辦法雖然是我國法制對於網路服務提供者之唯一定義，但是該辦法之位階僅爲法規命令之地位，並且前述分類的方式所分類之依據標準爲何不明，其中網路平臺服務提供者、網路內容服務提供者二者之定義又相去不遠，如何分辨著實有困難。以提供全球資訊網服務爲例，雖歸類於網路平臺服務提供者，然檢視業者提供的服務內容，包括提供新聞、娛樂等資料、網站檢索等功能，似乎包涵

[186]網路服務提供者，學者依其提供服務內容的不同，通常將之區分爲網路連線服務提供者（Internet Access Provider, IAP）、網路內容服務提供者（Internet Content Provider, ICP）及網路平臺服務提供者（Internet Platform Provider, IPP）三種型態。參照張雅雯著，「網路服務提供者就網路違法行爲之法律責任」，律師雜誌，第二二八期，一九九八年九月，第四十四頁。

[187]網路接取服務提供者依電腦網路內容分級處理辦法第二條第三項規定係指「以專線、撥接等方式提供網際網路連線服務之業者」；網路平臺服務提供者依同條第四項規定係指「提供全球資訊網、電子郵件、全文檢索等網際網路資訊相關服務之業者」；網路內容服務提供者依同條第五項規定係指「實際提供網際網路資訊相關服務之業者」。

在前揭辦法所指之網路內容服務提供者之定義中，因此前揭定義的參考價值令人質疑。綜上，電信法、通訊保障及監察法、第二類電信事業管理規則第二十七條等規定，所規範的對象僅限於「電信事業」，並無法涵蓋所有的網路服務提供者；而電腦網路內容分級處理辦法，雖然賦予網路服務提供者之定義，但參考價值仍待質疑。

綜上理由，本研究認爲有必要在網路服務提供者協助偵查法制中，明確網路服務提供者之定義，並且擴大其範圍。至於具體的定義，本研究擬參酌歐盟網路犯罪公約對於服務提供者之定義「提供用戶有能力經由電腦系統進行通訊的任何公眾或私人機構」及南非共和國於二〇〇三年一月二十三日公佈之「Regulation of Interception of Communication and Provision of Communication–related Information Act」對於網路服務提供者之定義「任何人提供網路連線或任何予網路有關的服務予另一個人，並且不論這些連線或服務是否根據電信法第五章取得電信事業執照」（Internet service provider means any person who provides access to, or any other service related to, the Internet to another person, whether or not such access or service is provided under and in accordance with a telecommunication service licence issued to the first-mentioned person under Chapter V of the Telecommunications Act）[188]。換言之，網路服務提供者係任何提供網路相關服務之個人或機構，而不侷限電信事業。

5.2.1.2 專法規範對象之類型

網路服務提供者的定義係指任何提供網路相關服務之個人或機構，惟網路服務提供者提供的服務，隨著寬頻網路的發展，提供的服務內容從原本單純提供連

[188] See Regulation of Interception of Communication and Provision of Communication –related Information Act sec.1，網址：http://www.internet.org.za/ricpci.html#internetserviceprovider.

線服務逐漸多元化，爲便於探討提供不同服務內容之提供者擔負協助偵查之責任及事項，本研究以爲有細分其類型之必要，茲嘗試加以區分如後。

I　區分服務類型

i　連線服務

提供用戶連結網路的服務，無論是使用電話線、寬頻或是透過有線電視提供的纜線連結網路，均屬之。

ii　通訊服務

通訊服務係指提供用戶有能力傳送及接收電子通訊之網路服務，例如網路電話、電子郵件，即時通訊、ICQ。以電子郵件爲例，張三連結上網後，透過電子郵件主機伺服器，將電子郵件傳送至李四。

iii　資訊（內容）服務

網路服務提供者所提供之服務內容並非通訊服務，而係自己編輯資料訊息，利用網路傳遞方式提供訊息予不特定人可以瀏覽查閱，此種服務類型與美國犯罪偵查通訊法所指之「資訊服務」（information services）的定義「經由電信而產生、取得、儲存、轉換、處理、擷取、利用或製造可取得資訊之功能」大致相同[189]，具體服務內容包括線上學習、線上遊戲、線上圖書館、線上新聞網、數位影音服務、雅虎搜索網、蕃薯藤網站。

iv　空間服務

網路服務提供者提供的服務係提供用戶伺服器空間，使用戶得以利用該空間進行全球資訊網隨意瀏覽、進行電子郵件的發送與接收及進行即時通訊，例如

[189]See 47 U.S.C. §1001(6).

bbs、論壇、聊天室。

v 提供網路連線場所服務

網路服務提供者提供的服務內容係提供使用者場所，而使用者得以利用該場所之連線設備上網查詢、收發電子郵件等等，例如圖書館、學校等，其中最爲特殊的爲近幾年興起的網路咖啡店（簡稱網咖）。

網路咖啡店原本經營的方式係以提供飲料或餐食，並提供電腦供人上網查詢資料、收發電子郵件、網路聊天、線上遊戲等多樣服務，惟目前的網路咖啡店業者主要從事電腦設備設置遊戲光碟或上網擷取網路遊戲軟體，以供人娛樂之營業行爲[190]。網路咖啡店的興起，如同傳統的公共電話亭一般，提供使用者另一種選擇，使用者不再僅能於家中或辦公室才可以使用網路，對於促進網路使用帶來很大的效用。惟由於網路咖啡店提供便利的連線網路服務，對於犯罪行爲人而言，具有高度的隱匿性，以致犯罪行爲人透過網路咖啡店從事犯罪行爲時，偵查人員往往只能循線追查到該網路咖啡店，而無法追查到實際之行爲人，於是網路咖啡店成爲網路偵查很大的盲點，透過網路咖啡店從事犯罪行爲的數量也逐年增加[191]。

各國爲瞭解決網路犯罪行爲人利用網路咖啡店提供的服務從事犯罪行爲，已開始著手立法加以規範，例如中華人民共和國制訂之「互聯網上網服務營業場所管理條例」[192]；南韓則制訂之「碟片影帶及遊戲物管理法」[193]規範網路咖啡店。

---

[190]參閱曾惠仙，網咖經營之適法性與法令問題，網址：http://www.cqinc.com.tw/grandsoft/cm/093/aru931.htm。最後瀏覽日期：二〇〇五年七月二十三日。

[191]參閱內政部警政署全球資訊網統計資料，網址：http://www.npa.gov.tw/stats.php?page=content06_1&id=72&tr_id=73&pages=5.。最後瀏覽日期：二〇〇五年七月二十三日。

[192]參閱中國網，網址：http://big5.china.com.cn/chinese/PI-c/216517.htm。

[193]參閱經濟部全球資訊網，「南韓對網路咖啡業管理現況、作法暨有關法令規範」，網址：http://www.moea.gov.tw/~meco/doc/ndoc/pub_901023_2.doc。最後瀏覽日期：二〇〇五年七月二十三日。

而我國爲防範在網路咖啡店的犯罪行爲，經濟部亦擬定「資訊休閒業管理條例草案」[194]送交立法院審議中。該草案中第十二條即明文要求網路咖啡店業者應在營業場所設置防止賭博及色情網路內容篩選過濾設備、現場錄影監視器及警民連線裝置、使用者登錄之歷史紀錄檔設施等。惟本文認爲網路咖啡店提供網路連線場所服務，應涵蓋於網路服務提供者之定義內，可納入網路服務提供者協助偵查法一併討論。

II　區分的目的

區分各種不同服務內容的網路服務提供者，在於決定其可以協助偵查事項之種類，而爲方便說明各類型服務提供者各自應負之協助事項，本文以下謹針對主動過濾內容、刪除及阻斷服務、儲存及提供使用者之資料、儲存及提供通信紀錄，協助實施通訊監察等五項協助偵查事項分述如後：

i　連線服務提供者

網路連線服務提供者提供用戶得以連結上網路之服務，因無法事先監控用戶傳遞之內容，無須擔負過濾之責任之外，其他包括刪除及阻斷服務、儲存及提供使用者之資料、儲存及提供通信紀錄，協助實施通訊監察等協助事項，仍須負擔協助責任。

ii　通訊服務提供者

通訊服務提供者提供用戶在網路上有能力傳送及接收電子通訊服務，對於透過其服務傳送的通訊內容均能有所監控，因此負擔的協助事項較多，包括主動過濾、刪除及阻斷服務、儲存及提供使用者之資料、儲存及提供通信紀錄，協助實

[194] 參閱經濟部全球資訊網，焦點新聞，網址：http://w2kdmz1.moea.gov.tw/user/news/detail-1.asp?kind=1&id=8946。最後瀏覽日期：二〇〇五年七月二十三日。

施通訊監察（限於技術許可之情形下）等事項。

iii　資訊服務提供者

資訊服務提供者因係提供自行編輯訊息之服務，原則上不會發生有犯罪行爲人利用其服務從事犯罪之行爲，因此原則上無須負擔協助偵查之責任。

iv　空間服務提供者

空間服務提供者無法事先或即時掌握利用其服務所從事之任何利用網路之行爲，無法事先過濾內容，也無法協助配合實施通訊監察，因此只須負擔儲存提供使用者資料、事後刪除、阻斷服務及儲存及提供相關通信紀錄之協助責任。

v　場所服務提供者

場所服務提供者係提供場所、設備供客戶上網連線、查詢資料、發收電子郵件等服務，其性質如同個人使用的電腦一般，可以設置過濾裝置以過濾不法之資訊，因此負有主動過濾之義務。其他協助刪除、阻斷服務、儲存及提供使用者資料、儲存及提供連線通信紀錄等等協助事項亦可提供。惟在協助實施通訊監察部分，我國目前並無類似美國關於「機動性監聽（Roving Wiretaps）」之法制，故偵查人員無法在提供連線的場所實施通訊監察。

5.2.2 強化協助義務

面對網路發展及網路犯罪的泛濫現象，本研究認爲我國現行法令確實有所不足而有必要加以檢討，並建議應明文規定網路服務提供者協助偵查之義務，強化網路服務提供者在偵查過程中的角色，以利於網路犯罪偵查，順利偵破網路犯罪行爲。惟因本研究主題及範圍乃限縮於在網路犯罪偵查過程中之「偵查階段」，亦即從偵查人員受理案件到調查完畢移送法院審理爲止之階段，至於「偵查前」及「偵查後」之部分則非本研究探討之部分。因此，以下針對網路服務提供者協

助偵查法中應強化網路服務提供者之具體建議，僅限縮在網路服務提供者於網路犯罪偵查之「偵查階段」所應強化協助義務事項，茲分述如後。

5.2.2.1 強制刪除、阻斷不法資訊[195]

I 規範理由

i 降低不法資訊流通之機會

任何網路上傳遞的資訊，不論是合法或不法的資訊，都必須透過網路服務提供者的服務才能在網路上傳遞，因此對於網路上傳遞或張貼之不法資訊，例如色情網站上張貼含有色情或猥褻的圖片或文字或在 BBS 站上散佈販售槍、毒品等不法資訊，甚至透過電子郵件夾帶電腦病毒企圖損害他人的電腦等等，網路服務提供者如能負有適時地予以阻斷、刪除之責任，透過網路服務提供者協助，使該等不法資訊無法繼續在網路上流傳，除可達到預防網路犯罪的目的，亦可減少可能造成的損害程度。例如刪除網路上張貼的色情文字或圖片，使得青少年無法取得該不法資訊，避免造成青少年身心發展之偏差。

ii 明確業者之責任

目前我國電信法第八條第二項及第二十二條但書規定，係賦予電信業者停止傳遞、刪除不法資訊服務之權利，而非加諸其刪除之義務；再加上電信業者負有審酌使用者傳遞之資訊是否符合「以提供妨害公共秩序及善良風俗內容爲營業」或「顯有危害國家安全或妨礙治安」等要件之責任，而這些要件均屬於「不確定的法律概念」，如何認定著實困難；更何況，一旦發生認定錯誤，現行條文並無

[195]中華人民共和國電信條例第六十二條規定，在公共資訊服務中，電信業務經營者發現電信網絡中傳輸的資訊明顯屬於本條例第五十七條所列危害國家安全、擾亂社會秩序，破壞社會安定等不法內容，應當立即停止傳輸，保存有關記錄，並向國家有關機關報告。參閱中國互聯網絡資訊中心全球資訊網，網址：http://www.cnnic.net.cn/html/Dir/2000/09/25/0651.htm。最後瀏覽日期：

