國立交通大學

科技法律研究所

碩 士 論 文

網路時代通訊監察與個人資料保護之法制研究

Legal Framworks of Surveillance and Data Retention on Internet Communications

研 究 生：蘇三榮

指導教授：林志潔 博士

中華民國九十八年六月

網路時代通訊監察與個人資料保護之法制研究

Legal Framworks of Surveillance and Data Retention on Internet Communications

研 究 生：蘇三榮　　Student：Su San-Jung

指導教授：林志潔博士　　Advisor：Dr. Lin Chih-Chieh

A Thesis
Submitted to Institute of Technology Law
College of Management
National Chiao Tung University
in partial Fulfillment of the Requirements
for the Degree of
Master
in
Technology Law

June 2009
Hsinchu, Taiwan, Republic of China

中華民國九十八年六月

網路時代通訊監察與個人資料保護之法制研究

學　　生：蘇三榮

指導教授：林志潔博士

國立交通大學科技法律研究所碩士班

摘 要

通訊監察為警方偵查中相當重要之手段，以往對於傳統電話之通訊監察，已行之多年，亦有通訊監察中心負責統合通訊監察相關事宜，制度上相對成熟。但針對近年來興起的各種網路通訊，不論在通訊監察的技術或是法制上，皆尚未建立標準及程序，造成警方辦案之困難，及侵害人權之憂慮。

故本文以現行通訊保障及監察法之規定為基礎，詳細討論針對網路通訊監察所應遵守之程序規範，並介紹目前實務運作之狀況，以及所遇到之困難。對於警方所遇到之困難，以及人權保障之問題，本文介紹美國體制化之網路通訊監察，作為我國之參考，並提供建議及解決方案，希冀未來在網路通訊監察之部分，能建立一套完整、成熟之制度，兼顧犯罪偵查及人權保障這兩個國家重要利益。

另一方面，與通訊監察息息相關的通聯記錄保存，亦為警方不可或缺的偵察方式。隨著網路時代的來臨，通聯記錄的範圍及重要性日與劇增，已漸漸涉及人權保障之核心，面對如此的改變，現行法制顯然不足因應，而有修正之必要，以符合實務之需求以及保護人民之資訊隱私。

關鍵字：通訊監察、網路通訊、肉食者系統、攔截封包、通訊隱私、不定點監聽，通聯記錄。

Legal Framworks of Surveillance and Data Retention on Internet Communications

Institute of Technology Law
National Chiao Tung University

Student：Su San-Jung

Advisor：Dr. Lin Chih-Chieh

ABSTRACT

Electronic surveillance is a crucial method for criminal investigation which has been utilized for several years. There is also a competent authority responsible for all surveillance monitoring and supervising. However, as the rapid development of Internet communications, it seems that both the technology and legislation does not quite follow the step of innovation, causing difficulties of criminal investigation. It also raises the concern of the right of privacy.

Therefore, this article starts out from the current wiretap law of Taiwan, discussing the procedural and practical issues of surveillance on Internet communication, analyzing problems that the police encounter and the possible threat to the right of privacy. Furthermore, this article presents the system of Internet surveillance in United States to help us understanding how others operate and evaluate the whole system.

In the end, this article provides some suggestions and opinions toward those issues and problems above, hoping that Taiwan can soon establish a complete system and legal frameworks of surveillance on Internet communications, and find a balance between criminal investigation and protection of human right.

Key words：Wiretap, internet communication, carnivore system, packet intercepting, privacy of communication, roving surveillance, data retention.

誌 謝

本篇論文脫胎於刑事警察局之研究計畫「第二類電信監察之法制研究」，感謝劉尚志老師主持計畫，李榮耕老師提供顧問諮詢，王煌玄、王俊凱兩位學長統籌處理所有行政事務，以及我的研究夥伴王思涵，與我一起完成計劃全文。並感謝通訊監察中心及各縣市刑警大隊之警官們，提供寶貴的實務現況及意見。

論文寫作期間，感謝林志潔老師接手擔任指導教授，對於論文架構，寫作技巧等大方向給予指導，並再次感謝劉尚志老師及李榮耕老師義不容辭擔任口試委員，讓這篇不成熟的論文有修正的機會。

最後感謝科法所所有老師給我的教導與鼓勵。感謝辛苦的所辦助理們，在學校的每件事情，都有你們的幫助。感謝我的學長姐、同學、學弟妹，兩年之中給我許多美好回憶，謝謝科法所的大家。

蘇三榮 謹誌于
交通大學科技法律研究所
九十八年六月

目　錄

表目錄

壹、前言

一、緣起

台灣電信產業於民國八十五年通過電信三法後開啟電信自由化發展，之後隨著一連串電信業務開放民營，加上電腦網路與電信科技的快速發展，不管有線或無線寬頻逐漸滲透民眾日常生活當中。其中於民國 85 年 2 月電信法中第十一條規定將電信事業分為第一類電信事業以及第二類電信事業，交通部並於 86 年 2 月 18 日依電信法第十七條第二項規定，訂定發布「第二類電信事業管理規則」，同時廢止「電信加值網路業務管理規則」。90 年 6 月配合 WTO 修正發布「第二類電信事業管理規則」開放語音轉售服務，包括語音單純轉售服務、網路電話服務及批發轉售服務如（電話卡、公用電話等）等，對於治安之衝擊為最大。

依據國家通訊傳播委員會最新統計資料（97 年 7 月）顯示，台灣寬頻上網人口數已經突破六百八十萬人[1]。隨著寬頻時代來臨，一般民眾除了一般資料傳輸外（如文字、圖片、檔案、e-mail…等），繼之而來的網路電話與多媒體影像傳輸的方式，即將成為民眾平常生活所不可或缺的溝通方式。因應通訊技術發展，交通部於 90 年 6 月 28 日開放網路電話服務，提供經營者可透過網際網路傳送與接收所提供之語音服務予國人使用，是為網路電話正式服務開始。

據統計，截至 94 年 8 月止，我國電信市場已有八十餘家經營者提供此項服務。行政院財經會報於 93 年 11 月 1 日第五次會議決議「請交通部儘速完成規劃網路電話服務之號碼核配措施，俾實現有線及無線網路電話服務」，為配合政策目標、引進寬頻創新應用服務，豐富國人選擇電信服務權利，提高市場競爭強度，爰參考日本、韓國及德國等國作法，核配 E.164（為國際電信聯合會對電信號碼編定規格書之編號）用戶號碼予網路電話服務，交通部電信總局業於民國 94 年 11 月 15 日開放 E.164 用戶號碼網路電話服務之申請，核配 070 字頭 11 碼長之 E.164 用戶號碼予網路電話服務。

網路電話服務係指透過網際網路所提供之語音服務，由於網際網路具有全球相連之特性，以及易於整合語音、數據及影像訊號進行處理與傳輸之優勢，因此網路電話服務較傳統公眾電話 PSTN 或行動電話服務更能符合整合性（convergence）、全球化（globalization）、即時性（immediacy）與移動性（mobility）之通訊市場主流趨勢，因此，IP（Internet Protocol）技術未來將成為通信技術主流。

[1] 寬頻上網帳號數，國家通訊傳播委員會網站: http://www.ncc.tw/chinese/news_detail.aspx?site_content_sn=327&is_history=0&pages=0&sn_f=7425（最後點閱時間:2008 年 12 月 10 日）

有鑒於 IP 網路電話與網路影像的傳輸成本比傳統便宜非常多，加上寬頻網路的普及，所以很快吸引大量使用者使用。網路電話服務未來極可能成為語音通信的主流，國際間正熱烈討論相關監理議題，網路電話究係應如何配合警察機關監察，是各國防制網路電話流於犯罪溫床的防制重點。隨著網路電話與多媒體溝通工具普及，以往政府仰賴傳統電信監理來預防與打擊犯罪的機制，可能產生非常大的漏洞。雖然國際間針對網路電話服務所衍生的問題，猶處於研究階段，尚未有明確規範，我國仍應密切觀察國際間之發展，並著手研究相關議題之可能解決方案。

二、網路監察之技術特性與問題

(一) 網路監察制度未建立

我國警方對於傳統的 PSTN 網路以及行動電話通訊之監察，已有一套行之多年的完整制度，亦有通訊監察中心負責統合通訊監察相關事宜，可以說已做到滴水不漏的掌握，鮮有通訊監察之漏洞存在。但針對網路監察之部分，卻尚在起步階段，不論在技術面、法律面，都未有一套制度化的監察體系，常需依靠臨時監察的單兵作戰方式處理，使得網路通訊監察的運用非常有限，造成犯罪偵查之死角，尤其現在所謂的犯罪集團，包括走私集團、詐騙集團等皆將其網路通訊當成其主要之通訊方式。相對應的，警方對於通訊監察之重心，亦應慢慢轉移到網路這個部份。

故在網路通訊當中，通訊監察的對象很容易利用各種方式隱匿自己的存在，逃避司法機關的偵查。因此在通訊監察聲請書中，有關監察對象、監察通訊種類及號碼等足資識別之特徵與監察處所等內容即難以確定，例如行為人是利用區域網路所分配的虛擬 IP ，那麼所能追查到的，便只有對外連線的實體 IP 位址，或者行為人使用的是隨機配發 IP 位址的上網服務，也不能單就 IP 位址直接特定出網路使用者，而必須搭配 ISP 業者所留存的通訊記錄與客戶資料加以交叉比對才可能得知使用者的身份，再者，網路使用人也可能使用隱藏 IP 的軟體，便可能造成追查上的困難。

除此之外，行為人亦可能透過後門程式來遠端遙控該 IP 位址所代表的電腦進入網際網路，在這種情形下，該 IP 位址所代表的電腦只不過是犯罪行為人的「跳板」，並不是真正的通訊來源，即便被得知入侵該「跳板」電腦，入侵之人也可能以斷線等各種方式來擺脫執法者的追蹤偵查而不留痕跡。再者，即便該 IP 位址真的是通訊來源，如果該 IP 位址所代表的電腦是多數人或不特定人所得操

作者，例如圖書館、網咖等，由於使用者眾多，因此亦不能直接由 IP 位址得知何人為真正的網路使用者。

故相較於傳統電話、行動電話等通訊設備，網路通訊具有較高的不特定性，犯罪當事人雙方若每次進行犯罪聯絡時，都在不同的地點上網，且網路犯罪者得利用特殊之電腦技術，使執法者難以在同一節點進行攔截追蹤，如此一來，要選擇哪一個節點進行截取通訊內容，就發生實際運作上的困難，自然加深偵查的困難度。

且網路通訊係在虛擬的網際網路世界進行，和現實世界中，傳統電話通訊的概念有所不同。然而目前通訊監察書之記載，皆是以現實世界為準，在適用到虛擬的網路世界時，即可能會發生困難。

(二) 資料保存（Data Retention）法制的不足

網路服務業者提供多樣化的上網服務，理論上，只要某一用戶連接上網路後，該用戶的一舉一動，都會被業者所記錄下來，個人在網路上的虛擬行蹤，可說是無所遁形。如此資料量暴增所帶來的衝擊，已遠遠超過傳統通聯記錄所能含蓋的範圍。如此巨大的量變，也就連帶產生了質變。故網路上的個人資料之重要性，已不能等閒視之。

而目前法制關於偵查機關調閱個人資料程序上，仍然沿用傳統關於通聯紀錄的取得方式，亦即警方以公文函送電信業者業者即將警方所需資料傳送回來，這樣的程序顯得太過容易、簡略，既沒有相當的要件要求，亦無專責的監督機關，造成個人資料被濫用的可能性大幅增加，在個人資料重要性日益增加的情況下，目前的個人資料保護法制，可能必須有所改變。

另一方面，警方面對大量的上網紀錄，究係可調取哪些資料，要用何種程序取得，目前不論是法規命令、實務見解、學說意見皆未有詳細規定及討論，導致警方在偵查時有無所適從之感覺，故資料保存法制之建立，是刻不容緩之議題。

(三) 網路通訊與傳統電話之差異

由於傳統電信網路和 IP 電信網路的架構上之差異，IP 網路的電信監察和傳統電信網路的電信監察在技術上有很大的差異。傳統電信網路是所謂的電路交換（Circuit Switch）網路，通話內容會經由固定的線路進行傳輸，監察通話內容必須先判別傳輸所使用的實體線路，然後從實體線路上分接的監察線路上監錄通話的內容。而 IP 網路則是屬於分封交換（Packet Switch）網路，通訊的內容會分

解成多個封包在 IP 網路中傳輸，其封包資料會在發話端和收話端之間直接傳輸，且其傳輸的路徑由 IP 網路中的各個節點決定，語音資料不會經過單一固定伺服器端，也無法保證其傳輸路徑。

故網路電話因為 IP 網路交換原理，係以分散式的方式運作，這與傳統電信網路交換係以集中式的方式不同，以往電信監察、警調單位所仰賴之電信監察系統將不足以應付。亦造成傳統電信監理實務上所使用的方法，不足以應付 IP 網路上之新型態犯罪方式，原先適用於傳統語音電信技術監察的規範與機制亦出現不合時宜之現象。警調、監察體系需要針對 IP 網路特性，利用更先進的通訊監理技術加以補強，以便更有效率的來因應 IP 網路普及所衍生帶來的新型態犯罪手法。

而若偵查機關針對網路傳輸之分散性，以攔截封包之方式執行網路監察，容易攔截到不相干第三人之資訊，引發過度侵害隱私權及不符合最小手段性之質疑，本文亦針對此爭議進行探討。

(四) 電信業者配合義務與程度尚未明朗

在電信產業開放競爭之後，需配合執法機關進行通訊監察者，不再僅限於如中華電信公司之傳統電信業者，許多 ISP 業者、網路內容服務提供者（Internet Content Provider）等網際網路業，都可以利用各種網路監看設備，過濾、分析、監看自己系統中的網路狀況，以電子郵件為例，電子郵件主要在郵件伺服器內進行操作，此種郵件伺服器不僅中華電信可以提供服務，許多民間業者都可以提供相同的服務。另以網路聊天室為例，許多聊天室由於技術層面不高，不需要中華電信等大型電信公司才有能力架設，一般私人亦可成立聊天室，因此網路通訊監察的配合對象，與傳統電話不同，不再由中華電信公司等傳統電信業者獨占。

故在此情形下，需要配合通訊監察之業者數量大幅增加，衍伸出網路服務業者如何配合通訊監察，以及經費負擔之問題。尤其在網路服務業者的資本額普遍不大的情況下，如何配合犯罪偵查，又不至於讓網路服務業者負擔過重，是個困難的問題。

(五) 跨國犯罪之衍生

由於網路無國界的特性，許多網路上犯罪可能存在於單一國家，但也可能不再侷限於某一特定國家或某一特定區域，而跨越國界成為跨國性的犯罪，例如跨國性的毒品案件偵查，販毒者可能分別身處在 A 國與 B 國，但是通訊監察的節點可能會在第三國 C 國。針對此種跨國性的犯罪，必須透過國際合作的機制，

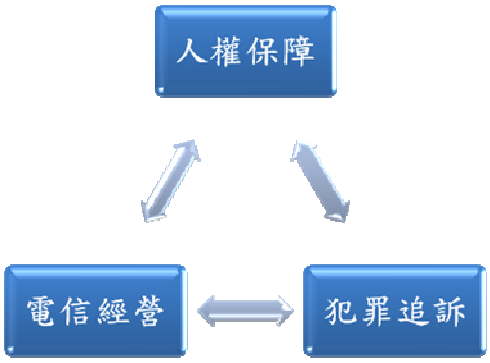
才能在第一時間確實掌握犯罪者的動態。因此，傳統的犯罪偵查模式在網路世界中已經逐漸無法完全適用，若無法突破跨國合作之困境，網路將可能成為犯罪的天堂[2]。

(六) 不同領域的競合

網路通訊監察涉及許多層面，有賴不同領域間的合作：傳統電信通訊監察法規多著墨在第一類電信服務，然而隨著現今社會趨勢，網路電話多媒體溝通工具蔚為風潮，而由於網路電話與傳統電信運作方式大不相同，因應偵查實務進行，現行通訊技術與設備，亦需發展出進一步系統化的通訊監理技術；有完善法源依據及先進設備的支持，偵查才得以順利展開。

而新的監察技術，將改變犯罪偵查的運作方式，亦造成新的隱私權侵害態樣形成訊技術、偵查實務、法律問題三方交錯之情況，涉及層面極廣，故本文希望對此做整合性之討論。

(七) 不同利益的拉鋸



[2] 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(2002)。

網路通訊監察亦涉及不同利益間的衝突。以犯罪追訴觀點出發，網路服務的特色使得通訊監察包含範圍越廣，越有利於犯罪偵查與起訴，然於此就進逼人權保障的壁壘，侵犯人民隱私與通訊自由；再相對應電信經營業者，為配合犯罪偵查需建置與維持系統，經費負擔是否過重，又該如何平衡；電信經營業者為配合檢察機關或內部分析，保存大量用戶私人資料，是否有侵害個人隱私之嫌；相對地若追求人權保障的完整，犯罪追訴難度勢必增加，三者之間的利益拉鋸就此而生。本文的目標為不偏廢任何一方，而找出三者之間最佳的平衡點。

三、預期達成之目的

傳統電信監察機制只針對第一類電信業者所經營的語音業務與系統進行監察。但科技進步，IP Based 的語音電話監察技術卻與以往第一類電信語音服務的監察技術極大不同，且難度頗高，因為 IP 網路交換原理是分散式的，並不同於以往第一類電信語音服務所使用的系統是集中式的架構。加上 IP 網路服務多樣性，遠遠超出以往第一類電信服務的電信系統。

因此本文擬針對現有之電信管制與法制架構下，因應 IP 電信網路技術發展現況與未來趨勢，進行 IP 電信網路監察技術評估與相關現有法制分析，針對現有電信網路監察法制與程序機制，因為 IP 網路發展而不足之部分，提出相關建議。其內容包括：

1. 通訊監察規範範圍之界定(網路語音、通聯紀錄、通訊內容等)
2. 網路監察相關法制之分析
3. 隱私權合理期待之分析
4. 網路監察之技術與相關法律問題
5. 網路監察的法定程序
6. 網路監察完結後之程序
7. 通聯資料保存之法制分析
8. 第二類電信業者配合義務之探討

四、研究限制

(一) 研究深度部分

由於網路監察之問題為科技進步所產生之新興問題，相關討論尚在起步階段，文獻資料亦不齊全，本文希望盡可能將相關議題皆納入討論，點出其問題所在，故本文範圍相當龐大繁雜，每一章皆可延伸成一獨立之研究主題，難免在深

度部分有所不足，希望能以本研究作為起點，未來能有更深入之論文延續，使我國監察相關法制更加完整。

(二) 未納入國安通訊監察

雖然國安通訊監察亦為通訊監察中不可或缺之一環，重要性甚至可能高過警方之通訊監察，但由於國安通訊監察之目的、對象皆與警方通訊監察有顯著差異，實有分開討論之必要，美國亦將兩者分開立法，以資區別。雖然我國將兩者合併立法，但並非恰當之作法。且國安通訊監察涉及國家機密，外人難窺其全貌，討論上亦有其困難及限制。

故基於以上理由，本文認為國安通訊監察與警方通訊監察有分開討論之必要，而本文僅探討警方通訊監察之部分。

五、研究架構與方法

(一) 訪談及實務現況之調查

由於通訊監察涉及偵查實務及電信技術等專業問題，故除以文獻歸納法，外國立法例比較法外，採用訪談專業人士之方式處理，包括與通訊監察中心之警官每週一次之會議，以及與刑事警察局偵九隊、台北市警察局刑事警察大隊、高雄市警察局刑事警察大隊中，負責通訊監察相關事務之警官進行訪談，以期真正了解實務運作之現況及問題，訪談內容及具體意見將於以下各相關章節中呈現。

(二) 其他國家政府針對 IP 網路監察運作機制資訊蒐集

透過期刊、圖書、網際網路，蒐集世界其他國家政府針對 IP 網路監察運作機制相關之因應或規畫資訊，以先進國家政府 IP 網路電話監察運作機制為典範，縮短摸索研究時程。

(三) 法制差異比較與分析

就上述蒐集之資料進行分析，針對 IP 網路電話監察機制可能影響之各個層面問題加以探討。希望藉由運用 IP 網路電話監察科技打擊犯罪與預防犯罪、保護社會安全體制的同時，能藉由法律層面的分析與探討，建立一套符合民主法治標準的作業規範，保障憲法所賦予人民隱私權與通訊自由權力不會因為公權力之執行過當而侵害。

(四) 網路監察及資料保存法制之改革建議

並依據上述分析之結果，比較國內現有電信監察之業務規範，提出網路監察及資料保存法制之改革建議。

貳、通訊隱私的法律地位及法制

本章闡述通訊隱私之法律地位，從最上位的「隱私權」出發，介紹其概念發展和內容。探討到屬於隱私權一部之「通訊隱私」。並進而具體的以美國憲法裁判實務、我國憲法規定、大法官解釋之演進，分析通訊隱私的法律地位。

接著本章介紹與通訊隱私相關之法律規定包括「通訊保障及監察法」「電腦處理個人資料保護法」「刑事訴訟法」「電信法」等。

最後介紹外國法制，包括「美國電子通訊隱私法(the Wiretap Act)」，及「歐盟個人通訊資料保存指令(Directive 2006/24/EC)」，分述如下：

一、隱私權之概念

隱私權的概念，原本並不存在於傳統西方思想中，在實務偶有使用此一名稱時，亦未見對其概念有任何說明。真正將隱私權當作一項獨立概念加以探討者，應始於1890年Harvard Law Review 上刊載之The Right to Privacy 一文，二位作者Warren 和Brandeis 於文中從習慣法上對誹謗和著作權相關的規範，導引出個人對於因其情感表達而成的文書和作品有決定是否公諸於世的權利；並界定隱私權為「生活的權利」（right to life）和「不受干擾的權利」（right to be let alone），內容為個人對其自身事務公開揭露的決定權利，其所保障的是個人的「思想、情緒和感受」。在界限上，則指出「公共利益」和「同意」是兩項主要限制。這許多論點對後來的實務和學說至今仍有相當之影響[3]。

對於隱私權的概念發展和內容，如果以美國法院的判決為主要觀察對象，可以歸納出以下的面向：

(一) 個人空間隱私權

包含個人的物理空間和心理空間不受侵擾的權利。具體言之，有搜索扣押、侵入住宅、噪音、強迫收聽收看等議題。

(二) 資訊隱私權

包含個人資料和通訊不被揭露的權利。具體言之，在個人資訊方面有個人肖像、聲音、過去經歷（尤其犯罪記錄）、醫療記錄、財務資料、一般人事資料、犯罪被害人資料、招致誤導的情節等課題；在通訊隱私權方面有測謊、郵件、通話等面向的討論。

[3] 詹文凱，隱私權之研究，台灣大學法研所博士論文，頁 13,19(1998)。

(三) 個人自主性隱私權

即個人私生活的自我決定權，包含生育、家庭和個人切身事務等三方面之自主權。具體言之，生育自主性包括避孕、中止懷孕、懷孕和生育、強制絕育、代理孕母等議題；家庭自主性包括子女教養、結婚與離婚、家庭關係等方面的議題；個人自主性包括性行為、猥褻行為或物品、藥物使用、個人形象、個人姓名、自殺和安樂死等方面的討論[4]。

二、通訊隱私之定義

從以上討論可知，通訊隱私為隱私權之其中一個面向，而本文對通訊隱私之定義為：是對個人領域的私人通訊事務之控制權。詳言之，其主體為個人，客體為私人通訊事務，作用則是控制。

首先，所謂個人應指自然人，通訊保障及監察法第4條規定：本法所稱受監察人，除第五條及第七條所規定者外，並包括為其發送、傳達、收受通訊或提供通訊器材、處所之人。因為僅有自然人方能憑藉自由意識，與通訊相對人溝通、傳遞訊息，做意思交流。而法人僅為法律上擬制之人格，無機關之輔助即無法發出訊息。縱以法人名義和他人通訊，須由自然人代為之，實際上仍是自然人之通訊。

其次，通訊隱私之客體應為私人之通訊事務，即通訊相對人不欲公開之秘密通訊事務，且客觀上有隱私或秘密之合理期待者。若通訊之事務屬於公開之事務，或客觀上已被第三人所知悉，即非屬通訊隱私之範圍。

最後，通訊當事人對於通訊隱私應有其控制權，個人可以將自身事務開放，使他人或公眾知悉、參與，也可以封閉其個人領域，排除他人或公共權利的介入或支配。這種選擇的權利是個人對其自身事務處理的權利。賦予個人控制的權利，便是讓個人可以決定在何時、何地、何種程度下，何人可以知悉或參與其自身事務的部分，以便維持個人的獨立和不受支配[5]。

三、憲法上的地位

(一) 美國憲法裁判實務

---

[4] 前揭註 3，頁 47-121。

[5] 陳仲嶙，電子化政府之資訊保護--以個人資料保護為中心，頁 5，網址: http://www.is-law.com/OurDocuments/PR0001CL.pdf(最後點閱時間:2008 年 12 月 17 日)。

1. 從「物理入侵原則」到「合理隱私期待」

在*Olmstead V. United States* 案[1]，該案當事人Olmstead 被控違反國家禁酒法（National Prohibition Act），共謀違法持有、運送、販賣酒品，聯邦官員未取得法院令狀，而在被告住所外之電話線上裝置竊聽器，該案件偵破雖然偵破，但卻因此產生爭議。本案之爭點在於聯邦官員未依法定程序向法院聲請核發令狀，而在被告住所外之電話線裝置竊聽器，是否違反美國憲法第四修正案。最高法院認為電話線路並非被告家宅的一部分，聯邦官員並未侵入被告之居所，亦未扣押憲法第四修正案中所保護之有體物，並無搜索扣押之問題，監察所取得之內容為合法取得之證據。換言之，本案最高法院見解認為，憲法第四修正案是在保障人民身體、住宅、文件及其他財產等「具體有形物」，至於口頭談話等內容並不包括在保護之範圍內[3]，即以「有無物理侵入」為通訊監察是否合法之判斷標準，聯邦官員未依法定程序聲請，而在被告住所外之電話線裝置竊聽器，並未侵入被告之居所，取得通訊監察之內容為合法取得之證據；反之，若未依法定程序聲請令狀而侵入被告之居所，則所取得證據並非合法[6]。

物理入侵原則直到1967 年的*Katzv. United States*[7] 一案中才被推翻，在本案中，聯邦調查局官員得知被告Katz 經常使用特定的公共電話對外聯絡，而在電話亭外裝置竊聽器監察被告的通話，最高法院認為公共電話雖非被告的財產，且裝置的竊聽器亦無物理的入侵，但仍排除依此獲得的證據。因為被告進入電話亭並關上門時，被告已表現出對其通話內容有合理隱私權的期待，而政府的行動侵犯被告使用電話亭時的合理期待，已構成第四修正案的「搜索」，因聯邦調查局事先未聲請法院令狀，故排除依此所獲得的證據。自此，第四修正案轉化為對資訊隱私權保障的規範，並以「合理隱私期待原則」做為是否適用第四修正案的判斷標準。

2. 風險承擔原則

聯邦最高法院雖然改以合理隱私權期待原則做為是否適用憲法第四修正案的判斷標準，擴大第四修正案的適用範圍。因此，當執法單位欲實施通訊監察處分時，如涉及個人隱私期待場合，仍需事前向法院聲請令狀（warrant），始屬合憲。然而，最高法院之後也承認令狀原則有其例外，例如被告的同意及第三人的同意。其中有關第三人同意，或稱風險承擔原則（assumption of risk）對網際網路隱私權的判斷，更有決定性的影響。最高法院在*United States v. Miller*[8] 案與

[6] Olmstead V. United States, 227 U.S. 438 (1928)。
[7] 389 U.S. 347(1967)。
[8] 425 U.S. 435(1976)。

Smith v. Maryland[9] 案中，均認為只要是對第三人（third party）揭露的資訊，都沒有第四修正案的適用，一般稱此為揭露原則。

在*Unite States v. Miller* 案中，最高法院認為，憲法第四修正案並未禁止第三人透露其取得的個人資訊給政府機關，即便該資訊限定在特定目的使用或規定第三人不得私自揭露時亦然。因此，假設某人將其個人秘密告訴他的朋友，依一般社會常情均會認該人主觀上具有合理的隱私期待，但最高法院仍舊認為依憲法意旨，此期待不是合理的。

最高法院對於揭露原則的見解，在處理有關通訊系統（communications Networks）是否有第四修正案隱私權保障的適用時，具有重大的影響。因為通訊系統在傳遞資訊時，必須揭露部分或全部的資訊給系統業者，才能完成通訊內容的傳遞。例如在傳統郵件通訊，如寄信人與收件者雙方的地址；電話通訊，如通話雙方的電話號碼等，這些有關通訊的來源與目的地資訊（to and from information）等資訊，都是「信封資訊」（envelop information）。信封資訊乃使用者必須揭露給系統業者的資訊。在揭露原則下，最高法院無異議地駁回「信封資訊」適用第四修正案的請求。在傳統郵件通訊，法院認為郵件使用人對於郵件及包裹的外觀並無合理的隱私期待，因為此類資訊在寄送過程中必須揭露給郵務人員，因此政府人員不須聲請法院命令或搜索票即可檢查信件的外觀資訊[10]。

在電話通訊系統，最高法院認為電話號碼應排除在第四修正案的適用之外，因為使用者在撥打電話時，必須揭露其電話號碼給電話公司[11]。涉及網際網路通訊時，最近地方法院也認為網路使用者對於傳遞給ISP 業者通訊內容以外的資訊，不能主張具有合理的隱私權期待[12]。另外，涉及「內容資訊」是否適用第四修正案的判斷上，揭露原則仍然扮演著重要的角色。

一般而言，法院認為資訊只有在處於封存（seal）狀態，讓系統業者、一般大眾無法輕易得知其內容的情形下，使用者才能主張具有合理的隱私權期待。在傳統郵件通訊中，封緘的信件內容可以主張隱私權期待，但未封緘的明信片及包裹不具有合理的隱私期待[13]。

在電話通訊，發話端及受話端雙方的通話內容享有隱私權期待，但如果電話使用者係使用廣播電波的電線電話時，由於該電波係一般大眾能夠自由收聽，因

---

[9] 442 U.S. 735(1979)。

[10] United States v. Hinton, 222 F.3d 644,675(9th Cir. 2000)。

[11] *See* Smith v. Maryland, 442 U.S. 735(1979), at 745-46。

[12] *See* Guest v. Leis, 255 F.3d 325, 335-36(6th Cir. 2001); United States v. Hambrick, 55 F. Supp.2d 504, 508-509(W.D.Va. 1999),aff'd, 255 F 2d 656(4th Cir. Aug. 3, 2000);United States v. Kennedy, 81 F. Supp.2d 1103,1110(D. Kan.2000)。

[13] *See* Ex parte Jackson, 96 U.S. 727, 733(1877)。

此不具有合理的隱私權期待[14]。目前而言，法院尚未就將揭露原則適用於網路通訊上，但有認為由於網路通訊傳遞時，內容資訊與信封資訊常常混雜一起傳遞至 ISP 業者的伺服器中，因此法院很有可能比照判斷明信片及無線電話情形，繼續援用揭露原則，而否定網路使用者合理隱私期待的主張。

(二) 我國憲法規定

我國憲法雖未明文規定「隱私權」，但從憲法已有的條文可以知道，制憲者有意將隱私權納入憲法的規範中。例如第十二條明定「人民有秘密通訊之自由」，隱含有「隱私權」概念。憲法第十條隱含著人民享有在居住空間中，不受國家或他人不當侵入的權利。也就是說，人民對於其住宅或處所享有不受侵擾的隱私權利。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，也可以解釋為保障隱私權的概括規定。從這一些憲法規定，我們也可以歸結出隱私權屬於憲法所保障的基本權利的結論。

但是，隱私權並不是一個絕對的權利，在符合憲法第二十二及二十三條時，國家仍然可以予以限制。在刑事訴訟程序中，為了取得證據可以搜索處所或是監察人民的秘密通訊便是適例。

(三) 司法院大法官釋字第六三一號解釋

從釋字第六三一號解釋所援用的憲法條文及法理依據來看，大法官是從人民的秘密通訊自由（憲法第十二條）及正當法律程序出發。大法官首先指出，人民所享有的秘密通訊自由包括了「人民就通訊之有無、對象、時間、方式及內容等事項，有不受國家及他人任意侵擾之權利。」這一個權利，同時也是憲法所保障的隱私權的具體型態之一。

在憲法本文或是增修條文中，並沒有隱私權的明文規定。然而，早在釋字第二九三號解釋，大法官就已經開始使用隱私權這樣的字句，釋字第二九三號解釋主文中說明：「銀行法第四十八條第二項規定『銀行對於顧客之存款、放款或匯款等有關資料，除其他法律或中央主管機關另有規定者外，應保守秘密』，旨在保障銀行之一般客戶財產上之秘密及防止客戶與銀行往來資料之任意公開，以維護人民之隱私權。」。

之後，大法官釋字第五○九號解釋雖未明白表示隱私權是憲法所保護的基本權利，但在主文中提到：「言論自由為人民之基本權利，憲法第十一條有明文保障，國家應給予最大限度之維護，俾其實現自我、溝通意見、追求真理及監督各

[14] *See* Berger v. New York, 388 U.S. 41, 44-45(1967)。

種政治或社會活動之功能得以發揮。惟為兼顧對個人名譽、隱私及公共利益之保護，法律尚非不得對言論自由依其傳播方式為合理之限制。」

而第五三五號解釋說明道：「臨檢實施之手段：檢查、路檢、取締或盤查等不問其名稱為何，均屬對人或物之查驗、干預，影響人民行動自由、財產權及隱私權等甚鉅，應恪遵法治國家警察執勤之原則。」

第五五四號解釋理由書表示道：「刑法就通姦罪處一年以下有期徒刑，屬刑法第六十一條規定之輕罪；同法第二百四十五條第一項規定，通姦罪為告訴乃論，使受害配偶得兼顧夫妻情誼及隱私，避免通姦罪之告訴反而造成婚姻、家庭之破裂；同條第二項並規定，經配偶縱容或宥恕者，不得告訴，對通姦罪追訴所增加訴訟要件之限制，已將通姦行為之處罰限於必要範圍，與憲法上開規定尚無牴觸。」

另外，第五八五號解釋提到：「同條例第八條第四項前段規定『本會行使職權，不受國家機密保護法、營業秘密法、刑事訴訟法及其他法律規定之限制』、同條第六項規定『本會或本會委員行使職權，得指定事項，要求有關機關、團體或個人提出說明或提供協助。受請求者不得以涉及國家機密、營業秘密、偵查保密、個人隱私或其他任何理由規避、拖延或拒絕』，其中規定涉及人民基本權利者，有違正當法律程序、法律明確性原則。」以及第五八七號解釋理由書中說明：「此種訴訟雖係為兼顧身分安定及子女利益而設，惟得提起否認之訴者僅限於夫妻之一方，未規定子女亦得提起否認之訴，或係為避免涉入父母婚姻關係之隱私領域，暴露其生母受胎之事實，影響家庭生活之和諧。」以上解釋文及理由書中，都援引了隱私權的概念及相關原則為說理及論證的依據。

從2005年開始，大法官會議更正式在釋字第六○三號解釋的主文中承認，隱私權雖然不是憲法明文列舉的基本權，但是「基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障。」這一號解釋也被釋字第六三一號解釋所援用。所以，隱私權作為憲法所保障的基本權利應該已經毋庸置疑。

四、憲法對通訊監察的誡命-釋字第六三一號解釋

釋字第六三一號解釋表示，通訊自由屬於憲法所保障的隱私權，不過，大法官也承認，在符合正當程序的前提下，國家還是可以限制人民的秘密通訊自由。在這號解釋中最重要的一點當屬檢察官不得核發通訊監察書。

(一) 國家進行通訊監察所需遵守的正當程序

憲法上明文地保障了人民的秘密通訊自由，但是，大法官同時也肯認立法者可以為了「確保國家安全、維護社會秩序」，制定必要的法律，授權偵查機關得於符合法定的實體及程序要件時，限制通訊自由。以現行的法規範來說，通保法便是授權偵查機關就人民通訊為監察的具體規定。

本號解釋指出，國家機關所為的通訊監察，是以過濾及監察人民通訊的方式，蒐集相關紀錄，並以之作為認定犯罪事實的依據；在性質上，屬於強制處分的一種。但是，通訊監察對於人民基本權利的侵害比一般強制處分所造成的更為嚴重。這是因為，在執行通訊監察時，不需要（也不可能）事先通知受監察人或是事前取得同意，也沒有給予其有防禦的機會(如保持緘默或委任律師)。再者，通訊監察屬於持續性的強制處分，也不會受到有形空間的限制。

最後，通訊監察不只會侵害到受監察人的通訊自由，也無可避免地會影響到無辜第三人的通訊自由。所以，大法官指出，立法者在制定相關法律時，所規範的要件必須要具體及明確、不得逾越必要的範圍，所踐行的程序也必須要正當且合理。

(二) 通訊監察書只得由法院核發

修正前通保法第5條第一項規定：「有事實足認被告或犯罪嫌疑人有下列各款罪嫌之一，並危害國家安全或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者，得發通訊監察書。」大法官肯認其對於實施通訊監察的要件規定具體且明確；但是對於核發通訊監察書的程序規定，卻有著相當嚴厲的批評。

就結論來說，大法官認為現行容許檢察官核發通訊監察書的規定不符合正當程序的要求，且與憲法保障秘密通訊自由的意旨有違。釋字第六三一號解釋說明道，國家固然有追訴犯罪及蒐集證據的利益，但是，因為通訊監察對於人民基本權利的侵害非常強烈及廣泛，所以，在設計通訊監察的審查程序時，應減少不必要的侵害及制衡偵查機關的權限。依照憲法上正當程序的要求，檢警機關在有監察人民通訊的必要時，原則上，應該要向「客觀、獨立」的法院聲請核發通訊監察書，使機關間的權力能夠有所制衡；也就是說，負責犯罪偵查的檢警機關不得自行審查通訊監察的必要性。

現行的通保法第5條第二項欠缺這樣的設計，容許檢察官核發通訊監察書，違背了前述憲法的誡命，因而違憲。除此之外，大法官也提醒道，於核發通訊監

察書時，法院應該要嚴格審查通訊監察的聲請是否符合通保法第5條第一項的要件；即便認為有監察人民的通訊自由的必要時，法院也必須遵守最小侵害原則；法院也應該要隨時監督通訊監察的執行情形。在本號解釋主文中，大法官指示道，依照正當程序的要求，通訊監察書應由「客觀、獨立」的法官核發， 所以，修正前的通保法容許檢察官決定通訊監察的規定違憲。這樣的文字，或明示或暗示檢察官並不是客觀獨立的司法官員，是故，在決定涉及人民隱私的侵害的強制處分時，檢察官不是適合的審查機關。這個立場，與美國的相關判決相仿。美國聯邦最高法院一貫地認為，檢察官不是中立且超然的司法官員，所以不適於核發搜索票[15]。

五、法律上的對通訊隱私之保護

而憲法上的隱私權，亦表現在具體的法律規範上，諸多法律已經承認隱私權的重要性，許多規定皆在落實隱私權之保障，例如：

(一) 通訊保障及監察法

通訊保障及監察法第一條規定：通訊保障及監察法之立法目的，係為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。

由於通訊科技日益發達，若以通訊作為犯罪工具，不僅將嚴重侵害他人權益，並將影響國家安全及社會秩序，因此，乃有制定通訊保障及監察法之必要性與急迫性。而人民之秘密通訊自由，若遭人任意監察，則憲法上所保障之基本權利亦將形同具文[16]。因此，藉由通訊保障及監察法之制定，不僅可以使日後偵查機關在實施通訊監察時，有明確之規範可資依循，同時更能藉由通訊監察法制之建立，使人民之基本權利受到完善之保護。

1. 通訊保障及監察法對隱私權保護基本規定及原則

由於我國憲法對於隱私權無直接加以明示保護，但從憲法保障人民有居住之自由、通訊秘密之保障以及憲法承認隱私權之基本人民權利，以保障個人之私領域以及自決空間。通訊監察及保障法規定，除了確保國家安全以及社會秩序外，不得為之；在通訊監察法第3條亦引入對於具有隱私或秘密之合理期待為限，第13條規範對於受監察對象以及範圍必須明確具體。監察之手段以截收、監察、錄

[15] 蔡榮耕，「I Am Listening to You (上)－釋字第六三一號解釋、令狀原則及修正後通訊保障及監察法」，台灣本土法學雜誌，第104期，頁51 (2008)。
[16] 參見陳愛娥，通訊監察與秘密通訊之自由，憲政時代，第 23 卷第 2 期，頁 16(1997)。

音、錄影、攝影、開拆、檢查、影印或類似之必要方式，但不得於私人住宅裝置竊聽器、錄影設備或其他監察器材。

為避免通訊監察濫用情形嚴重，我國通訊保障及監察法設下幾項要點限制來規範執法人員，分述如下：

(1) 重罪原則：依通訊保障及監察法第5條之規定，通訊監察的要件必須以三年以上有期途刑之罪或通訊保障監察法所列舉之罪，其情狀危害國家安全或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者，始得發通訊監察書。

(2) 最後手段性原則：通訊保障監察法第2條及第5條第1項。通訊監察之實施必須有事實足認被告或犯罪嫌疑人，危害國家安全或社會秩序情節重大，而有相當理由可信其通訊內容與犯罪有關，且不能或難以其他方法蒐集或調查證據者，始能對其實施通訊監察。換言之，如有其他偵查手段可資實施，即不應以通訊監察作為蒐集或調查犯罪證據之方法。

通訊監察雖為現代偵防犯罪之方法，但因影響人民秘密通訊自由權及隱私權甚鉅，除應權衡比例原則，限於已有存在客觀性證據，足以認定其有重大犯罪或利用通訊工具犯罪之嫌疑，而危害國家安全或社會秩序情節重大者外，尚應以不能或極難以其他方法為偵查者，或雖有其他調查方法，但極有可能不發生效果，始可認為有實施通訊監察之必要，如能以其他方法為之者，仍宜以其他方法行之，此乃「最後手段性原則」。

(3) 相關性原則：有關必要性原則係表現於本法第5條第1項：「有事實足認被告或犯罪嫌疑人.....，而有相當理由可信其通訊內容與本案有關，.....。」。因此，通訊監察之實施前，必須有一合理且客觀的事實存在，而不能單憑執法人員之主觀認定或情感判斷作為實施通訊監察之依據。

又為避免不當侵害其他無關之人，通訊監察之手段與偵查犯罪之目的必須有相關性。此乃因通訊之本質屬於由一方傳達意見、一方回覆意見之雙方溝通模式，雖被告或犯罪嫌疑人之通訊內容有可能傳遞或顯示犯罪跡證，但並非與被告或犯罪嫌疑人通訊者均與犯罪有關。為保護通訊隱私，對於被告或犯罪嫌疑人以及第三人之通訊監察，應限於與犯罪有關，並具有客觀性證據之存在，否則即不應加以監察。此項對於通訊監察範圍之限定稱之為「相關性原則」。

(4) 令狀原則：由於通訊監察動輒侵犯人民之權益，故為求慎重並使通訊監察的實施有明確依據及界限，通訊監察書應由法官核發，並以書面為之，此即「令狀原則」。

(5) 最小侵害性原則：有關最小侵害性原則係表現於本法第2條：「通訊監察，除為確保國家安全、維持社會秩序所必要者外，不得為之。前項監察，不得逾越所欲達成目的之必要限度，且應以侵害最少之適當方法為之。」及第13條：「通訊監察以截收、監察、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法為之。但不得于私人住宅裝置竊聽器、錄影設備或其他監察器材。執行通訊監察，除經依法處置者外，應維持通訊暢通。」。

在實施通訊監察之方式上，執法機關應以侵害最小之適當方法為之，避免影響當事人之通訊權利，亦即以沒有外觀侵犯性之通訊監察手段為之，故嚴禁於私人住宅內裝設通訊監察器材，以保障人民之住居權，避免國家公權力無限上綱，此即所謂「最小侵害性原則」。

(6) 若執法人員失職則重罰：執行通訊監察的公務員或從業人員，若假借職務或業務上進行違法監察，依據通訊監察及保障法規定違法監察他人通訊者，處五年以下有期徒刑。執行或協助執行通訊監察之公務員或從業人員，假借職務或業務上之權力、機會或方法，犯前項之罪者，處六月以上五年以下有期徒刑。意圖營利而犯前二項之罪者，處一年以上七年以下有期徒刑。

(7) 保護人民資訊隱私：依通訊保障及監察法第17條之規定，監察通訊所得資料，應加封緘或其他標識，由執行機關蓋印，保存完整真實，不得增、刪、變更，除已供案件證據之用留存於該案卷或為監察目的有必要長期留存者外，由執行機關於監察通訊結束後，保存五年，逾期予以銷燬。監察通訊所得資料全部與監察目的無關者，執行機關應即報請通訊監察書核發人許可後銷燬之。前二項之資料銷燬時，執行機關應記錄該通訊監察事實，並報請通訊監察書核發人派員在場，而監察通訊所得資料全部與監察目的無關者應銷燬之，且依該法第十八條規定，監察通訊所得資料，原則上不得提供他人使用。

2. 現行通訊監察法之缺失

(1) 犯罪監察及國安監察混為一體

現行通保法包含了以偵查犯罪為目的（犯罪監察）及以維護國家安全為目的（國安監察）的通訊監察。但其實兩者性質不同，為偵查犯罪所進行的通訊監察所涉及的，多是在境內的本國人，所以，特重基本權利的保障、避免不當侵害及

有效達成偵查目的。但是，國安監察多半會涉及在境外的人士或外國人，目的也與犯罪監察不同。是故，兩者所適用的原則，應該會有所不同。

以美國的立法例來說，關於犯罪監察的主要規範是聯邦通訊監察法；涉及國安監察的，則是另外訂定「外國情報監察法（Foreign Intelligence Surveillance Act of 1978）」[17]，而不是以同一個法律規範犯罪偵查及國安偵查。這樣的立法技術，值得參考。

(2) 通訊監察令狀的聲請人與偵查實務之落差

從第5條的規定可以知道，發通訊監察書的聲請權，是由檢察官獨占，司法警察並沒有通訊監察的聲請權。這樣的設計，與刑事訴訟法第128條之一的規定不相一致。刑事訴訟法規定，除了檢察官可以聲請搜索票之外，司法警察官也可以在經過檢察官許可後，向法院聲請搜索票。

如此之立法可能係為維持檢察官偵查主體之地位，但與偵查實務有所落差，因為實務上從鎖定偵查目標、填寫通訊監察書，到實際進行通訊監察，皆由警方一手包辦，檢察官實際上僅負責簽名，並無實質參與或審查，造成通訊監察中多一段無意義的公文往返流程，無助於實務運作。且通訊監察書之核發由法院把關，應無須擔心警察機關濫權之問題。故即便不賦予司法警察獨立的通訊監察聲請權，也應該採行刑事訴訟法第128條之一的模式，讓司法警察也可以在經檢察官同意後，向法院聲請通訊監察書。

(3) 證據排除法則之規範不當

通保法第5及6條所規定的是所有的「通訊」「監察」行為，但是，這兩個法條的證據排除規定只規範到違法的「監察行為」。按照文義解釋，似乎除了聲音以外的符號、文字、影像或其他訊息之違法監察皆不包含在內。但依據釋字第六三一號解釋保障人民的通訊自由及隱私之意旨，應擴張解釋至所有通訊監察之類型，而在未來有做文字修正之必要。

另外，這兩個法條的「情節重大」的意義為何，立法者並沒有給予定義，所以還需要司法判決的累積。不過，加上了這一個要件後，其操作的結果將會與刑事訴訟法第158條之四一樣，會有審查結果難以預測的問題。是故，如果通保法中的證據排除法則要有這樣的要件規定，就不如不要增訂，讓所有違法監察的案件一律回歸到刑事訴訟法加以判斷[18]。

(4) 執行機關與建置機關的混亂

[17] The Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511, 92 Stat. 1783.

[18] 蔡榮耕，I Am Listening to You（下）—釋字第六三一號解釋、令狀原則及修正後通訊保障及監察法，台灣本土法學雜誌，105 期，頁 48-49，2008 年。

通保法第11條規定有通訊監察的「聲請機關」、「執行機關」及「建置機關」。依據同法第5及6條，聲請機關為檢察官，應無疑義。但是，執行機關及建置機關之規定就頗有問題。

依照同法第11條第二項的定義，執行機關是指「蒐集通訊內容之機關」，建置機關指的是「單純提供通訊監察軟硬體設備而未接觸通訊內容的機關」。由此看來，執行機關應該是指通訊監察中心或是調查局，而建置機關應該是電信業者，如此的解釋亦與現行通訊監察之運作模式最為一致。

但從同法第14條第四項可以知道，電信業者是僅是「協助建置機關建置、維持通訊監察系統」，而不是建置機關。如此之規定是否意味「執行機關」及「建置機關」僅為通訊監察中心或調查局之內部編組，將通訊監察中心或調查局分為執行組」及「建置組」，如此之分類是否有意義，令人質疑。

(5) 對電信業者監督之空白

在通保法的整個實施層面裡，包括了執行機關、建置機關及電信業者（也就是協助建置機關者）。為了避免實施通訊監察時，人民的通訊隱私被不當侵害，對於前述的執行機關、建置機關及電信業者，通保法都應該有妥適的監督機制。對於前兩者，通保法都提供了偵查中或審判中的監督方式，但是，對於電信業者，卻沒有任何明文的規定。也就是說，無論是偵查中或是審判中，檢察官及法院都無法監督電信業者是否妥適地協助進行通訊監察。這也是前述對建置機關定義不當之衍生問題，造成通訊監察法制上的一大漏洞，也造成了人民通訊自由保障上的隱憂。

當然透過迂迴的解釋，檢察官可命執行機關就電信業者協助執行通訊監察的情形進行報告，間接監督電信業者。法官亦可在透過通訊監察書的指示權限，經由執行機關來監督電信業者。不過正本清源的方式還是修正建置機關之定義，較為簡單直接。

(二) 刑事訴訟法

搜索、扣押這一類的強制處分，對於人民隱私會造成極大的侵害。搜索所發動的客體，常常是住所、居所或是一定的處所。在這一些地方，人民常有著較為私密活動，或是放置有不願為外人所知的物件或文書。與通訊隱私相比較，搜索所涉及的隱私可謂有過之而無不及。是故，國家對於其所為的限制手段， 也應該要「有法律依據，限制之要件應具體、明確，不得逾越必要之範圍，所踐行之程序並應合理正當」，方符合憲法保障。

是否發動搜索，應該要由「獨立、客觀行使職權之審判機關」來作事前的審查，檢察官並不適合作這樣的決定。是故，現行刑事訴訟法中搜索票只得由法官簽發的規定，應屬於憲法上得要求，而不僅是法律上的要求。

而刑事訴訟法第135條規定：郵政或電信機關，或執行郵電事務之人員所持有或保管之郵件、電報，有左列情形之一者，得扣押之：一、有相當理由可信其與本案有關係者。二、為被告所發或寄交被告者，但與辯護人往來之郵件、電報，以可認為犯罪證據或有湮滅、偽造、變造證據或勾串共犯或證人之虞或被告已逃亡者為限。

此為刑事訴訟法關於搜索、扣押之特別規定，明定對於郵政或電信機關，或執行郵電事務之人員所持有或保管之郵件、電報，須符合有相當理由可信其與本案有關係者，或是為被告所發或寄交被告者為限，方可扣押。

而刑事訴訟法2001年修法時亦將電磁紀錄列入搜索、扣押客體，使得與電子郵件的通訊監察，也可能產生競合，使得通訊監察與搜索的區別滋生疑義。

(三) 刑事訴訟法與通訊保障及監察法之競合

對於郵件、電報之扣押，在刑事訴訟法135條有特別規定，已如前述。但根據通訊保障及監察法第3條第二款，通訊之定義包括郵件及書信，此時偵查機關在調查郵件內容時，應遵循何種程序，即有問題。本文認為，通訊保障及監察法之程序為特別規定，應優先於刑事訴訟法135條之適用。

首先，刑事訴訟法135條及通訊保障及監察法皆為保障人民隱私權之規定，但通訊保障及監察法係針對通訊隱私之特別法規，規範目的較為明確及特定，其程序規定亦較完整及具體。而人民對於其郵件內容之隱私，應為通訊隱私之一環，偵查機關對於郵件內容之取得，適用通訊保障及監察法較符合及規範目的。

其次，比較刑事訴訟法135條及通訊保障及監察法之規定，可發現刑事訴訟法135之要件僅需「有相當理由可信其與本案有關係者」，或「為被告所發或寄交被告者」。而通訊保障及監察法之要件需符合「危害國家安全或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者」，要件顯然較嚴格。

且在通訊保障及監察法中，對於監察票之核發有重罪原則，需為最輕本刑為三年以上有期徒刑之罪，或通訊保障及監察法第5條所列舉之罪，方可核發監察票。而刑事訴訟法並無重罪原則之規定。

而唯一刑事訴訟法規定較週延的地方，在於刑事訴訟法135條第二款但書：「但與辯護人往來之郵件、電報，以可認為犯罪證據或有湮滅、偽造、變造證據或勾串共犯或證人之虞或被告已逃亡者為限。」對於被告與辯護人來往之郵件、電報之扣押，做了相當程度的限縮。而通訊保障及監察法中並無類似規定。

此規定之法理在於被告之「辯護權」及辯護人之「拒絕證言權[19]」，保障被告不至於陷入自正己罪之窘境，以及避免架空辯護人之「拒絕證言權」，為對被告保護較週之立法。但通訊保障及監察法中並無此規定，故在適用時可考慮援用「不自證己罪」及「拒絕證言權」之法理，或類推適用刑事訴訟法135條第二款但書之規定，方能保障被告之權利。

綜上所述，若偵察機關可藉由刑訴法搜索扣押的相關規定，命電信業者提出使用者之通訊資料，似可規避通保法之程序規定，有架空通保法之虞，故對於電信業者提供之電子郵件等服務實施強制處分時，亦應遵守通保法之相關規定。

至於有論者認為應區分已閱讀及未閱讀之信件，分別適用刑事訴訟法以及通訊保障及監察法[20]，本文對此看法存保留態度。因為通訊應是個持續性的概念，在電子郵件的通訊中，通訊相對人讀取郵件後，未必代表通訊已終了，其仍可回覆郵件，故整體來看仍為持續不斷之通訊，尚不能謂閱讀後通訊即為終了，無通訊可言。故從理論上區分已閱讀及未閱讀，理論上未必正確。

且實務上對於電子郵件之取得，皆是向電子郵件服務提供者索取，警察機關聲請監察票時，事實上無從得知存在服務提供業者主機中之電子郵件究係已閱讀或未閱讀，若硬要區分兩者，分別適用不同程序，將會造成警察機關無所適從。例如警察機關依通保法之規定取得監察票，而向服務提供業者索取電子郵件，卻發現該封電子郵件標示已閱讀，難道要因為其非通訊，不適用通保法，而重新聲請一張搜索票？如此一來將徒增偵查實務之困擾。

(四) 電腦處理個人資料保護法

電腦處理個人資料保護法第1條規定：為規範電腦處理個人資料，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。

---

[19] 刑事訴訟法 182 條規定：證人為醫師、藥師、助產士、宗教師、律師、辯護人、公證人、會計師或其業務上佐理人或曾任此等職務之人，就其因業務所知悉有關他人秘密之事項受訊問者，除經本人允許者外，得拒絕證言。

[20] 陳信郎，資訊隱私權保障與網路犯罪通訊監察法制，政大法研所碩士論文，頁 112-114。

近年來，個人資料保護的議題炙手可熱，顯現了人民隱私權意識逐漸高漲，亦也顯示了在電子商務及電子化政府的浪潮下，隱私權所受的威脅日甚一日，令人不得不予以關注。我國在1995年通過了「電腦處理個人資料保護法」，提供我們以法律從事個人資料保護的一個基礎。以下對於「電腦處理個人資料保護法」之基本原則及規定做介紹：

1. 個人資料

個資法第3條第一款對個人資料的定義是：「自然人之姓名、出生年月日、身分證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社會活動及其他足資識別該個人之資料。」

而個人資料的「個人」指涉的是「自然人」，這在個資法第3條的定義中也說得很清楚（「自然人之姓名、出生年月日.....」），因此法人的資料，就不是個人資料。這是因為保護個人資料的目的是維護個人的隱私權，僅有自然人有人性尊嚴可言，才會有隱私感情受到傷害的問題[21]。

2. 受拘束客體

個資法是否僅規範電腦處理的個人資料？若單從個別法條似乎仍有解釋空間，例如第18條：「非公務機關對個人資料之蒐集或電腦處理，非有特定目的.....」、第23條：「非公務機關對個人資料之利用，應於蒐集之特定目的必要範圍內為之.....」，似乎對於人工處理之資料，「蒐集」、「利用」仍有受規範的可能，但事實上，從第3條用詞定義第二、四、五款對照來看，可知規範的都是儲存於電磁紀錄物或其他類似媒體之個人資料，也就可說是電腦處理的個人資料。再從法規名稱為「電腦處理個人資料保護法」及第1條：「為規範電腦處理個人資料.....」，故一般均認為本法僅規範電腦處理的個人資料。

但如此之限縮是否合理，值得商榷。的確由於電腦強大的傳輸能力，使得個人隱私更容易受到侵害。但與非電腦處理的個人資料相比，僅有量的差別而非質的差別。這跟刑法增訂318條之一[22]之規定如出一轍，係立法者對於電腦之恐懼及無知所致。

3. 受拘束主體

[21]陳仲嶙，電腦處理個人資料保護法掃描─總則篇，頁 4：http://www.is-law.com/OurDocuments/PR0010CL.pdf(最後點閱時間:2008 年 12 月 24 日)。

[22] 刑法第 318 條之一：無故洩漏因利用電腦或其他相關設備知悉或持有他人之秘密者，處二年以下有期徒刑、拘役或五千元以下罰金。

(1) 公務機關

依個資法第3條第六款之規定，所謂「公務機關」，指依法行使公權力之中央或地方機關。

(2) 非公務機關

依個資法第3條第七款之規定，受個資法規範的所謂 「非公務機關」，包括(一)徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人；(二)醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業；(三)其他經法務部會同中央目的事業主管機關指定之事業、團體或個人。

至於未被列舉，又沒有經指定者，就不在本法規範範圍內。

4. 個人資料保護的法律原則

個資法第6條規定：「個人資料之蒐集或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍。」此規定揭示了兩個重要的法律原則，分別是誠信原則及比例原則。

誠信原則是法律上之帝王條款，此處即指蒐、利用個人資料時應尊重當事人之權益，依誠實及信用方法為之。

而比例原則之內涵包括三項子原則：適當性原則、必要性原則、衡量性原則（或稱狹義比例原則），行政程序法第七條謂：「行政行為，應依下列原則為之：一 採取之方法應有助於目的之達成。二 有多種同樣能達成目的之方法時，應選擇對人民權益損害最少者。三 採取之方法所造成之損害不得與欲達成目的之利益顯失均衡。」該第一、二、三款，即分別為適當性原則、必要性原則、衡量性原則內涵之說明。雖然在個資法第六條中，文字上只有「必要」二字，但鑒於憲法第二十三條以及諸多行政法規中也僅有「必要」之文字，學說上仍解為比例原則之展現，故本條應有比例原則之意旨存焉，更何況比例原則作為重要一般法律原則之地位，即令未有明示，亦應受其拘束[23]。

5. 公務機關對於資料之處理

個資法第7條規定：「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，不得為之：一、於法令規定職掌必要範圍內者。二、經當事人書面同意者。三、對當事人權益無侵害之虞者。」

[23]前揭註 21，頁 9。

而特定目的外之利用規定在第8條：

(1) 法令明文規定者。如檢察官及司法警察，依刑事訴訟法規定，有偵查犯罪之職權，故其如為偵查犯罪所需，而向某公務機關請求提供某特定人之個人資料時，該受請求提供之公務機關，即得依本款之規定，提供其所需之個人資料。

(2) 有正當理由而僅供內部使用者。如內政部戶政司掌管全國戶政資料，此戶政資料係為戶政管理而蒐集者，若依本法精神，原則上其利用應限於此特定目的，但是戶政資料為國家施政的基本資料，許多施政計畫皆須參考戶政資料才能制定，譬如內政部社會司，為推動有關殘障人士的社會福利措施，為了解國內殘障人士的區域分布、家族概況，有必要取得國內殘障人士的戶籍資料，乃向戶政司索取，此屬有正當理由，且為內政部機關內的使用，故戶政司可將此等個人資料提供予社會司。

(3) 為維護國家安全者。如徵兵規則第十三條第三項規定：「徵兵檢查委員會應依體檢結果及體檢狀況，分別製成役男身高、體重、疾病及徵兵檢查人數統計表，送直轄市、縣 (市) 政府彙報內政部、國防部」，依本條的規定，兵役單位辦理徵兵及齡男子體格檢查的資料，也括每一部位檢查結果及指紋資料等，係為供體格檢查組判定體位之用，直轄市、縣 (市) 政府應予妥為保存，除彙報內政部、國防部外，不得隨意提供他人或作為其他目的使用。惟若敵對國派遣之間諜對本國實施顛覆活動，以爆裂物進行攻擊，司法調查或警察機關依爆炸現場採得之證據或指紋，向兵役單位調借歷年徵兵及齡男子的體格檢查及指紋資料，以供比對，則兵役單位為維護國家安全予以提供，當為法所准許。

(4) 為增進公共利益者。

(5) 為免除當事人的生命、身體、自由或財產上的急迫危險者。

(6) 為防止他人權益的重大危害而有必要者。

(7) 為學術研究而有必要且無害於當事人的重大利益者。如稅捐稽徵人員對於納稅義務人的所得額、納稅額及其證明關係文據以及其他方面的陳述與文件，除對納稅義務人本人及其代理人或辯護人、合夥人、納稅義務人的繼承人、扣繳義務人、稅務機關、監察機關、受理有關稅務訴願機關以及經財政部核定的機關與人員外，應絕對保守秘密，所得稅法第一百十九條第一項定有明文。另同法條第三項規定：「稽徵機關對其他政府機關為統計目的而供應之資料，並不洩漏納稅義務人之姓名者，不受保密之限制。」依上開條文的規定，稅捐稽徵人員對於納稅義務人的所得額、納稅額及其證明關係文據以及其他方面的陳述與文件，除對特定人員及機構外，固應絕對保守秘密，惟對其他政府機關為統計目的而供應的資

料，並不洩漏納稅義務人的姓名者，即不受保密的限制。如有學術單位或研究機構為進行「賦稅之公平與改革」研究，需大量納稅義務人的所得額、納稅額及其他有關資料，俾予以統計、分析與運用，而請求稅捐機關提供以上資料時，稅捐機關於不洩漏納稅義務的姓名的情況下，提供該學術單位或研究機構參考，依本款規定的精神在准許之列。

(8) 有利於當事人權益者。如甲縣市政府社會局欲提供住居所於某地的居民得享有補助或其他利益，戶政機關即得依本款規定，提供相關戶籍資料予有關機關參考。

(9) 當事人書面同意者。

6. 非公務機關對於資料之處理

個資法第第18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，不得為之：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、為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。」

而特定目的外之利用規定在第23條：「非公務機關對個人資料之利用，應於蒐集之特定目的必要範圍內為之。但有左列情形之一者，得為特定目的外之利用：一、為增進公共利益者。二、為免除當事人之生命、身體、自由或財產上之急迫危險者。三、為防止他人權益之重大危害而有必要者。四、當事人書面同意者。」

另外對國際傳遞及利用之限制規定在第24條：「公務機關為國際傳遞及利用個人資料，而有左列情形之一者，目的事業主管機關得限制之：一、涉及國家重大利益者。二、國際條約或協定有特別規定者。三、接受國對於個人資料之保護未有完善之法令，致有損當事人權益之虞者。四、以迂迴方法向第三國傳遞及利用個人資料規避本法者。」

7. 救濟制度

對公務機關之求償規定在第27條：「公務機關違反本法規,致當事人權益受損害者，應負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，

並得請求為回復名譽之適當處分。前二項損害賠償總額，以每人每一事件新臺幣二萬元以上十萬元以下計算。但能證明其所受之損害額高於該金額者，不在此限。基於同一原因事實應對當事人負損害賠償責任者，其合計最高總額以新臺幣二千萬元為限。第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。」

第28條則規定對非公務機關之求償：「非公務機關違反本法規定,致當事人權益受損害者，應負損害賠償責任。但能證明其苶故意或過失者，不在此限。依前項規定請求賠償者，適用前條第二項至第五項之規定。」

(五) 電信法

我國電信法第 7 條：「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序，由電信總局訂定之。電信事業用戶查詢本人之通信紀錄，於電信事業之電信設備系統技術可行，並支付必要費用後，電信事業應提供之，不受第一項規定之限制；電信事業用戶查詢通信紀錄作業辦法，由電信總局訂定之。」

1. 第一類電信事業

「電信事業處理有關機關查詢電信通信紀錄實施辦法」第 5 條規定：「

前條第一類電信事業通信紀錄之保存期限如下：一、市內通信紀錄：最近三個月以內。二、國際、國內長途通信紀錄，最近六個月以內。三、行動通信發信通信紀錄：最近六個月以內。」

而有關機關查詢通信紀錄之程序規定在第3條：「有關機關查詢通信紀錄應先考量其必要性、合理性及比例相當原則，並應符合相關法律程序後，再備正式公文或附上電信通信紀錄查詢單(格式如附件)，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。但案情特殊、情況緊急之查詢，得由法官、軍事審判官、檢察官、軍事檢察官、查詢機關首長或其書面指定人先以電話或公文傳真，並經回叫確認為之，查詢後應於三個工作日內補具正式公文或加蓋印信之電信通信紀錄查詢單正本。前項之查詢，經查詢機關與電信事業雙方認證同意，得以經加密之電子郵件為之，該電子郵件並視同正式公文或電信通信紀錄查詢單正本。」

2. 第二類電信事業

第二類電信事業管理規則27條規定「經營者對於調查或蒐集證據，並依法律程序查詢電信之有無及其內容者，應提供之。前項電信內容之監察事項，依通訊保障及監察法規定辦理之。經營者對於第一項電信通信紀錄應至少保存期間如下：一、語音單純轉售服務通信紀錄應保存六個月。二、網路電話服務通信紀錄應保存六個月。三、網際網路接取服務：（一）撥接用戶識別帳號、通信日期及上、下網時間等紀錄應保存六個月。（二）非固接式非對稱性數位用戶迴路（ADSL）用戶識別帳號、通信日期及上、下網時間等紀錄應保存三個月。（三）纜線數據機用戶識別帳號、通信日期及上、下網時間等紀錄應保存三個月。（四）張貼於留言版、貼圖區或新聞討論群之內容來源IP位址與當時系統時間應保存三個月。（五）免費電子郵件信箱及網頁空間線上申請帳號時之來源IP位址及當時系統時間應保存六個月。（六）電子郵件通信紀錄應保存一個月。四、虛擬行動網路服務通信紀錄應保存六個月。經營者應核對及登錄其用戶之資料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。虛擬行動網路服務經營者或E.164用戶號碼網路電話服務經營者應將使用者資料載入其系統資料檔存查後始得開通；以預付卡或其他預付資費方式經營虛擬行動網路服務者或E.164用戶號碼網路電話服務者，亦同。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或E.164用戶號碼網路電話服務經營者另應包括所指配號碼。第四項之虛擬行動網路服務經營者或E.164用戶號碼網路電話服務經營者應於受理申請二日內完成其使用者資料之載入。」

關於資料保存之法制分析及建議，本文將於第六章詳述。

表一、我國通訊監察法制彙整表

<table>
<tr><th colspan="2">類型</th><th>法規依據</th><th>保護強度</th></tr>
<tr><td rowspan="2">通訊資訊</td><td>通訊內容本身之資訊</td><td>通訊保障及監察法</td><td>較強</td></tr>
<tr><td>通訊內容以外之資訊</td><td rowspan="2">電信法、電腦處理個人資料保護法</td><td rowspan="2">較弱</td></tr>
<tr><td colspan="2">通訊以外之資訊</td></tr>
</table>

六、外國法之引介

(一) 美國電子通訊隱私法(the Wiretap Act)

1. 通訊監察之許可程序

依據美國電子通訊隱私法第2516(1)條之規定：就本章第2156(1)條所列之各種犯罪，得製作通訊監察聲請書，經聯邦檢察總長(Attorney General)、副檢察總長(Deputy Attorney General)助理檢察總長(Associate Attorney General)及任何經檢察總長在刑事司(Criminal Division)內特別指定之檢察總長助理(Assistant Attorney General)、代理檢察總長助理(acting Assistant Attorney General)、檢察總長副助理(Deputy Assistant Attorney General)、代理檢察總長副助理(acting Deputy Assistant Attorney General)之許可，向有管轄權之聯邦法官聲請核發「有線通訊」及「口頭對話」之通訊監察書，該聯邦法官得依據本章第2158條之規定核發由聯邦調查局(the Federal Bureau of Investigation，即FBI)或其他負有調查犯罪職務之聯邦司法警察機關(a Federal agency)執行通訊監察。

而第2516(3)條之規定：就「聯邦重罪」(Federal felony)，得製作通訊監察聲請書，經依據「聯邦刑事訴訟規則」(the Federal Rules of Criminal Procedure)定義之「檢察官或政府律師」(attorney for the Government)的許可，向有管轄權之聯邦法官聲請核發「電子通訊」之通訊監察書，該法官得依據本章第2158條之規定核發由各犯罪調查機關或其他負有調查犯罪職務之執法官員(an investigative or law enforcement officer)執行通訊監察。依據「聯邦刑事訴訟規則」第1條(b)(1)之規定，前開所謂之「檢察官或政府律師」係指檢察總長或其助理(the Attorney General or an authorized assistant)、聯邦檢察長或其助理(a United States attorney or an authorized assistant)及依法執行檢察官職務之政府律師(any other attorney authorized by law to conduct proceeding under these rules as a prosecutor)。而前揭所謂之「各犯罪調查機關或其他負有調查犯罪職務之執法官員」，依據同法第2510(7)條之規定係指美國聯邦或州及其所屬機關之依法有權執行調查或逮捕本法所列各種犯罪之官員，或執行檢察權限之檢察官而言。

第2518(1)(a)條之規定：通訊監察聲請書上應載明之事項包括負責製作聲請書之「各犯罪調查機關或其他負有調查犯罪職務之執法官員」的身份。

表二、美國電子通訊隱私法許可程序

類型	得通訊監察之犯罪	有權許可之官員	法令依據
有線通訊	電子通訊隱私法第2516(1)條所列之特定重大犯罪	司法部特定高階長官	電子通訊隱私法第 2516(1)條
口頭對話	電子通訊隱私法第2516(1)條所列之特定重大犯罪	司法部特定高階長官	電子通訊隱私法第 2516(1)條

電子通訊	電腦	所有「聯邦重罪」(Federal felony)	司法部特定高階長官	電子通訊隱私法第 2516(3)條、檢察官操作手則 9-7.100
	傳真機	所有「聯邦重罪」	司法部特定高階長官	電子通訊隱私法第 2516(3)條、檢察官操作手則 9-7.100
	呼叫器	所有「聯邦重罪」	「聯邦檢察長」(United States Attorney)	電子通訊隱私法第 2516(3)條、檢察官操作手則 9-7.100

[24]