任何免責規定，因此又可能因冒然停止用戶網路服務，而陷入違反與用戶間服務契約及侵害使用者言論自由遭到請求賠償之囹圄。因此業者考量本身之利益及不負有強制刪除義務之雙重因素下，業者往往不願自行刪除不法資訊，放任不法資訊持續在網路上流通，使得前揭電信法規根本無法達到其規定之目的，因此本文認爲應以立法方式明確網路服務提供者負有強制刪除、阻斷之責任，及配合偵查作爲的免責規定，才有可能達到防堵不法資訊的流通及預防網路犯罪的目的。

II　適用要件

i　應刪除、阻斷的資訊爲「不法」資訊

網路服務提供者刪除或阻斷使用者在網路上傳遞之資訊，乃嚴重侵害到侵害到使用者的言論自由之行爲，因此保障使用者的權利，對於網路服務提供者應刪除或攔截的資訊必須限縮其範圍，即限於依現行法令或實務判決，足以認定爲「不法」之資訊，才能予以刪除或阻斷。換言之，該被刪除或阻斷之的資訊，必須經認定含有「妨害公共秩序及善良風俗、危害國家安全或妨礙治安」等內容。

ii　刪除、阻斷的目的係基於維護國家安全或社會治安

透過立法方式強制網路服務提供者配合刪除、阻斷不法資訊流通的目的，必定是基於維護國家安全、社會秩序等等公益之需要，所不得不爲之手段。例如我國反恐怖行動法草案第六條第四款即規定「爲處理重大恐怖攻擊事件之需要，避免人民遭受緊急危難，國家安全局得命阻斷或限制相關通信」[196]。

iii　經治安機關或主管機關通知

二〇〇五年七月二十三日。

[196]參閱法務部主管法規資料庫查詢系統－法規草案，網址：http://mojlaw.moj.gov.tw/ShowScript.asp?id=2898。最後瀏覽日期：二〇〇五年七月二十三日。

網路服務提供者逕自強制刪除、阻斷不法資訊，雖然應刪除、阻斷的資訊均屬於不法的資訊，惟所謂「妨害公共秩序、善良風俗內容爲營業」或「顯有危害國家安全或妨礙治安」等要件，屬於「不確定的法律概念」而必須做判斷，對於網路服務提供者而言，不見得有能力去做違法與否的認定。從使用者的角度來看，網路服務提供者並非偵查或審判機關，逕由其自行認定是否屬於不法資訊，進而刪除或阻斷其傳遞，有過度擴張其權力而嚴重侵害到使用者的言論自由。因此，爲避免發生網路服務提供者享有過度刪除的權力而影響使用者的言論自由，以及避免網路服務提供者陷入認定違法與否的困境，本研究建議網路服務提供者經治安機關（包括警調單位、地檢署、法院）或主管機關（交通部電信總局）認定屬於不法資訊，並書面通知網路服務提供者後，再執行刪除資訊、阻斷服務的作爲。

iv 書面通知或公告

網路服務提供者執行刪除資訊、阻斷服務的作爲後，應書面通知使用者，如不能通知者（例如無法查明使用者的身份）應予以公告。按網路服務提供者經治安機關或主管機關通知並刪除資訊、阻斷服務的作爲，係屬於侵害使用者的權利之行爲，而前揭治安機關或主管機關的通知，其性質可視爲行政處分，因此本文建議仿照行政程式法第九十六條之規定應書面通知行爲人，一則提供使用者有提出救濟之機會；二則透過事後通知的方式，使執行人員更謹慎爲之，防止更進一步可能造成人權的侵害。

5.2.2.2 主動舉發

I 規範理由

網路服務提供者爲提供用戶最好的服務，會不定時的檢查內容及維護系統，對於用戶利用其網路服務從事犯罪行爲乙事，遠比偵查人員更早發掘，因此網路

服務提供者如能在發現在違法之情事，立即保存證據並向偵查單位舉報，除能掌握偵查網路犯罪的契機、避免偵查時程的延宕，以達到迅速偵破的目標[197]。

II 適用要件

i 明顯屬於犯罪之內容

網路服務提供者負有主動舉發、保存證據的責任，必須限定於明顯即可判斷爲犯罪內容之資訊，按不明顯屬於犯罪行爲的資訊，逕自提供給偵查機關，不但會侵害到使用者的言論自由，且會加諸網路服務提供者擔負認定責任，造成額外的經營成本及壓力。

ii 相關犯罪證據必須由偵查機關依法定程式取得

網路服務提供者雖負有保存犯罪通訊內容之義務，但此舉係爲了保全犯罪證據，避免日後因證據滅失，致無法繼續偵查所不得不爲之作爲，但網路服務提供者仍不得逕自提供給偵查機關，而必須由偵查機關依法定程式取得，以免過度侵害到用戶之隱私權。

5.2.2.3 使用者資料範圍應包括付款資料

I 規範理由

網路偵查的第一步驟就是要清查過濾行爲人的身份，而清查身份的方式就是透過向網路服務提供者調閱使用者的資料，包括申請連線帳號、免費電子郵件、免費網站所登記之資料，惟由於前述使用者資料由於業者無法認證，導致偵查單位調閱到的使用者資料根本是錯誤的，而無法繼續偵查下去。事實上，在傳統犯罪偵查實務中，偵查機關向電話業者調閱電話申登資料中，申請「預付卡」所填

[197]同前註 196。

寫的資料大多不正確，即使申請「易通卡」，其個人基本資料與實際使用人之基本資料也常不符合的情形。爲解決用者申請資料及實際身份無法吻合的問題，交通部電信總局要求電信業者對新申裝用戶，全面實施「雙卡」身分證件查核措施，換言之，國人申請電信服務必須同時出示「國民身分證」、「健保卡」或其他有效之身分證明文件接受查核[198]，惟電信業者缺乏辨別申請人真實身份之能力，縱使拿出的證明文件均是僞造的，電信業者亦無法發覺。更遑論，目前網路服務提供者提供免費電子郵件及網站之申請，均是在網路線上直接填寫個人資料辦理，根本無須提出任何證明文件，更是無從稽查申請人之實際身份。

因此爲了有效查明使用者的身份，美國愛國者法將可以調閱的使用者資料擴大到客戶付款的資料[199]，按取得使用者的金融資料，是除了以現金方式支付外，如果係以轉帳或是刷卡方式，均會有相關信用卡資料及銀行帳戶資料，由於這些金融資料牽涉到金錢，其正確性較高，故得以做爲偵查機關辨別嫌疑人身份之用。本文建議應仿照美國愛國者法案，擴大偵查機關得調閱的使用者資料範圍至用戶的付款資料。

II　適用要件

個人之金融機構帳戶資料除爲私人隱私權外，亦具有財產權對外存在之形式，均應受保護，原則上對於上開財產權政府應避免干涉介入，於例外情況下，依憲法第二十三條之規定，政府並非不得以法律限制之。如司法警察機關之犯罪調查，屬於「維持社會秩序」之必要手段，於相關法律規定授權下，得以侵害最小之方式下，向網路服務提供者調閱客戶所留存之金融帳戶資料，所實施之調閱

---

[198] 參閱交通部電信總局全球資訊網，網址：http://www.dgt.gov.tw/chinese/News-press/93/press-dgtnews-930429.shtml。最後瀏覽日期：二〇〇五年七月二十三日。

[199] See USA Patriot Act of 2001 §210 (1) (F).

金融帳戶資料雖有其必要性，相對於個人之姓名、地址、聯絡方式之隱私權更深，爲避免偵查單位透過一般公文肆意調閱使用者之相關金融資料，而過度侵害到使用者之隱私權，對於金融資料的調閱的程式[200]應比調閱一般使用者資料來的嚴格，本文建議仿照目前偵查機關向金融機構調閱客戶金融資料的方式，其調閱的程式如下：

i　經單位主管同意

查詢金融相關資料應經單位主管事先核可，以法務部調查局爲例，查詢金融相關資料前，必須經該局局長(副局長)審核認定爲必要者，始可以正式公文向銀行調閱相關資料。

ii　基於偵辦案件之需要

調閱金融相關資料的目的，必須是出於辦案需要，並且調閱公文內容中，必須載明調閱的目的係爲偵辦案件需要，同時註明案由。

iii　調閱對象應爲特定之帳號

調閱金融資料乃嚴重侵害人民隱私權的行爲，必須審慎爲之，若允許偵查機關調閱不特定對象之金融資料，係過度擴張偵查機關的調查權力，因此必須限定某特定對象。例如偵查機關只能調閱某特定電子郵件帳號之金融資料，而非針對某特定人調閱相關金融資料。

iv　以網路服務提供者有留存者爲限

網路用戶付款的方式不限於使用信用卡或轉帳，且網路服務提供者並無任何

[200]目前調閱金融資料程式，係依據行政院金融監督管理委員會於二〇〇五年三月二日公佈之「重新發布司法等機關向銀行查詢客戶存放款等相關資料之規定」辦理。參閱行政院金融監督管理委員會銀行局全球資訊網，網址：http://www.boma.gov.tw/ct.asp?xItem=219890&ctNode=1571。

權力限定用戶付款的方式，故網路服務提供者不一定會留存用戶之金融資料，因此偵查機關調閱金融資料只能以網路服務提供者有留存之資料爲限。

5.2.2.4 自願揭露已儲存之通訊內容

I 規範理由

網路通訊的內容，例如傳遞電子郵件的紀錄及內容，均會留存於網路服務提供者的主機伺服器裡。對於網路偵查而言，網路服務提供者所保存之犯罪相關通訊內容，如能主動揭露予偵查機關，由於偵查人員能迅速掌握犯罪相關證據，有利於後續案件的推動，不但能大大縮減偵查時效，亦可避免發生因證據之遺失而無法繼續偵查的情形。惟由於我國目前法制欠缺關於取得已儲存於網路服務提供者之通訊內容之任何規定，更遑論關於自願揭露已儲存之通訊內容之相關規定。

反觀美國關於網路服務提供者自願揭露資訊之規定，對於主要是規定在電子通訊隱私法，依該法規遠距電腦服務或電子通訊服務提供者（a provider of remote computing service or electronic communication service to the public）等網路服務提供者可否自願揭露資訊予偵查機關，當首需區分網路服務提供者所提供之服務是否供「公眾」使用。假設網路服務提供者並未向公眾提供服務，則該法對於內容之揭露，並未設置任何限制[201]；反之，網路服務提供者係向公眾提供服務，則禁止揭露內容予偵查機關，除非符合該法第 2703 條（b）（6）之例外規定「若通訊內容係網路服務提供者非不慎取得或通訊內容與犯罪行爲有明顯關聯，服務提供者可以揭露通訊內容給執法機關」[202]（A person or entity may divulge the contents of a communication to a law enforcement agency, if such contents: (A) were

---

最後瀏覽日期：二〇〇五年七月二十三日。

[201]See 18 U.S.C. §2702 (a).

[202]參閱錢世傑著，同前註 147 揭書，第六十頁。

inadvertently obtained by the service provider; and (B) appear to pertain to the commission of a crime.）[203]。美國 911 恐怖攻擊事件發生後，爲防止類似恐怖攻擊事件再度發生，美國於 2001 年通過愛國者法案，修正擴大電子通訊隱私法有關內容揭露之例外規定[204]，依該規定電子通訊服務提供者在合理相信對於任何人生命或嚴重身體傷害之緊急情況存在時，應立即主動將用戶的通訊內容及紀錄等資料揭露給執法單位[205]（A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information）。

事實上，隨著網路的發達，使得網路成爲通訊的重要工具，甚至成爲犯罪份子彼此連結犯罪計畫的工具，雖然網路通訊享有其通訊秘密之權利，但面對可能造成人民生命、身體遭受侵害的緊急時刻，若網路服務提供者能機先掌握犯罪的通訊內容，並提供給偵查機關，使偵查機關得以事先掌握相關情資，應能順利化解可能發生的傷害及損害。因此本文建議可參酌美國相關法規，賦予網路服務提供者在一定條件下有自願揭露通訊內容之權力。

II 適用要件

i 適用對象限於對公眾提供服務之網路服務提供者

ii 犯罪有明顯危害任何人生命或嚴重身體傷害之緊急情況

網路通訊內容，除非是公開之資訊外，享有高度秘密通訊的自由，因此網路

[203]See 18 U.S.C. §2702 (b) (6).
[204]See USA Patriot Act of 2001 §212.

服務提供者對於使用者任何之通訊內容，原則上均不得予以窺視或揭露，否則即違反憲法之規定，甚至可能影響到網路使用者對於網路的信任，而造成使用者的恐慌，對於網路發展而言並非有利。網路服務提供者主動將網路通訊的內容保存，並提供給偵查機關，比前述經治安機關或主管機關通知而刪除資訊或阻斷服務之作為，侵害使用者的隱私權、言論自由更為嚴重，惟因此必須嚴格限制其適用條件，本文建議網路服務提供者只有在合理相信有事實顯示危害任何人生命或嚴重身體傷害之緊急情況件下，由於保障生命、身體權等法益比維護隱私權更重要，方例外允許主動提供相關犯罪內容給偵查機關。若通訊內容顯示並不危害到生命、身體法益，雖然與犯罪行為有明顯關聯，網路服務提供者亦不得自願揭露網路犯罪內容，以免違反憲法之比例原則，此時可依本文前述保存證據，並向偵查機關舉發，再由偵查機關透過法定程式（以搜索扣押方式）取得該犯罪證據。

5.2.2.5 通信紀錄提供應有明確法律授權依據

I 規範理由

網路上的通訊紀錄是協助犯罪調查之重要工具，即使不在犯罪調查程式中，要求網路服務提供者留存相關通信紀錄，在技術上不但可行，並不違反民主社會中對民眾隱私權保護與犯罪偵查必要性的比例原則[206]。因此，有強制網路服務提供者保存通信紀錄之必要。然而，我國目前要求網路服務提供者保存及提供相關通信紀錄，係依據第二類電信事業管理規則第二十七條之規定；由於該規定管理規則屬於法規命令之性質，而其規範的內容卻涉及實質侵害民眾秘密通訊的權利，顯然並不符合憲法保留原則，因此有必要以法律方式規定，明確網路服務提供者應負有保存及提供之義務。

---

[205]同前註 203。

II 適用要件

i 調閱的機關應限定爲治安機關

強制網路服務提供者負有保存及提供通信紀錄，其目的在於透過保存之通信資料，尋求蛛絲馬跡，作爲偵查網路犯罪之參考，因此只限於治安機關才能調閱，而不包括行政機關。至於新修正之電信法規定用戶得調閱本人之通信紀錄乙節，因與本文並無相關，不予贅述[207]。

ii 調閱對象應爲特定之帳號

治安機關調閱通信紀錄，必須以某特定電子郵件帳號爲對象，而不得以某特定人爲對象調閱相關通信資料。

iii 調閱的資料不包括通訊內容本身

iv 以正式公文辦理

調閱通信紀錄必須以正式公文辦理，且公文中必須表明係爲偵辦案件需要並註明案由。

5.2.2.6 儲存通信紀錄的期間應延長

I 規範理由

從偵查實務的流程分析，網路案件發生時間與受理時間往往有一定之差距，偵查流程從案件立案、清查過濾、調查證據、案件執行到移送，亦必須耗費相當之時間，以清查過濾行爲人階段做說明，偵查人員與網路服務提供者之公文往返須耗費時間；研閱比對向網路服務提供者調閱之資料以過濾出行爲人亦須耗費時

---

[206]參閱吳炎琰著，論網路環境下的通訊監察法制，科技法律透析，二〇〇五年二月，第五十頁。
[207]參閱交通部電信總局全球資訊網，網址：http://www.dgt.gov.tw/chinese/Regulations/5.1/Telecom-

間，更遑論類比之的偵查作爲往往要重覆幾次，因此在時間的耗費是無法估計的。特別是電子郵件通聯紀錄之保存期間僅短短的一個月，根本無法滿足偵查實務之需求，因此有必要延長儲存期間。

II　延長期間

儲存通信紀錄的期間延長的期間究竟多長才合理，除了考量網路犯罪偵查的需要外，於必須考量網路服務提供者的技術能力及經營成本，按時間愈長對於網路犯罪偵查最好，但相對地網路服務提供者必須花費更多的金錢及人力去保存。對此美國相關法規並未規定通信紀錄之保留期限，因此有提供者保留數個月，有則數小時，亦有完全不保留，此種制度可能導致偵查機關取得適當合法命令強制揭露之前，證據可能遭毀損消逝[208]，本文認爲沒有參考之價值；而歐盟關於通聯紀錄的保存規定，依據在二〇〇二年七月十二日公佈之「隱私及電子通訊指令」(Directive on privacy and electronic communications)[209]修改一九九五年個人資料保護指令（Directive 95/46/EC）特定條文之適用，對於通信紀錄的部分，該指令容許各會員國立法要求強制網路服務提供者留存通信紀錄一定期間[210]，之後歐洲議會又提出「留存通訊紀錄決定草案」(Draft Framework Decision on the retention of traffic data and on access to this data in connection with criminal investigations and prosecutions）[211]，建議歐盟要求各國政府立法強制提供通訊服務提供者留存所有的通訊紀錄，期限從十二個月至二十四個月不等。惟依前述草案之規定似乎過

Acts.shtml。最後瀏覽日期：二〇〇五年七月二十三日。

[208]參閱黃育勳，電腦之搜索扣押，國立臺北大學法學學系碩士論文，八十九年六月，第一一七頁。

[209]參閱立法院全球法律資訊網，網址：http://npl.ly.gov.tw/do/www/billIntroductionContent?id=22。最後瀏覽日期：二〇〇五年七月二十三日。

[210]參閱 Directive 2002/58/EC §15，轉引至吳炎琰，論網路環境下的通訊監察法制，科技法律透析，二〇〇五年二月，第五十頁。

[211]參閱http://www.statewatch.org/news/2002/aug/05datafd.htm。轉引至吳炎琰，同前註揭書，第五十

長，而易造成網路服務提供者過多的負擔。本文認爲通聯紀錄保存的期限，可參照法務部公佈之電腦犯罪統計分析中，依該統計資料顯示各地檢察署偵辦電腦犯罪案件平均結案日數爲五十二日做爲基準[212]，由於依目前犯罪案件偵查流程，多是先經司法警察機關進行偵查後，移送至各地檢察署，再由檢察官進行偵訊，而司法警察機關受理網路犯罪時，通常是證據相當薄弱，因此必須從頭開始，因此其偵查時程比檢察官偵查的日數約爲二倍以上的時間，再加上網路犯罪不易發覺的特性，常有延遲報案，情形，因此本文建議保留期間應介於六個月以上至十二個月間爲宜。

5.2.2.7 擴大協助通訊監察案件適用之範圍

I 規範理由

我國通訊保障及監察法爲符合憲法的比例原則，因此限定其實施通訊監察，必須係符合第五條、第六條、第七條所規範之特定的罪[213]，然而網路犯罪中常見的網路色情、網路賭博、網路誹謗，甚至是妨害網路使用罪章各罪等罪，並不在前述特定犯罪之內[214]，且因爲這些類型的網路犯罪之最輕本刑均爲在三年有期徒刑以下，因此亦不符合第五條第一項第一款之規定，換言之依目前通訊保障及監察法根本無法實施通訊監察。然而網路犯罪日益擴大，且造成的損害不比傳統犯罪小，不僅會破壞社會秩序，甚至可能影響國防安全，其影響程度事實不容覷。再加上網路犯罪偵查困難，若單純考量網路監察對於人民隱私權的侵害，而仍依比例原則的原理考量，堅持若非特定之重罪，不准許偵查機關運用通訊監察的方

頁。最後瀏覽日期：二〇〇五年七月二十三日。

[212]參閱法務部全球資訊網－法務統計，網址http://www.moj.gov.tw/tpms/statanal2.aspx。最後瀏覽日期：二〇〇五年七月二十三日。

[213]參閱全國法規資料庫，網址：http://law.moj.gov.tw/Scripts/NewsDetail.asp?no=1K0060044。最後瀏覽日期：二〇〇五年七月二十三日。

[214]參閱蔡美智，同前註 110 揭書，第四十一頁。

式蒐集網路犯罪證據，將難以遏止日益泛濫的網路犯罪。綜上可知，現行通訊保障及監察法所規定的特定之罪，確有檢討之必要。因此，爲在人民隱私權與國家安全、社會利益之間尋求適當的平衡，本文認爲應就各種不同類型的網路犯罪所可能造成的損害及實施通訊監察之必要性加以評估，網路犯罪類型中，包括網路賭博、網路侮辱、網路誹謗、網路色情等等，因爲屬於侵害性輕微的網路犯罪，且從偵查角度而言，證據的蒐集並不困難，因此不宜納入實施通訊監察之範圍內；惟網路犯罪類型中的網路入侵、網路病毒等等，所可能造成的損害及影響重大，例如電腦駭客入侵企業或政府機構的電腦系統並加以破壞，往往會造成企業的重大損害或危害國家安全，此類型之網路犯罪若無法實施通訊監察，對於偵查機關進行犯罪偵查以維護人民、國家安危，會有極大的阻礙。因此有必要將這類型的網路犯罪納入得實施通訊監察之範圍內。換言之，爲遏止網路犯罪的泛濫，以提供更安全的網路空間，本文建議應將刑法妨害電腦使用罪章之罪責納入得實施通訊監察之範疇。

II　適用原則

i　比例原則

通訊監察作爲高度侵害用戶隱私權，雖然爲了偵查網路犯罪之需要而不得不實施，但爲平衡公益與私益間的衝突，因此必須以比例原則爲實施通訊監察之最高指導原則，亦即務求以最小的侵害達到所欲達到的目的，在實務的運作上須考量三項重要性因素，其一爲人性不可侵害，其二爲公益之重要性，其三爲手段之適合性程度[215]。我國目前通訊保障及監察法之設計即是秉持遵守比例原則，因此

[215]參閱城仲模，行政法之一般法律原則，三民書局股份有限公司發行，一九九四年八月初版，第一二二至第一二六頁。轉引錢世傑，同前註 147 揭書，第一〇四頁。

除強調保障私人通訊自由，亦必須考量業者的配合能力。因此對於實施通訊監察的要件、監察書核發機關、監察期間及監察方式等，應有嚴格之規定[216]。

ii　書面監察原則

爲避免執行時發生爭議，應使用核發書面通訊監察書方式，做爲實施通訊監察之依據[217]。

iii　透明化原則

爲降低或免除人民對於偵查機關實施通訊監察之疑慮及恐懼，偵查機關於執行通訊監察結束後，應即通知受監察人[218]。

iv　保護人民隱私權原則

明文規定縱使依法對於人民之通訊實施通訊監察，其實施通訊監察所得之資料，除非有法定理由外，不得使用。且所得資料全部與監察目的無關者，應即銷毀[219]。

v　重罪原則

重罪原則係指通訊監察實施之對象以涉嫌重大犯罪者方可爲之[220]。按通訊監察係截取、監錄特定人網路的通訊內容或瀏覽紀錄，對於網路使用者的隱私權侵害甚大，爲避免過度侵害使用者之隱私權，實施通訊監察的對象應限定爲涉及重大犯罪者。不過如本文前述，有些網路犯罪雖然侵害性輕微，但卻可能造成國家遭受危害、社會嚴重損害，這些類型的網路犯罪仍有必要准予其實施通訊監察。

---

[216]參閱蔡美智，同前註 110 揭書，第三十四頁至三十五頁。
[217]同前註。
[218]同註 215。
[219]同註 215。
[220]參閱錢世傑，同前註 147 揭書，第一〇六頁。