2. 通訊監察之執行

第2518(3)條規定：聲請截取有線或電子通訊或口頭對話之准許或追認命令，須以書面為之，且應在有管轄權法官前為宣誓或確證，以及陳明聲請人應有權提出聲請。每一聲請書上必須記載執法機關人員與授權提出聲請人員之身分，以及所有之事實與情狀之詳盡聲明，以作為正當化聲請人確信應核發監察令狀與建立之可能原因。可能原因之聲明必須包括四個要素：一、所調查之罪名。二、截取之場所與設備。三、所欲截取之通訊型態。四、被監察人之身分。此四個要素必須提出充分證明，以支持法官認為具有可能原因。

法官核准聲請後，須於監察令狀上記載：一、被監察人之身分，如已知悉者其人與所欲截取之通訊。二、授權截取之通訊設備之性質與位置。三、所欲截取之通訊型態之特定描述及與其有關特定犯罪之聲明。四、標示授權截取會話之機關與授權人之身分。五、授權截取之期間，包括有關當所欲截取之通訊第一次獲得後，是否自動終止之聲明。除上述之特定要求外，監察令狀上必須有若干指示，以限定令狀之範圍[25]。第2518(5)條規定，要求監察令狀上必須記載「儘速執行」之指示，並且無論如何不得逾達成授權目的所必須之期間，而最長不得逾三十

[24]黃謀信，境外貪污案件偵查之研究--以美國聯邦通訊監察制度為中心，赴美國哈佛大學法學院研習訓練報告，頁 12(2007)。

[25] 18 U.S.C. § 2518(4)。

日。延長期限之聲請，僅以符合本條第一項、第三項規定者為限，且延長之期限係由法官加以審酌，但延長期限最長不得逾三十日。同時，監察之執行機關須以最小限度截取通訊，且不得截取與本章無關之通訊，而核發監察令狀之法官得要求執行機關提出有關達成授權目的之進度與繼續截取需要之報告[26]。

3. 通訊監察的監督

第2516(6)條規定發給命令之法官，得在命令上要求提出報告說明截取行為之進行情形，以及有無繼續截取之需要。而在依本法第二五一八條命令或每次延長期限命令屆滿時，或追認截取命令作成後三十日內，發給命令或駁回聲請之法官，須向聯邦行政法院之行政辦公室報告二類事項：其一為聲請發給命令或聲請延長期限命令之事實。其二為聲請發給命令或聲請延長期限命令之種類，包括依本條第十一項審酌之情形[27]。

此外，於每年四月，聯邦法院行政辦公室主任應向國會提出關於上年度中，聲請准許或追認截取有線、電子通訊或口頭對話之件數，以及准許或駁回聲請、准許或駁回延長期限聲請之件數之完整報告。報告內容並應包括第二五一九條第一項與第二項數據之檢討與分析，而聯邦法院行政辦公室主任有權對製作報告之內容與程式，發布具有拘束力之規則[28]。

(二) 歐盟個人通訊資料保存指令(Directive 2006/24/EC)

歐盟「資料保存指令」主要是統合歐盟會員國要求其國內電信業者、或網路服務提供者對所擁有通訊資料的保存義務，以確保這些通聯資料能及時被應用在協助執法單位進行重大犯罪偵察與起訴上。適用範圍包含所有自然人或法人之通聯資料與位置資料，以及其他用來識別發話者與受話者所必須的資料；但不得適用於通訊實質內容之保存。

在資料保存內容部分，依其保存項目之不同，主要分為6大類：

1. 追查與識別通訊之資料；
2. 識別通訊地點之資料；
3. 識別通訊日期、時間與通聯時間長短之資料；
4. 識別通訊類型之資料；
5. 識別用戶所使用之溝通器材及可能使用器材之資料；以及
6. 識別行動通訊位置之資料等。

---

[26] 18 U.S.C. § 2518(5)(6)。
[27] 18 U.S.C. § 2520(1)
[28] 18 U.S.C. § 2519(3)

依據歐盟「資料保存指令」第6條之規定，各會員國需確保上述資料得保存6個月以上（但最多不得超過24個月），並確保被保存之資料可隨時配合執法單位調查而提出，以協助執法調查時的參考利用。

但為避免保存之資料因不慎外洩或遭不當利用，而造成人民隱私的重大侵害，本指令特別在第7條要求被保存資料的保護等級，應等同於資料傳輸時的保護，並應避免受保存之資料遭到因故意或過失所造成遺失、破壞或刪除；而對於超過保存期限的資料，除非有特殊情況，否則應立即銷毀。

為確保資料得以妥善保存不受侵害，各會員國應明確指定相關單位負責監督資料保存與運用之情形，且僅得為有法律授權之使用者所使用。若有非經法律允許而故意使用或交換受保存之資料者，各國應制定有效且合適的刑罰，以嚇阻惡意或不當利用或儲存之行為[29]。

關於歐盟資料保存指令之詳細介紹與借鏡，以及資料保存之法制分析及建議，本文將於第六章詳述。

[29]張耀中「從歐盟「資料保存指令」看我國資料保存之規範」，
http://www.ithome.com.tw/itadm/article.php?c=39970 (最後點閱時間:2008 年 12 月 24)。

參、網路服務之定義與分類

一、網路服務之通訊定義及監察容許性

(一) 通訊之定義

所謂「通訊」是指人與人之間意思傳遞與意思表達的手段。惟學說上對於通訊的範圍有兩種不同的看法；一說著重於人與人之間的「意思交流」，所衍生的定義就是人類社會中人與人之間資訊的傳遞[30]；另一說將重心放在「藉由傳遞工具」的概念，所衍生的定義是指以書信、電報、電話或其他方法，向他人傳達其意思而言[31]。兩者的差異在於後者多了傳遞媒介，亦即發話與受話兩方的意思傳遞係藉由工具傳達；而前者不限於傳遞的媒介，亦即沒有工具的意思交流也屬於通訊之列。

綜合言之，通訊的定義應為：「當事人藉由任何方式傳遞秘密訊息為意思交流之行為。」詳言之，所謂「通訊」在行為主體方面，必須有雙方當事人存在；在行為方式方面，通訊手段究竟有無媒介傳遞在所不問，只要可以達到兩方傳遞意思的目的即可；在行為客體（傳遞的訊息）方面，只要發話方傳遞給受話方即可，並不限於何種訊息，著重點並不在於涉及自己或他人的意思表示，也不論他人是否可以理解、內容有無意義[32]；在行為特性方面，通訊必須是傳遞當事人所認為秘密性的訊息，若有任何一方自願性同意接受監察，則表示秘密性遭破壞，而不具有保護利益之情事[33]。

(二) 網路服務之監察容許性

隨著網際網路的日漸普遍，除了傳統的信件、電話、傳真之外，網路也躍升為現代人通訊的熱門工具之一。而網路監察的運用，主要是透過網路調查及其他線索取得嫌疑人使用的電話，藉以調查嫌疑人的犯罪事實及掌握其犯罪動態。

另外，由於網路通訊與傳統電話通訊在內容上有著很大的不同：在傳輸協定上，傳統的電話，其資料交換的方式係採電路交換（Circuit Switch）系統，亦即當發話端與受話端通話時，系統會建立一條專屬線路，供雙方使用，網路頻寬不

---

[30] 蔡墩銘，「通訊監察與證據排除」，刑事法雜誌，第39卷第1期，頁1(1995)。

[31] 林紀東，中華民國憲法逐條釋義第一冊，頁 159，(1990)。法治斌、董保城，中華民國憲法，頁 159，(2001)。陳志龍，「秘密通訊自由之保障及郵件扣押合法性之商榷」，刑事法雜誌，第 22 卷第 3 期，頁 37。

[32] 蔡聖偉，「妨害秘密罪章之新紀元（下）」，月旦法學，第 71 期，頁 99。

[33] 曾正一，「反恐怖行動法制中通訊監察規範之研究－反恐怖行動法、國家情報工作法與通訊保障暨監察法之交錯」，第三屆恐怖主義與國家安全學術研討會論文集，頁 164-165。

與其他人共享；而網際網路則係採封包交換（Packet Switch）系統，亦即網路提供通信資源給大家共用，並未專屬任一使用者，使用者將資料切割成符合網路標準的資料封包（Packet），由網路送到受話端，產生虛擬電路，因此同一條實體線路上有許多條邏輯通道存在同時通信，當檢警調單位持通訊監察書實施網路監察時，很有可能會截收到嫌犯以外之人的通訊[34]。我國通訊保障及監察法是否容許網路監察？即有疑問。

通訊保障及監察法第三條第一項規定：「本法所稱通訊如下：一、利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信。二、郵件及書信。三、言論及談話。」以上定義，幾乎已經囊括現代人類所有可能的溝通方式，包括如 E-mail 、ICQ 和手機等新型態的溝通方式。不過，本法又加上「前項所稱之通訊，以有事實足認受監察人對其通訊內容有隱私或秘密之合理期待者為限」（第二項）的限制，明顯係援引美國最高法院在 *Katz v .United States* 一案[35]中所建立的「合理隱私權期待原則」，認為只有在能夠合理期待且與隱私或秘密有關者，才屬於本法所保障的通訊範圍。

我國通訊保障及監察法是否容許網路監察？對此，學者多採肯定說[36]。蓋網路監察係對流通於網際網路或電腦網路上的電子資料進行監察，持有機關為網路服務業者或公司內部網路的管理單位。依本法第三條第一項第一款規定所謂通訊包括「利用『電信設備』發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線『電信』」，而「電信」依電信法第二條第一款的定義係指「利用有線、無線，以光、電磁系統或其他科技產品發送、傳輸或接收符號、信號、文字、影像、聲音或其他性質之訊息」，另「電信設備」依同條第二款則指「電信所用之機械、器具、線路及其他相關設備」。電腦設備可用來「發送、傳輸或接收符號、信號、文字、影像、聲音或其他的訊息」當無疑義。且電腦設備係「利用有線、無線」亦無疑義，再者，電腦設備亦可解釋為「其他科技產品」的一種。因此，根據電信法的定義，發送網路通訊的電腦設備應屬於「電信設備」的一種[37]。而網路通訊是利用電信設備發送、傳輸或接收符號、文字、影像、聲音或其他訊息，因此屬於通訊保障及監察法的適用範圍，應無疑義。

根據我國電信法之規定，得經營網路服務之事業，為第二類電信事業，故本文對於網路服務之討論，即以第二類電信事業所提供之服務為基礎，對其做分類以及剖析，以下就先針對第二類電信事業之定義做介紹。

[34]蔡美智，「通訊保障及監察法關於網路監察的相關爭議」，資訊法務透析，頁 35-37(1999)
[35]389 U.S.347(1967)。
[36]前揭註 34，頁 38。
[37]陳信郎，資訊隱私權保障與網路犯罪通訊監察法制，政大法研所碩士論文，頁 107。

二、第二類電信事業之定義

根據電信法第十一條之規定，電信事業分為第一類電信事業及第二類電信事業。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。而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。

由以上電信法之定義可得知，指並未設置電信機線設備，而自第一類電信事業租賃該等設備並提供加值電信服務之事業。

三、第二類電信事業所提供之服務

交通部依電信法第十七條第二項規定，訂定發布「第二類電信事業管理規則」。該規則第一條將第二類電信事業之服務分為特殊業務及一般業務。

其中特殊業務包括語音單純轉售服務、E.164 用戶號碼網路電話服務、非 E.164 用戶號碼網路電話服務、租用國際電路提供不特定用戶國際間之通信服務或其他經主管機關公告之營業項目者。

而一般業務為特殊業務以外之第二類電信事業業務。包括公司內部網路通信服務、批發轉售服務、公用電話轉售服務、預付式電話卡轉售服務、行動網路業務經營者、虛擬行動網路服務、行動轉售服務、行動轉售及加值服務網際網路接取服務、存轉網路服務、存取網路服務等。

以上為電信法對於第二類電信事業所提供之服務所做出之分類，但其分類之目的在於電信管制，與本文所要討論的電信監察並無關聯，故本文必須先以通訊監察之角度出發，做出以下之分類，作為往後討論之基礎。

四、第二類電信事業服務之分類

以下分類之目的，在於界定第二類電信事業所提供之服務，哪些服務會符合通訊保障及監察法第三條中「通訊」之定義，以及使用該服務時，使用者是否有隱私或秘密之合理期待，進而判斷偵察機關對於取得第二類電信事業服務使用者之相關資訊時，有無通訊保障及監察法之適用，是否應遵循相關之規定。

(一) 根據有無通訊相對人，第二類電信所提供服務態樣可以區分為：

1. 有通訊相對人：網路電話服務、簡訊、網路聊天等。

有通訊相對人之服務，主要有網路電話、電子郵件、網路聊天等。此類服務皆有兩方以上之通訊當事人，透過第二類電信業者之電信設備發送、接收文字、影像、聲音，而互相溝通交流、傳達意思表示，符合通訊保障及監察法第三條第一款「利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信。」所定義之通訊無疑義，在有隱私權期待的情況下，偵查機關進行通訊監察時須符合通訊保障及監察法之相關規定。

2. 無通訊相對人：網際網路接取服務等。

無通訊相對人之服務，主要為網路接取、瀏覽服務，即俗稱上網服務。此類服務僅有一方使用者，藉由指令操作，向網路服務提供者索取資訊。由於通保法對於通訊的定義，很明顯係建立在人與人間通訊的假設之下。個人網路瀏覽行為並非係與人的通訊，而是一種人與電腦間（human-to-computer）的通訊，亦即使用者先鍵入指令給電腦，指示電腦傳遞指令給遠端主機（即所欲連結的網站主機），遠端主機再回傳封包資料回使用者電腦，電腦重組封包後，再顯示畫面於使用者螢幕上。因此無通訊相對人的服務，應不符合通訊保障及監察法第三條定義之通訊，而無通訊保障及監察法之適用，但仍可能適用電信法及電腦處理個人資料保護法。

第二類電信所提供之服務	
有通訊相對人	**無通訊相對人**
網路電話 電子郵件 網路聊天	網路接取服務

(二) 根據通訊技術是否需要留存通訊內容複本（copy），第二類電信所提供的服務態樣可以區分為：

1. 無須留存複本：語音單純轉售服務、網路電話服務、E.164 用戶號碼網路電話服務、非 E.164、用戶號碼網路電話服務、公司內部網路通信服務 、語音會議服務、視訊會議服務等。

網路電話、視訊等服務，因其通訊之技術、性質，在通訊傳輸之過程中，並不會留存複本。在一般情況之下，通訊之內容僅有通訊雙方當事人使得知悉，故此類通訊之雙方對其通訊內容有隱私或秘密之合理期待者，符合通訊保障及監察法第三條但書「必須以有事實足認受監察人對於其通訊內容有隱私或秘密之合理期待者為限」定義之通訊。故對此類通訊之監察，必然要遵守通訊保障及監察法之規定。

2. 須留存複本：電子郵件、簡訊、網路聊天等。

電子郵件、簡訊等服務，由於技術性質使然，傳輸時必定會留下複本，使電信業者知悉。此時通訊人是否仍有隱私或秘密之合理期待，取得這一類的通訊內容是否仍需聲請通訊監察書，即有爭議。

若單純就電信業者存有複本的角度觀之，通訊當事人之通訊內容已盡為電信業者，即第三人所知悉。此時通訊當事人對於通訊內容已無隱私或秘密之期待可言。縱通訊當事人主觀上仍有秘密通訊之期待，此並非合理之期待，蓋第二類電信用戶本應了解此服務會留存複本，而在使用此類服務時，承擔通訊內容為第三人所知悉之風險。故對於需留存複本之服務進行監察時，似無通訊保障及監察法之適用

但從通訊隱私保障之角度觀之，不論有無留存複本之通訊服務，使用者皆是利用電信設備傳輸文字、影像、聲音等訊息給通訊相對人，兩者並無二致。一般使用者皆認為僅有通訊相對人方能知悉通訊內容，故對於隱私權的期待，兩種服務應該相同。不該因為技術和性質上之偶然，而對於留存複本服務之使用者之隱私權生差別待遇。

且縱使電信業者存有複本，在龐大的資料量之下，業者實際上無可能逐一檢視而知悉其通訊內容，故與其說電信業者「知悉」，不如說其僅「保存」。再者縱然電信業者實際上已知悉通訊內容，依據契約約定或是誠信原則，業者亦有保密義務，使用者仍可期待該通訊為其隱私或秘密。

當然，業者與消費者之契約，實際上有無納入保密條款，可能會有疑問，許多業者甚至在定型化契約中，要求消費者放棄保護其隱私之權利。並且，是否能從抽象、不確定的誠信原則中導出業者的保密義務，進而認為有合理隱私期待，論述上亦有難度。不過，由於電子郵件為人民極為重要的秘密通訊管道，認為其有合理隱私期待，似為不得不然之解釋方向。

而美國在 *United State v. Maxwell*[38]一案中，因為有人指出有兒童色情物品透過ISP 業者AOL 散佈，因此AOL 向FBI 報案，而FBI 以具有80 個電子服務帳戶名稱（screen name）的令狀來搜索AOL 的電腦，法院認為，因為由於令狀上的帳戶名稱有誤，而AOL 在令狀範圍外給予正確的帳號，以及在尚未取得令狀前，AOL 就已在FBI 的指示下進行資料的蒐集，因此這次搜索扣押的行為是有瑕疵的，但要對此搜索扣押行為加以爭執的前提要件是，電子郵件必須要有合理的隱私期待[39]。

法院認為在AOL 上的電子信件傳輸有合理的隱私期待，理由是電子郵件傳輸的隱私期待取決於其傳送形式與接收者，例如說寄到聊天室或轉寄的信件就沒有隱私的問題，而寄給多數的收件者也會使隱私的期待大大地減低。而在本案中，電子郵件信息較網路上的其他信息有較多的隱私，因為電子郵件被私密地放置在AOL 所設置的集中的、私人擁有的電腦主機中，AOL 自己的政策是不給有權限者以外之人來閱讀或公開使用者的電子郵件，這在聯邦法令之外，提供了契約上的隱私保護，所以美國法院亦認為在此情形中，使用者仍有合理隱私期待。

故本文認為不應區分有無留存複本，只要該服務符合通訊保障及監察法所定義之通訊，對於該通訊服務之監察，皆應符合通訊保障及監察法之相關規定與程序進行，方符合憲法上保障通訊隱私之意旨。

(三) 根據是否為通訊內容本身，第二類電信所提供的服務態樣可以可區分為：

1. 內容資訊（content information）：即通訊內容本身。在電子郵件服務即為其內文。在網路電話服即為其對話內容。

[38] U.S. v. Maxwell，42 M.J. 568(A.F.Ct.Crim.App. 1995)。
[39]謝昆峰，電子郵件的取得與保全－合理隱私期待與法定程序，頁 2，網址: www.is-law.com/Others/ESSAY0011KunFeng.pdf(最後點閱時間:2008 年 12 月 15 日)

此類資訊為通訊內容，通訊當事人對其享有通訊隱私權，對於該通訊之監察須符合通訊保障及監察法之相關規定，應無疑義。

2. 信封資訊（envelope information）：即從服務外表即可得知，未涉及內容本身之資訊。在電子郵件服務即為其郵件地址及帳號，在網路電話服即為其電話號碼及帳號。此外像是通聯記錄、發話地點、電子郵件通信紀錄等資訊亦屬之。

關於電話號碼及帳號此類資訊，一般而言為公開資訊，服務使用者對其並不享有通訊隱私權，無通訊保障及監察法之適用，但第二類電信業者在處理此類資料時，仍須注意電信法及電腦處理個人資料保護法之適用。

而像是通聯記錄等資訊，雖然服務使用者對其有隱私權之期待，但因為此類資訊非屬通訊內容本身，且消費者在使用通訊服務時，電信業者皆會把通聯記錄保存下來，理論上我們會認為消費者明知通聯記錄會被保存下來，仍執意使用通訊服務，就必須承擔通聯記錄被保存，甚至揭露給第三人之風險，而對其無合理之隱私期待。

故傳統上非通訊隱私之核心領域，在各國法制及實務見解上，皆給予較低之保護，而無通訊保障及監察法嚴格程序之適用，但第二類電信業者在處理此類資料時，仍須注意電信法及電腦處理個人資料保護法之適用。

<table>
<tr><th colspan="3">第二類電信所提供之服務</th></tr>
<tr><th colspan="2">有通訊相對人</th><th>無通訊相對人</th></tr>
<tr><td colspan="2">網路電話
電子郵件
網路聊天</td><td rowspan="3">網路接取服務</td></tr>
<tr><td>內容資訊</td><td>信封資訊</td></tr>
<tr><td>通訊內容
本身</td><td>通聯記錄
發話地點</td></tr>
</table>

(四) 小結

首先，本文將網路服務區分成「有通訊相對人」及「無通訊相對人」，由上述討論可得知，僅有「通訊相對人」之服務方符合通訊保障及監察法第三條所定義之通訊，此區分使得「無通訊相對人」之服務，例如網路接取、瀏覽服務，排除通訊保障及監察法之適用。

再者，在「有通訊相對人」通訊服務中區分成有「須留存複本」及「不須留存複本」兩種，而經過分析討論之結果，本文認為不論是否留存複本，通訊當事人皆應有隱私或秘密之合理期待，對於其通訊內容之監察皆須符合通訊保障及監察法，對於人民隱私權之保障方為周全。

最後，根據通訊之所傳送之資訊，區分為內容資訊（content information）及信封資訊（envelope information），通說認為信封資訊（envelope information）為公開資訊，或非屬通訊隱私核心領域之範疇，故僅有內容資訊（content information）為秘密資訊，有通訊保障及監察法之適用。

表三、網路服務之分類

類型		服務項目	適用法規	相關章節
有通訊相對人	內容資訊	網路電話、電子郵件、網路聊天	通訊保障及監察法	第肆章
	信封資訊	通聯記錄、發話地點、帳號地址	電信法、電腦處理個人資料保護法	第伍章
無通訊相對人		網際網路接取服務		

五、外國法對通訊的定義

(一) 美國

美國於1934年制訂「聯邦通訊法」（Federal Communications Act of 1934）用以規範通訊監察事務，直至1968年，因聯邦最高法院之 *Berger v. New York* 及 *Katz v. United States* 兩個案件，乃在「犯罪防制及街坊安全法」（The omnibus Crime Control and Safe Street Act）之第3篇（Title III）的第2510條至第2520條中規範通訊監察，一般稱之為「聯邦通訊監察法」（Federal Wiretap Act）。

「聯邦通訊監察法」（Federal Wiretap Act）之通訊監察客體僅限於對「有線通訊」（wire）及「口頭對話」（oral）進行通訊監察，並未包括新興之通訊

類型，例如電子郵件、傳真等，因為前開法案對新興的「電子通訊」（electronic communication）可否進行通訊監察引發極大之爭論。

直到1986年，美國國會始將「電子通訊」亦納入得通訊監察之範圍，並將第119章更名為「有線通訊、電子通訊及口頭對話之截取」章（Wire And Electronic communications Interception And Interception of Oral Communications），一般稱之為「電子通訊隱私法」（Electronic Communications Privacy Act，簡稱為ECPA），修正後之得進行通訊監察之客體包括「有線通訊」、「口頭對話」及「電子通訊」等3種類型[40]。

相較於我國，美國通訊監察法規範的通訊，僅限於傳送中的通訊（communication in transmission）。至於儲存中的通訊則是由美國聯邦儲存中通訊監察法（the Stored Communications Act）來規範。

根據「電子通訊隱私法」（Electronic Communications Privacy Act），「截取」指「透過使用任何電子、機械或其他裝置，聽取或取得任何有線、電子或口頭通訊的內容」

而在「電子通訊隱私法」（Electronic Communications Privacy Act）的定義中，「有線通訊」的定義是得以聽覺感知，並且藉由有線線路及設備傳送的通訊。在這一個定義下，有線通訊必須是可以經由聽覺所感知（aural）。如果是無法以聽覺得知內容的（如圖片或是文字），即便是以有線的線路傳送，也不是這裡所定義的有線通訊。

而「電子通訊」指「任何性質的信息、信號、文字、圖像、聲音、數據或情報， 其全部或部份藉著電信設備、無線電、電磁、光電子或光學系統進行的任何傳遞」。大部分網路通訊（包括電子郵件）均屬電子通訊。但電子通訊並不包括下列通訊：任何電信或口頭通訊；任何透過只具音頻系統的傳呼裝置發出的通訊；任何由追蹤裝置發出的通訊；或金融機構在通訊系統儲存作電子儲存及轉撥資金用途的電子轉帳資料。

若和我國通保法相比較可以知道，通保法規範了傳輸中及已經為一定設備所儲存的通訊；再者，通保法所定義下的通訊包括了可以或是無法以聽覺感知的訊息。美國聯邦通訊監察法所規範的通訊只包含傳輸中且可以以聽覺感知的訊息。從這一點來看，通保法所涵蓋的通訊類型比美國的更為廣泛。

[40]黃謀信，境外貪污案件偵查之研究--以美國聯邦通訊監察制度為中心，臺灣板橋地方法院檢察署出國進修報告，頁 16-17。

表四、我國通保法與美國電子通訊隱私法通訊定義之比較

類型	台灣	美國
聽覺	V	V
非聽覺	V	
傳輸中	V	V
已儲存	V	

(二) 英國

在英國，政府截取通訊是存在已久且眾所周知的行為。在1985年之前，英國並無任何整體的法定架構規管該種行為，而僅是藉著不同條例的條文管制部分的截取通訊行為。因此，截取通訊的法律依據並不清晰。而事務大臣獲賦予權力，可發出手令授權截取郵遞及電報通訊。這意味著截取通訊的過程是受行政當局而非法定架構管制。

在1957至1981年間，英國政府曾向公眾發表3份官方報告書：「1957年Birkett報告書」、「1980年白皮書」及「1981年Diplock 報告書」。這些報告書檢討了有關截取通訊的程序、保障措施及監管安排，但均沒有建議訂立單一的法律架構，以涵蓋所有截取事宜。

直到1985年，政府才在一份白皮書中表明有意就截取通訊訂定立法例。此次立法需要，乃歐洲人權法院於1984年就 *Malone v. UK* 一案的判決引致。在該個案中，法院裁定英國的本土法例雖訂有規管截取通訊的詳細程序，卻沒有清楚表明有哪些截取權力的元素已納入法律規則，有哪些元素則仍然屬行政當局的酌情範圍。法院進一步裁定，警方截取個人通訊的做法，違反了「歐洲人權公約」第八條。

在發出「1985 年白皮書」後，當局制定了「1985年截取通訊法令（The Interception of Communications Act of 1985）」。該法例首次就截取郵遞或公眾電訊系統的通訊訂立法定基礎，把非法截取通訊的行為列為罪行，並在法例中訂定令狀制度的運作架構，以及訂立保障、監察及投訴機制。

自「1985年截取通訊法令」制定以來，電訊科技及通訊服務出現了巨大變化，例如流動電話及互聯網通訊日趨普及、私營電訊網絡擴展，以及提供包裹和文件送遞服務的私營公司數目大增。上述種種變化引發了新的人權問題，而這些問題已超出了「1985年截取通訊法令」的規管範圍。因此，英國政府了解到有需要訂立1999年發表的諮詢文件所述的新法例。

一年後，當局廢除了「1985年截取通訊法令」，並以「2000年調查權力規管法令（The Regulation of Investigatory Powers Act）」取代，後者便成為英國規管截取通訊的主要法例。

一如「1985年截取通訊法令」，「2000年調查權力規管法令」訂明，任何人如無合法權力而故意截取英國公共郵政服務或公眾電訊系統的通訊，即屬犯罪。然而，與「1985年截取通訊法令」不同，「2000年調查權力規管法令」把規管範圍擴大至私人電訊，包括流動電話、傳呼機及經電腦網路傳送的電子訊息。

根據「2000年調查權力規管法令」，任何人在通訊傳送過程中，透過改變或干擾傳送系統或監察傳送情況，讓「該通訊的發送者或預定接收者以外的其他人士， 取得傳送中通訊的部分或全部內容」，即屬截取通訊。「2000年調查權力規管法令」把通訊界定為「在傳送過程中」及/或「儲存於傳送系統中」的通訊。因此，「已儲存的通訊」亦受到「2000年調查權力規管法令」的規範[41]。

從以上「2000年調查權力規管法令」之規範可得知，其範圍亦涵蓋第二類電信業者所提供之通訊服務類型，故值得作為我國立法上之參考。

[41]黃少健，選定司法管轄區對截取通訊的規管，香港立法會秘書處資料研究及圖書館服務部研究報告，頁 3-5。

肆、網路通訊監察之法制與實務

一、前言

由第貳章的討論，我們得出，若要對於通訊內容進行通訊監察時，所適用之程序規定即為通訊保障及監察法。但通訊保障及監察法於1999年7月14日制訂公布，當時網路技術尚未成熟，普及率亦不佳，立法者無法預知網路通訊將成為通訊服務之主流，故並未從網路通訊之角度思考，造成目前偵查實務上對第二類電信進行通訊監察時適用法規之不明確。如此適用上之困難，本文希望透過解釋或修法建議來解決，以下將分項討論：

二、通訊監察的事由

(一) 一般通訊監察

1. 通訊保障及監察法之規定

依據通訊保障及監察法第五條第一項之規定，有事實足認被告或犯罪嫌疑人有下列各款罪嫌之一，並危害國家安全或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者，得發通訊監察書。

(1) 最輕本刑為三年以上有期徒刑之罪。

(2) 刑法第一百條第二項之預備內亂罪、第一百零一條第二項之預備暴動內亂罪或第一百零六條第三項（單純助敵罪）、第一百零九條第一項、第三項、第四項（洩漏交付國防秘密罪）、第一百二十一條第一項（不違背職務之受賄罪）、第一百二十二條第三項（違背職務受賄罪及行賄罪）、第一百三十一條第一項（公務員圖利罪）、第一百四十二條（妨害投票自由罪）、第一百四十三條第一項（投票受賄罪）、第一百四十四條（投票行賄罪）、第一百四十五條（利誘投票罪）、第二百五十六條第一項、第三項（製造鴉片、毒品罪）、第二百五十七條第一項、第四項（販賣運輸鴉片、毒品罪）、第二百九十八條第二項（加重略誘罪）、第三百條（收藏隱避被略誘人罪）、第三百三十九條（普通詐欺罪）、第三百三十九條之三（違法製作財產權之處罰）、第三百四十六條（單純恐嚇罪）之罪。

(3) 貪污治罪條例第十一條第一項、第二項之罪。

(4) 懲治走私條例第二條第一項、第三項或第三條之罪。

(5) 藥事法第八十二條第一項、第三項或第八十三條第一項、第四項之罪。

(6) 證券交易法第一百七十一條或第一百七十三條第一項之罪。

(7) 期貨交易法第一百十二條或第一百十三條第一項、第二項之罪。

(8) 槍砲彈藥刀械管制條例第十二條第一項、第二項、第四項、第五項或第十三條第二項、第四項、第五項之罪。

(9) 公職人員選舉罷免法第八十八條第一項、第八十九條第一項、第二項、第九十條之一第一項、第九十一條第一項第一款或第九十一條之一第一項之罪。

(10) 農會法第四十七條之一或第四十七條之二之罪。

(11) 漁會法第五十條之一或第五十條之二之罪。

(12) 兒童及少年性交易防制條例第二十三條第一項、第四項、第五項之罪。

(13) 洗錢防制法第九條第一項、第二項之罪。

(14) 組織犯罪防制條例第三條第一項後段、第二項後段、第六條或第十一條第三項之罪。

(15) 陸海空軍刑法第十四條第二項、第十七條第三項、第十八條第三項、第十九條第三項、第二十條第五項、第二十二條第四項、第二十三條第三項、第二十四條第二項、第四項、第五十八條第五項、第六十三條第一項之罪。

由以上通保法第5條之規定可知，通訊監察之法定程序，須符合下述要件始得聲請核發通訊監察書：

(1) 列舉之重罪原則：即並非所有犯罪皆得聲請通訊監察，須符合本法(即通訊保障及監察法以下簡稱之)第五條第一項所列舉之罪名，始得作為法定之監察對象。

(2) 相關性原則：即本法第五條之規定「有相當理由可信其通訊內容與本案有關」者，即除了須為列舉之已發生犯罪，尚須「有事實足認被告或犯罪嫌疑人具充足之犯罪嫌者」，始足該當此一要件。

(3) 補充性原則：即最後手段性，因本法第五條尚有規定須以「不能或難以其他方法蒐集或調整證據者」為限，故須窮盡所有偵查方式仍不可得者，始得行之。

2. 分析檢討

根據訪談對象指出，目前最常使用監察做為偵察手段之罪名，大致為「槍砲彈藥刀械管制條例」之罪[42]以及詐欺，其他就是販毒、販槍枝、洗錢、恐嚇少部份，或其他符合通訊監察法的最輕本刑三年以上之罪[43]。

訪談對象認為，目前最需要通訊監察，卻礙於列舉原則而無法實行之罪名，應係「竊盜」，因其被害利益若是貴重物品來說，可能超過詐欺，在偵查實務上屬於重大案件，但刑法上並無如此分級[44]，故無法實行通訊監察。其實在理論上，所有案件都可能有運用通訊監察之需求，但如此一來又太浮濫了。故在立法論上，也許可以考慮以被害標的的價值，去判斷是不是可以實施通訊監察[45]。

而由於寬頻網路的普及，各式的網路犯罪亦隨之興起，包括網路駭客、洩密、散佈猥褻物品等等，而偵查網路犯罪最有效率的方式，即是網路通訊監察。近年刑法修正，增加許多與電腦、網路相關之犯罪類型，但通訊保障及監察法並未全盤跟進，以致偵查實務上出現漏洞[46]。

例如一般駭客入侵則涉及刑法第三百五十二條第二項之罪嫌，網路賭博涉及刑法第二百六十六條規定之罪嫌，偽造變造電磁紀錄，涉及刑法第二百十條以下之罪名，利用電腦或其相關設備觸犯洩密罪，涉及刑法第三百十五條以下之罪名，販賣大補帖與色情光碟則分別觸犯著作權法與刑法第二百三十五條罪嫌等罪名，未能包括其中；除此之外，網路還有許多新型態之犯罪，例如竊取線上遊戲「天堂」之天幣等，涉嫌觸犯刑法第三百二十條竊盜罪之規定。

因此，這些犯罪型態，也許在現實社會中影響較為輕微，因此通訊保障及監察法在立法過程中，並未將之納入得進行通訊監察之範疇，但是網路的特性，使得在現實社會中也許情況侵害法益並不嚴重，在網路上卻可能造成嚴重之傷害，例如璩美鳳遭偷拍案件，獨家報導隨書附贈偷拍光碟，並進行銷售之行為，馬上被檢察官搜索扣押，防止某種程度之繼續擴散，但是在網路上流傳的部分，因網路傳播速度過快，不但色情網站以贈送偷拍光碟作為銷售手法外，許多犯罪者更藉由網路傳播，將偷拍光碟內容以檔案型態販售給其他網路用戶，造成難以防止

42 台北市警察局刑事警察大隊訪談(以下簡稱北市警訪談)Q2。
43 刑事警察局偵九隊訪談(以下簡稱偵九隊訪談)Q2。
44 北市警訪談 Q3。
45 同前註。
46 北市警訪談 Q4。

的侵害，對於遭偷拍者之侵害難以估計；又例如網路駭客之入侵往往造成企業、政府機構系統之嚴重損害。此種網路之犯罪因為無法符合現行通訊保障及監察法之規定，而無法實施通訊監察，僅能依法向有關ISP 業者調閱相關資料，對於執法機關進行犯罪偵查，維護人民安危確實有所阻礙。有主張針對足以影響公序良俗之重大犯罪態樣，如嚴重影響兒童及青少年身心之色情網路犯罪，納入刑法增修及通訊監察之特定犯罪內，以使網路色情等犯罪之通訊監察，取得正當之法律程序基礎，健全網路良性發展[47]；有認為應就個別犯罪類型，檢討納入監察容許之必要性，但色情、賭博、侮辱、誹謗等犯罪行為，其可非難性未必較高，就偵查技術而言並非相對困難，依比例原則衡量，不宜將之列入通訊監察之範圍內[48]。

故本文建議對於適用通訊監察之罪名，以具有網路犯罪之特性、且需要進行網路通訊監察之罪名為前提，做適度修正，增加以下幾種犯罪類型：

(1) 刑法第二百三十五條（散布、販賣猥褻物品及製造持有罪）。

(2) 刑法第第三百一十八條之一（無故洩漏因利用電腦或其他相關設備知悉或持有他人之秘密罪）

(3) 刑法第三百三十九條之三（違法製作財產權罪）。

(4) 刑法第三百五十八條（入侵電腦或其相關設備罪）

(5) 刑法第三百五十九條（破壞電磁紀錄罪）

(6) 刑法第三百六十條（干擾電腦或其相關設備罪）

(7) 刑法第三百六十二條（製作犯罪電腦程式罪）

(二) 緊急通訊監察

有事實足認被告或犯罪嫌疑人有犯刑法妨害投票罪章、公職人員選舉罷免法、總統副總統選舉罷免法、槍砲彈藥刀械管制條例第七條、第八條、毒品危害防制條例第四條、擄人勒贖罪或以投置炸彈、爆裂物或投放毒物方法犯恐嚇取財罪、組織犯罪條例第三條、洗錢防制法第十一條第一項、第二項、第三項、刑法第二百二十二條、第二百二十六條、第二百七十一條、第三百二十五條、第三百二十六條、第三百二十八條、第三百三十條、第三百三十二條及第三百三十九條，為防止他人生命、身體、財產之急迫危險，司法警察機關得報請該管檢察官以口

[47] 林煒程，網際網路猥褻犯罪之研究，國防管理學院法律研究所論文，頁 32-36 (1998)。

[48] 謝名冠，網路行為規範之研究，臺灣台北地方法院檢察署八十九年度研究報告，臺灣台北地方法院檢察署印行，頁 200-201(2000)。

頭通知執行機關先予執行通訊監察。但檢察官應告知執行機關第十一條所定之事項，並於二十四小時內陳報該管法院補發通訊監察書；檢察機關為受理緊急監察案件，應指定專責主任檢察官或檢察官作為緊急聯繫窗口，以利掌握偵辦時效。

法院應設置專責窗口受理前項聲請，並應於四十八小時內補發通訊監察書；未於四十八小時內補發者，應即停止監察。

三、通訊監察的程序

(一) 通訊監察書應載事項

依據通訊保障及監察法第十一條之規定，通訊監察書應記載下列事項：

一、案由及涉嫌觸犯之法條。
二、監察對象。
三、監察通訊種類及號碼等足資識別之特徵。
四、受監察處所。
五、監察理由。
六、監察期間及方法。
七、聲請機關。
八、執行機關。
九、建置機關。

此為書面主義之規定。故通訊監察時需使用書面文件，亦即通訊監察書，將特定事項予以載明。如此一來，一方面可使執行通訊監察之人員，在進行通訊監察之實施時，有明確之遵循依據。另一方面，法院在審核通訊監察書時亦可具體、實質的為通訊偵查的必要性等要件把關。

(二) 網路通訊監察之「監察對象」與「監察通訊種類及號碼等足資識別之特徵」

由於網路犯罪具有匿名性的特徵，與傳統犯罪監察對象甚為明確亦不相同，因此，如何具體載明「監察對象」、「監察通訊種類及號碼等足資識別之特徵」，也是相當重要的課題。

然而，我國通訊保障及監察法施行細則並未針對網路犯罪的「監察對象」及「監察通訊種類及號碼等足資識別之特徵」的內容有所規定，只能由個別檢察官或法官依個別案件具體事實審酌之。一般而言，在核發通訊監察書時，有關「監

察通訊種類及號碼等足資識別之特徵」欄位，通常係記載網路服務提供業者之被監察主機所在地址、網路線代號，及監察對象的用戶編號(或撥接用戶的編號)及分配的IP位址[49]。如果監察客體是電子郵件的話，除記載電子郵件主機外，通常須另記載該電子郵件位址[50]。

(三) 美國法上之不定點監察（Roving Surveillance）

不定點監察的指的是，於通訊監察書中，不特定受監察的地點或設備。也就是說，授權偵查機關監察所有被告或犯罪嫌疑人可能進行通訊的設備（如室內電話或行動電話）。對犯罪偵查來說，不定點監察是相當有力的證據蒐集方式，因為其可以有效地避免犯罪嫌疑人以不斷地更換通訊設備（如行動電話號碼）的方式來避免偵查機關所進行的通訊監察。尤其在網路通訊中，通訊相對人的IP 會不斷變換，也可以重複註冊好幾個「分身」帳號，若依照傳統通訊監察書記載的方式，會變的掛一漏萬，無法因應網路世界中「狡兔三窟的情形」。然而，不能否認的是，因為不定點監察不需要特定受監察的地點及設備，對於通訊自由的侵害勢必更為廣泛及嚴重。

依通保法第一一條規定，通訊監察書必須要記載「監察通訊種類及號碼等足資識別之特徵」及「受監察處所」。由此可知，我國並不承認不定點監察。相較於通保法的規定，美國則是在一九八六年已經制定了「電子通訊保護法（The Electronic Communications Protection Act of 1986, ECPA）」[51]，在美國聯邦通訊監察法中增訂了不定點監察的監察方式[52]。根據其規定，法院在核發不定點通訊監察書時，不需要特定受監察的地點、設備及號碼[53]。

在美國，不定點監察引起相當大的討論。主要的問題在於，其可能違反了美國聯邦憲法第四修正案。為了有效進行監察，不定點監察不需要特定監察的地點及設備，但是，第四修正案明白地要求令狀上必須要載明進行搜索的地點(the place to be searched)，從而，不定點監察有違憲之疑慮。然而，仍有不少的美國學者及聯邦判決都認為，不定點監察不違反第四修正案的要求。這是因為，按照美國聯邦通訊監察法的規定，只有在嫌疑人可能使用該設備時，才可以進行通訊監察[54]。所以，受到偵查的地點及設備還是可以因而特定。再者，進行監察時，

---

[49] 偵九隊訪談 Q4、Q12，北市警訪談 Q5。

[50] 陳慥銘，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，頁84-85(1999)。

[51] The Electronic Communication Protection Act of 1986, Pu. L. No. 99-508, 100 Stat. 1848 (1986).

[52] 18 U.S.C. § 2518(11) 。

[53] Clifford S. Fishman, *Interception of Communication in Exigent Circumstances: The Fourth Amendment, Federal Legislation, and the United States Department of Justice*, 22 GA. L. REV. 1, 8-9 (1987)。

[54] United States v. Petti, 973 F.2d 1441 (9th Cir. 1992), Michael Goldsmith, *Eavesdropping Reform: The Legality of Roving Surveillance,* 1987 U. ILL. L. REV. 410, 419 (1987) 。

偵查機關還是要遵守最小侵害原則，所以，在實務運作上，不至於會有不當的侵害。最後，現今社會中，越來越複雜的犯罪型態，也使得法制上有承認不定點監察的必要[55]。

(四) 小結：因應網路監察時通訊監察書應載事項之解釋及修正建議

由前述討論可知，網路監察及傳統電話監察之差別在於，傳統電話監察之通訊方式為固定線路傳送，通訊相對人於特定之現實世界地址對話，偵查機關為開啟通訊監察，所撰寫之通訊監察書，對於記載「監察對象」、「監察通訊種類及號碼等足資識別之特徵」及「受監察處所」並無困難，故要滿足通保法規定之通訊監察書應載事項並無問題。而實際上通保法對於通訊監察書應載事項之規定，正是針對傳統電話監察所設計。

但網路通訊係在網路上，以封包傳送資訊，通訊之型態及方式與傳統電話通訊有所差異，故會發生記載通訊監察書應載事項之困難。首先，偵查機關從事網路通訊監察時，通常是在網路節點上放置監察設備，攔截封包。故在此一虛擬網路世界，通訊當事人之現實通訊地點就顯得無足輕重。縱使詳載了現實之「受監察處所」，亦無助於特定監察之範圍及處所。如此一來，「受監察處所」之記載，就變的毫無意義。且網路通訊當事人可能隨時、不斷地變換現實處所，甚至在發動網路通訊監察時，偵查機關可能僅知道通訊當事人之帳號，而未必能得知之其現實處所究係為何處[56]。這些問題都增加了撰寫通訊監察書之難度。

實際上，真正有記載「受監察處所」實益的地方，在於非使用通訊器材的口頭通訊，如此之談話由於通訊當事人皆處於同一地點，此時記載受監察處所方有其意義。

並且，在傳統電話通訊中，通訊相對人不斷變換電話號碼或手機門號的成本較高，手續較麻煩，但在網路通訊中，每次上網都可能用不同的IP ，亦可以使用多個帳號[57]，幾乎不用太多的成本跟麻煩，故在通訊監察書的記載上，可能出現掛一漏萬的情形，而使得犯罪嫌疑人輕易躲避偵查。

---

[55] *Id.*(“Investigative complexity may also justify an expanded search.”)。

[56] 北市警訪談 Q5，偵九隊訪談 Q8。

[57] 北市警訪談 Q9。

針對此一問題，可考慮引進美國法承認之不定點監察，在某些特定狀況下允許偵察機關在通訊監察書上，不須記載「受監察處所」及「監察通訊種類及號碼等足資識別之特徵」，迴避現實處所、通訊設備、方式、帳號無法特定之困難。

再者，關於「監察對象」之記載，由於網路世界「匿名性」之緣故，偵查機關可能難以得知受監察人之真實姓名。故可考慮記載受監察對象之網路暱稱、用戶名等虛擬名稱，取代其真實姓名。

最後，關於記載「監察通訊種類及號碼等足資識別之特徵」，則記載網路服務提供業者之被監察主機所在地址，及監察對象的用戶編號(或撥接用戶的編號)及分配的IP位址。若監察客體是電子郵件的話，應記載電子郵件主機，及該電子郵件位址。

四、通訊監察的執行

(一) 通訊監察的方式

通訊保障及監察法第十三條規定：監察通訊以截收、監察、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法為之。但不得於私人住宅裝置竊聽器、錄影設備或其他監察器材。執行通訊監察，除經依法處置者外，應維持通訊暢通。

(二) 監察的客體

1. 以特定IP 為客體

IP 是電腦主機在網路上的位置，在網際網路上每個連線的電腦有其獨立的IP 位址，機關內部電腦網路亦分別對每台電腦主機分配一個IP ，所以監控的對象如為某特定的主機，設定監控的位置，就是該主機的IP 。通常網路上IP 的分配是將某一區域或內部網路分配予一定範圍的IP ，因此檢警調單位追查到某封涉嫌的電子郵件是由某個IP 位址發出來的時，就可以追縱到該IP 大約的物理位置(實體位置)，如該信件是由某個公司或某個機關、學校的電腦所發出來的。如此，即可縮小偵查範圍。另外，目前網路服務公司多有提供虛擬主機或硬碟空間的租用，即網站設置不是在個別主機以專線連線後，取得獨立IP ，而是附設在ISP 的主機內，有的有提供獨立IP ，有的只是單獨硬碟空間的租用，附屬在ISP某IP 主機下的特定目錄，不過，此種方式仍可以透過對提供虛擬網路業者IP 主機的監控，間接查出租用人資料。

監察IP 的時機，在於某網頁可能含有網路犯罪內容，或是其主機是某駭客或犯罪者經常入侵或藉以轉站，或傳輸郵件以外的資料時使用的主機，此外於網路電話、影音電話或視訊會議的監察也有適用。由於一部主機的傳輸資料非常大，且除非設定為點對點的監控，否則容易取得很多不相干使用者的資料，基於比例原則及偵查的經濟效益，以IP 監察的作法應審慎。通常多只有在已調閱通聯錄並掌握通訊來源，如國內人在某國外主機租用網頁，即可在國內聯外的關鍵節點，監控聯往國外主機（有特定IP）的資料，從中找出國內的聯繫者[58]。

由於IP 未必與偵查目標有直接相關，無法從IP 特定出受監察對象，故通常警方非以IP 做為監察對象[59]，仍須以特定網路線及帳號來做偵查標的。

2. 以特定帳號為客體

監察特定帳號的目的有二，一為藉由帳號的通聯紀錄，得知寄件人及收件人的E-mail 帳號，再由郵件帳號追查使用者身分；另一為監看該特定郵件的內容，藉以蒐集犯罪嫌疑人的犯罪證據。由於二種方式涉及適用法規的不同，因此有分別討論的必要。關於前者，本文將其定義為通訊內容以外之資訊，不適用通保法，而將於第陸章加以討論。

但是如果檢警調單位是想監看特定郵件內容時，由於涉及「截收」通訊內容，則必須符合通訊保障及監察法的規定，先向檢察官或法官聲請通訊監察書，得到許可後，再依通訊監察書要求電信業者或網路服務提供業者，利用管理電子郵件的伺服器軟體，由通訊監察書的期間起始日，將受監察人所收受的所有電子郵件，轉寄給聲請通訊監察的執法人員，之後便儲存於各該執行執法人員的電腦上，且各該執法人員的電腦設有密碼及帳號，非執法人員者，原則上無法進入電腦，取得及閱讀該電子郵件[60]。

不過透過業者轉寄郵件的方式，有時緩不濟急，且若受監察對象收信或發信後，立即把郵件刪除，警方即無法掌握。故實務上仍有必要要求業者做到即時的信箱資料備份跟傳送，或是針對電信線路，發通訊監察書給電信公司，電信公司針對監察的對象，把資料導引到警方的機器設備作解析[61]。

而若是語音的通訊監察，例如Skype或是MSN的網路電話服務，即必須使用攔截封包之方式進行，方法在以下詳述。

---

[58] 前揭註 50，頁 79-80。
[59] 北市警訪談 Q5，偵九隊訪談 Q15。
[60] 林岡輝，電子郵件之截收處分，國立臺北大學法律研究所論文，頁 22(2002)。
[61] 高雄市警察局刑事警察大隊訪談(以下簡稱高市警訪談)Q3、Q 4。

(三) 網路監察之方式

1. 主機內複製資料

而關於網路監察，第一種監察方式，係在通訊直接使用的主機內（網頁主機或信件主機）監察特定人的通訊內容，此在向網路服務提供業者租用網頁主機、信件主機，或是機關內部網路主機的情形，特別可適用。其監察方式比較單純，只要在其主機內置監察程式複製通訊內容或通聯紀錄即可，範圍固定，不致截取到他人資料。應注意的是，電子郵件的收發分成有寄信主機及收信主機，雖然二者通常通同，但是可以設定為不同，在監控上要區別目的而設置。

2. 設立節點攔截封包

第二種監察方式，則是在網路節點上放置監察設備，攔截封包。此種方式極易看到與犯罪嫌疑人毫不相關之人的封包。所謂「節點」，通常是指在骨幹網路（backbones）上的通訊交換點。此種方法乃是在犯罪嫌疑人可能經過的網路節點上，放置監察設備，攔截封包。在越下游的地方放置監察設備，所收聚的範圍就越窄，所須過濾的不相關人的封包就越少。對此，先需了解各節點配置的情形，先了解其IP 所在主機的實際位置，通常TWNIC 分配IP 予各個網路服務提供業者，再由各大網路服務提供業者將上開IP 分配予其客戶，其分配方式通常會有一定的區域分布，此區域分佈可向各大網路服務提供業者查詢。取得IP 的實際位置後，再參照該區域的網路分佈圖，尤其各區域網路的交換節點及聯外節點，再依監控的目的、技術可行性及經濟原則選擇監控的節點。

3. 實務執行狀況及問題

首先，本文介紹傳統電話及手機之監察方式與原理，並透過訪談及文獻資料，整理出目前網路監察之運作模式，再將電話與網路監察的方式加以比較分析，得出兩者之差異，突顯目前網路監察之問題所在。

(1) PSTN 網路(室內電話)監察方式

傳統電話所用之公眾電信網路通稱為PSTN (公共交換電話網路 -- Public Switched Telephone Network)，為電路交換網路的代名詞，也就是技術上是以電路(circuit-switched)方式進行傳輸，系統保留一條點對點傳輸的頻寬，以64Kbps速率傳送語音，當電話接通，這段頻寬便完全佔線，直到兩端通完電話為止，亦即兩端通話中，任何第三人皆無法使用該段頻寬，而由通話雙方獨占，故PSTN網路傳輸的特性即為「集中式」、「單一線路」。

而此種特性影響到監察的部份在於，當受監察對象撥打電話時，警方即可上線監察，在傳輸線路上設立節點、攔截其訊號。而由於同一時間該線路被受監察對象之通話所獨占，警方攔截訊號時，不可能攔截到受監察對象以外之訊號，對不相干之第三人侵害甚小。亦即傳統電話的監察，在技術上可做到排除不相干訊號之攔截，對人權侵害範圍不至於過度擴張，為較安全、限縮之作法。

(2) GSM 網路(行動電話)監察方式

而關於行動電話監察方式，因為行動電話的通訊傳輸路徑分為兩段，第一段為手機至基地台的傳輸，這個部份以無線電波作為傳送媒介。第二段為基地台至交換機房的路線，這個部份以實體線路傳輸，與室內電話相同。

故警方針對不同的路徑，有相對應的監察方式。在無線電波之部分，警方可出動載有監察設備之偵防車，在基地台或受監察對象的通訊地點附近，攔截無線電訊號，即可獲得受監察對象之通訊內容。但此種攔截無線電波之方法，是全面攔截之作法，容易攔截到無辜地三人之訊號，使用上應較審慎。

而第二種為目前警方在一般情形下最常使用的方式，由於行動對話仍有一段路徑需經由實體線路傳輸，以如上所述，警方即在實體線路上設立節點、攔截其訊號，其運作方式，與上述的室內電話監察方式，並無二致，基本上為同一原理。

值得一提的是，不論是關於手機或室內電話(固網)的通訊監察，皆由通訊監察中心統一操作及控管，有一套相當完整之監察制度。警方透過檢察官向法官聲請了通訊監察書之後，需將通訊監察書投單至通訊監察中心，由該中心統一進行上線監察，制度上較為嚴謹透明，再加上前述關於傳統電話「集中式」、「單一線路」的特性，使得通訊監察時較難牽涉到無辜地三人，故傳統電話通訊監察不論在制度上或執行技術上較無太大弊端及問題。

(3) 網路監察方式與現狀之問題

首先必須說明的是，目前我國針對網路通訊監察，仍處於臨時監察時期，並無如傳統電話一般，建置完整的通訊監察系統，由通訊監察中心統一作業，亦無與電信業者之連線系統，警方若有網路通訊監察之需求時，僅能臨時將通訊監察設備帶至電信業者機房安裝[62]，或要求業者錄製光碟交予警方[63]，屬於克難式的臨時監察。

A. 業者配合問題

[62] 偵九隊訪談 Q3、Q5，北市警訪談 Q15。

[63] 北市警訪談 Q1。

如此克難式的臨時監察，當然是因為法律規範及體系制度的架構，跟不上通訊科技發展之速度，造成犯罪偵查之困難。由於目前未有統一之作業標準，使得警方用臨時裝機的方式，碰到業者不配合，或聲稱技術不可行之情況[64]，故縱使辛苦聲請了一張通訊監察書，但遇到不合作之業者，前實務上似乎無可奈何，僅能另起爐灶，找尋其他偵查方式。而這就是網路通訊監察未達成制度化所發生之最大問題。

B. 侵害過廣問題

因為網路上所有的資訊皆是用封包的方式來傳輸，當然網路通訊亦不例外，所謂封包(Packet)技術，資料在傳遞之前，先將要傳送的資料分為數個大小相等的區塊，加上某些檔頭資訊之後，透過不特定的路徑在網路中傳遞。故不論是網路電話、電子郵件、即時訊息等網路通訊之傳輸，皆是將一份通訊資料切割成多數的封包區塊，從使用者的電腦產生封包資訊，經由Gateway 發送出去，分散在整個網際網路中傳輸，每個封包無固定傳輸路徑，僅有相同目的地，故每個封包可能皆經過不同的線路，而每條線路上會充斥著不同使用者、不同資料的封包。最後同一份資料的封包會在目的地集合，還原成使用者可以理解之資料。故此種網路資料的傳輸，其特性為「分散性」「無固定路徑」。

而由於上述網路資料傳輸之特性，造成警方使用攔截封包的方式進行通訊監察時，勢必要將經過某特定線路的所有封包全部複製下來，再進行人工過濾，將不需要之資訊(例如第三人之封包、受監察對象使用其他網路服務之封包等)刪除，僅留下受監察之帳號其通訊資訊，進而檢視其通訊內容[65]。

故這樣的監察方法，與傳統電話監察不同地方就在於，警方在進行攔截、解碼、過濾的監察過程中，勢必會接觸到大量與監察標的無關之資訊，這是網路特性及監察技術使然，無可避免之結果。而如此大量之資訊該如何過濾、保存或使用，目前並無法規、命令能夠依循，僅能靠警方內規或職業道德約束[66]。而這仍然是網路通訊監察未形成制度所難以監督控管之問題。

C. 監察範圍問題

雖然警方的網路通訊監察須以帳號為標的，理論上僅能監看通訊監察書內記載帳號之內容[67]，但由於技術上須從受監察對象的通訊封包經過之路線上進行攔截，故再通訊監察書樣亦要記載警方所欲攔截的線路編號[68]。

---

[64] 北市警訪談 Q5，偵九隊訪談 Q21。
[65] 北市警訪談 Q16、Q17。
[66] 北市警訪談 Q9。
[67] 北市警訪談 Q9、Q10、Q11。
[68] 北市警訪談 Q5、偵九隊訪談 Q3。

而法官在核發通訊監察書時，除會審視犯罪事實、該帳號與受監察對象之關係外，亦會對該線路進行審查，這是因為前述關於網路傳輸之特性，同一條線路上必定有大量的封包在上面傳輸，包括不相干第三人之封包，亦即一條線路越多人在使用，警方就會攔截到越多人之封包，故法官要對這條線路的使用狀況進行了解，若為公用網路或使用狀況複雜，難以具體個化，法官可能會考量對隱私權侵害過廣而不予核發通訊監察書。

根據訪談結果，受訪警官所聲請的通訊監察書中，絕大多數為家庭上網用戶之線路[69]，亦即需特定到該條線路僅有一戶家庭使用，法官才認為不至於牽涉過廣，或是一棟住宅分租給多個房客之情況，法官亦會許可[70]。

但若將監察範圍擴及至住有數十或數百人之公寓大廈[71]、公司企業[72]、網咖[73]等不特定多數人使用之公眾線路時，法官通常會考量其牽涉範圍過於廣泛、太過不特定而不核准其通訊監察書。如此結果造成目前通訊監察實務上，幾乎僅能監看個人裝機用戶，或家庭用戶，若超出此一範圍，例如受監察對象利用公司、網咖等公眾網路進行網路通訊時，基本上無法進行通訊監察，造成偵查上很大的漏洞。

縱使法官能夠放寬上述要件之審核，以目前監察技術來看，警方之監察設備亦無法承載過於大量的封包攔截，故無法在網際網路的上游線路(不特定多數人之封包傳輸時必經的主要幹道)做攔截動作，造成法令上及技術上的雙重限制。故目前實務上對於網路通訊監察的適用範圍，仍然非常限縮狹隘。

鑒於以上諸多制度上、技術尚未成熟所造成之問題，本文以下將介紹美國全面性、制度化的網路監察系統及方法，作為參考和借鏡之依據。

(四) 美國Carnivore系統

1. Carnivore的源起

西元2000年3月，美國總統網路非法行為工作小組（President's Working Group on Unlawful Conduct on the Internet）所公佈之報告中，內容指稱網路具有隱密性、一對多、快速散佈等特性，導致網路不法行為逐漸增加，且網路犯罪手段日趨成熟，色情、賭博、智慧財產權之侵害、槍枝毒品、網路詐欺等傳統

[69] 偵九隊訪談 Q23、北市警訪談 Q8。
[70] 北市警訪談 Q18。
[71] 偵九隊訪談 Q23。
[72] 北市警訪談 Q7，Q18。
[73] 偵九隊訪談 Q8。

犯罪已從實體社會逐漸移轉至網路世界[74]。除此之外，美國聯邦調查局（FBI）發現，恐怖主義、間諜行為、兒童色情、惡性重大之詐欺行為與資訊戰爭等犯罪得因網路而加強其侵害性。有鑑於此，為防止網路成為偵查犯罪與恐怖活動的死角，美國聯邦調查局（FBI）遂發展出Carnivore 系統，以因應未來網路犯罪或恐怖活動的發展[75]。

在未讓大眾充分瞭解之情況下，聯邦調查局開始運作Carnivore 系統，西元2000年7月初，華爾街雜誌(Wall Street Journal)的「FBI 暗中調查電子郵件，引發法律及隱私權爭議」一文披露，讓Carnivore系統在世人面前曝光，並引發軒然大波。美國人民一方面希望該系統能加強功能，遏止不法份子與恐怖組織的力量，防範恐怖份子利用網路對美國人民進行危害，但卻也質疑是否會侵害隱私權，產生嚴重之矛盾心態。

2. Carnivore 之運作

Carnivore 系統具有「備位性」，僅在ISP 業者無能力對特定對象進行網路監察，美國執法單位始安裝該系統[76]。該系統之功能可以監看經由ISP 業者之通訊內容，以電子郵件為例，可監看送件者與收件者、郵件主題與郵件內容等；另外，亦可分析ISP 業者之客戶網路瀏覽習性與使用狀況。總之，只要網路上的任何行為，包括檔案傳輸、訊息公佈、新聞群組、電子商務等內容，Carnivore 理論上都可以完全掌控。

Carnivore 系統架構包括：(1) 連接乙太網路之單向竊聽設備（1-Way Tap）；(2) 過濾與蒐集資料之電腦；(3) 其他負責蒐集與檢視資料之控制電腦（control computer）；(4) 連結蒐集資料電腦（collection computer）之線路，該電腦並無鍵盤、螢幕等設施，係以pcAnywhere 之遠端監控軟體，由他處之其他電腦經由線路進行操控，Carnivore 軟體係安裝在該「蒐集資料電腦」中[77]。

Carnivore 系統之運作流程，在法律的授權範圍內，由美國聯邦調查局（FBI）與ISP 業者共同確認最小侵害之節點（access point），由美國聯邦調查局（FBI）在此一節點連接單向的竊聽設備（1-Way Tap），於避免干擾網路正常運前提下，將此節點所有通訊內容製作完整的備份，所得資訊再傳送至資料收集系統

---

[74] President's Working Group on Unlawful Conduct on the Internet, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet*, U.S. Dep't of Justice, http://www.usdoj.gov/criminal/cybercrime/unlawful.htm (last visited Jan. 13,2009)。

[75] 前揭註 2，頁 160。

[76] Johnny Gilman, *Carnivore: The Uneasy Relationship Between the Fourth Amendment and Electronic Surveillance of Internet Communications*, 9 COMMLAW CONSPECTUS 111, 124(2001)。

[77] IIT Research Institute,Independent Technical Review of the Carnivore System：Final Report，at viii(2000)，*available at* http://www.justice.gov/archive/jmd/carniv_final.pdf。

（collection system），並經由過濾器（Filter）將不屬於法律授權範圍之內容加以過濾，過濾後資料存放在永久儲存設備（permanent storage media），以作為偵查與審判的依據[78]。

當將Carnivore 系統安裝於ISP 的伺服器上時，蒐集資料電腦將會符合關鍵字的封包從網路封包中過濾出且儲存在儲存設備中。單向的監察設備確保Carnivore 系統不能透過網路傳輸任何資料，且欠缺通訊協定使得Carnivore 系統無法對外溝通，也無法改變或加入新的封包資料。控制電腦則位在執法人員所在地，當透過電話線路或其他網路設備連結資料電腦時，操作人員可以設定並改變過濾設定，決定開始及停止截取封包，以及檢視所截取的資訊。在控制電腦中的Packeteer 與CoolMiner 軟體，可以將通過目標IP 的封包回復成可讀的內容。其中Packeteer 軟體係處理從Carnivore 系統所傳送未經處理的資料，並將之從IP封包中重建為高階協定，CoolMiner 軟體則製作統計表與以瀏覽器顯示Pen register蒐集模式與Full-collection蒐集模式的資訊[79]。

Carnivore 系統可分為Pen register 蒐集模式與Full-collection 蒐集模式，前者可以蒐集到電子郵件中寄件人與收件人的郵件地址，以及HTTP 網頁及FTP檔案的IP 位址，後者可以檢視完整電子郵件內容、網頁內容及檔案內容。Carnivore系統的操作人員是匿名的，沒有顯示操作人員身分，且所有的使用者均以「管理者」（administrator）的身分紀錄。Carnivore 系統沒有能力自動過濾特定封包，而是取決於操作人員是否能正確且完整地達成目標的能力。預設模式並沒有截取任何封包，但只要一個按鍵就可以截取通過特定IP的所有流量封包，也可以選擇截取特定通訊協定（包括POP3 或STMP）上的電子郵件。

Carnivore 系統通常使用在截取特定IP 位址上的封包，但決定者乃操作人員，而非軟體本身。在使用者介面方面，分成基本視窗與進階視窗二種，基本視窗讓操作者檢視蒐集資料的統計，與從所有封包切割輸出的檔案；進階視窗則可讓操作者決定過濾的標準，及蒐集資料的範圍。在進階視窗中，若能增加過濾要件的設定，將可監察範圍限縮在特定的目標中，將減少許多與監察範圍無關的資料，例如將截取的範圍限縮在特定的通訊協定上。

簡單來說，Carnivore 系統的運作模式是先把所有通過一定路徑的資訊通通複製下來放在硬碟裡，然後再把特定資訊轉儲存至壓縮軟碟中，再透過關鍵字以及特定IP 位址來過濾出特定資訊。這樣的運作模式雖然在理論上FBI 只會接觸到經過過濾的資訊，換句話說，如果在設定上只讓Carnivore 系統取得標頭資訊的話，那麼通訊內容便不可能被揭露。

[78] 前揭註 2，頁 161。
[79] 前揭註 37，頁 145。

但是其運作模式和單純的撥號記錄器或追蹤裝置並不相同，撥號記錄器和追蹤裝置只會記錄通訊內容以外的其他資料，而Carnivore 系統事實上已經先取得通訊內容資訊後，再把通訊內容過濾掉。如果Carnivore 系統可以用撥號記錄器的方式加以設置的話，那麼便會產生一個潛在危險，那就是在過濾器失效或因執法者有故意過失地不依令狀操作之情形下，所有的通訊內容會被一網打盡。

此外有學者指出，即便Carnivore 完全依照FBI 的說法加以運作，在實務上還有問題存在，例如說，透過過濾器來進入軟碟機加以記錄的資訊也有數百MB，技術人員如何從這數百MB 的資料中決定哪些是和犯罪有關的？即便特定了傳送路徑、收件信箱、傳送信箱、關鍵字，仍然有許許多多無關的資料混雜地被複製到軟碟內，這些資料要如何即時判斷和犯罪有關？面臨加密的郵件時，要如何處理[80]？因此，Carnivore 系統所可能造成的大規模隱私侵害潛在可能性，現階段仍然不可忽視。

3. Carnivore系統獨立最終技術檢視報告

由於Carnivore 系統引發隱私權的重大爭議，美國司法部與IIT Research Institute 及Illinois Institute of Technology Chicago-Kent College of Law（以下簡稱IITRI）簽訂契約，由IITRI 針對Carnivore系統進行評估與分析。IITRI 於西元2000年12月8日提出「Carnivore 系統獨立最終技術檢視報告」（Independent Technical Review of the Carnivore System：Final Report）。

(1) 針對 Carnivore 之評估與見解

IITRI 所提出的最終報告，針對前述三大問題作出結論：

A. Carnivore操作取得之資料，不會逾越法院命令授權之範圍；

B. 除非ISP 業者必須改變其網路以符合Carnivore 之要求，否則 Carnivore 操作過程中，不會對ISP業者之網路系統造成操作或安全之危險；

C. Carnivore 系統僅能降低但無法完全消除聯邦調查局（FBI）人員故意或非故意未授權獲得電子通訊資訊的危險，至於其他非聯邦調查局（FBI）之人員，卻可能增加不法使用之危險[81]。

(2) 對於Carnivore系統之建議

---

[80] E. Judson Jennings，*Carnivore：US Government Surveillance of Internet Transmission*，6 VA. J.L. & TECH. 10(2001)。

[81] IIT Research Institute, *supra* note 77,at xii。

IITRI 提出之報告中，雖然對於Carnivore 系統之評價，基本上仍屬正面，但仍擔憂Carnivore 系統存在之缺點，將引發隱私權團體之強烈關注，降低人民對於隱私權保護的要求，且增加民眾憂慮執法人員未經授權而侵害個人隱私。因此IITRI 在報告中提出下列建議[82]：

A. 應繼續使用 Carnivore 系統，因為與其他Ether Peek等系統相比較，Carnivore系統能夠符合法院命令的要求，精確限縮蒐集資料的範圍。只要依據Title III之法院命令正確設定，不會發生過度蒐集之現象。

B. 由聯邦層級負責控制 Carnivore 系統，並要求資料蒐集之聲請，必須獲得司法部的授權。

C. 明顯區分 Pen register 蒐集模式與完整蒐集模式。因為若將兩種模式放在一起，可能會因誤用之意外發生，而超過法院命令的授權範圍。

D. 規範個人責任與審查程序。每一個設定、開始、停止與恢復，都應由特定人加以追蹤，對於何人設定蒐集程序，何人開始下載資料，何時設定蒐集程序，何時開始下載資料等，以釐清責任。

E. 提升對於Carnivore 系統之控制。可以增加保護裝置，如在設備外圍、鍵盤、監視器、滑鼠等連接處封印。若ISP 業者或其他人士企圖侵入，將導致封印毀損，即可顯示所蒐集之證據遭到竄改。

F. 藉由紀錄過濾設定、增加檢查或加密的數值（checksum），將蒐集的資料與蒐集時所作的設定結構（configuration）相結合，存放在相同的檔案中，以方便事後審查。

4. 小結

必須說明的是，美國這套Carnivore 系統，可說是全面網路監控的系統，FBI在各大重要網路傳輸路徑及美國對外網路連結線路，皆設置有這套系統。警方在有通訊監察需求時，即可隨時上線監察，其作法幾乎超越了需要特定對象的通訊監察，而近似於無對象之臨檢，因為警方可隨時將通過任一節點之封包全部攔截下來，判斷有無犯罪資訊，雖然FBI 聲稱其僅觀看非屬內容之信封資訊，不需法院令狀即可為之，但實際狀況外人無從得知，加上網路之特性使得內容資訊及信封資訊區分上之困難，更增加操作人員不法濫用之可能性。

[82] *Id*. at xiv-xv,5-1-5-4。

故我國目前究係有無如此強烈需求，而採取類似美國之做法，需要進一步之討論及審慎評估，本文採保留態度。但目前我們可以學習的是美國制度化的網路通訊監察，該系統不論在操作準則、程序規範、監督機制上，皆可以作為參考的依據，進而解決前述實務上所遇到之困難，以及網路通訊監察未制度化所造成之問題。本章在結論部分亦提出相關制度化之建議。

五、通訊監察的協助

通訊保障及監察法第十四條第二項之規定：電信事業及郵政事業有協助執行通訊監察之義務；其協助內容為執行機關得使用該事業之通訊監察相關設施與其人員之協助。

而因協助執行通訊監察所生之必要費用，於執行後，得請求執行機關支付；其項目及費額由交通部會商有關機關訂定公告之。

電信事業之通訊系統應具有配合執行監察之功能，並負有協助建置機關建置、維持通訊監察系統之義務。但以符合建置時之科技及經濟上合理性為限，並不得逾越期待可能性。

協助建置通訊監察系統所生之必要費用，由建置機關負擔。另因協助維持通訊監察功能正常作業所生之必要費用，由交通部會商有關機關訂定公告之。

按電信事業及郵政機關對於通訊監察之公務，自有容忍及協助配合之義務，而為有效達成執行監察之目的，其通訊系統自應具有配合執行監察之功能。協助通訊監察執行之電信事業及郵政機關(構)，因協助執行所支出之必要費用，在通訊監察實施結束後，自得向執行機關請求支付。有協助執行通訊監察義務之電信事業及郵政機關(構)，若違反協助執行通訊監察之義務者，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(通訊保障及監察法第三十一條)。