III　適用要件

i　通訊監察的案件必須仍在進行中

實施通訊監察是對於「活案」，即仍在進行中的案件，才有實施通訊監察蒐集相關事證之必要。如果案件已經成爲「死案」，根本沒有實施通訊監察之必要。因此在實施通訊監察前必須先審酌犯罪行爲人是否仍進行犯罪或將會繼續從事犯罪行爲。

ii　通訊監察的標的限於傳輸中的電子通訊

實施通訊監察的目的在於即時蒐集網路線上之即時通訊，換言之，通訊監察之標的必須是針對傳輸中的電子通訊，例如針對正在傳輸中的電子郵件，在傳遞過程中之某節點予以攔截，如果已經進入郵件伺服器內的電子郵件，即不得使用通訊監察方式取得，而應採取探索扣押的偵查作爲取得該電子郵件。

iii　通訊監察的標的必須爲特定線路

偵查機關實施通訊監察必須針對特定線路，包括針對連線的電話線或電子郵件帳號等，不得針對特定人做爲通訊監察的標的。

iv　通訊監察對象與偵查案件有相當之關聯

偵查人員向檢察官或法官聲請實施通訊監察，必須提供相關事證，證明欲實施通訊監察之對象，與犯罪案件間有相當之關聯，無法證明有相當關聯性，不得准予實施通訊監察。

v　實施通訊監察是最後不得已之選擇

通訊監察截取、監錄犯罪行爲人之網路通訊內容，對於偵查機關而言，爲最有效的偵查手段，惟因其侵害性最大，故必須審慎評估其實施之必要性。同時，

檢視目前偵查實務，通訊監察已經成爲偵查人員在偵查時的利器，爲避免偵查機關過於仰賴通訊監察，導致偵查人員偵查能力的退步，必須嚴格實施通訊監察必須限定在利用其他偵查手段均不能或難以其他方法調查證據時才能利用通訊監察。

vi　在技術可行的範圍內

強制網路服務提供者配合偵查機關實施通訊監察，必須在現行網路技術可行的範圍內，否則縱使網路服務提供者願意提供協助也無法做到，則此一強制規定便達不到成效。以時下最流行的利用 P2P 通訊技術的即時通訊（IM）及 PC to PC 類型之網路電話，由於所提供之通訊服務，是提供使用者點對點直接進行通訊，而並不需要經過伺服器，因此依現行技術上根本無法實施通訊監察，縱使強制其配合實施通訊監察亦是枉然。更何況，利用 P2P 通訊技術的即時通訊（IM）及 PC to PC 類型之網路電話，雖然不能透過提供服務之網路服務提供者進行通訊監察，但是偵查人員只要能掌握犯罪行爲人上網連線線路，仍可透過提供連線的網路服務提供者進行通訊監察，達到截錄犯罪行爲人通訊內容之目的。如此一來，似乎也不見得要強制提供即時通訊（IM）及 PC to PC 網路電話之提供者積攢配合實施通訊監察之責任。

5.2.2.8 通訊設備的建置以法律規定

目前關於要求網路服務提供者擬定配合執行通訊監察所需軟硬體設備、建置時程及費用之建置計畫，以配合偵查單位實施通訊監察，均是依據僅有法規命令位階的通訊保障及監察法施行細則，而前述要求網路服務提供者配合的事項，除了涉及業者的營業權、財產權外，更涉及人民的隱私權，因此應以法律規定其建置之義務，才不會有違反憲法法律保留原則。

5.2.2.9 強制提供解密方法

I　規範理由

加密技術的發達，使得電子通訊內容透過加密技術，轉化爲一團雜亂無序的數字及字母，除了擁有解密金鑰的收信人，其他人根本難以辨識通訊之真正內容。不過加密技術保障了使用者通訊的隱私，但也有愈來愈多的犯罪行爲人利用加技術來躲避偵查機關的追查。更何況，偵查機關爲偵查犯罪所需，在經由前述之嚴格程式後，得以透過實施通訊監察之方式蒐集犯罪證據，雖然利用通訊監察可以取得受監察對象之電子通訊內容或是上網瀏覽紀錄，惟若該通訊經加密後，偵查人員根本無法判讀或是必須花費相當時間去進行解譯後才能判讀相關通訊內容。如此一來，偵查人員實施通訊監察以取得相關之犯罪證據的目的完成無法達成。

外國對於要求業者提供解密方法的部分，美國犯罪偵查通訊協助法第一〇〇二條[221]規定，「除非加密係由電信業者所提供，或電信業者擁有解密資訊，否則電信業者對於用戶所爲之通訊加密，並無責任解密或確保政府有能力解密」[222]，依本條文之反面解釋，只要係由電信業者提供之加密的情形，電信業者便負有協助解密的責任；另外英國對於經加密的電子通訊，於二千年七月通過「調查權力規制法」該法第一〇〇二條規定，政府可以強制網路服務提供者提供解密金鑰以解讀經加密保護的電腦，且不配合提供解密方法者，將會受二年以下之有期徒刑[223]。

反觀我國現行法制對於網路服務提供者是否有義務將經用戶加密的資料予以

---

[221]See 47 U.S.C. §1002（b）.
[222]參閱錢世傑，同前註 147 揭書，第一九五頁。
[223]See RIPA sections 49 to 56.

解密後，提供給偵查機關；或是提供解密方法給偵查機關，均未有任何明文規定，以致在偵查機關無法要求網路網路服務提供者提供協助解密，對於經加密的資訊只能望之興嘆，或是耗費大量人力、時間去解密，徒增犯罪偵查之困難及時程之延宕，因此本文以爲有立法強制網路服務提供者提供解密的方式之必要。

II　適用要件

i　基於偵查犯罪之需要

強制網路服務提供者協助提供解密方式給偵查機關，必須限定是基於偵查犯罪之需要，按用戶使用加密技術之目的，凸顯出不願他人知悉其通訊內容的強烈意願，因此對於通訊隱私權的要求更多。而透過解密方法破譯用戶加密之通訊內容的作爲，嚴重侵害用戶通訊隱私權，因此除非是基於偵查犯罪之需要外，不得強制網路服務提供者協助解密。

ii　限定提供加密服務之網路服務提供者

用戶使用之加密方法若非由網路服務提供者提供，由於網路服務提供者也未擁有解密金鑰，若強制其提供解密方法或是已解密之通訊內容，將耗費網路服務提供者之人力、時間，造成其必須負擔額外的經營成本，將嚴重影響其經營權，因此必須限定對象爲提供加密服務之網路服務提供者。

iii　配合通訊監察使用

強制網路服務提供者提供解密方法之目的，主要在於將經實施通訊監察所截取、監錄之已加密的通訊予以破譯，以免因偵查機關無法判讀而失去實施通訊監察的目的，及避免犯罪行爲人利用此偵查漏洞遂行犯罪行爲。惟強制網路服務提供者提供解密方法破譯用戶加密之通訊內容，乃嚴重侵害用戶通訊隱私權之行爲，必須嚴格其適用時機，因此只能限於偵查人員依法定程式實施通訊監察作爲

時，才能強制網路服務提供者提供解密方法。

5.2.3 其他配套措施

爲了要讓專法之設計能達到其目的，即讓網路服務提供者能毫不顧忌克盡其協助偵查之責任，使偵查機關在網路犯罪偵查中，能獲得相當的奧援，進而迅速偵破犯罪，達到防治網路犯罪的終極目標，除了前述之內容外，尚必須有其他配套之規定，茲分述如後。

5.2.3.1 行政檢查

網路偵查過程中需要網路服務提供者協助提供使用者資料、通信紀錄等資料，甚至配合實施通訊監察，假設網路服務提供者保存之資料若發生不正確或不完整的情形，致偵查人員取得有誤或缺漏的資料；或是因相關監察設備未依法定要求建置完成或有損壞不能用之情形，而無法順利截錄到受監察人的通訊內容，均會導致網路偵查的失敗。而爲避免因網路服務提供者未依法完成相關之設備，致發生無法繼續偵查的情形，有必要制訂由主管機關（電信總局）或是負責協調之偵查單位（如法務部調查局、內政部警政署），定期實施行政檢查之規範。

5.2.3.2 成本補助

我國現行法制對於補助網路服務提供者協助偵查之部分，係依通訊保障及監察法第十四條之規定，惟立法者似乎僅將費用補償請求權限制在協助各次具體通訊監察措施所生之費用，並不包括事前因監聽設備之設置所生的費用[224]，亦不包括維護、管理該設備所支付的人事、材料等費用。至於網路服務提供者負擔提供使用者資料、通信紀錄等資料協助偵查責任，係採取使用者付費方式（即調閱者

[224]參閱錢世傑，網路通訊監察對於貪瀆案件犯罪偵查影響之探討，法務部調查局九十一年廉政工作年報，第二二一頁至第二四二頁。

支付調閱之費用），而未有任何補助規定。然而，不論是何種協助偵查責任，對於網路服務提供者而言，均是經營上額外負擔的成本，雖然考量偵查犯罪的公益，而立法強制網路服務提供者負擔協助偵查的責任，但對於配合協助偵查的額外負擔，不應由網路服務提供者獨自負擔，否則該網路服務提供者無法支應負擔該額外成本，是否即不用負有協助偵查之責任，因此本文建議應對於協助偵查所設置之相關設備、維護管理所支出之額外成本制定出相關的補助規範。

5.2.3.3 免責規定

網路服務提供者協助網路犯罪偵查，由於所提供協助的事項，不論是主動過濾、刪除或阻斷服務、提供使用者資料或通信紀錄及配合實施通訊監察等，均屬侵害到用戶的隱私權、言論自由等憲法保障的人權或會違反與用戶間使用契約條款之作為，因此為避免網路服務提供者基於公益之需要提供協助偵查，招致用戶請求賠害賠償，有必要制定相關免責規定，使網路服務提供者能無後顧之憂地協助偵查網路犯罪。

5.2.3.4 罰責

I　不配合之行政罰責

網路服務提供者既然是依法律之規定負有協助偵查之作為義務，一旦發生網路服務提供者不履行作為義務之情形，亦即不配合提供協助偵查之情形時，本文建議為了避免發生骨牌效應，本文建議應對不履行作為義務者加以處罰。至於處罰的方式，由於係屬於行政罰的性質，可依不同輕重程度的情節，處以罰鍰、暫停營業，最重至撤銷執照、停止營業。

II　洩密之刑罰

網路服務提供者協助網路犯罪偵查，所提供協助的資料，包括使用者資料、通信紀錄及監察所得的內容等，均屬於用戶享有高度隱私權的資料，雖然基於防

治網路犯罪之公益需要，可選擇以採取立法方式剝奪用戶的隱私權，但取得前揭資料的偵查人員，只能限定在偵查犯罪的時候才能運用，並且應負有保密的義務，以免用戶因資料外洩，造成其隱私權第二次遭到侵害，因此本文建議應制定保密規定並輔以刑責規定，讓偵查人員警惕及防止發生資料外洩之情事。

5.2.3.5 獎勵規定

政府基於防治網路犯罪之公益需要，立法強制網路服務提供者負有協助偵查之責任，並規定不配合之罰責，惟此種作法畢竟只能達到網路服務提供者被動配合協助偵查的效果，而可能會發生法律未規定之項目，縱使是網路犯罪偵查中重要的一環，網路服務提供者也不會主動提供協助，例如目前過濾網路內容的部分，因考量技術的問題，尚無法立法強制網路服務提供者負有過濾所有資訊之責任，也無法加諸行政罰責。因此，本文以為除了制定罰責規定外，必須另輔以制定獎勵之規定，提供協助偵查之誘因，其具體做法，包括在實質上可以獎勵金、補助款方式為之；而在形式上可以仿照類似國際標準組織（International Organization for Standardization，簡稱 ISO）[225]或中國農業標準(Chinese Agricultural Standards，簡稱 CAS)[226]等認證制度，建立優良網路服務提供者標章之認證制度，使網路服務提供者能積極主動配合協助網路偵查作為。

5.3 合憲性討論

5.3.1 合憲性審查

本研究雖然主張應建置網路服務提供者協助偵查法，賦予偵查機關更大的偵

[225]參閱 ISO 輔導網，網址：http://www.eternaliso.com/intro.htm。最後瀏覽日期：二○○五年七月二十三日。

[226]參閱陳俊龍，ＣＡＳ優良食品制度之推行及成效，行政院農業委員會全球資訊網，網址：http://www.coa.gov.tw/8/208/213/882/1803/3877/3877.html。最後瀏覽日期：二○○五年七月二十

查權力以面對各類型的網路犯罪，並透過網路服務提供者的協助更有效提昇網路犯罪偵破率，達到防治網路犯罪的目的。但由於本法所規範的內容，涉及網路使用者所享有憲法保障的言論自由、隱私權及網路服務提供者所享有憲法保障的營業自由權、工作權。換言之，賦予偵查機關偵查權力的同時，將可能嚴重侵害網路使用者或網路服務提供者所享有的基本人權，因此有必要針對網路服務提供者協助偵查法進行合憲性的審查，以決定其建置之可行性。