按電信事業及郵政機關 (構)對於通訊監察之實施，若違反其協助之義務時，自應由公權力施以相當程度之制裁，若在制裁後仍不願配合協助通訊監察之執行者，則對於此些違反協助義務之電信事業及郵政機關 (構)，自得以較重之管制罰，撤銷其特許或許可[83]。

六、通訊監察的終止

[83] 參見林錫堯，行政法要義，頁 311(1998)。

通訊保障及監察法第十五條之規定：第五條、第六條及第七條第二項通訊監察案件之執行機關於監察通訊結束時，應即敘明受監察人之姓名、住所或居所報由檢察官、綜理國家情報工作機關陳報法院通知受監察人。如認通知有妨害監察目的之虞或不能通知者，應一併陳報。

法院對於前項陳報，除認通知有妨害監察目的之虞或不能通知之情形外，應通知受監察人。

前項不通知之原因消滅後，執行機關應報由檢察官、綜理國家情報工作機關陳報法院補行通知。

關於執行機關陳報事項經法院審查後，交由司法事務官通知受監察人。

為使通訊監察透明化，維護人民權利主體之地位，如同其他之強制處分，通訊監察之執行機關應以書面告知被監察人。如其通知有妨害監察目的之虞或不能通知者，因其不宜通知或無法通知，在經法院許可後，則可不通知被監察人，法院對於應否通知受監察人、通知有無妨害監察目的之虞，應有所監督審查。惟為充分保障受監察人之權益，於不通知之原因消滅後，應立即補行通知。

七、通訊監察取得資料之處理

通訊保障及監察法第十七條規定：監察通訊所得資料，應加封緘或其他標識，由執行機關蓋印，保存完整真實，不得增、刪、變更，除已供案件證據之用留存於該案卷或為監察目的有必要長期留存者外，由執行機關於監察通訊結束後，保存五年，逾期予以銷燬。

監察通訊所得資料全部與監察目的無關者，執行機關應即報請通訊監察書核發人許可後銷燬之。

前二項之資料銷燬時，執行機關應記錄該通訊監察事實，並報請通訊監察書核發人派員在場。

為維護監察通訊所得資料內容之完整真實，並避免發生洩漏情事，監察通訊所得之資料，應加上封緘或其他之標識。同時應由執行機關蓋印，不得增、刪或變更，以求其完整。除已為案件之證據，應依一般案件證據之處理程序留存於該案件，或因監察目的之需要，應長期保存者外，執行機關應將該資料保存五年，逾期則依一般行政上銷燬程序予以銷燬。又在經監察通訊後，如所得資料全部與監察目的無關，為保護人民之隱私權益，該項資料應即銷燬。

而為便於日後考察且昭公信，執行機關於銷燬資料時，應摘要記載該通訊監察之案由、實施對象、通訊種類、執行處所、執行期間等事實，並應由通訊監察書核發人派員在場。值得注意的是，即使在當事人未受通知而不知悉之情形下，雖然行政機關之行為只在內部進行，惟其客觀上已對當事人之隱私權益造成侵害，故仍應將此種隱私限制之情況除去[84]，亦即所獲得之資料仍應銷燬之。

此外，依據通訊保障及監察法第十八條之規定，依本法監察通訊所得資料，不得提供與其他機關（構）、團體或個人。但符合第五條或第七條之監察目的或其他法律另有規定者，不在此限。

蓋通訊監察所得之資料與人民之隱私權攸關，執行機關應保守秘密，不得提供給其他機關（構）、團體或個人。但例外如有關機關在符合其他法律規定，或本法第五條或第七條之監察目的時，則應可提供予其他機關、團體或個人，以收證據互用，避免重複偵查而浪費國家資源故也[85]。

八、通訊監察的監督

(一) 我國通保法之規定

通訊保障及監察法第十六條規定：執行機關於監察通訊後，應按月向通訊監察書核發人報告執行情形。通訊監察書核發人並得隨時命執行機關提出報告。通訊監察書核發機關應派員至執行處所，監督通訊監察執行情形。

按通訊監察之實施，攸關人民之基本權益至鉅，因此，執行機關應審慎為之，並應按月向通訊監察書核發人報告執行之情形。同時為確保執行機關妥適執行通訊監察，通訊監察書核發人並得隨時命執行機關提出報告，以說明通訊監察之實施情形。除了提出報告以外，通訊監察書核發機關為促使執行機關確實依法執行通訊監察，並應派員至執行處所，監督通訊監察之執行情形，如此方能使通訊監察書核發人瞭解通訊監察實際上之執行情形。

(二) 實務現況

執行通訊監察的警察必須定期向指揮檢察官和核發通訊監察書之法官報告，一個月報告兩次，一次為期中，一次為期末。另外還有單位內部的公務倫理報告機制

[84]許宗力，法與國家權力，頁 384(1992)。
[85]徐智明，通訊監察之保障與規範，中正大學法研所碩士論文，頁 65。

報告內容就是現在聽到何種程度、聽到什麼內容、與監察犯罪內容是否相符，有沒有必要下一次通訊監察終止前，再針對某一項目減縮或擴張監查內容。格式上就用各個法院規定的格式，或是執行單位及通訊監察中心的格式。

程序上是警方向檢察官報告，檢察官向法官報告，因為檢察官案件眾多，無法實質參與監察，但警方要把監察的錄音結果交給檢察官，檢察官有權力調閱，但檢察官不可能每個案子都聽，通常是請檢察事務官去聽，並考量個案有無必要，以及對受指揮單位的信任感[86]。

(三) 美國電子通訊隱私法之規定

有關通訊監察監督之規定，包括三個部分，其一為向聯邦法院行政局提出「個案報告」，其二為向聯邦法院行政局提出「年度報告」，其三為向國會提出報告，分述如次：

1. 向聯邦法院行政局提出「個案報告」

依法通訊監察之有效期間屆滿後，或駁回通訊監察聲請後三十日內，受理通訊監察聲請之法官應向聯邦法院行政局（the Administrative Office of the United States Courts）提出報告，此屬於「個案報告」之性質。報告事項包括：(1)聲請令狀或延長期限之事由；(2)聲請令狀或延長期限之種類；(3)聲請令狀或延長期限經准許、修正或駁回之事實；(4)令狀所許可之監察期限與案號，及延長期限之有效期間；(5)令狀、聲請書或延長期限令狀上所記載之犯罪；(6)提出聲請之有調查權限或執行法律公務員，與聲請機關及批准聲請書之人；(7)被截取之設施或處所，其性質與位置。

2. 向聯邦法院行政局提出「年度報告」

每年一月，聯邦檢察總長或其指定之助理檢察總長，或州檢察長，或州以下各級機關檢察長，須向聯邦法院行政局提出「年度報告」，內容包括(1)上一年度中，聲請發給令狀或延長期限令狀中，關於上述(1)至(7)所定之事項；(2)包括依據監察令狀所為截取行為之概述，包括(A)所截取之犯罪通訊或對話之大概性質與次數；(B)其他所截取之通訊或對話之大概性質與次數；(C)被截取通訊或對話之大概人數；(D)使用於截取行為之大概性質、數量、人力消耗與其他資源；(3)依據截取結果逮捕人犯之人數及所犯罪名；(4)因截取結果導致審判之案件；(5)對於截取行為異議之件數，及異議成立與不成立之件數；(6)因截取結果經判

[86]偵九隊訪談 Q14，北市警訪談 Q20。

決有罪之件數及罪名，及截取行為重要性之一般評估；(7)上年度中關於(2)至(6)之資料。

3. 向國會提出報告

每年四月，聯邦法院行政局主任應向國會提出關於上一年度准許或追認通訊監察之件數，及准許與駁回聲請、准許與駁回延長期限聲請件數之完整報告，報告之內容應包括上述之檢討與分析。聯邦法院行政辦公室有權針對上述製作報告之內容與型式，發布有拘束力之行政規則[87]。

(四) USA Patriot Act 增訂使用Carnivore 系統之規範：

新法在§3123(a)(3)增加要求執法人員必須在安裝設備或程式後的三十天內向法院提出報告，報告中應載明1. 安裝及操作該裝置人員的身份；2. 安裝、操作及解除安裝的日期與時間；3.該裝置安裝時的結構及之後的修正；4. 所獲得的資訊。

(五) 小結：監督機制之補強

針對建置機關的監督，通保法第16條第二項規定，偵查中由檢察官，審判中由法官為之。監督的方式，可以是派員至建置機關處，也可以是以電子設備來監督。也就是說，在偵查中，法院無法監督建置機關。會有這樣的設計，或許是因為按照同法第11條第二項的定義，建置機關並不接觸通訊的內容，所以立法者並未一併授權法院也可以在偵查中監督建置機關。但是，法院作為決定通訊監察的決定者，卻在偵查中有無法監督的機關，著實令人不解[88]。

再者，在前述關於通訊監察書撰寫的部份，本文建議在撰寫通訊監察書時，區分傳統電話監察及網路監察，而做不同的處理，或是考慮引進不定點監察。如此關於「書面原則」之鬆綁，可增加犯罪偵查的靈活度。但另一方面，亦增加偵查機關濫權之可能，故有必要對監督機制做一定之補強。

並且，在前述針對網路監察之方式，本文認為在攔截封包方式的網路通訊監察之下，雖然使得無辜第三人隱私被侵害之風險增加，但在目前科技侷限之下，似乎已是不得已，且最有效率的作法，且若監察人員能依法正確操作監察系統，亦可使無辜第三人隱私被侵害之可能降到最低。而如何確保偵查機關堅守監察最小侵害性原則，不致於濫用公權力，則有賴監督機制的發揮。

---

[87] 18 U.S.C. § 2519。
[88] 前揭註 18，頁 52。

故我國對於監察機制之改進，可參考美國法，成立專責監督機關，區分為個案報告及年度報告，並且詳列應報告之事項，方不至於使監督機制流於形式。另外亦可考慮增加第二層之監督，即國會監督，以確保整個監督機制之完善運作。並且，在執行層面，要求偵查機關在使用監察系統後，須向法院即提出報告，說明執行細節，方能及時且有效之監督。

九、通訊監察執行後的救濟

(一) 民事責任

通訊保障及監察法第19條規定：違反本法或其他法律之規定監察他人通訊或洩漏、提供、使用監察通訊所得之資料者，負損害賠償責任。

被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。

前項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。

本條為侵權行為法之特別規定，按人民秘密通訊之自由，乃憲法所保障之基本權利之一，若有違反本法或其他法律之規定監察他人通訊或洩漏、提供、使用監察通訊所得之資料者，無論其為公務員或一般人民，均已嚴重侵害他人通訊及隱私之權益。而須負損害賠償。同時本條為「無過失責任」，避免造成被害人因舉證困難而求償無門之窘境，以充分落實對人民通訊權益之保障。

另外通訊保障及監察法第二十條規定：前條之損害賠償總額，按其監察通訊日數，以每一受監察人每日新台幣一千元以上五千元以下計算。但能證明其所受之損害額高於該金額者，不在此限。前項監察通訊日數不明者，以三十日計算。

(二) 刑事責任

1. 違法通訊監察

通訊保障及監察法第24條規定：違法監察他人通訊者，處五年以下有期徒刑。執行或協助執行通訊監察之公務員或從業人員，假借職務或業務上之權力、機會或方法，犯前項之罪者，處六月以上五年以下有期徒刑。意圖營利而犯前二項之罪者，處一年以上七年以下有期徒刑。

通訊保障及監察法第25條規定：明知為違法監察通訊所得之資料，而無故洩漏或交付之者，處三年以下有期徒刑。意圖營利而犯前項之罪者，處六月以上五年以下有期徒刑。

2. 合法通訊監察

通訊保障及監察法第27條規定：公務員或曾任公務員之人因職務知悉或持有依本法或其他法律之規定監察通訊所得應秘密之資料，而無故洩漏或交付之者，處三年以下有期徒刑。

通訊保障及監察法第28條規定：非公務員因職務或業務知悉或持有依本法或其他法律之規定監察通訊所得應秘密之資料，而無故洩漏或交付之者，處二年以下有期徒刑、拘役或新台幣二萬元以下罰金。

(三) 國家賠償責任

通訊保障及監察法第22條第一項規定：公務員或受委託行使公權力之人，執行職務時違反本法或其他法律之規定監察他人通訊或洩漏、提供、使用監察通訊所得之資料者，國家應負損害賠償責任。

按公務員或受委託行使公權力之人，執行職務時違反本法或其他法律之規定監察他人通訊或洩漏、提供、使用監察通訊所得之資料者，為確保被害人能實際獲得賠償，以貫徹保障人民之自由權利，應採「國家代位責任」主義，使國家對公務員執行職務之不法行為所造成之損害負賠償責任[89]。

十、阻卻違法事由

(一) 我國通保法之規定

通訊保障及監察法第29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。

[89]參見廖義男，國家賠償法，頁 9(1997)。

(二) 美國電子通訊隱私法（ECPA）之規定

ECPA 第一部分有關即時通訊內容的截取，原則上需向法院聲請核發令狀始可執行，但ECPA 也容許若干例外情況。在USA Patriot Act 修正前，令狀的例外共有五種。亦即：

1. 通訊一方當事人同意之例外（the consent exception）[90]：包括通訊一方為執法者的事前同意；以及同意之一方雖非執法者，但基於調查違反憲法或法律之目的，同意仍為合法。

2. 提供者之例外（the provider exception）[91]：通訊服務提供者得基於保護自身權利財產的目的，截收或揭露通訊。但應予注意者，乃此種例外乃服務提供者專屬的特權，不得讓渡予執法人員。因此，執法人員不得代替服務提供者執行截收個人通訊。

3. 電話分機之例外（the extension telephone exception）[92]：允許服務提供者基於商業的目的監察與工作有關內容的電話分機通訊內容。

4. 善意取得證據之例外（the inadvertently obtain criminal evidence exception）[93]：服務提供者基於善意所獲取附屬（pertain）於特定犯罪的通訊，可將所獲得的通訊內容揭露給執法人員。

5. 公眾可接觸之例外（the accessible to the public）[94]：允許任何人在公眾可接觸的通訊系統內，截取電子通訊內容，例如網路聊天室、新聞群組等。

(三) USA Patriot Act 的增訂：

由於上開例外情形或專屬服務提供者特權，或屬於服務提供者揭露範圍，並未提供執法人員基於調查犯罪目的主動調查時之例外，USA Patriot Act 為平衡犯罪偵查與個人隱私保障，乃另增訂「電腦入侵者」之例外（the computer trespasser exception）[95]。首先，在18 U.S.C §2510 增列電腦入侵者的定義，指個人未經授權進入受保護電腦（protected computer）而言，並規定受保護電腦持有人不得主張合理隱私權期待，以利犯罪之偵查。另外，在§2511（2）增列第（i）項，規定執法人員可以截取受保護電腦所傳送進、出、或經過的通訊，但應符合

[90] 18 U.S.C. §2511（2）（c）-（d）。
[91] 18 U.S.C. §2511（2）（a）（i）。
[92] 18 U.S.C. §2510（5）（a）。
[93] 18 U.S.C. §2511（3）（b）（iv）。
[94] 18 U.S.C. §2511（2）（g）（i）。
[95] USA Patriot Act，§217。

下列條件：（A）該受保護電腦的所有人或操作者授權截取；（B）截取通訊的人必須是合法進行調查之人；（C）須證明有合理的依據認為所截取的通訊與正在進行的調查有關；（D）所截取的通訊必須是入侵者所寄出或收到的訊息。此項例外提供執法人員偵辦電腦駭客之案件時，不需事前取得法院令狀，即可實施通訊監察處分。

以上增定係由於以駭客為主之網路侵入行為屢見不鮮，例如侵入電腦後，再偷偷植入程式，破壞或竊取網站內資料，往往造成政府機關、網路業者與個人網站等難以估計之損害。在前述法令修正前，若要截取網路侵入行為，必須經過冗長之聲請程序始得為之，然網路侵入行為往往在轉瞬間即完成，若必須經由聲請程序始得進行通訊監察，則將造成無法打擊網路侵入行為之結果。因此，前述法令修正後，不但規定電腦侵入者（computer trespasser）無合理隱私權之期待，且執法機關只要獲得電腦網路擁有者或操作者之授權，即可截取電腦侵入者傳送至受保護之電腦之有線或電子通訊行為。

(四) 關於例外規定之修正建議：

我國通保法關於無需令狀之通訊監察規定，僅有三項，前兩項規定依法令之行為，其內涵並不明確，故真正有意義之規定僅有第三項得一方同意之情形。反觀美國電子通訊隱私法列舉五項除外規定，具體明確地規定其行為態樣。若仔細探究其內涵，會發現這五項規定並未不當的擴張偵查機關的權限，僅是將歷年來實務判決所承認之「無合理隱私期待」，及「得一方當事人同意」之具體態樣，落實於明文規定之中，其實未創造出新的例外事由。如此一來可使偵查機關有更明確的準則可以依循。故此一規定，值得我國立法上之參考。

至於美國愛國者法案增訂，「電腦入侵者」之例外，使偵查機關對付網路駭客更加有效，但是此種網路監看較缺乏司法機關之監督，易生弊端。故我國是否該增訂此種例外，宜審慎評估。

十一、結論

(一) 建立系統化的網路監察制度

1. 建立標準監察作業流程

目前網路通訊監察之當務之急，即是建立標準的監察作業流程，不論是設備安裝、系統操作、或是與業者連線，皆應有統一規範，以擺脫目前臨時監察所造成的混亂，以及制度未建立造成業者配合度不高之問題。

2. 制訂明確的行為準則

針對監察之執行，應制定詳細之操作守則，規範每一個動作之實行，包括設定、開始、停止與恢復等等，並詳細記錄每次使用監察系統之情況，以釐清責任，並避免監察之執行逸脫監察票所載範圍。

3. 降低系統操作錯誤之可能性

監察系統之操作十分複雜，縱使監察機關非蓄意違法監察，仍可能應操作錯誤而侵害人民之通訊隱私，故在系統設計上應盡量降低操作錯誤之情形，例如監察對象所有網路使用內容時，必須使用確認對話框（confirmation boxes），以防止錯誤機會的增加，而侵害民眾之權利。

4. 內容資訊（content information）及信封資訊（envelope information）之區別

由於網路資料的封包可能包括文字、圖形、聲音及其他各種檔案內容，故本文一再強調必須區分內容資訊與信封資訊，分別適用不同法律規定。對於信封資訊之取得，是用電信法及電腦處理個人資料保護法。若要取得內容資訊則一定要取得監察票方可執行。

5. 考慮公開系統技術

社會大眾對於隱私權侵犯之疑慮，來自於對偵查機關之不信任及對監察系統之不了解。故政府機關應公開整個監察技術及流程，將監察流程公開化。有論者謂，必須對於監察技術的內容保密，以防止駭客因為得知系統內容，而得以技術上逃避通訊監察，但亦有論者認為，過度封閉的制度反而會發生問題與危險，將問題攤在陽光下，由更多人一同來檢視，反而可以減少問題的發生，例如可以由大家集思廣益找出軟體系統的漏洞。故應否公開，如何公開，公開到什麼地步，都是必須思考的問題。

6. 建立完整之監督機制

由於網路監察牽涉範圍較廣，亦增加偵查機關濫權之可能性，故應建立一套完整之監督機制，將人權侵害的副作用降到最低。

(二) 放寬網路通訊監察限制

1. 通訊監察書要件之放寬

從以上討論可得知，在傳統電話通訊監察中，關於通訊監察書的撰寫，不論是「監察對象」、「監察通訊種類及號碼等足資識別之特徵」及「受監察處所」等項目，實務上行之有年，運作上並無太大困難。

但在網路通訊監察的部份，因為虛擬網路世界的概念與現實世界有所不同，故在通訊監察書的撰寫上，若要完全依照現行通保法所列舉的應記載事項填寫，恐怕會發生扞格之處。為避免阻礙偵查實務之進行，對於通訊監察書應記載事項的審查，應從寬認定，甚至在為來修法方向上，免去某些與網路通訊監察無實際關係之記載，例如犯罪嫌疑人每次上網都可能用不同的IP，亦可以使用多個帳號，幾乎不用太多的成本跟麻煩，使得在通訊監察書的記載上，可能出現掛一漏萬的情形，而使得犯罪嫌疑人輕易躲避偵查。

故若可引進美國法承認之不定點監察，在某些特定狀況下允許偵察機關在通訊監察書上，不須記載「受監察處所」及「監察通訊種類及號碼等足資識別之特徵」，可迴避現實處所、通訊設備、方式、帳號無法特定之困難。以免打擊犯罪之時機稍縱即逝。

2. 偵查手段之放寬

由於傳統電話通訊是由固定線路傳送，要監察通話內容必須先判別傳輸所使用的實體線路，然後從實體線路上分接的監察線路上監錄通話的內容。這種監察方法可準確的監察犯罪嫌疑人之對話內容，而不會額外取得其他不相干第三人之通訊。故如此之監察方式，符合最小侵害性原則及比例原則，實施上並無太大問題。

但在網路通訊監察的部份，使用攔截封包的方式，將特定節點所有通訊內容製作完整的備份，傳送至資料收集系統進行篩選，找出需要之內容。這樣的方式，幾乎無可避免會攔截到無辜第三人的封包，引發過度侵害人權，不符合最小侵害性原則的疑慮。

然而，若參考前述IITRI 提出的「Carnivore 系統獨立最終技術檢視報告」，文中提到該系統能精準的篩選出所需的資料，再加上操作人員能正確操作該系統，輔以適當的監督機制，能將對無辜第三人的侵害降到最低。如此一來即可在

人權侵害相對輕微的情況下，順利進行通訊監察，似為人權保障及犯罪追訴的平衡點，值得我國立法及技術上之參考。

3. 監察範圍之放寬

法官在核發通訊監察書時，若屬於網路通訊監察時，會對該受監察之線路的使用狀況進行了解，若為公用網路或使用狀況複雜，難以具體個化，法官可能會考量對隱私權侵害過廣而不予核發通訊監察書。例如受監察對象利用公司、網咖等公眾網路進行網路通訊時，基本上無法進行通訊監察，造成偵查上很大的漏洞。

但若未來我國能依據前述之建議，建立系統化的網路監察制度，使得操作人員的行為皆能受到完整規範，系統上亦能做到設計完善，將隱私權侵害過廣的問題做有效抑制，應可說服法官在核發通訊監察書時，放寬監察之線路，擴大通訊監察之範圍，以利實務運作。

(三) 加強監督機制

雖然本文建議放寬網路通訊監察的限制，包括通訊監察書要件之放寬，以及偵查手段之放寬，但若一味放寬卻沒有配套措施，可能使民眾權益受到嚴重侵害，大開人權倒車。故在放寬的同時，本文也建議要加強監督機制，不論是事中或是事後，行政、司法或立法，皆要有一定的制衡力量，方能取得人權保障及犯罪追訴的平衡。

1.監察過程之監督

首先，在操作網路監察的過程中，必須規範個人責任與審查程序。每一個設定、開始、停止與恢復，都應由特定人加以追蹤，對於何人設定蒐集程序，何人開始下載資料，何時設定蒐集程序，何時開始下載資料等，以釐清責任。

2.系統設計之監督

而在監察系統設計上，必須提升對於監察系統之控制。並可以增加保護裝置，如在設備外圍、鍵盤、監視器、滑鼠等連接處封印。若ISP 業者或其他人士企圖侵入，將導致封印毀損，即可顯示所蒐集之證據遭到竄改。

3.事後之監督

在監督的單位上，除現有的司法部門(法官)之監督外，可考慮增加行政、司法之監督，並成立專責監督機關，明定執行機關須向監督機關做區個案報告及年度報告，並且詳列應報告之事項，使監督機制更加完善。

伍、網路通聯資料保存及保護之法制分析

一、前言

本文在第貳章將第二類電信所提供之服務區分成有通訊相對人之服務及無通訊相對人之服務，在有通訊相對人之服務當中，再根據通訊之所傳送之資訊，區分為內容資訊（content information）及信封資訊（envelope information）。如此區分之結果，使得內容資訊之監察適用通訊保障及監察法，而無通訊相對人之服務及信封資訊則適用電信法及電腦處理個人資料保護法[96]。

但如此之分類僅是現狀之描述，並不代表本文完全接受如此之區分，尤其在網際網路之時代，「內容／非內容」已非截然分立，有模糊化之趨勢，且內容以外之資訊，包括個人資料、上網紀錄等等，因為電腦儲存能力緣故，資料量大幅暴增，已非以往「通聯記錄」之概念可完全涵蓋。故傳統分類標準，有重新檢討之必要。更重要的是，如何因應網路世界之需求，制定出符合科技、時代潮流需求，並兼顧人權保障之「資料保存法制」，為急迫之議題。以下即提出幾點問題做探討：

(一) 通訊內容與通聯記錄區分之模糊化

目前不論我國法制，或美國ECPA 規定，皆係以是否涉及通訊內容做為適用法律的區分標準。此種「內容／非內容」的立法結構在傳統郵件及電話通訊系統是很容易區分的。例如在電話通訊中，通話雙方所撥打的電話號碼即屬信封資訊，而雙方的對話內容則屬內容通訊。一般而言，通訊內容不會被儲存（有合理隱私之期待），但通聯紀錄則會被電信業者保存下來（無合理隱私之期待），故偵查機關在調取這兩種資訊時，也是依循不同管道，兩者可截然區分。

但此區分在網際網路通訊中，則較為困難，其主要原因乃是網際網路乃封包交換系統，所有的通訊資訊均分解成封包型態傳遞。封包在網際網路中係以一連串的0與1之型態傳遞，電腦之間透過傳送及接收各式各樣的數字來傳遞訊息。當透過網路傳遞訊息時，訊息會先分解成封包，並創造出一個封包頁首（packet header）指引封包們到達目的地，到達目的地電腦後，電腦會將封包頁首丟棄，重組封包還原為原始內容資訊。故此時信封資訊指封包頁首，包括IP 位址等資訊，內容資訊則指封包到達目的後，拋棄掉封包頁首，重組封包之原始訊息內容。至於電子郵件，有關收件人、寄件人之郵件地址，皆為信封資訊。

[96] 參見本文第參章，表三、網路服務之分類。

由以上說明可知，以往我們認為通訊內容有合理隱私之期待，但通聯紀錄或信封資訊則否，故給予不同程度之保護，這樣的概念在傳統電話通訊及郵件通訊當然沒有問題。但在網路通訊中，不論是通訊內容或是信封資訊，皆是以封包傳送，不論在資訊的型態上，及接收之方式，皆無不同。偵查機關在攔截封包時，無法只攔截信封資訊，而不攔截內容資訊，僅能在後續階段利用過濾方式排除不需要或禁止取得之資訊。

既然內容資訊及信封資訊在網路傳輸上，都是一連串0與1的數字，兩者之命運可說是同生死、共存亡，其區分就變得毫無意義，我們是否仍能如此肯定，說內容資訊有隱私權期待，信封資訊則無，進而分別適用不同法律，給予差別待遇，即有重新討論之必要。

(二) 通聯記錄的重要性大幅增加

傳統第一類電信業者僅提供電話通訊服務，服務項目相對單純。但第二類電信業者除網路電話外，亦提供多樣化的上網服務，故第二類電信業者所可能保留之資料，已不侷限於通訊內容及通聯記錄，而是擴及到上網紀錄、會員資料、留言版訊息、網路空間等等之資料，業者可保存的資料量可說是大幅增加，理論上，只要某一用戶連接上網路後，該用戶的一舉一動，都會被業者所記錄下來，個人在網路上的虛擬行蹤，可說是無所遁形。

如此資料量暴增所帶來的衝擊，已遠遠超過傳統通聯記錄所能涵蓋的範圍。如此巨大的量變，也就連帶產生了質變。故網路上通聯記錄之重要性，已不能等閒視之。試想若偵查機關調閱了某位民眾過去半年以來的上網紀錄，詳加研讀分析後，可能就可以掌握該位民眾之日常生活作息，嗜好習慣，甚至是個性怪癖，以及對最親密的朋友也不願透露的秘密。如此之偵查手段，甚至比單純監察其通話內容還要有效，相對的對人民隱私權之侵害也更加嚴重。故以往對於個人資料之不重視，導致其保護強度相較於通訊內容有嚴重落差，在通聯記錄之重要性與通訊內容並駕齊驅，甚至是凌駕於上的情形之下，目前法制關於偵查機關調閱個人資料程序上，顯得太過容易、簡略，既沒有相當的要件要求，亦無專責的監督機關，這樣的制度，可能必須有所改變。

(三) 資料保存內容之複雜化及多元化

調取通聯記錄為警方偵查中不可或缺之方式，不論是做為通訊監察的前置過濾作業[97]，或是掌握嫌犯行蹤、清查身分的手段[98]，皆相當有效且準確。而通聯

[97] 北市警訪談 Q9。
[98] 北市警訪談 Q22。

記錄之資料量及類別，在網路時代大幅增加已如前述，如此龐大的資料量，對警方而言看似是一大利多，但由於法律規範的架構趕不上資訊發展之速度，導致法律規範密度不足，不論在保存項目上，或者是查詢方式，皆無法與目前實務需求相符。尤其業者通常會認為法律未規定就無義務提供，因此就算業者保有某些資料，或查詢方式，亦會推辭而拒不提供[99]。例如電信業者通常只提供正向查詢，例如以帳號查詢使用者資料，但卻不提供反向查詢，就是以使用者資料查詢其申請之帳號，理由就是法律未規定[100]。而往往反向查詢才是真正有用的偵察方式，造成法制規定不足拖累的警方的偵辦腳步，故對於通聯資料保存之法制，從警方的角度而言，亦應重新檢討。

故本章先檢視我國電信法、電腦處理個人資料保護法之規範即不足，並介紹美國及歐盟在資料保存上之法制，與之做比較，最後針對現有法制提出建議及修正方向。

二、我國現況

（一）電信法

我國電信法第 7 條：「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序，由電信總局訂定之。電信事業用戶查詢本人之通信紀錄，於電信事業之電信設備系統技術可行，並支付必要費用後，電信事業應提供之，不受第一項規定之限制；電信事業用戶查詢通信紀錄作業辦法，由電信總局訂定之。」

（二） 第一類電信事業

「電信事業處理有關機關查詢電信通信紀錄實施辦法」第 5 條規定：「前條第一類電信事業通信紀錄之保存期限如下：一、市內發信通信紀錄：最近三個月以內。二、國際、國內長途發信通信紀錄，最近六個月以內。三、行動通信發信通信紀錄：最近六個月以內。」

而有關機關查詢通信紀錄之程序規定在第3條：有關機關查詢通信紀錄應先考量其必要性、合理性及比例相當原則，並應符合相關法律程序後，再備正式公文或附上電信通信紀錄查詢單（格式如附件），載明需查詢之電信號碼、通信記

[99] 北市警訪談 Q29。
[100] 北市警訪談 Q28。

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。但案情特殊、情況緊急之查詢，得由法官、軍事審判官、檢察官、軍事檢察官、查詢機關首長或其書面指定人先以電話或公文傳真，並經回叫確認為之，查詢後應於三個工作日內補具正式公文或加蓋印信之電信通信紀錄查詢單正本。

前項之查詢，經查詢機關與電信事業雙方認證同意，得以經加密之電子郵件為之，該電子郵件並視同正式公文或電信通信紀錄查詢單正本。

第4條規定「關機關查詢之通信紀錄，於電信事業之保存期限以內者，始予受理；已逾電信事業資料保存期限，致無法提供者，電信事業應函覆說明之。」

第6條規定「電信事業處理查詢通信紀錄，應以不影響其營運作業，並依受理查詢日期先後之順序為原則。但案情特殊、情況緊急之查詢，不在此限。電信事業受理前項案情特殊、情況緊急之查詢時，應優先處理；其因優先處理所生公司營運作業及人員安全之費用，由查詢機關負擔之。」

第9條規定「有關機關申請查詢之公文，各電信事業受理單位應以專冊登記列管，並保存二年，逾期予以銷毀。」

第10條規定「經辦查詢作業之人員，對於查詢作業之過程及所查得資料之內容等，應予保密，不得外洩。」

（三） 第二類電信事業

第二類電信事業管理規則27條規定：經營者對於調查或蒐集證據，並依法律程序查詢電信之有無及其內容者，應提供之。前項電信內容之監察事項，依通訊保障及監察法規定辦理之。經營者對於第一項電信通信紀錄應至少保存期間如下：

1. 語音單純轉售服務通信紀錄應保存六個月。
2. 網路電話服務通信紀錄應保存六個月。
3. 網際網路接取服務：
   (1) 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。
   (2) 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。
   (3) 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。
   (4) 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。

(5) 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。
(6) 電子郵件通信紀錄應保存一個月。

4. 虛擬行動網路服務通信紀錄應保存六個月。

經營者應核對及登錄其用戶之資料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。

虛擬行動網路服務經營者或E.164 用戶號碼網路電話服務經營者應將使用者資料載入其系統資料檔存查後始得開通;以預付卡或其他預付資費方式經營虛擬行動網路服務者或E.164 用戶號碼網路電話服務者，亦同。

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或E.164用戶號碼網路電話服務經營者另應包括所指配號碼。

第四項之虛擬行動網路服務經營者或E.164 用戶號碼網路電話服務經營者應於受理申請二日內完成其使用者資料之載入。

（四） 電腦處理個人資料保護法

電腦處理個人資料保護法為保護儲存在電腦上個人資料的基本法，內容有「個人資料」的定義、「受拘束客體」、「受拘束主體」、「個人資料保護的法律原則」、「公務機關對於資料之處理」、「非公務機關對於資料之處理」、「救濟制度」等[101]

（五） 檢討

由以上介紹可知，我國對於網路通聯紀錄及個人資料的取得，依據「電信事業處理有關機關查詢電信通信紀錄實施辦法」，是以公文或電信通信紀錄查詢單向電信業者索取，只要程序無誤，電信業者即有義務提供。如此的程序，似乎過於簡便，且並無專責之監督機關。

因此現有法制對於通聯記錄之保護程度過低,雖非內容通訊資料之保護程度低於通訊內容，但從法位階與要件之嚴謹程度觀之，此一實施辦法僅為法規命

[101] 詳細內容請參見本文第肆章關於電腦處理個人資料保護法的介紹。

令，所設定之要件亦較通保法簡略甚多，亦容易侵害第三人之隱私權[102]，以此實施辦法做為侵害人民受憲法保障之秘密通訊自由之法源依據，在正當性上顯然有所欠缺，有違法律保留原則與隱私權保護原則。

並且，此一實施辦法並無法涵蓋「所有的非內容通訊資料」：前面所提到關於電腦紀錄檔與封包頁首資訊此類非內容網路通訊資料，顯然無法涵蓋於本實施辦法對通信紀錄之定義之內，對於無法涵蓋之類型，檢調機關是否即可任意調取該等資料，易生爭議。

此外，「電信事業處理有關機關查詢電信通信紀錄實施辦法」僅在形式上符合明文授權之規定，並免除業者依此辦法提供通訊紀錄而未履行電信法第7條第1項之守密義務，雖可解決規範衝突問題，但卻對於用戶之隱私權保護顯然未予重視[103]。

而對於公務機關所取得之資料，以及業者依法保存之紀錄，雖可依電腦處理個人資料保護法加以規範，但該法實際上為個人資料保護的一般性規定，並未針對電信事業及通訊資料有特別規定，太過概括，難以具體適用。且在個人資料的搜集、利用上，個資法在第七條雖限制在三種事由，但隨即在第八條規定了九種例外，導致公務機關十分容易正當化其搜集、利用行為，故個資法之規定，恐怕不足以因應網際網路時代的個人資料保護。

另外，個人資料的重要性，在網路時代已大幅增加，已如前述。如此的改變，造成有心人士盜取、濫用個人資料的誘因大增，再加上資料取得方式十分簡便，使得個人隱私權暴露在極高的危險之中。若不及早因應從法制面著手檢討，遲早會出現問題。

因此，以下本文介紹外國之立法例，作為比較參考。

三、美國電子通訊隱私法（ECPA）關於資料保存之規定

（一）ISP 應保存之資料

[102] 例如欲調閱一人之通訊情況，卻調閱出上千人之通聯紀錄，可能有違狹義比例性原則而有違憲之疑慮。張家豪，通訊監察資訊系統及其相關之科技與法律問題—以第二類電信通聯調閱管理系統為例，國立台北大學資訊管理研究所碩士論文，頁 92(2006)。

[103] 石世豪，「電信自由化下之通訊安全規範的轉型趨勢：通訊秘密、個人資料保護與電信事業的管制變革」，全國律師，2005 年 5 月號，頁 47-48(2005)。

U.S.C. § 2703(c)(1)(C)明訂各種ISP 應保存之客戶基本資料，包括：

1. 姓名。
2. 住址。
3. 電話帳單。
4. 電話號碼及其他客戶號碼或身份。
5. 客戶使用的服務類型與使用時間長短。
6. 付費的方法與來源（包括信用卡號碼與銀行帳戶）。

（二）取得程序

ECPA 第2703 條提供政府機關五種強制揭露的方式，包括：

1. 傳票（subpoena）：可取得的資訊包括客戶基本資料及ECPA 規範範圍以外的資訊。

2. 須先行通知的傳票（subpoena with prior notice to subscriber or customer）：可取得的資訊包括無須傳票即可取得的資訊、RCS 所持有所有電子通訊的內容、任何位於電子通訊系統之電子儲存器超過一百八十天之電子通訊之內容。

3. 法院命令（§2703（d）court order）：可取得的資訊包括無須告知之傳票所可獲得的資訊、除ECS 與RCS 持有之通訊內容外，任何有關客戶之紀錄或其他資訊。法院命令須由聯邦治安法官、地區法院或相等之州法官等，審核政府機關所提供之特定及具體事實，有合理理由足以認為有線或電子通訊之內容、紀錄或資訊，係與現正進行中的犯罪偵查相關時，方可核發（to obtain the order must offer specific and particularly facts establishing reasonable grounds to believe the information to be obtained is both relevant and material to an ongoing criminal investigation）。

4. 須先行通知的法院命令（§2703（d）court order with prior notice to subscriber or customer）：可取得的資訊包括無須告知之法院命令即可獲得的資訊、RCS 所持有之所有通訊內容。亦即除儲存在電子儲存器內且一百八十天未開啟的檔案外，皆可存取。

5. 搜索令狀（search warrant）：執法機關可依聯邦刑事規則第四十一條之規定，本於相當理由，向中立的治安法官聲請核發搜索令狀。可取得的資訊包括：須事先告知之法院命令可獲得的資訊及一百八十天內所有儲存在電子通訊系統之電子儲存器之通訊內容。

（三）分析與說明

由於美國ECPA法制關於儲存資料之取得，包括內容及非內容兩部分(與我國僅規範非內容部份不同)，故若要取得以儲存之內容資料，就須取得搜索令狀（search warrant）或審判命令，即需經過司法審查。而若非係非內容之資料，則只要透過行政命令（administrative subpoena）即可，而美國法上的administrative subpoena極為類似我國之法規命令。

（四）愛國者法案（USA Patriot Act）的修訂

愛國者法案把U.S.C§2703(c)中所列舉的個人資料增加。在U.S.C§2703(c)中，原先只有姓名、住址、使用服務的期間、以及付費的方式等，這些列舉規定適用在網路通訊會產生諸如帳戶名稱、IP 位址可不可以取得的問題，因此愛國者法案增列「(登入)次數以及期間的紀錄」(records of session times and durations)以及「暫時分配的網路位址」 (any temporarily assigned network address)[104]。

這樣的增列讓網路上常用資訊的取得可以有適當的程序規定，含括在這增修規定的資訊包括以撥接或計時制 ADSL 上網時，ISP 隨機提供給予客戶使用的 IP 位址，以及客戶使用的信用卡號碼與銀行帳戶，透過這些資訊與客戶個人資料或其他通訊資料（例如登入所使用的電話），可以更確定受調查人的身份[105]。

四、美國Pen Register與Trap & Trace 裝置

（一） Pen Register與Trap & Trace裝置之定義與用途

1. 206章Pen Register and Trap & Trace Devices之規定

Pen Register 與Trap & Trace 裝置在通訊監察作業中，屬於重要之科技裝備，主要規定在美國法第18 篇犯罪與犯罪程序(Crimes And Criminal Procedure)第206章Pen Register and Trap & Trace Devices，茲將定義分述如下：

Pen Register 之定義為「紀錄或解密電子或其他脈衝之裝置，該電子或其他脈衝能認證該裝置電話線中所傳送之撥號或其他內容，但並不包括任何有線或電子通訊服務提供者或消費者用以製作帳單或附隨帳單紀錄之設備，或任何有線通訊服務提供者或消費者作為日常商業行為中成本會計或其他類似目的之設備」

---

[104] USA Patriot Act §210。

[105] USDOJ, *Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001*, *available at* http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm (last visited Jan 13,2009)。

[106]，Trap & Trace 裝置之定義為「截取進來的電子或其他脈衝之裝置，該電子或其他脈衝能認證傳送有線或電子通訊之器具或設備之來源號碼」[107]。

2. 愛國者法（USA Patriot Act）的修訂

美國愛國者法（USA Patriot Act）將Pen Register與Trap & Trace裝置分別加以修正，擴張其適用範圍，其中將Pen Register 之定義修正為「紀錄或解密由傳送有線或電子通訊之器具或設備所傳送之撥號、路徑、地址或訊號資訊之裝置或過程，然而並不包括通訊內容」；Trap & Trace 裝置之定義修正為「截取進來的電子或其他脈衝之裝置或過程，該電子或其他脈衝能認證由有線或電子通訊器具或設備所傳送之撥號、路徑、地址或訊號資訊，然而並不包括通訊內容」[108]。

原本此二裝置主要目的在於解讀撥出與撥入之電話號碼，但美國愛國者法（USA Patriot Act）修正後之定義，依據字面解釋已不限於電話號碼之範圍，可擴及適用於網路，包括電子郵件、網路瀏覽（Web surfing）與其他型態之電子通訊，雖然有助於未來通訊監察過程中，解讀受監察人網路通訊中有關撥號內容、連結路徑、位置等基礎資料。但是，此與傳統專用於電話系統Pen Register 與Trap & Trace 裝置，其所能擷取之內容超過傳統電話的通聯記錄，已如前述，對於人民權利之侵害較為嚴重。

（二） 規範內容

1. 聲請安裝Pen Register 與Trap & Trace 裝置之程序

檢察官得向有管轄權之法院，請求授權准許Pen Register 或Trap & Trace 裝置之安裝與使用的法院命令（court order）。各州之調查或法律執行官員亦可請求各州法院授權准許此二裝置之安裝與使用。前述聲請書之內容包括聲請機關、執行機關、取得之資訊內容與正在進行調查之本案有關証明[109]。法院開具之令狀內容應記載下列事項：（1）裝置Pen Register 或Trap & Trace 設備之電話線租用者；（2）犯罪調查對象；（3）電話號碼與位置；（4）違法行為之說明。在期間方面，不得逾六十日，得再次聲請，期間亦以六十日為限。擁有或租用線路者，或提供令狀聲請人協助者，在法院開立其他令狀前，必須保密，不得揭露此二設備之安裝使用、被調查電話用戶或其他人之存在[110]。

---

[106] 18 U.S.C. §3127(3)。
[107] 18 U.S.C. §3127(4)。
[108] USA Patriot Act §216。
[109] 18 U.S.C. §3122。
[110] 18 U.S.C. §3123。

2. 愛國者法（USA Patriot Act）的修訂

愛國者法（USA Patriot Act），將前述規定修正如次：（1）檢察官向法院證明Pen Register 或Trap &Trace 裝置使用與安裝所取得之資訊與正在進行之犯罪有關，法院得依據聲請授權在「美國境內任何地方」（anywhere within the United States）使用與安裝此二裝置；（2）州執法機關與調查人員向法院證明此二裝置使用與安裝所取得之資訊與正在進行之犯罪有關，法院得在「該法院管轄權內」授權此二裝置之使用與安裝；（3）執法機關在提供公眾服務之電子通訊服務提供者之封包轉換資料網路（packet-switched data network）上安裝自己Pen Register或Trap & Trace 裝置，此機關須確保相關記錄加以保存，包括（a）安裝設備之官員或任何進入設備中從網路取得資訊之官員；（b）設備安裝與移除之日期與時間，與每一次進入設備取得資訊之期間；（c）設備原始安裝時之結構，與其後對於結構所作之修正；（d）任何從設備中所蒐集之資訊[111]。

修正前述規定之目的，主要在於強化執法機關偵查作為之機動性，不必因為同一案件有不同管轄法院，而必須大費周章向不同法院聲請，修正後之規定，執法人員只要向其中一個法院聲請即可。因此前述美國愛國者法針對法院跨管轄區域開具令狀之問題，讓聯邦法院法官得授權在「美國境內任何地方」（anywhere within the United States）使用與安裝此二裝置。

3. 協助安裝與使用之義務

在協助安裝與使用方面，有線或電子通訊服務提供者、房東、管理人或其他人對於依法安裝使用Pen Register 設備，應立即提供所有的資訊、設備與技術以協助完成安裝；對於法院授權得接收Trap & Trace 設備之政府檢察官或執法人員，應立即協助在合適的線路上安裝Trap & Trace 設備，並應提供任何有關設備之安裝與操作之資訊、設備與技術協助，Trap & Trace 設備所取得之資料應提供給取得法院授權命令之人。對於完成前述安裝與使用義務所需之合理費用，得請求補償[112]。

4. 違法安裝使用之除外規定

任何人在未取得本章第3123條[113]或外國情報通訊監察法之法院令狀，不得安裝或使用Pen Register 或Trap & Trace 裝置，違反者處以一年以下有期徒刑或科或併科罰金。但以下情形則可以安裝與使用：（1）為「有線、電子通訊服務之操作、維持與測試」、「服務提供者財產或權利」、「用戶」等之保護，免於服

[111] USA Patriot Act of 2001 § 216。
[112] 18 U.S.C. §3124。
[113] 18 U.S.C. §3123。

務之濫用與不法使用；（2）為保護服務提供者、為完成有線通訊而提供服務之其他服務者、用戶，免於服務之詐欺、不法與濫用，對於有線、電子通訊之開始與結束之事實加以紀錄；（3）用戶之同意[114]。

5. 緊急安裝與使用

在緊急狀況方面，由檢察總長、代理檢察總長、副檢察總長、助理檢察總長、任何代理助理檢察總長，或任何州、次級政府機關依據州法之主任檢察官所指派之調查人員與執法機關官員，認為有生命、身體之急迫危險或組織犯罪陰謀活動之緊急情況時，得安裝與使用Pen Register 或Trap & Trace 裝置，並於四十八小時內向法院聲請補發令狀。若已取得資訊、聲請遭法院拒絕或已逾前述四十八小時之期間，即應立即停止監察[115]。

五、歐盟「資料保存指令」規範

（一） 發展歷史

1. 個人資料保護指令（Directive 95/46/EC）

1995年歐盟通過了「個人資料保護指令」[116]，本指令首先確立了保護自然人基本人權及自由，尤其是關於其個人資料隱私權保護之立場，該指令明確涵括了員工的個人資訊與客戶的資訊 。基本上，蒐集而來的所有個人資訊都必須加以保護，防止意外或非法破壞、損失、修改，以及未經授權的公開或存取。保護指令之基本原則大致如下：「資料之品質原則」、「資料處理合法原則」、「敏感資料處理原則」及「告知當事人原則」，而資料當事人則有「接觸權利」、「更正刪除或封存個人資料」與「反對權利」。

2. 電信事業個人資料處理及隱私保護指令（Directive 97/66/EC）

1995年個人資料保護指令並未區隔特定行業規範，亦即適用對象並未限制，然由於在此同時數位技術不斷精進且已適用於公眾電信網路（Public Telecommunications Networks），有鑑於新型態電信服務對使用者之個人資料及隱私必須特別予以注意，尤其對整合服務數位網路（Integrated Services Digital Network; ISDN），因此，歐盟即於1997年12月15日制定了1997年「電信事業個人資料處理及隱私保護指令（Directive 97/66/EC）」

[114] 18 U.S.C. §3121。
[115] 18 U.S.C. §3125。
[116] Directive 95/46/EC。

本指令特別強調係適用於在共同體內經由公眾電信網路（Public Telecommunications Services)之公眾電信服務相關之個人資料處理，尤其是經由整合服務數位網路（Intergrated Services Digital Network; ISDN）及公眾數位行動網路（Public Digital Mobile Networks）者。關於本指令，較特殊之議題包括：（1）本指令要求公眾電信服務提供者，應採取適當之技術方法防衛其所提供服務之安全。（2）要求各會員國必須確保公眾電信網路及公眾電信服務之通訊秘密。（3）用戶及使用者之關於通話之記錄應於通話結束時即予消除。（4）必須提供發話之使用者一種免費之方式就個別之通話得除去來話顯示。（5）必須確保任何一位用戶有權停止來自第三者之通話自動轉接。

3. 電子通訊中個人資料處理及隱私保護指令（Directive 2002/58/EC）

歐洲議會與歐盟理事會於2002年7月通過「電子通訊中個人資料處理及隱私保護指令（Directive 2002/58/EC）」，取代了1997年之「電信事業個人資料處理及隱私保護指令」（Directive 97/66/EC），為整個歐盟境內之電子通訊確立新的規範框架。

該指令意識到網際網路進化了傳統市場的結構，其為廣大範圍的電子通訊服務提供一個共同的、全球性的基礎設施。以網際網路提供公眾使用之電子通訊服務，雖一方面為用戶提供一個新可能性，但也同時對其個人資料和隱私產生新的風險，特別是網際網路之個人資料與隱私權的保護之上。對此，針對公共通訊網路，特別是針對日益增強之訂戶和用戶之個人資料自動儲存與處理能力部分，提供法律上的、管制政策上的和技術上之特別規定，以使得自然人基本權利和自由與法人權益能獲得妥善的保護。

該指令，一方面要求要對於個人資料之通訊機密保障，另一方面盡可能僅使用最少個人資料之方案來提供服務。再者，該指令並積極要求會員國、相關服務提供者，與共同體之主管機關，應該共同合作介紹和開發將數位化或原始資料與個人資料處理之利用限制在必要最小範圍之相關技術。又對於防止未經批准之訊息及與之相連接之資料內容的通路與公共通訊網路與公開電子通訊服務所為之訊息傳遞之機密，該指令也要求各會員國應採取一定之保護措施。

（二）個人通訊資料保存指令（Directive 2006/24/EC）

1. 立法目的與適用範圍

（1）本指令的目標為調和各會員國關於公共電子通信服務提供者及關於公共通訊網路產生或傳輸的資料保存責任規定，確保資料可供各國國內法定義下的重大犯罪調查、偵查和起訴目的之利用。

（2）本指令適用在法人及自然人的資料傳輸與位置、可辨認出特定用戶的資料。但不適用於通訊實質內容之保存[117]。

2. 資料保存責任

（1） 若無法達成2002/58/EC 第5、6、9條的要求，會員國應採取措施確保本指令第5條所界定的資料，其保存相符上述法條規定，包含轄區內由公眾電子通信服務提供者或公共通訊網路產生或傳輸的資料。

（2） 前段所述資料保存責任，應包含第5條所界定關於未接來電（unsuccessful call attempts），及由各會員國轄區內公眾電子通信服務提供者或公眾通訊網路產生或傳輸和保存的電話通訊資料或紀錄（logged）的網路資料[118]。

3. 資料取得途徑

會員國應採取必要措施，確保符合本指令的資料只能提供給有權國家機關，且範圍限定特定案件並須符合國家法令。獲得資料或保存資料的過程情況，必須具備必要性且符合比例原則，此必要性與原則各會員國可自行以國家法律定義，但須符合歐盟法令或公開的國際法規，特別是歐洲人權法院（ECHR）的解釋[119]。

4. 資料保存內容

（1） 在本指令下，會員國應確保下列目錄所列資料之保存：

（A） 追蹤或辨別通訊來源必要的資料。

（a）固定網路的電話或手機：

（i） 電話號碼。

（ii）登記用戶名字及地址。

（b） 網路存取、電子郵件及網路電話：

（i） 配置（allocated）的使用者身分。

（ii） 使用者身分及任何通訊登入公共電話網路的號碼。

（iii） 登記用戶名字及IP 位址，同時間通訊的使用者身分或電話號碼。

---

[117] Directive 2006/24/EC ，Article 1。
[118] Directive 2006/24/EC ，Article 3。
[119] Directive 2006/24/EC ，Article 4。

（B） 辨別通訊目的地必要的資料。

（a） 固定網路的電話或手機：

（i） 撥號號碼，在有附加服務（如轉接）的案件中所有號碼。

（ii） 登記用戶名字及地址。

（b） 網路存取、電子郵件及網路電話：

（i） 預期接收網路電話的使用者身分及電話號碼。

（ii） 登記用戶名字及地址及預期接收通訊的使用者身分。

（C） 辨別日期、時間、通訊期間必要的資料。

（a） 固定網路的電話或手機：日期、通訊開始與結束時間。

（b） 網路存取、電子郵件及網路電話：

（i） 特定時區下登入登出網路存取服務日期、時間、浮動或固定IP位址、登記用戶身分。

（ii） 特定時區下登入登出電子郵件或網路電話服務日期、時間。

（D） 辨別通訊類型必要的資料。

（a） 固定網路的電話或手機：使用的電話服務。

（b） 網路存取、電子郵件及網路電話：使用的網路服務。

（E） 辨別使用者通訊設備必要的資料。

（a） 固定網路的電話：電話號碼。

（b） 手機：

（i） 電話號碼。

（ii） 撥號方國際行動用戶識別碼（IMSI）。

（iii） 撥號方國際行動設備識別碼（IMEI）。

（iv） 接收方國際行動用戶識別碼（IMSI）。

（v） 接收方國際行動設備識別碼（IMEI）。

（vi） 在預付匿名服務情況：日期、第一次使用時間、方位。

（c） 網路存取、電子郵件及網路電話：

（i） 撥號方數據機之電話號碼。

（ii） 數位用戶迴路（DSL）或其它原始通訊終端。

（F） 辨別行動通訊設備方位必要的資料。

（a）通訊開始的方位標籤（Cell ID）。

（b）通訊期間參考方位標籤（Cell ID）辨別地理位置的資料。

（2） 涉及通訊內容的資料不能根據此指令保存[120]。

[120] Directive 2006/24/EC，Article 5。

5. 保留期間

會員國應確認第 5 條所定義下的資料,保存期間為自通訊日期起算六個月以上兩年以下[121]。

6. 資料保護與安全

在不違背95/46/EC 與2002/58/EC 指令條款的情況下，每個會員國應確保公眾電子通信服務提供者及公眾通訊網路至少應遵守下列資料安全原則：

（1） 保存的資料應為相同品質，提供如在網路上的安全保護。

（2） 資料應以適當科技和有組織的方式保存，以防意外或非法破壞、意外損失或改變、非法儲存、訴訟、存取或揭露。

（3） 資料應以適當科技和有組織的方式保存，確保只有特定有權機關可存取。

（4） 除了曾被存取並保留的資料以外，保存期間經過後應銷毀[122]。

7. 資料保存的要求

會員國應確保第5條所定義保存資料或其他相關必要訊息，可在必要時傳送給主管機關而無延遲[123]。

8. 監督機關

（1） 每一會員國應委任一個以上的公共管理機構，負責監督關於第7條的資料儲存安全。這些官方管理機構可和95/46/EC 中管理機構相同。

（2） 前段所述管理機構進行監視監督時，應完全獨立[124]。

9. 補救,責任與懲罰

（1） 每個會員國皆應採取必要措施，確保實行 95/46/EC 第三章，提供法律上的補救、責任，遵守 EC 法令的資料處理。

（2） 每個會員國尤其應採取有效、合比例、勸戒的行政罰或刑罰，不允許任何有意違反本指令的資料的傳輸或轉移行為，並加以處罰[125]。

[121] Directive 2006/24/EC，Article 6。
[122] Directive 2006/24/EC，Article 7。
[123] Directive 2006/24/EC，Article 8。
[124] Directive 2006/24/EC，Article 9。
[125] Directive 2006/24/EC，Article 13。

10. 內國法化

（1） 每個會員國應立即的告知相關委員會，最遲應於 2007 年 9 月 15 日前訂立相符此指令的法案。發布立法時應包含或相符此指令。

（2） 會員國與其國會應充分溝通，確定主要法條內文涵蓋本指令的內容。

（3） 每個會員國得暫緩實施本指令關於網路存取、電子郵件及網路電話的通訊資料保存，直到 2009 年 3 月 15 日之前。任一會員國預計使用此段指令前，應通知委員會（council and the Commission）公告，此公告必須刊登在 EU 官方出版刊物（journal）[126]。

（三） Directive 2006/24/EC 適用準則

針對「Directive 2006/24/EC」，Data Protection Working Party 認為此一指令對於資料之處理欠缺充分且特定之保護措施。因此建議各會員國應該採取以下幾項標準，制訂一體適用的八項準則：

1. 目的特定（Purpose Specification）：公權力要求提供個人資料的目的必須特定。指令中「重大犯罪（Serious Crime）」一詞太過含混，應予以釐清。

2. 接觸限制（Access Limitation）：要求提供個人資料的公權力機關應予以特定且必須限於必須因調查、偵查及起訴的機關，並公告周知該等機關的名單給民眾。對於調閱資料之記錄應呈報給監督機關以利有效監督。

3. 資料最低調閱（Data Minimization）：資料調閱必須以最低必要為原則並詳列清單。如有清單異動，應採最低必要原則（Strict Necessity test）檢視。

4. 資料探勘禁止（No Data Mining）：為調查、偵察及起訴犯罪之需所為之資料蒐集不得進行該資料之進一步探勘以維護民眾自由旅行及使用通信的權利不受犯罪嫌疑之影響。

5. 有權接觸機關之司法或獨立檢驗（Judicial/Independent Scrutiny of Authorized Access）：調閱個人資料基本上是屬於個案（Case by Case）審查方式進行，且由特定機關為之並接受監督檢驗。是故，該等機關調閱資料時應詳載特定目的之個案需求及特定範圍資料之調閱。

6. 業者保留資料之目的（Retention Purposes for Providers）：業者在保存客戶資料時，除因應公權力機關之特定需求目的外，不得以其他理由進行客戶資料之不當留存（Retention）。

[126] Directive 2006/24/EC，Article 15。

7. 系統分離（System Separation）：進行因公權力機關需求為目的的客戶資料系統應與業者自行以商業目為資料儲存的系統分離。

8. 安全維護（Security Measures）：指令中應更進一步對於資料留存（Data Retention）的要求做規定，並要求業者對於技術及組織上的安全維護措施訂定依循的最低標準。

六、分析檢討及修正建議

在本章中，我們已經介紹了美國、歐盟以及台灣對網路通聯記錄之保存、取得規定，並指出由於通訊內容與通聯記錄區分，已有模糊化之趨勢，在網路時代，通聯記錄的重要性大幅增加，非傳統通聯記錄的概念可相提並論。故關於網路通聯記錄的保護以及取得程序上，不論在未來修法或立法上，均有重新檢討之必要。故以下即就各議題分項探討。

（一）網路通聯記錄保護之方向

對於非通訊內容的信封資訊以及個人資料，若政府部門或偵查機關有意取得時，究係適用何種法律，遵守何種程序，在學說討論上，已出現不同聲音，詳述如下：

1. 適用傳統關於取得通聯紀錄之規定

不論是台灣、美國以及歐盟的規定，都將非通訊內容的信封資訊以及個人資料，排除於通訊監察範圍之外。歐盟及台灣皆規定依法定程序（依正式公文載明所需資料）取得，美國則規定須取得法院命令（Court order）。但無論如何，皆無通訊監察中的嚴格要求，包括法官保留、重罪原則、補充原則性、最小手段性等等。

如此之規定有其歷史因素。在網際網路發展前，信封資訊及個人資料長期以來都未受到法院及立法者的重視。法院與立法者關心的是對於通訊內容的監察，故對其有嚴密周詳的保護規定。但有關通訊內容以外的資訊，往往規範的密度甚低。例如在郵件通訊中，至今蒐集郵件內容以外的資訊，甚至連法律規範都沒有，而是透過行政命令加以規範。至於有線通訊系統中通話內容以外資訊的保障，則是散見在電信法規及許多施行辦法當中。

然而，在網際網路的發展之下，對於通訊內容以外的資訊，如IP 位址、寄件人與收件人郵件地址，以及個人上網紀錄等，究應適用那些規定，在傳統對於「通訊/非通訊」、「內容/非內容」的思維上，當然將之歸類於類似通聯記錄的分類當中，而排除於通訊監察之範圍。故台灣即將此類資訊規定在「第二類電信事業管理規則」。而美國先前在ECPA 中的Pen/trap 規定並不明確，但司法部及FBI 等政府機關均認為，Pen/trap 的規定除適用於電話系統中，也應擴張網際網路系統，包括電子郵件及網路封包層次[127]。且依學者之觀察，司法實務也暗示同意這樣的看法[128]。例如，洛杉磯地方法院的治安法官Judge James McMahon 在核發法院命令時，曾書面表示雖然這樣的做法與立法者當初的意旨有所出入，但以現在的情況，使用Pen register 命令應該與法律規定相容的（compatible with the term of the stature）[129]。而USA Patriot Act 關於Pen/trap 定義的修訂，更是明確將網路，包括電子郵件、網路瀏覽（Web surfing）與其他型態之電子通訊納入其範圍。

而在實質理由上，網際網路系統中，雖然ISP 每月帳單大多僅記載每月上網費用及上網連線時間，並不會記載使用者所撥打的號碼，但一般使用者在傳送電子郵件時，主觀上應該都知道該電子郵件會先傳送給ISP ，並且，ISP 具有儲存郵件的設備。另外，使用者主觀上也會期待ISP 基於商業目的的考量，可以偶而或定時紀錄郵件資訊，以保存有關詐欺、猥褻之犯罪證據，因此，基於以上理由，網路使用者主觀上應不具有隱私權期待。再者，網際網路系統中使用者所傳送的電子郵件等資訊，也如同電話號碼一樣，會先儲存在ISP 的儲存設備中，因此使用者必須承擔ISP 可能基於商業或防制犯罪的目的，將電子郵件等資料交給執法人員的風險。所以基於上述「風險承擔原則」的法理，即便網路使用者主觀上具有隱私權期待，此種期待也不會被社會所承認。

如此立法發展及解釋的結果，贊成者認為，截取網際網路之信件資訊需依法聲請法院核發法院命令始得執行。以防止執法人員與私人以法律無明文規定為由，任意截取網際網路使用者之信件資訊，以保障個人資訊隱私權。但反對者則擔憂，法院命令具有強制ISP 業者配合執行的效果，使得政府機關不必仰賴ISP 業者自願揭露上開資訊，或以較嚴格的規定，取得法院監察票或搜索令狀，再強制ISP 業者揭露上開資訊，對通訊隱私之保障恐有不周。

2. 適用搜索、扣押之規定

---

[127] *See*USDOJ, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, *available at* http://cybercrime.gov/s&smanual2002.htm (last visited Jan 13,2009)。

[128] *See* Carl S. Kaplan, *Concern over Proposed Changes in Internet Surveillance*, N.Y. TIMES , Sep. 21,2001, at E1。

[129] *See* In re United States of America, Cr. No. 99-2713M（C.D. Cal. Feb. 4, 2000）。

在2001年新修正通過之刑事訴訟法中，新增加了對「電磁記錄」搜索扣押的相關規定，其中第一百二十二條規定電磁記錄得為搜索扣押的客體[130]，而第一百二十八條則把電磁記錄列為搜索票應記載之事項[131]。而電磁紀錄的定義在刑法第十條有加以闡述：「稱電磁紀錄者，謂以電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄。」這樣的規定賦予了搜索電腦取得電磁記錄一個明確的法源依據。

而電信業者所保存的個人資料，解釋上可包含在電磁紀錄的範圍內並無疑義，故若對於電信業者所保存個人資料的取得上，適用搜索扣押的意義在於引進法官保留原則，讓法官決定偵查機關對個人資料的取得，是否具有正當理由，對於人權保障較為周到。

3. 適用通訊保障及監察法之規定

由於我國通訊保障及監察法對於通訊的定義，未如美國電子通訊隱私法明確區分「內容/非內容」的不同，故在解釋上仍有將通聯紀錄及個人資料納入適用通保法保護範圍之空間，適用重罪原則、相關性原則及最小侵害手段性原則，如此對通訊隱私之保護最為嚴密。

4. 小結：合理隱私期待的概念之重新檢討

關於以上這三說，首先，主張適用搜索、扣押之規定的見解，其缺點在於雖然能使法官介入審查，但若電信業者自願放棄其對通聯紀錄的相關權利，則會構成令狀原則的例外，及當事人同意之搜索扣押，而仍無須法官審核。尤其在我國，電信事業經營係採許可制，業者必須相通過審核方可發給營業執照，故相關政府部門在審查作業上，可要求業者必須放棄對於通聯紀錄的相關權利，作為取得執照的前提。如此一來，可輕易架空刑事訴訟法關於搜索扣押之規定，使得通聯記錄的保護回到蠻荒時代，故此說並不可採。

而主張適用通訊保障及監察法之規定的見解，此說雖然可使人民的通訊隱私獲得最完整之保障，但似乎過於前衛，與現有的「內容/非內容」法制架構格格不入，觀諸美國、歐盟的相關規定，亦未採取如此分類。而且如此一來將嚴重衝擊現有的偵查實務架構與運作，本文對此說採保留態度。

---

[130] 刑事訴訟法第一百二十二條：「對於被告或犯罪嫌疑人之身體、物件、電磁紀錄及住宅或其他處所，必要時，得搜索之。對於第三人之身體、物件、電磁紀錄及住宅或其他處所，以有相當理由可信為被告或犯罪嫌疑人或應扣押之物或電磁記錄存在時為限，得搜索之。」

[131] 刑事訴訟法第一百二十八條：「搜索，應用搜索票。搜索票，應記載左列事項：一、案由。二、 應搜索之被告或應扣押之物。但被告或犯罪嫌疑人不明時，得不予記載。三、應加搜索之處所、身體、物件或電磁記錄。」

故本文認為，對於網路個人資料及通聯記錄的保護方向，仍以維持目前法制架構為佳，但由於通聯紀錄與通訊內容的區分已有模糊化的趨勢，再加上網際網路上所保存的資料重要性大增，民眾對於其上網紀錄等個人資料，多半希望保有其秘密隱私，而不願被他人知悉，而不像傳統的通聯記錄一般，無關緊要。故在主觀上民眾對於其個人資料有相當高的隱私期待，政府機關不應忽視。

就算由於網路傳輸的特性，而使得民眾在網路上所有的一舉一動，都可能被記錄下來，亦不可就此認為民眾自願接受可被記錄的上網服務，必須承受資訊被揭露的風險，而無合理客觀的隱私期待，因為我們不能因為科技的進步或發展，而使得個人的隱私權範圍越縮越小。假使上述的「風險承擔原則」成立的話，當有一天科技進步到可以監控所有人在世界上的一舉一動，那政府是否能夠以民眾自願生活在這個科技進步的社會，必須承受所有一舉一動被揭露的風險，而無合理客觀的隱私期待？如此的話，人民將無人權可言。

再者，人民在使用上網服務的時候，未必會認知到自己在網路上的足跡會被揭露之風險，在人民資訊不完整的情況之下，要人民承擔其從未想像過的風險，亦為不公平的作法。

5. 從*Kyllo v. United States* 一案看科技對隱私權的影響

1991年7月份Oregon 州的毒品調查員正著手調查Danny Kyllo 的鄰居Tova Shook ，但在調查期間調查局幹員William Elliot 發現Kyllo 才是犯罪嫌疑人。因為Kyllo 的妻子一個月前方因運輸毒品案件為警方逮捕，且依警方掌握的資訊發現Kyllo 與他的妻子具有栽種大麻的能力，另外經調閱Kyllo 與其鄰居的紀錄後，William Elliot 發現Kyllo 的用電習慣與居住地區用戶明顯不同，因此，William Elliot研判Kyllo 在室內種植大麻。在沒有法院令狀情形下，在1992年7月的某日凌晨三點半到四時左右，由Oregon 州的警官Daniel Hass 在住宅外的偵防車上使用「熱能顯示器」（thermal imaging device）掃描Kyllo 的住宅內部。機器顯示Kyllo 住宅車庫的屋頂及一面牆的溫度有異常的熱能，另外Kyllo 住宅的溫度也比鄰近住宅溫度高出許多。William Elliot 確信Kyllo 應在室內裝設許多燈具代替日光種植大麻，隨即以熱能顯示器蒐集到的資訊向治安法官聲請搜索令狀，搜查後確實發現住宅內有種植一百株以上的大麻。之後Kyllo 被控觸犯U.S.C.§841（a）（1）的製造毒品罪，由於無法排除搜索所得的證據，Kyllo 乃主張有條件的有罪抗辯。

地方法院與上訴法院均否定本案構成憲法第四修正案的搜索，理由為：（1）熱能顯示器不是一個侵入性的工具，因為它沒有發出任何光線或電波，也沒有顯示住宅內部的原始景像，更沒有顯示住宅內任何人類活動、通訊，故本裝置沒有

觀察到住宅內的任何私密活動（intimate details）。因此，本案法院核發之令狀係屬合法，所得證據不需排除。（2）依據*Katz* 案的見解，原告Kyllo 主觀上並沒有隱私期待，因為他沒有嘗試隱藏從住宅內散發出的熱能，即便Kyllo 主觀上有此期待存在，客觀上此期待也不認為是合理的，因為熱能顯示器至多只是顯示屋頂及外牆上的無形熱點（amorphous hot spots），並沒有曝露原告生活的任何私密活動[132]。

聯邦最高法院以5:4通過的多數意見，推翻了下級法院的見解，認為本案執法人員使用熱能顯示器來蒐集資訊構成憲法第四修正案的搜索，因此，本案在未取得法院令狀即對被告Kyllo 住宅所做的掃描（scan），推定為違憲[133]。由Scalia大法官主筆的法院多數意見首先強調「住宅」（home）在第四修正案中的特殊重要性，認為依據先前*Silverman v. United States*案[134]與*Illinois v. Rodriguez*案[135]一貫見解，除了少數例外情形之外，對於住宅的無令狀搜索都推定為不合理搜索，應屬違憲。最高法院緊接重申*Katz*案的合理隱私期待原則在住宅搜索仍有適用餘地，認為即便是住宅內搜索，如果個人無法證明其主觀上具有隱私期待，且此期待客觀上是合理的時候，則仍未構成憲法上的搜索[136]。

不過，法院也注意到科技的進步確實使得憲法第四修正案所保障的隱私權範圍逐漸縮小。因此，今日我們所要面對的課題乃是對於這些縮減隱私範圍的新興科技，有何限制。法院認為*Katz* 案的標準仍然可以運用在本案事實，亦即住宅內部的搜索，乃是承認隱私權保障的典型（prototypical），從普通法時期的起源起至今均承認此時應有最小程度（minimal）的隱私期待存在，而且此期待應認為係屬合理的。如果抽回個人此最小程度的期待，將間接鼓勵執法人員透過科技方法減少第四修正案保障的隱私權。因此，任何藉由加強感官功能（sense-enhancing）的科技設備，而沒有以進入住宅等方式，就可以從住宅外部蒐集住宅內的資訊時，應構成憲法上的搜索。至少在本案而言，此種科技設備也不是公眾可普遍使用的（is not in general public use）。

政府機關雖主張本案只是從住宅外部「偵測」（detect）而已，沒有搜索可言，但最高法院反對以此機械化的方法解釋*Katz*案的標準，認為這樣將使得住宅所有人成為科技進步的犧牲品。法院並且認為對住宅的保護，並不因所蒐集資訊的數量或品質而有所不同，事實上，住宅內的所有活動都是私密活動，因為住宅內的所有區域是隔絕政府監視的安全地帶。因此，本案所測得的熱能，也屬於住宅內的私密活動。