合憲性審查的內容，首先應考量是否符合法律保留原則，按依我國憲法第二十三條對於基本人權的限制之規定，除非係基於「防止妨礙他人自由、避免緊急危難、維持社會秩序或增進公共利益所必要」等條件，並且符合法律保留原則，才能予以限制，否則即有違憲之疑慮。而本研究建議制定網路服務提供者協助偵查法明文要求網路服務提供者協助執行法律，已符合憲法之法律保留原則。其次，，爲兼顧防治網路犯罪及保障人民基本人權的目的，仍應進一步採取嚴格之審查標準，具體審查此一立法之立法目的與立法手段是否合憲，亦即應先審查此一立法之目的所追求之利益是否爲相關急迫及非常重要的政府（公共）利益，其次審查爲達成該目的之手段是否爲達成該目的之必要且侵害最小的手段[227][228]。

5.3.1.1 立法目的的審查

網路服務提供者協助偵查法之立法目的，在於透過網路服務提供者之協助，

三日。

[227]參閱林子儀，言論自由與新聞自由，二〇〇二年十一月初版第二刷，第一四六頁。

[228]大法官釋字第六〇三號解釋，針對戶籍法第八條第二項「依前項請領國民身分證，應捺指紋並錄存。但未滿十四歲請領者，不予捺指紋，俟年滿十四歲時，應補捺指紋並錄存」及第三項「請領國民身分證，不依前項規定捺指紋者，不予發給」之規定做出違憲的解釋。依該解釋文內容，戶籍法強制人民按捺指紋並予錄存，否則不予發給國民身分證之規定，並無明文規定立法目的，於憲法保障人民資訊隱私權之意旨已有未合；縱使能達到國民身分證之防僞、防止冒領、冒用、辨識路倒病人、迷途失智者、無名屍體等目的而言，亦屬損益失衡、手段過當，不符比例原則之要求，與憲法第二十二條、第二十三條規定之意旨不符。參閱司法院大法官全球資訊網，網址：http://www.judicial.gov.tw/constitutionalcourt/p03_01.asp?expno=603。

有效提昇網路犯罪偵查之能力，達到防治網路犯罪泛濫、保障使用者使用網路之安全、促進網路發展及維護社會秩序與國家利益之目的。由於網路發展蓬勃，不僅提供網路犯罪行爲人新興犯罪方式，並且隨著網路科技的進步而網路犯罪的影響及所造成的損害日益擴大，網路犯罪可能造成的損害大小無法預測性、可能造成個人利益、社會秩序，甚至是國家安全損害嚴重性，遠比傳統犯罪行爲所造成的損害還大；同時，由於偵查機關欠缺偵查資源，在無法獲得網路服務提供者完全協助下，始終無法提昇偵破率，致網路犯罪行爲持續泛濫，因此制定網路服務提供者協助偵查法，無論是要求網路服務提供者提供使用者資料、通信紀錄或是協助實施通訊監察等事項，均是基於偵查犯罪之需要，其目的係爲有效迅速提昇網路犯罪偵破率，以達到維護重大的公共利益目的。

5.3.1.2 立法手段的審查

立法手段的審查係審查爲達成該目的之立法手段，是否爲達成該目的之必要且侵害最小的手段。事實上，防治網路犯罪泛濫的方法甚多，以新加坡及中國大陸爲例，係採取制定相關網路內容管理法規方式，嚴格控管網路內容的手段，雖然可以達到防治網路犯罪目的，卻恐將造成網路服務提供者擔心擔負不必要的民事、刑事責任而退卻，甚至不願從事提供網路服務行業，而不利於網路的發展，此種作法之手段與目的間顯然不具有合理的關連性。而制定網路服務提供者協助偵查法制，不採取控管網路內容，而係在網路犯罪發生之際，利用網路服務提供者之協助偵查犯罪，雖會侵害到使用者之隱私權及言論自由，惟遭限制之對象均爲特定之涉嫌人，非涉嫌人之使用者之基本權利非但不會遭受侵害，反而因防治網路犯罪之成果而享有更安全的網路使用空間，因此制定網路服務提供者協助偵查法制是侵害最小且能達到防治網路犯罪的最佳手段。

5.3.2 可能的疑慮

雖然網路服務提供者協助偵查法符合法律保留原則，其立法目的及立法手段亦符合憲法之要求，然而，實際擬定具體條文內容及實際執行面的部分，仍有可能發生違憲與否及是否會嚴重侵害到網路使用者基本權利等等疑慮，而這些可能產生的疑慮，均是立法過程中所必須正視及解決的議題。

5.3.2.1 違憲的疑慮

本研究基於防治網路犯罪之理由，主張制定網路服務提供者協助偵查法制，透過明確網路服務提供者協助偵查責任，強化偵查人員執行法律之權力，以利於網路偵查作爲，有效提昇網路犯罪偵破率。不過，在具體條文的制定部分，由於賦予偵查人員享有更多的偵查權力的同時，網路使用者原享有的言論自由、通訊隱私等基本權利可能因此而受到侵害或限制；另外，網路服務提供者亦因負有協助偵查之責任，致其原享有的營利自由及工作權受到限制。然而，無論是網路使用者享有的言論自由、通訊隱私或是網路服務提供者享有的營業自由、工作權，均屬於我國憲法所保障的基本人權。因此，具體條文的擬定時，可能會發生立法目的與立法手段並不具直接關聯而有違憲之疑慮。

5.3.2.2 嚴重侵害犯罪嫌疑人基本權利的疑慮

爲了防治網路犯罪，本研究主張建制網路服務提供者協助偵查法制，賦予偵查機關更大的偵查權力去面對各式類型的網路犯罪，針對網路犯罪嫌疑人進行偵查作爲，然而偵查機關享有的偵查權力愈大的同時，相對地，所可能造成犯罪嫌疑人基本權利之侵害或限制愈大。因此，容易讓人產生賦予偵查機關的偵查權力是否過大或是偵查人員會否濫用偵查權力，而嚴重侵害犯罪嫌疑人之基本權利的疑慮。

5.3.2.3 嚴重侵害非犯罪嫌疑人基本權利的疑慮

網路犯罪偵查過程中，偵查人員雖然係針對網路犯罪嫌疑人進行偵查作爲，

但是由於網路通訊技術係採取封包傳遞的方式，因而在實施通訊監察的過程中，容易蒐獲非犯罪嫌疑人之通訊內容，；另外，偵查人員亦有可能利用偵查案件之際，濫用其偵查權力，取得非犯罪嫌疑人之相關資料或是截取通訊內容，致使在適用網路服務提供者協助偵查法時，會產生嚴重侵害非犯罪嫌疑人之隱私權的疑慮。

5.3.2.4 第二次侵害基本權利之疑慮

無論是使用者資料、通信紀錄或是實施通訊監察所截取的通訊內容，均爲網路使用者享有憲法保障之隱私權，雖然偵查人員依網路服務提供者協助偵查法實施偵查作爲，取得使用者資料、通信紀錄或是實施通訊監察所截取的內容之偵查作爲，係基於偵查犯罪之需要，但對於使用者而言，仍屬於第一次侵害其享有的基本權利。而從實際執行法制面分析，一旦偵查人員將前揭資料使用於與偵查犯罪無關的事項或是對外揭露，將更嚴重侵害使用者享有之隱私權，而容易使人產生使用者基本權利受到第二次侵害的疑慮。

5.3.3 疑慮排除

網路服務提供者協助偵查法制具體條文之擬定及實際執行面，可能會產生是否違憲、嚴重侵害犯罪嫌疑人基本權利、嚴重侵害非犯罪嫌疑人基本權利及造成基本權利第二次受到侵害等等疑慮已如前述，惟本研究以爲這些疑慮可透過嚴格限縮各協助偵查事項之適用條文及事後審查制度等解決方式加以排除。

5.3.3.1 嚴格限縮適用要件（符合「比例原則」之要求）

制定具體條文的目的亦是爲了偵查案件之需要，由於個別條文所規定的協助偵查內容不同，所可能侵害或限制使用者之隱私權與言論自由或業者之營業自由亦不同，因此本研究以爲制訂相關條文時應嚴格限縮其通用要件，亦即相關具體條文之設計，必須符合「比例原則」之要求，才能符合達成該目的之必要且侵害

最小的手段之審查。

I　符合適當性原則

適當性原則係指行爲應適合於目的之達成。因此在制訂法規強制網路服務提供者擔負協助偵查責任，其內容必須能夠達到防治網路犯罪泛濫、保障人民隱私及維護網路使用安全的目的，換言之，偵查人員所有要求網路服務提供者協助偵查事項，必須是基於偵查犯罪之需要，才能符合適當性的要求。

II　符合必要性原則

必要性原則係指行爲不超越實現目的之必要程度，亦即達成目的須採取影響最輕微的手段。因此，制訂具體條文之適用要件時，必須考量不同偵查階段、不同類型的犯罪類型，加諸網路服務提供者不同的協助偵查責任。例如對於已經完成的案件，透過調閱通聯紀錄、使用者資料即可達到偵查目的之情形，偵查人員不得實施通訊監察，換言之，實施通訊監察只能限於針對進行中之案件，以符合必要性原則。

III　符合衡量性原則

衡量性原則，係指手段應按目的加以衡判，即任何干涉措施所造成之損害應輕於達成目的所獲致之利益，始具有合法性。制訂具體條文時，必須考量個別協助偵查責任之內容，其能達到的目的必須輕於可能造成之損害，以兼顧防治網路犯罪及維護人民隱私間公益與私益之平衡。以實施通訊監察爲例，由於實施通訊監察對於使用者之通訊隱私侵害性最大，若網路犯罪類型中屬於輕微案件之類型，例如網路誹謗、網路援交等，偵查人員均可對之實施通訊監察，相對於遭侵害的隱私權而言，顯然是以「大砲打小鳥」，並非可行之方案，因此本研究以爲得實施通訊監察之案件類型，必須嚴格限縮於重大犯罪類型或具有跨國性、集團

性犯罪類型；另外，實施通訊監察對象必須針對特定線路，而非針對特定人，例如針對某犯罪嫌疑人所有某特定電子郵件帳號或使用連結網路之電話線實施通訊監察，因爲特定人使用的線路不見得相同，亦可能會使用網路咖啡店或他人所提供之線路，若允許偵查人員針對假特定人實施通訊監察，恐將侵害眾多其他不特定人所享有的基本權利，而不符合衡量性原則。

5.3.3.2 排除適用不符合比例原則之偵查作爲

單從防治網路犯罪角度出發，爲能達到網路偵查的目的，惟有擴大偵查人員之偵查權力，然而，偵查權力愈擴大，對於使用者的基本權利影響及侵害愈大，因此爲了兼顧防治網路犯罪及保障人民隱私權的目的，賦予偵查人員之偵查權力的立法，必須符合比例性原則，否則將產生有違憲的疑慮。因此，經審查後不符合比例原則的偵查權力，縱使對於網路偵查有極大的幫助，在立法過程中亦應加以排除。

I 排除適用機動性監聽（Roving Wiretaps）

網路具有機動的特性，使得犯罪行爲人爲逃避追查，可能會以任何方式逃避偵查機關的追查，例如不斷地更換帳號、使用網路咖啡店提供之網路或不斷聲請不同免費的電子郵件帳號等等方式，避免偵查人員的追查。因此，爲解決無法即時追蹤犯罪行爲人及蒐集相關之事證之偵查瓶頸，美國愛國者法第二〇六條[229]規定在法院認定受通訊監察者有任何妨礙執法機關辨認身份之行爲時，可以擴張監察對象至任何特定人，使執法人員在取得法院命令後，得以監聽任何恐怖活動涉嫌人所使用之任何電話，換言之，將原本通訊監察的標的，由特定線路（phone

[229]See USA Patriot Act of 2001 §206.

to phone）改爲特定人(person to person)[230]，此種實施通訊監察方式稱之「機動性監聽」。舉例來說，依據美國愛國者法案之規定，偵查機關若能證明犯罪行爲人係使用網路咖啡店的某特定電腦連線上網，即能針對該電腦線路實施通訊監察。

惟本研究以爲改爲針對特定人所有使用的線路實施通訊監察，雖然可以解決網路犯罪行爲人躲避追查的難題，但卻亦會產生嚴重侵害到其他人隱私權之副作用。以前述偵查機關針對網路咖啡店之電腦線路進行通訊監察爲例，偵查人員所擬蒐集之標的爲犯罪行爲人之犯罪事證，但因使用遭監察線路的不特定人眾多，故偵查人員容易裁錄到非犯罪行爲人之通訊內容或瀏覽紀錄，導致這些無辜者的隱私權嚴重遭到侵害。換言之，採取機動性監聽方式，固然可以解決犯罪行爲人不斷更換使用帳號、使用網路咖啡店提供之網路或不斷聲請不同免費的電子郵件帳號，以逃避偵查人員追查之問題，但經比較可能導致不特定人的隱私權遭受侵害的嚴重性，顯然不符合比例性原則的要求，因此本研究不建議引爲立法之參考。

II　排除適用肉食者監控系統（Carnivore 系統）

肉食者系統（簡稱 Carnivore）係美國聯邦調查局爲防止網路成爲偵查犯罪與恐怖活動的死角，所發展出來的網路通訊監察設備。Carnivore 的使用方式，係在網路服務提供者之網路設備上，安裝單向的截取設備，於避免幹擾網路正常運前提下，將通過的網路通訊內容複製，傳送至資料收集系統，並經由過濾器將不屬於法院許可授權範圍之內容加以過濾，過濾後資料存放在儲存設備中，以作爲偵查與審判之依據[231]。至於，利用 Carnivore 所能取得的資料範圍，雖然美國官員

[230]參閱錢世傑，同前註 147 揭書，第五十八頁。
[231]參閱錢世傑，從 Magic Lantern 談網路通訊監察之相關問題研究，台灣網路法律中心，網址：http://www.chinalaw.org/professional.html。最後瀏覽日期：二〇〇五年七月二十三日。

在國會作證時，曾表示該系統僅截取電子郵件之標頭，不涉及郵件內容[232]；然而華爾街雜誌（Wall Street Journal）報導與部分隱私權團體卻揭露 Carnivore 可截取所有上網者之信件及網站瀏覽等相關活動紀錄[233]。

不過，縱使 Carnivore 系統能截取的內容僅有不含通訊內容的紀錄，但因 Carnivore 係針對不特定對象所進行廣泛蒐集網路資訊，而非針對特定案件或特定對象，因此，此種偵查作爲雖可以達到偵查犯罪的目的，卻會造成眾多無辜的民眾的隱私權受到侵害，更遑論若 Carnivore 能截取的內容尚包括不特定對象之通訊內容、瀏覽紀錄等有實質內容之資料，其造成隱私權的侵害有多大。因此，本研究以爲我國不宜引進美國 Carnivore 之制度。

III 排除適用「後門」程式

美國聯邦調查局爲偵查網路犯罪，已要求網路網路服務提供者提供「後門」程式給聯邦調查局[234]；另外，英國調查權力規制法亦強制網路服務提供者負有提供適合的設置使政府得以順利實施通訊監察，包括基於監視的目的要求網路服務提供者協助裝置「後門」程式[235]。然而，本研究以爲偵查機關使用「後門」程式，固然可以有效掌握網路上任何通訊內容或紀錄，但是由於偵查人員究竟係何時進入蒐集、如何蒐集及蒐集的內容爲何，網路使用者根本無法知悉，也無法進行任何監督作爲；同時開「後門」程式與使用 Carnivore 系統蒐集資訊相同，均可能會嚴重侵害到不特定人之隱私權，致使用者陷於使用網路行爲遭窺視及隱私

---

[232]參閱 Griffin S. Dunham, Carnivore, The FBI's Email Surveillance System: Devouring Criminals, Not Privacy，Federal Communication Law Journal, Vol. 54 Issue 3, p.545(2002)。轉引自吳炎琰，論網路環境下的通訊監察法制，科技法律透析，二〇〇五年二月，第四十一頁。

[233]美國政府運用肉食者監視系統相關討論參見〈http://www.cdt.org/security/carnivore〉網站。轉引自吳炎琰，同前註 209 揭書，第四十一頁。

[234]參閱財團法人資訊工業策進會科技法律中心科技法律要聞－網路法律新知，九十三年三月，網址：http://stlc.iii.org.tw/tlnews/net9303.htm#n1。最後瀏覽日期：二〇〇五年七月二十三日。

[235]See RIPA sections 12.

權遭侵害的恐懼中，對於網路長期發展而言，亦非正面的作法。因此，爲避免造成不特定使用者隱私權遭受侵害及考量網路的永續發展，本文以爲不宜強制網路服務提供者提供「後門」程式予偵查機關。

IV　排除適用使用鍵盤敲擊紀錄系統（Key Logger System）

美國聯邦調查局爲解決加密技術，致造成網路偵查的困難，研發「鍵盤敲擊紀錄系統」（Keylogger 或 Key Logger System，簡稱 KLS），所謂 KLS 係指「一種用來監視側錄使用者在特定電腦鍵盤打字時之任何敲擊之硬體設備或是小程式」（A keylogger is a hardware device or small program that monitors each keystroke a user types on a specific computer's keyboard）[236]，偵查人員透過裝置 KLS 設備，取得使用者鍵盤敲擊之紀錄後，運用還原技術加以解讀取得用戶之帳號、密碼或加密的金鑰，以解決犯罪行爲人利用加密技術躲避追查的之難題。惟由於 KLS 設備必須經偵查人員在取得任何法定允許下，私自侵入對象住所才能完成安裝，此舉已嚴重侵害到人民的隱私權、居住自由權，即使是在美國爭議頗大，更何況取得解密的金鑰或密碼，可依本文前述採取立法強制網路服務提供者提供的方式取得，而無須採取具高度侵害性的 KLS，因此本研究以爲不宜做爲我國法制之參考。

另外，美國聯邦調查局爲解決偵查人員無故侵入他人住宅裝置 KLS 之爭議，另研發類似「後門」程式之 Magic Lantern System（簡稱 MLS）[237]，偵查人員無須侵入對象之住宅，改透過網路將 KLS 程式植入對象電腦中，即偵查人員利用電子郵件中夾帶 KLS 程式的方式傳遞給對象，嗣對象打開後即安裝至對象之電腦中，進而側錄對象的敲擊鍵盤之紀錄，並將該紀錄回傳偵查機關，使偵查人員可

---

[236]參閱網址：http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci962518,00.html。最後瀏覽日期：二〇〇五年七月二十三日。
[237]同前註 229。

以取得對象之密碼及加密金鑰。惟 MLS 雖然無須侵入他人之住宅，但與 KLS 比較，二者侵害他人之隱私權程度並無不同，且 MLS 亦不具有使用之必要性，因此本研究以爲亦不宜作爲我國法制之參考。

5.3.3.3 建立事後審查制度

網路服務提供者協助網路犯罪偵查，所提供協助的資料，包括使用者資料、通信紀錄及監察所得的內容等，均屬於用戶享有高度隱私權的資料，雖然基於防治網路犯罪之公益需要，本研究主張以採取立法方式剝奪用戶的隱私權，並且爲了避免造成偵查權力過於擴大，除了明定所有偵查作爲必須係基於偵查犯罪所需要，並且嚴格限縮各偵查作爲之適用要件，但在實際執行的過程中，仍可能會發生取得前揭享有隱私權資料的偵查人員對外洩露使用者之用戶資料、通聯紀錄或通訊內容之情事，而造成使用者隱私權第二次遭到侵害。因此爲避免發生使用者隱私權第二次遭到侵害，本研究以爲在網路服務提供者協助法制應建立事後審查之制度，其具體作法如後：

I　第三人實施原則

任何偵查作爲必須透過網路服務提供者之協助執行，不得由偵查機關逕行爲之，例如通訊監察之實施，必須透過第三人（網路服務提供者）之協助才能實施，不得由偵查機關逕自爲之，其目的在於防範偵查機關無限過大偵查權力及避免事後無法監督。

II　採取「書面」原則

任何偵查作爲，包括調閱使用者資料、通信紀錄及要求網路服務提供者協助實施通訊監察，均必須檢附正式公文或通訊監察書向網路服務提供者辦理，以方便於日後審查之用。

III　行政檢查

爲避免偵查機關有濫用偵查權力的情事發生，應建立行政檢查的制度，透過上級機關實施檢查作爲，有效防止下級偵查機關濫權的情形。

IV　事後銷毀

偵查人員因辦案需要所取得之相關資料，因與網路使用者的隱私權息息相關，爲避免發生資料外洩的情事，應明定銷毀之規定，在一定要件下予以銷毀。

V　明定處罰規定

偵查人員實施任何偵查作爲，必須依據網路服務提供者協助偵查法或相關法規所明定之辦案程式辦理；並且對於所取得的使用者資料、通信紀錄或通訊內容等資料，負有保密的義務，對於違反相關辦案程式或違反保密規定者，應明定相關處罰規定，以防止發生違反偵查及資料外洩之情事。

5.4 小結

本研究基於有效提昇偵查人員網路偵查之能力，期能透過網路服務提供者之協助，進而提高網路犯罪偵破率，達到防治網路犯罪泛濫、維護使用者安全使用的目的，主張我國應參照美國、英國及歐盟等國家之制度，應建置網路服務提供者協助偵查法制。同時，爲了釐清建置網路服務提供者協助偵查法制可能造成之違憲疑慮，本研究分別就形式及實質方面進行合憲性審查後，證明建置網路服務提供者協助偵查法制之可行性及必要性。

在具體條文內容的擬定方面，本研究主張應嚴格限縮各項偵查作爲之適用要件，以符合憲法比例原則之要求，達到兼顧防治網路犯罪及保障人民基本人權之目的；另外，透過建立事後審查制度，避免偵查人員濫用偵查權力造成過度或第二次侵害到使用者人權的情事發生。

本研究認爲，網路服務提供者協助偵查法制的建立，確能達到防治網路犯罪

的目的，但仍應輔以建置相關保障人民基本權利之配套制度，才能去除各種疑慮，真正達到保障人民隱私權、建立安全的網路空間及促進網路使用之立法目的。


E
S
A
1896

6 結論

寬頻網路技術的快速發展的急速發展，確實爲人們帶來更爲便捷的通訊方式，但同時也帶來我們所不樂見的犯罪不法行爲，更令人擔心的是網路犯罪行爲隨著網路科技的發展，所可能造成的損害日益擴大。然而，偵查人員面對新興的網路犯罪行爲，由於欠缺任何偵查經驗及網路專業能力、人力的窘境下，卻早顯得捉襟見肘。並且，隨著點對點的網路電話及無線網路不斷推廣發展及使用，由於這些通訊技術具有高度隱匿使用者身分的特性，根本無法追尋到使用者的真實身分，偵查人員更是絲毫沒有招架之餘地。雖然內政部警政署刑事警察局及法務部調查局等偵查機關，已分別成立網路犯罪偵查專責單位，積極偵辦網路犯罪行爲，惟礙於欠缺專業人才及偵查能力，偵破率始終無法提昇，以致根本無法阻擋日益泛濫的洪流。

雖然，我國政府有鑑於網路犯罪的嚴重性，早已將防治網路犯罪列爲重點課題，並將網路犯罪行爲納入刑法規範；並且，爲了有效提昇偵查機關的偵查能力，以防堵網路犯罪行爲持續泛濫，交通部電信總局更是屢屢修訂相關法規，加諸電信業者儲存及提供使用者資料與網路通信紀錄及建置網路通訊監察設備配合偵查人員實施通訊監察等責任，惟由於現行相關法規的規範對象僅侷限於電信業者；同時相關協助偵查法制，如第二類電信事業管理規則，均係以法規命令規範限制或侵害使用者享有憲法保障之基本權利，而有違反憲法法律保留原則之疑慮。

綜上，本研究以爲有必要建置相關網路犯罪偵查協助法制，以解決偵查人員面對網路犯罪的困境及現行法制的適用疑慮。因此，本研究嘗試從網路犯罪偵查實務出發，先於第二章探討網路犯罪的意義、特性、犯罪手法及泛濫的程度；第三章藉由傳統犯罪偵查與網路犯罪偵查在案件偵查各個階段的偵查之差異性，以