---

[132] 190 F.3d 1041（9th Cir. 1999）。
[133] Kyllo v. United States, 533 U.S. 27, at33（2001）。
[134] 365 U.S. 505, at 511（1961）。
[135] 479 U.S. 177, at 181（1990）。
[136] California v. Ciraolo, 476 U.S. 207, at 211（1986）。

故美國聯邦最高法院認為，科技的進步雖然可能使個人隱私權範圍逐漸縮小，但仍應保有最小程度的隱私期待存在，而非被鯨吞蠶食，最後收縮至零。而在本案中，住宅內活動的隱私，為人民隱私權的核心領域，無論如何都不可侵犯。這樣的概念，或許可以適用到網際網路時代對於通聯記錄的保護上。也就是說，電信業者固然有能力蒐集所有用戶在網路上的一切行為，但並不能代表用戶即無隱私權之存在，而是仍應保有最小程度的隱私期待，即隱私權的核心領域，方符合人權保障的意旨。

6. 結論

雖然本文認為對於網路個人資料及通聯記錄的保護方向，仍應維持目前法制架構，但對於網路個人資料及通聯記錄，民眾仍有其通訊隱私之合理期待存在，雖然此種的隱私期待不若通訊內容的隱私期待來的強烈，但仍有一定的強度，而目前我國對於資料保存的強度，係建立在個人資料無隱私期待的前提之上，顯然未達應有的保護標準，有需要做相關的修正與加強。

(二) 網路通聯記錄保存法制修正之方向

1. 資料保存分類

與傳統電話服務不同，網路服務項目多樣化且極其煩雜。對於犯罪偵查項目勢必比傳統電話監察項目資料多元，但基於憲法保障個人隱私權與通訊自由，在比例原則考量下，執法機關應本最低隱私權侵害與通訊自由保障前提下，僅就犯罪偵防所需之監察項目資料訂定標準，不應無限擴大監察項目資料。依據歐盟「資料保存指令」，用來識別發話者與受話者所必須的資料，在資料保存內容部分，依其保存項目之不同，主要分為6大類，可以作為訂定我國執法機關選擇制定之監察資料範圍的參考。

2. 保存期限屆至後處理方式

我國目前僅規範電信業者保存之義務，與歐盟規範比較不同處，我國並未要求業者在保存期限屆至後，應將資料去名化或刪除之作法，歐盟「資料保存指令」要求保存期限屆至後，除非有特殊原因，各會員國必須要求其國內之業者將所保存之資料立即銷毀，以確保資料安全並保障人民之隱私不受侵害。

3. 對於業者資料保護義務的要求

歐盟國家在思考資料保存之議題時，同時也思考到人權與資料保護之議題，值得我國未來進行法律修正時之參考。為避免保存之資料因不慎外洩或遭不當利用，而造成人民隱私的重大侵害，在歐盟「資料保存指令」中，特別在第7條要求被保存資料的保護等級，應等同於資料傳輸時的保護，並應避免受保存之資料遭到因故意或過失所造成遺失、破壞或刪除。我國可參酌有關這方面上的保護規定，使通訊自由與隱私權的保障上更趨完整。

4. 罰則的制定

對於為遵守資料保存義務，或是無故洩漏、破壞或刪除資料的行為，可依其情節輕重，制定適當的行政罰或是刑罰，以明確嚇阻不法行為，保護個人資料。

5. 建置獨立的監督單位

為確保資料得以妥善保存不受侵害，歐盟「資料保存指令」要求各會員國應明確指定相關單位負責監督資料保存與運用之情形，且僅得為有法律授權之使用者所使用。若有非經法律允許而故意使用或交換受保存之資料者，各國應制定有效且合適的刑罰，以嚇阻惡意或不當利用或儲存之行為。

陸、電信業者的通訊監察協助義務與經費負擔

一、前言

關於通訊監察的主要爭議與問題，大多集中於人權保障與犯罪偵查之衝突，議題不外乎就是如何不偏廢一方，而取得兩者之平衡。整個通訊監察法制，幾乎就是人權保障與公權力實行之間互相牽制、彼此拉鋸的最佳示範。但由於通訊監察之執行，需要電信業者之配合，即電信業者之協力義務。而此一因素之加入，使得通訊監察的戰場已非兩雄對峙，而變成戰國時代，此一情形在二類電信開放之後尤為明顯，因此，由協力義務衍伸出的電信管制、科技創新、社會義務等等問題，已將議題層次拉高到國家政策與發展之等級，而非任一政府部門或機關能夠掌控全局，且關於國家政策之發展，有高度政治性格，通常很難有絕對的是非對錯，而取決於決策者之價值判斷及政策走向，非單純的技術或是法律問題。

此外，第二類電信事業關於網路通訊服務的發展，仍在起步當中，其中對於通訊監察設備的建置，當然還在試驗階段，究竟業者能夠配合到什麼地步，都在協調測試當中。縱使已有些協商成果，也不會對外公開，局外人無從得知。這也使得至今關於協力義務的討論，皆只有質疑跟爭議，而未能看到切確的結論。

而協助通訊監察屬於配合國家公共安全政策所需的作為，對電信事業本身的業務經營並沒有加值的作用，就業者而言，可說是累贅及負擔。此一配合通訊監察之義務，究係屬於第二類電信業者之社會義務，或已逾越其範圍，而成為「特別犧牲」，亦有爭議。而此一爭議亦影響到執照之核發，以及評估或決定網路電話開放配號、雙向互通，是否能以網路電話服務的通訊監察措施已規畫完善作為先決條件。再者，建置相關設備之成本及執行通訊監察之經費，亦與此一爭議息息相關。

若從公共安全及保護用戶通訊安全的角度出發，治安單位對於通訊監察的有效掌握卻又是不可小覷的重要環節，因此雖然電信事業「是否具備協助政府單位進行通訊監察的能力」無關乎電信事業經營業務是否具有競爭力、能否提供用戶品質更好、效益更高的服務，但在各項電信法規中仍然要求電信事業有義務配合經合法授權之政府機關進行通訊監察，並且要求確定電信事業有能力提供通訊監察所需的設備及系統。

而以往要求第一類電信業者具備配合通訊監察之能力，並無太大問題。因為我國對於第一類電信之執照採取特許制，使得取得執照之業者家數少，資本雄厚，對於通訊監察設備之建置，不論在資金或技術上，皆綽綽有餘。且我國對於第一類電信事業的嚴格管制，係基於電信普及服務的重大公益，故每一業者皆負

有較重的社會義務，此一義務在解釋上亦包含犯罪防治義務，與通訊監察的協力義務可說不謀而合。故國家在要求第一類電信業者配合通訊監察時，可說名正言順。

但網路電話業務在面臨到適用通訊監察相關規定時，由於第二類電信事業與第一類電信事業規模差異大的緣故，業界也產生了很多對於配合通訊監察義務「力不從心」的困境，尤其是配合執行通訊監察義務相關的規定中所提到必須建置通訊監察系統，此處的系統建置經費來源問題最是讓業者擔心，同時也是目前網路電話服務通訊監察系統尚未實際落實在業界的主要因素之一。

二、我國法制關於協助執行通訊監察義務之規定

（一） 設備建置義務

1. 傳輸至法院管理系統之設備建置義務

通訊保障及監察法施行細則二十二條規定：「為監督執行機關執行情形，司法院於必要時，得提出需求，由電信事業設置能立即自動傳輸行動電信通訊監察上線及下線資訊之設備，即時將有關第二十條第二項前段全部行動通訊監察上線及下線資訊，以專線或其他保密方式，傳輸至台灣高等法院通訊監察管理系統。行動以外電信有關前項通訊監察上線及下線資訊，電信事業應即時以專線或其他保密方式，傳輸至台灣高等法院通訊監察管理系統。」

2. 與建置機關「協商」與「建置計畫提出」義務

通訊保障及監察法施行細則二十六條第四項規定：「第一類電信事業新設、新增或擴充通訊系統者，為確認其通訊系統具有配合執行監察之功能，應由法務部調查局或內政部警政署提出監察需求，該電信事業盡速擬定應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，經法務部調查局或內政部警政署與該電信事業協調確定後，由國家通訊傳播委員會核發建（架）設許可證（函）後辦理建置，並經國家通訊傳播委員會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。」同條第四項規定：「第二類電信事業須設置通訊監察設備之業務種類，由國家通訊傳播委員會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。」

3. 審驗許可之必備文件

第二類電信事業管理規則第七條第一項第七款規定：「依通訊保障及監察法令規定應設置通訊監察設備之經營者，須附經通訊監察執行機關協商確定建置通訊監察系統或設備之證明文件。」

4. 通訊監察系統維持義務

通保法第十四條第四項規定：「電信事業之通訊系統應具有配合執行監察之功能，並負有協助建置機關建置、維持通訊監察系統之義務。但以符合建置時之科技及經濟上合理性為限，並不得逾越期待可能性。」

5. 場地提供義務

通訊保障及監察法施行細則二十六條第一項規定：「本法第十四條第二項所稱協助執行通訊監察之義務，指電信事業及郵政事業應使其通訊系統之軟硬體設備具有配合執行通訊監察時所需之功能，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。」

（二） 特定功能具備義務

通保法第十四條第二項規定：「電信事業及郵政事業有協助執行通訊監察之義務；其協助內容為執行機關得使用該事業之通訊監察相關設施與其人員之協助。」同條第四項規定：「電信事業之通訊系統應具有配合執行監察之功能，並負有協助建置機關建置、維持通訊監察系統之義務。但以符合建置時之科技及經濟上合理性為限，並不得逾越期待可能性。」

（三） 「第二類電信事業管理規則」修正新增通訊監察需求

2005年11月15日修正公佈之「第二類電信事業管理規則」當中，將「施行細則」第二十一條對電信事業建置通訊監察設備的要求統整後納入。「第二類電信事業管理規則」中規定業者欲申請經營第二類電信事業時，需檢具申請書、事業計畫書及相關文件申請許可。而根據增修的條文，業者所應檢具之計畫書內容新增一款：需載明「依通訊保障及監察法令規定須設置通訊監察設備之經營者，須附經通訊監察執行機關同意之通訊監察系統功能之建置計畫。」另外，如業者申請經營特殊業務之網路電話服務或語音單純轉售業務，由於此二者屬「依通訊保障及監察法令規定須設置通訊監察設備之經營者」，在取得許可函起六個月內尚

需檢附「經通訊監察執行機關協商確定建置通訊監察系統或設備之證明文件」與其它相關文件送主管機關申請審驗，經審驗合格後，發給許可執照與系統架構圖允其正式經營；而經營者待取得許可執照開始經營後，若欲新增或擴充原有之通訊系統而需變更計畫書內之系統架構，必須檢附「通訊監察執行機關同意之通訊監察系統功能建置計畫及其同意函」，向電信總局申請許可後辦理建置，建置完成後再依循先前申請許可執照的程序，附上各項必備之文件向主管機關申請審驗。

由「通訊保障及監察法施行細則」與「第二類電電信事業管理規則」修正的內容可以看出，為了配合2004年7月已公布的應設置通訊監察設備之第二類電信事業業務種類，確保公告範圍中的電信事業經營者，都能配合通訊監察的需要而架設必要的系統或設備；同時也正好配合網路電話服務開放過程中，一連串的法規配套措施修正，對於電信事業協助通訊監察義務的規範方向是將「取得通訊監察執行機關“對事業之通訊監察系統所應具備功能”的認可」明文規定，成為第二類電信事業通訊系統營運的先決條件之一，不論是新申請事業或是新增變更事業之系統架構，於新設或變更前，除了必須規畫或完成與經營相關的通訊系統以及各項相關的文件之外，凡是歸類在「需設置通訊監察設備」的業務種類也同時必須提出通訊監察系統計畫或建置文件，證明已經與調查局及警政署協調過建置通訊監察設備的事宜，而且該事業所提出的軟硬體設備、建置時程及費用之建置計畫，必須是符合調查局與警政署所提出之通訊監察需求，方能獲得此二機關之同意，並給予所需的同意書等證明文件。

（四）「與監察執行機關協調建置通訊監察設備」之法律性質

雖然通訊保障及監察法明定電信事業協助執行通訊監察之義務，但具體建置、實施之細節，涉及技術規格及偵查需求，縱使通訊保障及監察法實施細則有較詳細之規定，但僅憑藉該施行細則仍不足以完成協助義務之實際內容，且各家業者營運情況各異，有必要針對個案做不同的調整。故此部份有賴偵查機關與電信業者雙方之協調。

而此「協調」之性質究係為何？就實際情況而言，業者與偵查機關對於建置計畫、經費負擔等事項具體協商，互相折衝調整，雙方地位對等，且互負權利義務（業者負建置義務，偵查機關負費用義務），其性質顯然非行政法上「行政機關就公法上具體事件所為之決定，或其他公權力措施而對外直接發生法律效果之單方行政行為」，即所謂行政處分，而較類似於契約之概念。

而此一契約為行政（公法）契約或是私法契約？依據學界通說，關於行政契約和私法契約的區分標準，採取「契約標的與契約目的混合說」，即行政契約與私法契約之區別究應以契約標的或目的為判別標準，原則以契約之標的為尺度，但無法解決時則兼採契約之目的加以衡量，並另參酌下列契約之條款作綜合判斷：一、協議一方為行政機關。二、協議之內容係行政機關之一方負有作成行政處分或高權之事實行為。三、代替行政處分之協議。四、涉及人民之權利義務之關係。五、契約之條款有偏袒行政機關之條款[137]。

而契約標的為私法關係或是公法關係的區分理論，依據通說為「新主體說」[138]，即以法規之對任何人皆可適用，而發生權利義務之關係者為為私法；而公法則限公權力主體或機關所執行之職務法規，其賦予之權限或課予之義務則限上開公權力主體或機關，而非任何人。如刑法係司法機關所執行審判之依據為公法；民法則為任何人皆可適用，發生之權利義務關係為私法。

依據此判斷標準，偵查機關與電信業者之建置契約，其契約標的為配合通訊監察之協力義務，而此協力義務，適用之一方為國家公權力機關，非任何人皆可適用，依據「新主體說」，應為公法關係。若再觀諸其契約目的，為配合偵查機關追訴犯罪，係國家重大公益，為公法關係應無疑義。故偵查機關與電信業者之建置契約應為行政契約。

而確認其為行政契約之實益在於，雙方在協商的過程中擁有較大的形成自由空間，對於法律未規定或僅有蓋括規定之事項，可依據個案情況、視業者規模大小及執行機關需求，做適度調整，而不需僵硬的適用法律。

但此一建置契約仍必須遵守行政程序法關於行政契約之規定，尤須注意行政程序法第一百三十七條：「行政機關與人民締結行政契約，互負給付義務者，應符合下列各款之規定：一、契約中應約定人民給付之特定用途。二、人民之給付有助於行政機關執行其職務。三、人民之給付與行政機關之給付應相當，並具有正當合理之關聯。行政處分之作成，行政機關無裁量權時，代替該行政處分之行政契約所約定之人民給付，以依第九十三條第一項規定得為附款者為限。第一項契約應載明人民給付之特定用途及僅供該特定用途使用之意旨。」以及第一百四十六條關於行政機關單方調整或終止契約之權利：「行政契約當事人之一方為人民者，行政機關為防止或除去對公益之重大危害，得於必要範圍內調整契約內容或終止契約。前項之調整或終止，非補償相對人因此所受之財產上損失，不得為之。第一項之調整或終止及第二項補償之決定，應以書面敘明理由為之。相對人對第一項之調整難為履行者，得以書面敘明理由終止契約。相對人對第二項補償

[137] 吳庚，行政法之理論與實用，頁 423(2003)。
[138] 前揭註 139，頁 28-30。

金額不同意時，得向行政法院提起給付訴訟。」第一百四十七條關於情事變更後契約之調整或終止：「行政契約締結後，因有情事重大變更，非當時所得預料，而依原約定顯失公平者，當事人之一方得請求他方適當調整契約內容。如不能調整，得終止契約。前項情形，行政契約當事人之一方為人民時，行政機關為維護公益，得於補償相對人之損失後，命其繼續履行原約定之義務。第一項之請求調整或終止與第二項補償之決定，應以書面敘明理由為之。相對人對第二項補償金額不同意時，得向行政法院提起給付訴訟。」等規定。

三、對第二類電信服務業者的衝擊

雖然「通訊保障及監察法」與「施行細則」中對於第二類電信事業應負的協助執行義務與第一類電信事業並無不同，「第二類電信事業管理規則」新增條文亦只是將配合通訊監察的義務加以明文，沒有增加更高標準的管理規定，但是已經在網路電話服務的經營者之間引起不少的疑慮與緊張，一來擔心將建置通訊監察系統的計畫納入申請執照的審查條件之後，可能影響到網路電話業者取得許可執照的難易；另外由於實際建置通訊監察系統所費不貲，多半為中小型事業的第二類電信事業是否有能力建置也是業者心中的一項隱憂。

（一）許可執照之取得

我國自2001年7月開放第二類電信事業網路電話服務業務後，直到2004年7月經公告，將與固網、行動通訊互通的網路電話服務規範為需設置通訊監察系統的業務種類之一，使得網路電話業務與第一類電信事業一樣，必須依照「施行細則」的規定，負擔程度相當的協助執行通訊監察義務。以「施行細則」及「第二類電信事業管理辦法」修正的內容來看，網路電話服務經營者擔心目前面臨「必須先完成具可行性的通訊監察建置計畫，否則無法取得許可執照」的問題。

通訊保障及監察法施行細則草案於1999年7月推出時，類似的情況也發生在第一類電信事業身上。法務部所呈報行政院的施行細則草案中，採行警政署的提案，強制電信事業必須先配合建置通訊監察所需設備或系統，否則電信總局將不核發特許執照。此舉引起電信業者強烈的反彈，而交通部也認為應將「發照」與「建置通訊監察系統」兩者分開，對於不配合建置通訊監察系統的業者可以按通訊保障及監察法第三十一條由交通部處以五十萬元以上、二百五十萬元以下罰鍰及必要時撤銷執照等方式加以處罰，以此方式取代法務部採行的提案，交通部的意見於法務部呈報時納為附帶意見，併送行政院加以參考。

因此在 2000年3月15日正式發布的施行細則中，以「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。」規範電信事業配合通訊監察系統之義務，雖然仍顯示出要求電信事業於開始營運之時，通訊監察系統必須也已經建置完成，但已無「事業必須完成通訊監察系統建置，否則不發給執照」等尖銳字眼。

在第二類電信事業管理規則的修正公布之前，網路電話服務經營者多十分擔心出現強制業者進行通訊監察系統建置、或以「通訊監察設備的完成與否」做為核發執照之依據的規定。但分析修正內容：網路電話服務業者於提出申請之時就必須提交得到通訊監察執行機關同意之通訊監察系統建置計畫書，以待取得許可函後於六個月內再度與通訊監察執行機關協商「確定建置通訊監察系統設備」，最後才能經過審核取得許可執照。由於修正條文中要求電信事業於新設時做到的通訊監察建置程度，僅及於提出計畫書和提出確定建置之證明文件，尚未到達施行細則中所規定「於其通訊系統開始運作時同時協助執行通訊監察」—業者開始營運時亦必須做到已完成通訊監察系統的程度，因此可認為新增條文的範圍並沒有超越施行細則中的內容。

雖然第二類電信事業管理規則修正沒有超出施行細則規定的範圍，但適用法規時仍必須符合通訊保障及監察法以及施行細則的規定，因此網路電話服務經營者仍不能免除「於其通訊系統開始運作時同時協助執行通訊監察」的義務。

（二）市場進入之障礙

從傳統電話與網路電話所使用之技術上思考，傳統電話利用PSTN 網路及線路交換技術，屬於傳統電信市場之架構，其特徵為應用層至基礎網路層之垂直整合，語音傳輸服務植基於PSTN 網路之建設而無從分割，故傳統電話業者必須投入大量的沈沒成本，建設實體線路以供語音服務使用。而網路電話則是利用網際網路及封包交換技術，其特徵為水平分層，基礎網路並非專供網路電話使用，網路電話服務業者僅為網路上眾多應用服務之一[139]。從我國區分第一類、第二類電信事業而區分高低管制密度之差異對比之下，給予傳統電話業者比網路電話業者更多的管制與義務，似乎有其正當性。

而以設備之建置作為核發VoIP執照與否之市場進入門檻，其妥適性容有討論之處。首先必須釐清的是兩者連結之合理關連性是否正當，更明確的說，以便於執行通訊監察為理由，要求電信業者依照特定技術或標準建置電信設備，並對

[139] 李志仁，「電信資訊匯流下之法律爭議—以 Skype 為例」，科技法律透析，第 18 卷 12 期，頁 48-49(2006)。

不遵守者課予處罰，手段上是否過度干預私經濟部門之行為自由，而不當製造了市場進入障礙[140]？

因此，我們應考慮VoIP服務為二類電信事業，傳統上以服務導向、競爭導向為主之中小企業為主，但通訊監察設備之建置所費不貲，此等負擔已對中小型業者構成實質的市場進入障礙，造成在此一制度下，似乎惟有具備雄厚資本額之業者才「實質適格」於核配號碼網路電話服務之經營，可能使得二類電信市場走向一類電信市場之回頭路，成為獨占或寡佔之市場，與目前鬆綁的管制方向背道而馳。

故雖然通訊監察基於保障國家公共安全有其必要性，但探究目前適用於網路電話事業通訊監察法規時，卻發現許多值得爭議之處：通訊監察機關扛著保障公共安全的大旗，除了限縮民眾秘密通訊的權利不論，事實上也增加電信事業經營者法律上的義務，進而增加營業的負擔，與「電信法」中對第二類電信事業減少法律限制負擔、採取低度管制、開放競爭的原則有所扞格。

（三）對網路電話與其它第二類電信事業的差別待遇

我國現行網路電話服務市場上經營者眾多，但規模大小不一，有資本額超過上億元者，也有少於百萬元者，都同時被賦予協助執行通訊監察的義務。除了設置通訊監察系統的成本可能造成規模大小不同的網路電話經營者不同程度的負擔之外，網路電話應配合協助通訊監察的這項法律義務規定，將屬於第二類電信事業中業務之一的網路電話，套上屬於第一類電信事業的枷鎖；在強調對第二類電信事業採開放競爭、減少管制與負擔的同時，卻又給予網路電話服務、語音單純轉售及電子郵件服務與其餘的二類電信業務不同的對待。如此一來，可能造成政府政策對於網路通訊服務之歧視，造成實質上對於網路通訊服務產業之不支持。

（四）對VoIP 產業發展及科技創新之影響

1. VoIP 產業發展與法規管制密度

美國聯邦通訊委員會曾於2003年12月1日邀集網路電話專家及數州負責規制業務的官員，舉行聽證。在會中各方達成為保護此一新興行業，對於公共安全、法律執行等議題均以不予過度負擔為共識。

[140] 劉靜怡，「當法律成為全民公敵？數位時代隱私焦慮之分析」，收錄於監察法 vs.隱私權—全民公敵，傳播與法律系列研討會（七），政大傳播學院研究暨發展中心與理律法律事務所發行，頁 159-166。

隨著科技日新月異，對於資訊技術的發展相較於過去已不可同日而語，過去傳統電話線路僅為點對點固定傳輸路徑，相對顯得網路監察難度實屬不易，隨著VoIP 以及E-mail 的流行，此類問題已儼然成為國際上重要議題。荷蘭議會上議院於1998年4月通過一法律修正案，明確規定電信業者必須支援政府單位通訊監察相關功能機制，否則將撤銷該業者的電信服務經營權。英國的NCIS 也於1997年提出要求立法允許警政單位可攔截E-mail 進行通訊監察。

由於網路電話與傳統電話的基礎架構不同，網路電話還具備多重服務供應商的問題，因此誰有何種應盡的CALEA 法律義務在此規範中仍然沒有很明確的定義。

另外，網路服務型態與軟體科技的發展日新月異，例如網路電話服務Skype如今已經不再是美國聯邦通訊委員會（FCC）定義的純粹網際網路電話，將來還要計畫支援接收固網電話或行動電話的功能，這樣一來，就有可能被迫承擔各種義務，對其施加之法律責任將影響其技術發展與經營型態，也牽動到服務的收費方式。

參議院商務委員會成員對於是否在剛發展起來中的VoIP產業上施以這麼重的執法規定感到疑慮，聯邦通訊委員會（FCC）後續將再更明確地規範，何種規模的寬頻網路或網路電話服務業者必須在此規範內。

2. 通訊監察義務對研發創新之阻礙

FCC 前主席Michael Powell 曾呼籲，對網路電話產業之過度管制，可能阻礙產業創新之可能性[141]，因為要求網路電話業者配合協助建置通訊監察設備，可能過度增加業者之成本，在資本有限的情況下，部分用於研發創新的資金必須移做建置通訊監察設備之用，付出網路電話產業減少科技創新、發展遲緩之代價[142]，且最終該成本終究會轉嫁到消費者身上，形成由使用者支付費用讓執法機關監控使用者的弔詭情形。學者Lawrence Lessig 亦認為，網路電話業者身為一個羽翼未豐之新興產業，需要的發展空間遠較管制為重要，若使網路電話業者花在思考如何配合管制的時間與配合成本（compliance cost）壓縮了研發創新的空間，絕非正確的選擇[143]。

---

[141] *See* R.Alex DuFour, *Voice over Internet Protocol: Ending Uncertainty and Promoting Innovation through a Regulatory Framework*, 13 COMMLAW CONSPECTUS at 504 (2005)。

[142] Robert D. Atkinson, *Internet Telephone Service-A New Era of Competition in Telecommunications*,PPI Policy report,13, http://www.ndol.org/documents/VoIP.pdf (lastlast visited Jan.4,2009)。

[143] Lawrence Lessig, *Wire-tapping VoIP*, http://lessig.org/blog/2004/08/wiretapping_voip.html (last visited Jan. 4,2009)。

（五） 小結：社會管制與經濟管制之衝突

1. 經濟管制趨向放寬

經濟管制（economic regulation）是指在市場經濟體制之基礎下，基於保障特定公共利益與提高效率等原因，以公權力介入替代私營事業之部分決策，並以價格、競爭、市場進入或退出為手段，針對特定市場之不足，對市場決策直接干預，以促進公共利益之實現[144]。

而我國「電信法」將電信事業分為二大類別，並且針對此二類電信事業給予不同程度的管制：第一類電信事業因為所經營內容屬於重要的民生基礎通信事業，並且必須建置及維護大量的硬體設施與電信線路，為了保障這些基礎設施的完整與有效使用，因此對其經營者課以較多的法規義務；而第二類電信事業原本屬於附加在基礎線路上的加值性服務，本身並不負責建置或鋪設電信線路，因此沒有必要以第一類電信事業的標準來加以規範，復又為了促進其蓬勃開放和發展而盡量減少法律對它的干預。因此簡單的來說，我國對第一類電信事業的管理及經營門檻限制較為嚴格，而第二類電信事業則相對寬鬆許多。

2. 社會管制負擔偏重

政府課與社會管制（social regulation）之目的，在於重要社會政策諸如國民健康、安全、環境保護、消費者保護及社會諧和等之促進與實現。由於經濟管制之目標為競爭之促進，通常無法達成社會管制目標，甚至升高了與社會政策目的相違背狀態之風險。社會管制係以社會正義與重要社會政策之保護為考量，以管制之手段要求特定業者應為或不應為一定行為，以導正經濟活動所造成之副作用及外部性（externality），故又稱為保護性管制（protective regulation）[145]。通常社會管制並非針對特定產業而發，而係針對特定社會議題進行跨產業之管制，但在管制方式及管制密度上，仍會依照產業之特性作局部的調整。

而在第二類電信事業的社會管制上，最明顯且影響層面最大的就屬通訊監察之協力義務，國家基於犯罪偵查及社會安全之考量，要求第二類電信業者必須建置通訊監察設備以及協助執行通訊監察，具有社會管制的正當目的。

3. 兩種管制目的之調和

---

[144] 張玉山、李淳，「公用事業管制革新與管制組織的重新定位—以電力事業為例」，管制革新，劉孔中、施俊吉主編，頁 256-257(2001)。

[145] 陳櫻琴，「管制革新之法律基礎與政策調適」，管制革新，劉孔中、施俊吉主編，頁 24(2001)。

由以上討論可知，我們基於產業、經濟之目的，希望第二類電信業者能夠蓬勃發展，因而開放競爭，採取低度管制政策。但又為了社會安全之目的，課予網路通訊服務業者較重之配合通訊監察義務，但此一義務亦同時造成許多負面效果，例如市場進入之障礙、創新發展之遲緩等影響，造成社會管制與經濟管制之衝突。

但國家不可能因為配合通訊監察義務所帶來的負面效果，就對業者免除社會管制，在犯罪偵查上全面棄守，否則社會安全的漏洞將難以想像。故最理想的方法仍是找出兩種不同管制目的之間的平衡點，希望能兼顧社會安全，又不至於妨礙第二類電信產業發展。當然，此依問題茲事體大，有賴不同單位協調配合，固以下僅就配合通訊監察義務之中，業者應享有較大自主空間的部份，在不致影響通訊監察制度運作的前提之下，提供較折衷及鬆綁之建議：

（1）政府鼓勵建立產業標準之機制

在美國，為確保協助法律機關執行通訊監察之有效性與產業的全面化，檢察總長需協調聯邦、州、地方執法機關與通訊產業協會、標準設定組織、系統製造商與通訊支援服務提供者等進行諮商。通訊業者、系統製造商與通訊支援服務提供者必須遵守通訊產業協會、標準設定組織所制定之標準，或符合CALEA 第1006條（b）項規定聯邦通訊委員會（FCC）所訂定之標準，方屬符合本法第1002條有關協助通訊能力之規定，此即「安全港」（Safe harbor）條款。

即使尚未制定相關技術規定與標準，也不能排除通訊業者、系統製造商與通訊支援服務提供者應負責任與義務。如果通訊產業協會、標準設定組織並未制定相關標準，或是雖然有制定相關標準，但是其標準不足或有缺點，則政府機關或個人能請求聯邦通訊委員會（FCC）建立技術之要求與標準，其所建立之技術要求與標準，必須要以最具成本效益之方法達成第1002 條之需求，能保護通訊之隱私與安全，免於不法之侵害或截聽，減少納稅人的花費，達成國家鼓勵科技發展的政策，並訂定合理的時間與標準，使相關配合單位得以達成此一要求。基本上聯邦通訊委員會（FCC）建立技術之要求與標準僅具有補充性，仍應以通訊產業協會、標準設定組織所制定之標準為優先。

（2）國內電信業界自行投入研發網路電話通訊監察機制

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，初期無足夠人力、財力因應通訊監察規劃工作，政府可鼓勵協助業界籌組聯盟主動發起網路電話通訊監察機制之研發。

（3）通訊監察協力義務的折衷方案

考量犯罪偵查以及電信經營這兩種利益之平衡點，可依照業者規模大小，決定其是否應完全履行通訊監察協力義務。對於一定規模以上的大型電信業者，應課以其完全之通訊監察協力義務，以符合犯罪偵查之目的。但對於一定規模以下之業者，考量其資本較低及警方需求量較小，可考慮使用臨時監察之方式，亦即在警方有通訊監察需求時，再至業者機房裝機監察，滿足警方之需求。如此一來，似為兼顧犯罪偵查以及電信經營之平衡點。

四、美國協助法律執行通訊法（CALEA[146]）

1994年3月間，美國聯邦調查局（FBI）向國會提出審查「電子電話與通訊隱私促進法」（Digital Telephony and Communications Privacy Improvement Act of 1994），規範通訊業者協助政府機關進行監察，在美國聯邦調查局不斷努力下，國會終於通過該項法案，並稱為協助法律執行通訊法（Communications Assistance for Law Enforcement Act, CALEA），提供五億美元補助通訊業者變更設備的費用[147]，要求通訊業者必須採行必要的步驟，適時地更新設備，使得新科技發展之同時，不會阻礙執法機關進行通訊監察任務。

（一）要求業者具備協助執行通訊監察能力

本法要求電子通訊業者應確保其裝備設施或服務具有下列能力：

1.必須使政府有能力截取電子通訊業者提供服務中有線與電子通訊之內容[148]。

2.在有線與電子通訊傳送期間所合理取得之電話認證資料（call-identifying information），或者是從屬於通訊之電話認證資料，電子通訊業者必須使政府有能力取得。除此之外，由Pen Register或Trap & Trace裝置所取得之電話認證資料，不得包括任何能顯示用戶所在位置（physical location）之資料，除非從電話號碼中能得知用戶所在位置者，不在此限[149]。

3.電子通訊業者能傳送截取之電話內容與電話認證資料給執法機關[150]。

4.電子通訊業者必須使依法通訊截取與取得電話認證資料更加便利，對於用戶的侵害降到最低，並保護用戶通訊隱私與安全與前述資訊不會遭到違法監察[151]。

---

[146] 47 U.S.C. §1001-1010。
[147] 在西元 1995 年至 1998 年間，美國政府共撥付五億美元，針對相關通訊業者變更設備之費用加以補助。參照 47 U.S.C. § 1009。
[148] 47 U.S.C. § 1002(a)(1)。
[149] 47 U.S.C. § 1002(a)(2)。
[150] 47 U.S.C. § 1002(a)(3)。
[151] 47 U.S.C. § 1002(a)(4)。

在協助執行通訊監察能力要求之限制方面，可分成如下三個部分[152]：

1. 執法機關不得指定或限制採行特定設計：任何執法機關不得指定或限制任何電子通訊業者、設備製造商等之裝備、設施、服務、特徵或系統結構採行特定設計。

2. 適用範圍之限制：本法有關要求業者具備協助執行通訊監察能力之規定，不適用於資訊服務（Information services）、支援私人網路通訊或支援以交換電子通訊媒介（interconnecting telecommunications carriers）為單一目的之通訊裝備設施或服務。

3. 解密能力之限制：在加密方面，除非加密係由電子通訊業者所提供，或電子通訊業者擁有解密資訊，否則電子通訊業者對於客戶所為之通訊加密，並無責任解密或確保政府有能力解密。

（二）協助通訊能力之通告[153]

在CALEA立法通過後，為達到執法機關通訊監察能力之需求，必須給予業者一段緩衝期，該法針對此期間政府與業者權利義務關係，以及相關程序有明文規定。

（三）系統製造商與通訊支援服務提供者之合作

由於前述要求業者具備協助執行通訊監察能力，必須相關系統製造商與通訊支援服務提供者之通力合作，始得為之。故通訊業者在必要的時候，必須諮詢系統製造商與通訊支援服務提供者，以確保其設備、服務與數量能符合法律要求。為達成前述目的，系統製造商與通訊支援服務提供者在合理時間與費用範圍內，應讓通訊業者使用其設備、服務，與進行必要之修正[154]。

（四）通訊業者遵守設備需求所需花費之補償

西元1995年1月1日之前，通訊業者必須進行建置相關配備、設施與服務，對於通訊業者為遵守本法第1002條之規定，就其設備更改之合理費用，檢察長得同意支付。1995年1月1日以後，通訊業者得向FCC請求，並通知檢察長，由通訊委員會決定通訊業者在該日期後，是否係合理可完成的。FCC 必須在

[152] 47 U.S.C. § 1002(b)。
[153] 47 U.S.C. § 1002。
[154] 47 U.S.C. § 1005。

請求提出後一年內作出決定，除考量是否遵守規定，會增加通訊業者與用戶的困難性與多餘的花費，還應考量（一）公共安全與國家安全的有效性；（二）基本居住電話的有效性；（三）保護通訊隱私與安全的需求，免於不法侵入；（四）在成本效益原則下，達成第1002條規定對於能力協助要求的需求；（五）爭議中配備設施與服務種類與費用之有效性；（六）爭議中配備設施、服務操作之有效性；（七）美國鼓勵新科技與服務發展之政策；（八）通訊業者之財力；（九）通訊服務條款中競爭之有效性；（十）在西元1995年1月1日前，配備設施與服務之設計與發展之程度；（十一）其他因素。