凸顯網路服務提供者在網路犯罪偵查角色之重要性；第四章探討我國關於網路服務提供者協助偵查法制的現行規定，嘗試找出我國目前的法制缺失；第五章參考美國、英國及歐盟關於網路服務提供者協助偵查相關法制之規定，並提出相關的法制建議。期能透過網路服務提供者協助偵查法之建置，強化網路服務提供者協助偵查之責任，適度擴大偵查人員的偵查權力與偵查能力，以解決日益泛濫的網路犯罪問題，還給所有網路使用者一個安全、便捷的網路空間。

最後，再一次強調，由於礙於個人所學及實務經驗之不足，本研究針對網路服務提供者協助偵查法制所提出之相關論述及法制建議，或有錯誤或不足之處，但衷心期盼能透過本研究之論述探討，促使政府相關單位能儘速正視此問題，爲日後網路服務提供者協助偵查法制的催生盡一份心力。

參考文獻

壹、　中文參考文獻

一、 專書

1 吳俊瑩等五人，電腦、網路、通訊知識百科，初版，電腦人文化事業股份有限公司，二〇〇一年七月十四日。

2 王郁琦，資訊、電信與法律，初版，著者發行，二〇〇四年五月。

3 王銘勇，網路犯罪相關問題之研究，臺灣新竹地方法院，二〇〇一年十一月。

4 馮震宇，網路法基本問題研究（一），二版，學林文化事業有限公司，二〇〇〇年九月。

5 陳誌銘，網路犯罪偵查之研究，臺灣臺南地方法院，一九九九年。

6 廖有祿，李相巨，電腦犯罪－理論與實務，初版，五南圖書出版股份有限公司，二〇〇三年九月。

7 林山田，林東茂，犯罪學，增訂三版，一九九九年八月。

8 林燦璋，林信雄，偵查管理－以重大刑案爲例，初版，五南圖書出版股份有限公司，二〇〇四年三月。

9 林山田，刑法通論，增訂四版，一九九三年八月。

10 楊士隆主編，暴力犯罪－原因、類型與對策，初版，五南圖書出版股份有限公司，二〇〇四年五月。

11 駱宜安，刑事鑑識學，二版，明文書局股份有限公司，二〇〇三年八月。

12 沈政主編，法律心理學，初版，五南圖書出版股份有限公司，一九九二年二月。

13 林輝煌，論證據排除－美國法之理論與實務，初版，元照出版有限公司，二〇〇三年九月。

14 彭心儀主編，美國資訊通信法案例評析 1991~2002 案例精選，初版，元照出版有限公司，二〇〇二年五月。

15 許文義，個人資料保護法論，初版，三民書局股份有限公司，二〇〇一年一月。

16 謝瑞智，憲法新論，增訂版，正中書局，二〇〇〇年二月。
17 吳庚，行政法之理論與實用，增訂七版，著者發行，二〇〇一年八月。
18 蔡茂寅等四人，行政程序法實用，一版，學林文化事業有限公司，二〇〇一年十一月。
19 城仲模，行政法之一般法律原則，初版，三民書局股份有限公司發行，一九九四年八月。
20 林子儀，言論自由與新聞自由，初版第二刷，元照出版有限公司，二〇〇二年十一月。
21 戴豪君等，數位科技法律大未來，初版一刷，書泉出版社，二〇〇四年十一月。
22 劉孔中等，行動之鑰：台灣電信法律實務與案例深度解析，初版一刷，書泉出版社，二〇〇五年四月。
23 劉尚志，陳佳麟，網際網路與電子商務法律策略，初版第一刷，著作發行，二〇〇一年三月。
24 賴文智等，網路事業經營必讀，初版第一刷，元照出版有限公司，二〇〇一年五月。
25 周天等，網路法律高手，初版一刷，書泉出版社，二〇〇二年四月。
26 陳銘祥，通信的規範結構與通信變革，韋伯文化國際出版有限公司，二〇〇二年九月。
27 蔡淑美，企業網路經營法律實戰，初版，永然文化出版股份有限公司，二〇〇二年六月。
28 陸義淋等，電子商務法律通，初版一刷，書泉出版社，二〇〇三年十一月。
29 謝哲勝等，網路法律常識，初版，翰蘆圖書出版有限公司，二〇〇四年二月。
30 郭卫华等，网络中的法律问题及其对策，初版二刷，法律出版社，二〇〇一年八月。
31 张彦，计算器犯罪及其社会控制，初版一刷，南京大學出版社，二〇〇〇年四月。
32 （美）布萊恩・卡衡（Brian Kahin），查理斯・尼森（Charles Nesson）著，數位法律：網際網路的管轄與立法、規範與保護，巫宗融譯，初版二刷，遠

流出版事業股份有限公司，二〇〇〇年五月一日。

33 （美）勞倫斯・雷席格（Lawrence Lessig）著，網路自由與法律（CODE and Other Laws of Cyberspace），劉靜怡譯，初版，城邦文化事業股份有限公司，二〇〇二年七月二十九日。

34 黛安那・布琳森（J. Dianne Brinson），馬克・拉德克里佛（Mark F. Radcliffe）著，多媒體法與企業經營手冊，章忠信，劉文彬譯，初版，商業周刊出版股份有限公司，二〇〇〇年四月一日。

35 （美）布萊恩・隱內（Brian Innes）著，犯罪心理剖繪檔案（Profile of a Criminal Mind），吳懿婷譯，初版，城邦文化事業股份有限公司，二〇〇五年七月六日。

36 （美）凱斯・桑斯坦（Cass Sunstein）著，網路會顛覆民主嗎？，黃維明譯，初版一刷，新新聞文化事業股份有限公司，二〇〇二年五月。

37 （美）布魯斯・施奈爾（Bruce Schneier）著，秘密與謊言－如何建構網路安全防衛系統，吳蔓玲譯，初版，商周出版，二〇〇一年九月十六日。

二、 期刊

1 李相巨，「網路科技犯罪專責隊－刑事警察局」，透視犯罪問題第四期，第六十四頁至六十九頁，二〇〇四年九月。

2 參閱冯卫国，张立宇，「网络空间的犯罪与刑法面临的挑战」，網路法律評論（Internet Law Review），二〇〇二年七月。

3 謝立功，「電子商務發展之挑戰－網路洗錢相關問題之探討（上）」，資訊法務透析，二〇〇〇年十月號。

4 張雅雯，「網際網路連線服務提供者就網路內容之法律責任（上）」，資訊法務透析，第二十九至三十六頁，一九九八年三月。

5 張雅雯，「網際網路連線服務提供者就網路內容之法律責任（中）」，資訊法務透析，第十七至二十七頁，一九九八年五月。

6 張雅雯，「網際網路連線服務提供者就網路內容之法律責任（下）」，資訊法務透析，第二十二頁，一九九八年六月。

7 周慧蓮，「電信法中關於網際網路服務提供者權義規範簡析」，科技法律透析，第十至十四頁，二〇〇四年八月期。

8 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，

第三十二至四十五頁，一九九九年十二月。

9 蔡碧玉著，「從偷拍事件談隱私權保護之刑事立法」，法令月刊，第四十九卷第四期，第二十頁以下，八十七年四月。

10 劉靜怡，「資訊科技與隱私權焦慮」，當代雜誌第一二四期，第八十頁。

11 王郁琦，「網路上的隱私權問題」，資訊法務透析，第三十九頁，八十八年十月。

12 張雅雯，「網際網路管理辦法建議草案－出爐建議以業界自律爲管理主軸」，資訊法務透析，一九九八年八月。

13 張雅雯，「網路服務提供者就網路違法行爲之法律責任」，律師雜誌，第二二八期，第四十四頁，一九九八年九月。

14 吳炎琰，「論網路環境下的通訊監察法制」，科技法律透析，第三十六頁，二〇〇五年二月。

15 梁正清，「中共對網際網路的管控及其影響」，展望與探索，第五十八至九十三頁，二〇〇三年六月。

16 錢世傑，「網路通訊監察對於貪瀆案件犯罪偵查影響之探討」，法務部調查局九十一年廉政工作年報，第二二一頁至第二四二頁。

17 余若凡，「對網路服務業者於犯罪偵查中所扮演角色之探討」，網路法制與犯罪偵防研討論文集，第一頁至十六頁，二〇〇三年三月。

三、 學位論文

1 余德正，「不法使用網際網路之刑事責任」，東海大學法律研究所，碩士論文，一九九九年。

2 沈榮華，「網路犯罪相關問題之研究」，國防管理學院法律研究所，碩士論文，二〇〇二年。

3 錢世傑，「網路通訊監察法制與相關問題研究」，中原大學財經法律學系，碩士論文，二〇〇二年。

4 黃育勳，「電腦之搜索扣押」，國立臺北大學法學學系，碩士論文，二〇〇〇年。

5 蕭愛貞，「網際網路犯罪之責任內涵－兼論網路服務業者之責任」，輔仁大學法律學研究所，碩士論文，二〇〇〇年。

6 黃明凱，「網路犯罪輔助偵查專家系統雛型之建構」，中央警察大學資訊管

理研究所，碩士論文，二〇〇〇年。

7 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，二〇〇二年。

8 林一德，「電子數位資料於證據法上之研究」，國立台灣大學法律學研究所，碩士論文，二〇〇〇年。

四、 報章新聞

1 陳金章，「網路銀行破功，客戶遭盜冒貸」，聯合報，社會 A8 版，二〇〇三年十一月二十七日。

2 廖玉玲，「垃圾郵件泛濫，微軟反擊」，經濟日報，國際財經版，第十一版，二〇〇四年三月十二日。

3 聯合報，「駐韓外館機密遭截，電話電腦線路異常，調局偵測被動手腳應是間諜事件」，要聞 A1 版，二〇〇四年八月三十日。

4 張宏業，「碩士工程師找援交，遇霸王花」，聯合報，綜合新聞 B2 版，二○○四年一月四日。

5 朱正庭，「電腦是最佳玩伴，假日 5 成學子守著它，23%少年郎逛過色情網站」，星報，青春探索 C3 版，二〇〇四年五月二十八日。

6 陳一雄，「全台掃蕩戀童網，站主全是高中生」，聯合報，北市綜合 B4 版，二〇〇四年五月二十六日。

7 呂開瑞，「網路賭博，莊家慘賠，債主施暴」，聯合報，桃竹苗綜合新聞 B4 版，二〇〇四年九月八日。

8 陳一雄，盧德允，「3 軍人偷槍管，網上賣黑槍」，聯合報，話題 A5 版，二〇〇四年二月十八日。

9 陳素玲，「公平會監控 36 網路老鼠會」，聯合晚報， 經濟生活 6 版，二〇〇四年二月二十七日。

10 遊文寶，「刷卡存根外流，用於網路詐財，嫌犯利用卡號購物，騙得百萬元，供稱新光三越員工提供」，聯合報，社會 A8 版，二〇〇四年六月十七日。

11 陳崑福，「天堂偷寶物，四男一女就逮」，聯合報，高屏綜合新聞 B4 版，二〇〇四年二月十四日。

12 陳一雄著，「新聞辭典飛客+釣魚=網路釣魚」，聯合報，焦點 A3 版，二〇

○四年九月二十三日。

13 李若松，「殺手攻擊百萬台電腦－史上變種最快，傳播速度驚人，歐美災情嚴重，亞太感染趨緩，可能影響三億台電腦」，聯合報，生活 A6 版、二○○四年五月五日。

14 廖福本，賴孟科，「中市驚傳斷頭命案，男子顧炎成遇害，警方鎖定兩人」，東森新聞網，重點新聞，二○○四年十二月十七日。網址：http://www.ettoday.com/2004/12/18/545-1729166.htm。

15 許國禎，「冒辦外勞卡，賣出 20 萬張」，自由新聞網，網址：http://www.libertytimes.com.tw/2004/new/dec/2/today-so3.htm。

16 曹敏吉著，「土銀超貸案前經理求刑九年」，聯合報，高屏澎綜合新聞 C4 版，二○○四年十一月十一日。

17 苗君平，「調閱通聯免費，警方促比照同是辦案，地檢署有優待，中警一年支出逾三百萬，吃不消」，聯合報，中部綜合新聞，B4 版，二００四年五月六日。

五、 網站資料

1 高大宇，王旭正，「駭客入侵網路之偵查模式分析」，網址：http://163.25.10.166/lab/project/download/Network-%E5%88%91%E7%A7%91-%E9%A7%AD%E5%AE%A2%E5%85%A5%E4%BE%B5%E5%81%B5%E6%9F%A5%E6%A8%A1%E5%BC%8F%E5%88%86%E6%9E%90.PDF。

2 林宜隆，邱士娟，「我國網路犯罪案例現況分析」，網址：http://jitas.im.cpu.edu.tw/2003-2/6.pdf。

3 張維平，「我國網路犯罪現況分析」，網址：http://www.tcpsung.gov.tw/cybercrime/page2.htm。

4 林宜隆，楊鴻正，「網路交易犯罪之偵查要領─以網路詐欺犯罪爲例」，網址：http://www.ccu.edu.tw/TANET2001/scheduel/paper_abs/M105.html。

5 張雅雯，「網路犯罪之法律責任與防治建議」，網址：http://stlc.iii.org.tw/04-1-1.htm。

6 張雅雯，「立法管制網路犯罪與內容之必要性與妥當性」，網址：http://stlc.iii.org.tw/04-1-1.htm。

7 葉芳如，「從美國兒童網路隱私保護規則自如何保護兒童網路隱私安全」網

址：http://stlc.iii.org.tw/04-1-1.htm。

8 蔡美智，「美國重要之網路犯罪防制相關單位組織簡介」，網址：http://stlc.iii.org.tw/publish/89c.htm。

9 太穎國際法律事務所，「反制垃圾郵件的立法管制」，網址：http://www.elitelaw.com/05Publications/03promotion/%B2%C4%A4Q%A4@%B3%B9%A4%CF%A8%EE%A9U%A7%A3%B6l%A5%F3%AA%BA%A5%DF%AAk%BA%DE%A8%EE.pdf。

10 卜繁裕，「網路詐欺，防範重於破案」，財團法人中華民國消費者文教基金會全球資訊網，網址：http://www.consumers.org.tw/unit422.aspx?id=96。

11 賴左罕著，「高科技犯罪及電腦鑑識」，二〇〇四年一月二十七日，刊載於資安人全球資訊網－網路安全專題聚焦，網址：http://www.isecutech.com.tw/feature/view.asp?fid=155。

12 鄭進興，林敬皇，「台灣電腦鑑識領域現況與未來發展」，刊載於資安人全球資訊網－網路安全專題聚焦，網址：http://www.isecutech.com.tw/feature/view.asp?fid=449。

13 謝穎青，「建構新世代網路交易安全之新規範－人性尊嚴與商業利益孰終擅場」，太穎國際法律事務所全球資訊網，網址：http://www.elitelaw.com。

14 劉靜怡，「資訊社會的規範困境：台灣網際網路法律發展的歷史考察」，網址：http://140.109.196.10/pages/seminar/infotec4/4-3.doc。

15 劉靜怡，「網路色情的分析與規範：從台灣現行管制模式的粗暴與失焦談起」，網址：http://140.109.196.10/pages/seminar/sp/socialq/liu02.htm。

16 范傑臣，「各國網路內容管制政策之比較研究」，網址：http://www.ccu.edu.tw/TANET2001/scheduel/paper_abs/T103.html。

17 謝穎青，「通訊科技與法律的對話」，太穎國際法律事務所資訊網，網址：http://www.elitelaw.com/05Publications/03promotion/%B2%C4%A4Q%A4G%B3%B9%A8%D3%B9q%C5%E3%A5%DC%AA%BA%C1%F4%A8p%C5v%C4%B3%C3D.pdf。

18 章光明，「莫讓網路成爲犯罪天堂路」，我的 E 政府全球資訊網，網址：http://www.gov.tw/EBOOKS/TWANNUAL/show_book.php?path=3_011_001。

19 馮震宇，「網路犯罪與網路犯罪條約（上）」，財團法人亞太智慧財產權發

展基金會智權情報網，網址：http://www.apipa.org.tw/Search/Article-ViewADA.asp?strSearch=網路犯罪與網路犯罪條約&intADAArticleID=89。

20 曾惠仙，「網咖經營之適法性與法令問題」，網址：http://www.cqinc.com.tw/grandsoft/cm/093/aru931.htm。

21 陳俊龍，「ＣＡＳ優良食品制度之推行及成效」，行政院農業委員會全球資訊網，網址：http://www.coa.gov.tw/8/208/213/882/1803/3877/3877.html。

22 錢世傑，「從 Magic Lantern 談網路通訊監察之相關問題研究」，台灣網路法律中心，網址：http://www.chinalaw.org/professional.html。

23 陳佳溶，「網際網路發展過速，成爲犯罪滋生的溫床」，刊載於資安人全球資訊網－網路安全專題聚焦，網址：http://www.isecutech.com.tw/feature/view.asp?fid=360。

24 謝榮林，「網站管理不善之法律責任」，網址：http://www.lawbank.com.tw/fnews/news.php?nid=17069.00。

25 「網路上資訊隱私權保障問題之研究」，權平法律資訊網，網址：http://www.cyberlawyer.com.tw/alan4-0801.html。

26 「南韓對網路咖啡業管理現況、作法暨有關法令規範」，經濟部全球資訊網網址：http://www.moea.gov.tw/~meco/doc/ndoc/pub_901023_2.doc。

27 「我國與日本刑事案件偵查、執行及矯正統計之比較」，法務部資訊網，網址：http://www.moj.gov.tw/tpms/a90-1.aspx。

28 李雙其，「網絡犯罪偵查」，北大法律信息網，網址：http://article.chinalawinfo.com/article/user/article_display.asp?ArticleID=21759。

29 內政部警政署全球資訊網，網址：http://www.npa.gov.tw/index.php。

30 法務部全球資訊網法務統計，網址：http://www.moj.gov.tw/tpms/statanal2.aspx。

31 內政部警政署刑事警察局資訊網，網址：http://www.cib.gov.tw。

32 財團法人台灣網路資訊中心網站，網址：http://www.twnic.net.tw。

33 交通部電信總局全球資訊網，網址：http://www.dgt.gov.tw/Chinese/About-dgt/introduction.shtml。

34 台灣網際網路協會全球資訊網，網址：http://www.twia.org.tw/p02-self-policing.htm。

35 數位聯合電信股份有限公司全球資訊網，網址：http://service.seed.net.tw/adslrule.shtml。

36 奇摩 Yahoo 網址：http://tw.yahoo.com/info/utos.html。

37 法務部主管法規資料庫查詢系統－法規草案，網址：http://mojlaw.moj.gov.tw/ShowScript.asp?id=2898。

38 資訊安全網，網址：http://www.infosec.gov.hk/chinese/general/virus/type.htm。

39 行政院金融監督管理委員會銀行局全球資訊網，網址：http://www.boma.gov.tw/ct.asp?xItem=219890&ctNode=1571。

40 立法院全球法律資訊網，網址：http://npl.ly.gov.tw/do/www/billIntroductionContent?id=22。

41 全國法規資料庫，網址：http://law.moj.gov.tw/Scripts/NewsDetail.asp?no=1K0060044。

42 ISO 輔導網，網址：http://www.eternaliso.com/intro.htm。

43 中國網，網址：http://big5.china.com.cn/chinese/PI-c/216517.htm。

44 中國互聯網絡資訊中心全球資訊網，網址：http://www.cnnic.net.cn/html/Dir/2000/09/25/0651.htm。

45 財團法人資訊工業策進會科技法律中心全球資訊網，網址：http://stlc.iii.org.tw/。

六、 法院判決

1 臺灣臺北地方法院九十年度訴字第六九三號刑事判決。

2 臺灣臺北地方法院八十九年度訴字第一六〇六號刑事判決。

3 臺灣臺北地方法院九十一年度訴字第六九號刑事判決。

4 臺灣高等法院九十二年度上訴字第二七三號刑事判決。

5 臺灣新竹地方法院九十年度訴字第六四號刑事判決。

6 臺灣彰化地方法院九十二年度訴字第一四五九號刑事判決。

7 臺灣臺北地方法院八十八年度少連易字第八號刑事判決。

貳、 英文參考文獻

一、期刊論文

1 Susan W. Brenner, TOWARD A CRIMINAL LAW FOR CYBERSPACE：A NEW MODEL OF LAW ENFORCEMENT, Rutgers Computer and Technology

Law Journal. (2004).

2 Griffin S. Dunham, Carnivore, The FBI's Email Surveillance System: Devouring Criminals, Not Privacy, Federal Communication Law Journal, Vol. 54 Issue 3, p.545. (2002).

3 Robert Ditzion etal. , COMPUTER CRIMES, 40 AM. Crim. L. Rev. 285. (2003).

4 Natasha Jarvie, CONTROL OF CYBERCRIME-IS AN END TO OUR PRIVACY ON THE INTERNET A PRICE WORTH PAYING? PART 2, Computer and Telecommunication Law Review. (2003).

5 Cyndie Chang, EXPORING INTERNET PRIVACY THROUGH CABLE BROADBAND STRUGGLES: ISPS WALK A FINE LINE BETWEEN PRIVACY AND SECURITY, 22 LOY. LA. ENT. L. REV. 491. (2002).

6 James Adams, SUPPRESSING EVIDENCE GAINED BY GOVERNMENT SURVEILLANCE OF COMPRTERS, 19-SPG Crim. Just. 46. (2004).

7 Susan W. Brenner, TOWARD A CRIMINAL LAW FOR CYBERSPACE: A NEW MODEL OF LAW ENFORCEMENT? , 30 RUTGERS COMPUTER & TECK L.J. 1 (2004).

8 Justin Nackley, "OH, WHAT A TANGLES [WORLD WIDE] WEB WE WEAVE." THE DANGERS FACING INTERNET SERVICE PROVIDERS, AND THEIR AVAILABLE PROTECTIONS, 2005 Syracuse Sci. & Tech. L. Rep. 2 (2005).

9 Gideon A. Lincecum, ELECTRONIC SURVEILLANCE: PROTECTING THE PRIVACY ECOSYSTEM FROM THE FEDERAL BUREAU OF INVESTIGATION'S CARNIVORE, 28 Okla. City U. L. Rev. 291 (2003).

10 Susan Nevelow Mart, PROTECTING THE LADY FROM TOLEDO: POST-USA PATRIOT ACT ELECTRONIC SURVEILLANCE AT THE LIBRARY, 96 Law Libr. J. 449 (2004).

11 Robert A. Pikowsky, THE NEED FOR REVISION TO THE LAW OF WIRETAPPING AND INTERCEPTION OF EMAIL, 10 Mich. Telecomm. & Tech. L. Rev. 1 (2003).

二、網站資料

1 Declan McCullagh,Ben Charny,「 FBI adds to wiretap wish list 」, http://news.com.com/2100-1028-5172948.html.

2 Declan McCullagh,「FBI targets Net phoning」, http://news.com.com/2100-1028_3-5056424.html.

3 Declan McCullagh,「Feds step up push to wiretap VoIP calls」, http://news.zdnet.com/2100-1009_22-5157282.html.

4 Jeffrey Yunan Ren,Wesley Chiu,「Internet Café Regulation: PRC and Hong Kong」, http://www.perkinscoie.com/page.cfm?id=53.

5 Stefanie Olsen,「Patriot Act draws privacy concerns」,http://news.zdnet.com/2100-1009_22-275026.html.

6 Daniel A. Morris,「Tracking a Computer Hacker」, http://www.usdoj.gov/criminal/cybercrime/usamay2001_2.htm.

7 INTRODUCTION TO MODULE V: THE USA PATRIOT ACT, FOREIGN INTELLIGENCE SURVEILLANCE and CYBERSPACE PRIVACY, http://cyber.law.harvard.edu/privacy/Introduction%20to%20Module%20V.htm.

8 Simon Hayes,「Police target free email」, http://www.crime-research.org/news/2003/07/Mess2101.html.

9 愛國者法相關資料全球資訊網，http://www.epic.org/privacy/terrorism/usapatriot/#analysis.

10 網路犯罪相關資料全球資訊網，http://www.cybercrime.gov/

11 美國聯邦調查局全球資訊網，http://www.fbi.gov/

12 電腦犯罪研究中心全球資訊網（Computer Crime Research Center），http://www.crime-research.org/articles/.