在1995年1月1日後，相關配備設施與服務為達成本法第1002條規定之要求係不合理者，在通訊業者之聲請後，檢察長得同意支付為達成第1002條規定要求之其他合理的花費。若檢察長不同意此一花費，則通訊業者之配備設施與服務視為符合能力之要求。若在1995年1月1日前，通訊業者之配備設施與服務符合本法第1002條規定之要求，但檢察長未同意支付相關修改設施之費用，則此相關設施將被視為符合第1002 條規定之要求，直到此一相關設施取代、升級或有重大變更[155]。

（五）FCC 擴張CALEA 之適用至網路服務

2005年8月FCC 發佈了命令[156]，擴張CALEA 之適用至「網路寬頻服務提供者」及「與傳統電話業者互連之網路電話業者」。根據此一命令，FCC 認為，基於文義解釋、目的解釋及歷史解釋，在協助通訊監察法中「電信服務提供者」與「資訊服務」之概念無須與1996年電信法為相同之解釋，故若服務提供者落入協助通訊監察法之實質替代條款[157]（Substantial Replacement Provision）中，符合（1）提供有線、無線通訊之轉換或傳輸服務；（2）該服務之一部分實質上被認為是地方電話交換服務之替代；（3）將該服務認定為「電信服務提供者」符合公眾利益時，即為協助通訊監察法中之「電信服務提供者」，不受電信法中認定其為資訊服務之影響。因此，雖然與PSTN 網路互連而提供即時雙向通訊之之網路電話業者在1996年電信法中屬於資訊服務，但在協助通訊監察法中因符合實質替代條款，仍為「電信服務提供者」，必須於18個月內完成通訊監察設備之建置。

五、建置費用之負擔問題

根據我國修正後之通保法第十四條第三項規定，「前項因協助執行通訊監察所生之必要費用，於執行後，得請求執行機關支付」，此處所謂之必要費用，係

[155] 47 U.S.C.§ 1008。
[156] *See In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, 20 F.C.C.R. 14989。
[157] 47 U.S. C. §1001 (8) (B) (ii)。

指各次協助具體通訊監察實施所生之費用[158]，至於事前建置設備所生之費用，依照通保法第十四條第四項、第五項之規定綜合觀之，應由建置機關而非電信業者負擔[159]。而從以往固網與行動通訊業者之經驗來看，通訊監察系統之建置亦是由建置機關編列預算經費。

（一）由政府或業者分擔經費之得失利弊

1. 若由通訊監察執行機關提撥經費建置

若網路電話事業建置通訊監察系統也比照第一類電信事業，由通訊監察執行機關編列預算，提撥建置經費來支付業者建置通訊監察的方式，以網路電話服務經營者家數目前已遠超過第一類電信事業家數、申請經營第二類電信事業無資本額限制、新進業者增加數目相對快速的情況來看，勢必要耗費數字可觀的政府財務加以支應。即使法務部及內政部願意比照第一類電信事業模式，提撥經費建置通訊監察系統，也恐怕要分批、分年度進行。

但從業者經營事業的角度來看，沒有業者會願意成為第一批完成通訊監察設備建置之廠商，因為如此會造成該業者之服務使用者受到國家偵查機關更嚴密之監控，使消費者避之唯恐不及，無疑是宣告是業者的死刑。

另外，政府必須考慮到：提撥經費輔助業者建置系統的速度，是否趕得上經營者加入與退出市場的汰換速度？以及如何訂定有資格獲得經費補助之業者的審核標準，以避免花了大錢在經營者身上建置通訊監察系統後，經營者卻輕易終止其業務或因經營不善而倒閉，徒然浪費國家資源與經費。

2. 若由第二類電信業者出資建置

若採行由業者自行出資建置的方案，龐大的系統建設費用會成為網路電話業者申請經營此項業務的一大困難。如果比照第一類電信事業投入通訊監察系統所需要經費，能負擔的起的事業根本找不出幾家，而且即使有能力建置像第一類電信事業所建置的系統，因為企業規模的差異仍大，網路電話事業所感受到的負擔也會大於第一類電信事業。但就算以現實情形來說，由於使用的通訊技術與過往不同，網路電話服務建置、維護通訊監察系統設備的經費不必如第一類電信事業

[158]通訊保障及監察法施行細則第二十六條第七項：「本法第十四條第三項所稱必要費用，指電信事業及郵政事業因協助執行而實際使用之設施及人力成本。」

[159]通保法第十四條第四項：「電信事業之通訊系統應具有配合執行監察之功能，並負有協助建置機關建置、維持通訊監察系統之義務。」第五項：「前項協助建置通訊監察系統所生之必要費用，由建置機關負擔。」故可知電信業者並非建置機關。

建置所需的那麼龐大，但對中小型企業居多的網路電話服務經營者而言仍是不可忽略的一項重擔。

依照過去固網及行動通訊業者建置通訊監察系統的經驗，通訊監察系統的建置皆由法務部及警政署編列預算經費，的確十分驚人。以建置台灣大哥大、東信、泛亞、遠傳及和信五家民營行動電話通訊監察系統的「內政部警政署行動電話通訊監察工作中程計畫」為例，計畫內容包含前端及後端自動錄音分配系統、整合前後端系統、訓練專業監察作業人員及機房裝修等，計畫時程自1999年7月至2002年12月，總建置經費高達新台幣十二億七千八百九十七萬元[160]。龐大的系統建設經費、以及第二類電信事業經營家數眾多的情形之下，無論是由政府全額提撥經費或是由業者自行負擔，都有其所難以執行的困難所在。

（二）業者協力義務之法律性質分析

1. 社會義務或是特別犧牲？

觀諸大法官解釋「財產權」所提及之「財產權之社會義務」（例如釋字五六四號[161]、釋字五七七號[162]），所謂「財產權之社會義務」係指財產權人行使其財產時應有助於公共利益，換言之並非聽由財產權人任意為之而係必須注意公益，亦即若為增進公益，對人民依法取得之財產，並非不得以法律為合理之限制，然限制程度為何？須就相關手段、目的予以衡量，若尚屬適當而且輕微，則財產權人同時應負擔「社會義務」，惟個人行使財產權仍應依法受社會責任及環境生態責任之限制，其因此類責任使財產之利用有所限制，而形成個人利益之特別犧

[160] 行政院研究發展考核委員會，91管查字第02號，內政部警政署行動電話通訊監察工作中程計畫實地查證報告，頁2（2002）。

[161] 釋字五六四號：本號解釋係房屋所有權人於自家騎樓設攤遭主管機關以違反道路交通處罰條例開罰，其認為騎樓係指自家所有權為何不能使用？此限制有違憲之虞？對此釋字五六四號認為：「人民之財產權應予保障，憲法第十五條設有明文。惟基於增進公共利益之必要，對人民依法取得之土地所有權，國家並非不得以法律為合理之限制。道路交通管理處罰條例第八二條第一項第十款規定，在公告禁止設攤之處擺設攤位者，主管機關除責令行為人即時停止並消除障礙外，處行為人或其雇主新台幣一千二百元以上二千四百元以下罰鍰，就私有土地言，雖係限制土地所有人財產權之行使，然其目的係為維持人車通行之順暢，且此限制對土地之利用尚屬輕微，未逾越比例原則，與憲法保障財產權之意旨並無牴觸。」

[162] 釋字五七七號：本件聲請人認為菸害防制法第八條第一項課予聲請人標示之義務又於同法第二一條對於未標示者逕處罰鍰；非僅係違反比例原則而限制聲請人之言論自由，已對聲請人憲法第十五條所保障之財產權形成不當之限制，對此釋字五七七號認為：「國家為增進國民健康，應普遍推行衛生保健事業，重視醫療保健等社會福利工作。菸害防制法第八條第一項規定：「菸品所含之尼古丁及焦油含量，應以中文標示於菸品容器上。」另同法第二一條對違反者處以罰鍰，對菸品業者就特定商品資訊不為表述之自由有所限制，係為提供消費者必要商品資訊與維護國民健康等重大公共利益，並未逾越必要之程度，與憲法第十一條保障人民言論自由及第二三條比例原則之規定均無違背。又於菸品容器上應為上述之一定標示，縱屬對菸品業者財產權有所限制，但該項標示因攸關國民健康，乃菸品財產權所具有之社會義務，且所受限制尚屬輕微，未逾越社會義務所應忍受之範圍，與憲法保障人民財產權之規定，並無違背。另上開規定之菸品標示義務及責任，其時間適用之範圍，以該法公布施行後之菸品標示事件為限，並無法律溯及適用情形，難謂因法律溯及適用，而侵害人民之財產權。」

牲，社會公眾並因而受益者，應享有相當補償之權利。如因公用或其他公益目的之必要，國家機關雖得依法徵收人民之財產，但應給予相當之補償，方符憲法保障財產權之意旨。

而電信業者之協力義務，究係社會義務，亦或是特別犧牲，以第一類電信業者而言，由於中華電信、台灣大哥大等公司，其資本額皆在數十億、甚是數百億之譜，相較於建置通訊監察設備的義務或費用負擔，應可認為尚屬適當而輕微。且第一類電信業者為寡佔市場，掌握全國通訊服務之命脈，事關國家重要公益，故其市場進入門檻採取嚴格的特許制，本應比其他事業負擔更多的社會義務，應該在普及服務以及犯罪偵查上，配合國家的社會安全及電信政策。從此一角度觀之，配合通訊監察義務似可視為第一類電信業者之社會義務。

但觀諸第二類電信從第一類電信切割出來的管制模式，就可知道我國對第二類電信事業的態度採取開放競爭、管制鬆綁。故第二類電信業者普遍都是資本少、規模小，對於動輒屬百萬甚至數千萬的通訊監察設備，可能都超過其資本額總數。若命其自行負擔，必然會使多數業主無法生存，逾越適當且輕微之範圍，而進入特別犧牲之領域，國家機關應給予相當之補償。

2. 小結：國家應給予適當補償

通訊監察設備建置義務涉及對網路電話業者財產權及營業自由之限制，須有據以支持之公共利益，並在符合比例原則的情況下，始可為之。基於網路電話業者之配合對於偵查有效性之提升、其他替代方式之效果不彰及網路犯罪率攀升的情況下，此一對業者財產權等權利之限制尚屬適度，而在憲法上具備正當性[163]。

此一「行為義務」雖不違憲，但額外成本之「金錢負擔義務」，對財產權之限制，以不超過其應容忍的社會義務為限，而維護國家安全與社會秩序等公共利益之執行所生之費用，應由全民共同負擔始為合理，而非由電信或網路電話業者單獨承擔，亦不得轉嫁由傳統電信或網路電話用戶承擔[164]，因此建置配合通訊監察之設備，及協助執行所額外增加的成本，已逾越業者應負擔之社會義務，從國家責任之設計原理來看，應該由國家以全民繳納之稅捐加以補償更為適當，或至少政府應加以補助，始符合「有徵收，有補償」之法理。

六、結論：以比例原則檢視

[163] 許華偉，「ISP 業者在通訊保障及監察法中的配合義務試析」，資安季刊，第 5 期，頁 24-25(2004)。

[164] 詹鎮榮，「無償性通訊監察設備設置義務之合憲性疑義」，月旦法學，第 64 期，頁 108-111(2000)。

以上提出了許多關於業者協力義務之相關爭議，範圍涵蓋電信管制、創新發展、犯罪偵查等等層面，問題多而複雜，且彼此互相衝突矛盾，使得此義務之具體內容渾沌不明，各方爭論不休，至今仍無定論。

若本文僅提出質疑，而未提出建設性之見解，造成問號多於句號，只會增加此一議題混亂之程度，而流於口水之爭。故本文嘗試提出價值判斷，以公法爭議中常用比例原則，綜合上述提及之爭議，分階段做利益權衡，檢視目前管制手段及目的是否合理，找出各方利益角力之下的平衡點。

（一）審查標準之選擇

業者配合通訊監察義務涉及人民財產權之剝奪，以及營業自由之限制，從此一觀點來看，對人民基本權之侵害不可謂不重大，似應採取較嚴格的審查標準。但從另一角度觀之，此義務亦涉及電信管制之議題，與國家政策發展有重要關聯，因此，一旦涉及國家社會經濟政策之擬定時，通常必須尊重主政者對於國家方針之主導地位，而採取低度的審查標準。故衡量兩種不同之觀點，本文認為應採折衷之作法，選擇中度審查標準來做檢視。

（二）正當目的

國家命業者配合通訊監察，目的在於維護社會安全，避免新科技帶來治安的死角，應符合中度審查標準之下之重要國家之利益，為正當之目的。

（三）適當性原則

適當性原則指手段是否為達到目的之適合途徑，在此即指命業者配合通訊監察，是否為達到維護社會安全之適當手段。而從以往第一類電信事業配合通訊監察的經驗，若業者能夠充分配合，對於犯罪偵查之協助有顯著效果，而第二類電信所提供之服務與第一類電信相比較，雖然技術有所不同，但其通訊之本質仍未改變，應可比附援引先例，認為其手段符合適當性原則。

（四）必要性原則

「必要性原則」係指「最小侵害手段」，許多可達到目的之相同手段中，應選擇侵害最小者。亦即必須考慮可達成相同社會管制目的之其他手段，是否有侵害更為輕微之手段可資選擇。

理論上，達成協力義務之手段可能有很多種，以法規明文規定義務內容絕非唯一方法。故似可考慮使用較輕微之手段，例如以行政契約取代行政處分，獎勵補助取代嚴格管制，皆是較小的侵害手段。實際上，以普及服務為例，網路電話技術與服務如能運用於普及服務之提供，主管機關以獎勵或補助之方式，鼓勵網路電話服務提供者提出實施計畫成為普及服務提供者，比原始架構更有助於普及服務減少數位落差之目的，且對產業發展的影響亦較輕微。

但通訊監察義務與普及服務性質不同，屬於犯罪偵查之一部，公權力性質非常濃厚，涉及人民生命、身體、自由及財產等法益，國家有必要用強制之手段，確保人民上述法益得以被確實保護。故以課予罰鍰，或是做為申請執照的先決條件，能確實擔保其義務之履行，非用獎勵或其他較寬鬆之管制方法可比擬，故其他之手段雖然對人民侵害較小，但皆非可達到相同目的之手段。在能確實達到犯罪偵查目的之手段當中，以法規直接賦予業者配合義務，應為最小侵害手段。

（五）狹義比例性原則

狹義比例性原則又稱為禁止過度原則，係為了防止顯失均衡之利益成本衡量。如分析結果之效益大於成本，或效益雖小於成本，但相差不顯著時，應認為已通過狹義比例性原則之檢驗，惟如果效益遠低於成本而符合顯失均衡之情事，應認為不符合效率考量而不應為之。

但比例原則的操作上，仍然存有模糊且不確定之概念，故本文嘗試以更明確、客觀、具可預測性之方法用以操作比例原則，加入經濟學的觀點而以「成本效益分析」為工具。所謂成本效益分析（cost-benefit analysis），強調的是資源分配效率上之社會福利最大化，也就是將資源配置給能創造最高效率之活動或計畫。

1. 成本效益分析表(表五)

(1) 建置經費由業者負擔

	成本	效益	分析
第二類電信業者	1.市場進入門檻 2.建置、系統維護成本 3.許可執照之取得(協商成本) 4.對網路電話與其它第二類電信事業的差別待遇 5.研發經費之排擠 6.消費者對其服務之隱私權保障政策產生疑慮	無	成本＞＞效益

國家	1.管制成本 2.協商成本 3.業者將成本轉嫁給消費者 4.新興產業發展之阻礙	強化犯罪偵查及社會安全	效益≧成本

若建置經費由業者負擔，所產生之成本效益分析如上圖所顯示。在業者之部分，由於建置通訊監察設備對於其經營通訊服務本身並無任何加值效果，故應無任何效益可言。而在成本方面，本文已於先前詳述，並在上表中整理出六大項成本或負面效應。而依據先前之敘述，此六大成本將嚴重影響第二類電信業者之經營，甚至達到無法生存的結果，且又無任何效益，故對於此處之分析，本文認為成本遠大於效益，且達不成比例之程度。

而在國家機關方面，其效益為強化犯罪偵查及社會安全，為國家重大公益，應視為相當高之效益。但在成本方面，雖然免去了建置成本，但仍有業者將成本轉嫁給消費者之潛在風險，以及阻礙新興電信產業發展之不利影響，故本文分析認為，雖然效益勉強大於成本，但並非有顯著差異。

(2) 建置經費由國家負擔

	成本	效益	分析
第二類電信業者	1.許可執照之取得(協商成本)	無	成本≧效益
國家	1.管制成本 2.協商成本 3.建置成本 4.業者任意退出市場之風險	強化犯罪偵查及社會安全	效益＝成本

若建置經費由國家負擔，由上表可之對於業者之成本僅剩下取得許可執照之成本，及協商成本，如此一來將大幅降低業者進入市場之門檻，以及創新創發之阻礙。雖然其效益仍然是零，但在成本極小化之情況下，效益與成本以相去不遠，成為成本稍大於效益之結果。

而在國家方面由於增加了建置經費之負擔，使得成本大幅提升，但由於犯罪偵查及社會安全之效益極高，且若政府為了省一筆預算而不建置通訊監察設備，將造成治安維護及犯罪偵查之漏洞，未來仍要由全民承擔更大的社會成本，故此一經費為必要成本，與其所能達成之效益應屬於損益相當，故本文認為成本等於效益。

2. 結論

在綜合判斷之後，本文認為若建置經費由業者負擔，對於業者之成本將遠大於效益，且達不成比例之程度。而對國家之效益又未顯著大於成本，似成為損益失衡之狀況，而不符合狹義比例性原則。

而若由國家負擔，可大幅降低業者之成本，對第二類電信事業之發展有所助益，且與目前開放競爭、解除管制之政策方向不謀而合。相較於通訊監察所帶來之犯罪偵查效益，其建置成本為必要花費，比其他偵查方式較為經濟，故其效益應相當於成本，符合比例原則。

且若單純就業者協力義務之法律性質加以分析，本文認為並非業者之社會義務，逾越適當且輕微之範圍，而進入特別犧牲之領域，國家機關應給予相當之補償，方符合憲法上之要求，已如前述。故不論用成本效益之分析，或是憲法原理原則之檢視，本文皆認為其建置經費應由國家分承擔之。

柒、結論

一、網路電話與IP網路電信納入通訊監察範圍之探討

首先，本文將網路服務區分成「有通訊相對人」及「無通訊相對人」，僅有「通訊相對人」之服務方符合通訊保障及監察法第三條所定義之通訊，此區分使得「無通訊相對人」之服務，例如網路接取、瀏覽服務，排除通訊保障及監察法之適用。

再者，在「有通訊相對人」通訊服務中區分成有「須留存複本」及「不須留存複本」兩種，而經過分析討論之結果，本文認為不論是否留存複本，通訊當事人皆應有隱私或秘密之合理期待，對於其通訊內容之監察皆須符合通訊保障及監察法，對於人民隱私權之保障方為周全。

最後，根據通訊之所傳送之資訊，區分為內容資訊（content information）及信封資訊（envelope information），通說認為信封資訊（envelope information）為公開資訊，或非屬通訊隱私核心領域之範疇，故僅有內容資訊（content information）為秘密資訊，有通訊保障及監察法之適用。

二、網路監察之法制及執行規範建議

(一) 建立系統化的網路監察制度

1. 建立標準監察作業流程
2. 制訂明確的行為準則
3. 降低系統操作錯誤之可能性
4. 內容資訊（content information）及信封資訊（envelope information）之區別
5. 考慮公開系統技術
6. 建立完整之監督機制

(二) 放寬網路通訊監察限制

1. 通訊監察書要件之放寬

若可引進美國法承認之不定點監察，在某些特定狀況下允許偵察機關在通訊監察書上，不須記載「受監察處所」及「監察通訊種類及號碼等足資識別之特徵」，可迴避現實處所、通訊設備、方式、帳號無法特定之困難。以免打擊犯罪之時機稍縱即逝。

2. 偵查手段之放寬

若參考前述IITRI提出的「Carnivore系統獨立最終技術檢視報告」，文中提到該系統能精準的篩選出所需的資料，再加上操作人員能正確操作該系統，輔以適當的監督機制，能將對無辜第三人的侵害降到最低。如此一來即可在人權侵害相對輕微的情況下，順利進行通訊監察，似為人權保障及犯罪追訴的平衡點，值得我國立法及技術上之參考。

3. 監察範圍之放寬

若未來我國能依據前述之建議，建立系統化的網路監察制度，使得操作人員的行為皆能受到完整規範，系統上亦能做到設計完善，將隱私權侵害過廣的問題做有效抑制，應可說服法官在核發通訊監察書時，放寬監察之線路，擴大通訊監察之範圍，以利實務運作。

(三) 加強監督機制

1. 監察過程之監督

首先，在操作網路監察的過程中，必須規範個人責任與審查程序。每一個設定、開始、停止與恢復，都應由特定人加以追蹤，對於何人設定蒐集程序，何人開始下載資料，何時設定蒐集程序，何時開始下載資料等，以釐清責任。

2. 系統設計之監督

而在監察系統設計上，必須提升對於監察系統之控制。可以增加保護裝置，如在設備外圍、鍵盤、監視器、滑鼠等連接處封印。若ISP業者或其他人士企圖侵入，將導致封印毀損，即可顯示所蒐集之證據遭到竄改。

3. 事後之監督

在監督的單位上，除現有的司法部門(法官)之監督外，可考慮增加行政、司法之間，並成立專責監督機關，明定執行機關須向監督機關做區個案報告及年度報告，並且詳列應報告之事項，使監督機制更加完善。

三、通聯資料保存(Data Retention)法制之分析與建議

(一) 資料保存分類

與第一類電信監察不同，第二類電信服務項目多樣化且極其煩雜。對於犯罪偵查項目勢必比第一類電信監察項目資料多元，但基於憲法保障個人隱私權與通訊自由，在比例原則考量下，執法機關應本最低隱私權侵害與通訊自由保障前提下，僅就犯罪偵防所需之監察項目資料訂定標準，不應無限擴大監察項目資料。依據歐盟「資料保存指令」，用來識別發話者與受話者所必須的資料，在資料保存內容部分，依其保存項目之不同，主要分為6大類，可以作為訂定我國執法機關選擇制定之監察資料範圍的參考。

(二) 保存期限屆至後處理方式

我國目前僅規範電信業者保存之義務，與歐盟規範比較不同處，我國並未要求業者在保存期限屆至後，應將資料去名化或刪除之作法，歐盟「資料保存指令」要求保存期限屆至後，除非有特殊原因，各會員國必須要求其國內之業者將所保存之資料立即銷毀，以確保資料安全並保障人民之隱私不受侵害。

(三) 對於業者資料保護義務的要求

歐盟國家在思考資料保存之議題時，同時也思考到人權與資料保護之議題，值得我國未來進行法律修正時之參考。為避免保存之資料因不慎外洩或遭不當利用，而造成人民隱私的重大侵害，在歐盟「資料保存指令」中，特別在第7條要求被保存資料的保護等級，應等同於資料傳輸時的保護，並應避免受保存之資料遭到因故意或過失所造成遺失、破壞或刪除。我國可參酌有關這方面上的保護規定，使通訊自由與隱私權的保障上更趨完整。

(四) 罰則的制定

對於為遵守資料保存義務，或是無故洩漏、破壞或刪除資料的行為，可依其情節輕重，制定適當的行政罰或是刑罰，以明確嚇阻不法行為，保護個人資料。

(五) 建置獨立的監督單位

為確保資料得以妥善保存不受侵害，歐盟「資料保存指令」要求各會員國應明確指定相關單位負責監督資料保存與運用之情形，且僅得為有法律授權之使用者所使用。若有非經法律允許而故意使用或交換受保存之資料者，各國應制定有效且合適的刑罰，以嚇阻惡意或不當利用或儲存之行為。

四、業者協助通訊監察執法義務

(一) 落實協商和建置義務

現行通保法及施行細則關於業者協力義務之規定可說已相當向完備，並賦予偵查機關相當之協商、許可權限，就法制面上並無太大問題。但由於電信業者家數眾多，以及諸多前述所討論之問題及困難，使得在執行面上成效不彰，進度牛步化。偵查機關應盡速規劃可行之折衷方案及配套措施落實協商和建置義務。

(二) 國家應予以補償

對於電信業者課與協力義務雖不違憲，但額外成本造成之財產權限制，以不超過其應容忍的社會義務為限，而維護國家安全與社會秩序等公共利益之執行所生之費用，應由全民共同負擔始為合理，而非由電信或網路電話業者單獨承擔，亦不得轉嫁由傳統電信或網路電話用戶承擔，因此建置配合通訊監察之設備，及協助執行所額外增加的成本，已逾越業者應負擔之社會義務，從國家責任之設計原理來看，應該由國家以全民繳納之稅捐加以補償更為適當，或至少政府應加以補助，始符合「有徵收，有補償」之法理。

(三) 折衷方案

考量犯罪偵查以及電信經營這兩種利益之平衡點，可依照業者規模大小，決定其是否應完全履行通訊監察協力義務。對於一定規模以上的大型電信業者，應課以其完全之通訊監察協力義務，以符合犯罪偵查之目的。但對於一定規模以下之業者，考量其資本較低及警方需求量較小，可考慮使用臨時監察之方式，亦即在警方有通訊監察需求時，再至業者機房裝機監察，滿足警方之需求。如此一來，似為兼顧犯罪偵查以及電信經營之平衡點。

五、未來建議

(一) 目前網路通訊監察尚未成熟、制度化，相關作業及實施成效，未來須持續追蹤及評估。

(二) 對於目前法規尚非屬一類，亦非二類的 ISP 業者，該如何規範，或是納入通訊監察協助範圍，尚待進一步釐清和研究。

(三) 對於網路犯罪跨國性之特色，涉及複雜的國際管轄權及政治問題，亦為未來重要之課題及努力方向。

捌、參考文獻

一、書籍

1. 吳庚，《行政法之理論與實用》，增訂十版。元照出版，台北（2007）
2. 法治斌、董保城，《中華民國憲法》，空大出版，台北（2001）
3. 林紀東，《中華民國憲法逐條釋義(一)》，三民出版，台北（1998）
4. 林錫堯，《行政法要義》，復文出版，高雄（1998）
5. 許宗力，《法與國家權力》，元照出版，台北（1999）
6. 廖義男，《國家賠償法》，增訂版六刷，作者自版，台北（1997）

二、研討會論文

1. 曾正一，〈反恐怖行動法制中通訊監察規範之研究－反恐怖行動法、國家情報工作法與通訊保障暨監察法之交錯〉，收錄於《第三屆恐怖主義與國家安全學術研討會論文集》，中央警察大學主辦，桃園（2007）
2. 劉靜怡，〈當法律成為全民公敵？數位時代隱私焦慮之分析〉，收錄於《監察法 vs.隱私權—全民公敵，傳播與法律系列研討會（七）》，政大傳播學院研究暨發展中心與理律法律事務所合辦，台北（2000）

三、學位論文

1. 林岡輝，《電子郵件之截收處分》，國立臺北大學法律研究所碩士論文(2002)
2. 林煒程，《網際網路猥褻犯罪之研究》，國防管理學院法律研究所(1998)
3. 徐智明，《通訊監察之保障與規範》，國立中正大學法律研究所碩士論文(2004)
4. 張家豪，《通訊監察資訊系統及其相關之科技與法律問題—以第二類電信通聯調閱管理系統為例》，國立台北大學資訊管理研究所碩士論文(2006)。
5. 陳信郎，《資訊隱私權保障與網路犯罪通訊監察法制》，國立政治大學法律研究所碩士論文(2005)
6. 詹文凱，《隱私權之研究》，國立台灣大學法律研究所博士論文(1998)
7. 錢世傑，《網路通訊監察法制與相關問題研究》，中原大學財經法律研究所碩士論文(2002)

四、中文期刊

1. 石世豪，〈電信自由化下之通訊安全規範的轉型趨勢：通訊秘密、個人資料保護與電信事業的管制變革〉，《全國律師》，2005 年 5 月號，(2005)
2. 李志仁，〈電信資訊匯流下之法律爭議—以 Skype 為例〉，《科技法律透析》，第 18 卷 12 期，(2006)
3. 張玉山、李淳，〈公用事業管制革新與管制組織的重新定位—以電力事業為例〉，《管制革新》，劉孔中、施俊吉主編，(2001)

4. 許華偉，〈ISP 業者在通訊保障及監察法中的配合義務試析」〉，《資安季刊》，第 5 期，(2004)
5. 陳志龍，〈秘密通訊自由之保障及郵件扣押合法性之商榷〉，《刑事法雜誌》，第 22 卷第 3 期，(1978)
6. 陳愛娥，〈通訊監察與秘密通訊之自由〉，《憲政時代》，第 23 卷第 2 期，(1997)
7. 陳櫻琴，〈管制革新之法律基礎與政策調適〉，《管制革新》，劉孔中、施俊吉主編，(2001)
8. 詹鎮榮，〈無償性通訊監察設備設置義務之合憲性疑義〉，《月旦法學》，第 64 期，(2000)
9. 蔡美智，〈通訊保障及監察法關於網路監察的相關爭議〉，《資訊法務透析》，(1999)
10. 蔡墩銘，〈通訊監察與證據排除〉，《刑事法雜誌》，第39卷第1期，(1995)
11. 蔡聖偉，〈妨害秘密罪章之新紀元（下）〉，《月旦法學》，第 71 期，(2001)
12. 蔡榮耕，〈I Am Listening to You（上）－釋字第六三一號解釋、令狀原則及修正後通訊保障及監察法〉，《台灣本土法學雜誌》，第104期，(2008)
13. 蔡榮耕，〈I Am Listening to You（下）－釋字第六三一號解釋、令狀原則及修正後通訊保障及監察法〉，《台灣本土法學雜誌》，105 期，(2008)
14. 龔小文，「要等監察配套措施完備才上路，網路電話配號再等等吧」，民生報，第 A10 版，2005 年 4 月 16 日。

五、英文期刊

1. DuFour, R.Alex, *Voice over Internet Protocol: Ending Uncertainty and Promoting Innovation through a Regulatory Framework*, 13 COMMLAW CONSPECTUS (2005)
2. Fishman ,Clifford S., *Interception of Communication in Exigent Circumstances: The Fourth Amendment, Federal Legislation, and the United States Department of Justice*, 22 GA. L. REV. (1987).
3. Gilman,Johnny, *Carnivore: The Uneasy Relationship Between the Fourth Amendment and Electronic Surveillance of Internet Communications*, 9 COMMLAW CONSPECTUS (2001)
4. Goldsmith ,Michael, *Eavesdropping Reform: The Legality of Roving Surveillance,* 1987 U. ILL. L. REV. (1987).
5. Jennings, E. Judson, *Carnivore：US Government Surveillance of Internet Transmission*，6 VA. J.L. & TECH. (2001)。
6. Kaplan, Carl S., *Concern over Proposed Changes in Internet Surveillance*, N.Y. TIMES , Sep. 21,2001, at E1。

六、其他參考文獻

1. 行政院研究發展考核委員會，91 管查字第 02 號，內政部警政署行動電話通訊監察工作中程計畫實地查證報告，(2002)
2. 陳錡銘，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，(1999)

3. 黃少健，選定司法管轄區對截取通訊的規管，香港立法會秘書處資料研究及圖書館服務部研究報告，(2005)。
4. 黃謀信，境外貪污案件偵查之研究--以美國聯邦通訊監察制度為中心，臺灣板橋地方法院檢察署出國進修報告，(2007)。
5. 謝名冠，網路行為規範之研究，臺灣台北地方法院檢察署八十九年度研究報告，臺灣台北地方法院檢察署印行，(2000)

七、網路參考文獻

1. 寬頻上網帳號數，國家通訊傳播委員會網站：http://www.ncc.tw/chinese/news_detail.aspx?site_content_sn=327&is_history=0&pages=0&sn_f=7425（最後點閱時間:2008 年 12 月 10 日）
2. 陳仲嶙，電子化政府之資訊保護--以個人資料保護為中心，益思專文發表網址：http://www.is-law.com/OurDocuments/PR0001CL.pdf(最後點閱時間:2008 年 12 月 17 日)
3. 陳仲嶙，電腦處理個人資料保護法掃描─總則篇，益思專文發表網址：http://www.is-law.com/OurDocuments/PR0010CL.pdf(最後點閱時間:2008 年 12 月 24 日)
4. 張耀中「從歐盟「資料保存指令」看我國資料保存之規範」，IThome 網址：http://www.ithome.com.tw/itadm/article.php?c=39970 (最後點閱時間:2008 年 12 月 24 日)
5. 謝昆峰，電子郵件的取得與保全－合理隱私期待與法定程序，益思專文發表網址：www.is-law.com/Others/ESSAY0011KunFeng.pdf(最後點閱時間:2008 年 12 月 15 日)
6. IIT Research Institute,Independent Technical Review of the Carnivore System：Final Report, http://www.justice.gov/archive/jmd/carniv_final.pdf (last visited Jan. 13,2009)
7. Lawrence Lessig, *Wire-tapping VoIP*, http://lessig.org/blog/2004/08/wiretapping_voip.html (last visited Jan. 4,2009)
8. President's Working Group on Unlawful Conduct on the Internet, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet*, U.S. Dep't of Justice, http://www.usdoj.gov/criminal/cybercrime/unlawful.htm (last visited Jan. 13,2009)。
9. USDOJ,*Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001*, *available at* http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm (last visited Jan 13,2009)
10. USDOJ, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, *available at* http://cybercrime.gov/s&smanual2002.htm (last visited Jan 13,2009)。
11. Robert D. Atkinson, *Internet Telephone Service-A New Era of Competition in Telecommunications*, PPI Policy report, http://www.ndol.org/documents/VoIP.pdf (last visited Jan.4,2009)

玖、訪談紀錄

刑事警察局 偵九隊 訪談記錄	
訪 談 時 間：97 年 11 月 20 日 14 時 00 分至 16 時 00 分止	
訪 談 地 點：刑事警察局 偵九隊	出 席 人 數：4 人
受 訪 者：陳詰昌 警官、黃國能 警官	訪 問 者：王煌玄、蘇三榮、王思涵

一、通訊監察程序規範

1.問:當遇見第二類電信發動通訊監察應從何處開始準備？

答:外勤單位從犯罪偵查開始一直到鎖定某個對象，網路電話分兩種:電腦對電腦(P to P)，另一種則是有配室內電話門號，網路電話例如 skype 就沒辦法，所以就放棄，那如果有門號部分，就會請通訊監察調，由地檢署向法院申請，由法院審理，過了後票經過檢察官回來，再投給相關單位執行，這是大概流程。

2.問:主要是哪一類犯罪會比較多通訊監察需求?

答:目前偵九隊是詐欺案件居多，因為脫離不了經濟，還是要錢，其他就是販毒、販槍枝、洗錢、恐嚇少部份，基本還是符合通訊監察法的最輕本刑三年以上或特例的要項才會用。

3.問:目前 PC to PC 是否有在監察?

答: PC to PC 的話要上 user 端的網路線，而不是投通訊監察中心。

4.問:實務上就上網路線監察大約操作流程為何?

答:首先要知道這用戶的網路線的代號是幾號，例如中華電信可能會有一個 HN+六位 數字，就用這編號去請通訊監察票，下來後再投給中華電信，就會另拉一條(miro?)的線出來，有個機器就可把所有封包截錄下來，再根據 protocol 解碼，例如是 msn msg、yahoo msg、QQ…不同的 protocol 會分類到不同目錄，我們再還原回來。

5.問:接上題，上述流程是否需要透過通訊監察中心?

答:沒有，就是我們自己去投單給 ISP 業者去拉線出來，有點像室內電話，一樣沒有透過通訊監察中心，是我們自己到機房裝機，要到通訊監察中心基本上都是要透過交換機的才會。

6.問: 因為有多事務用戶可能同時使用一條線路，特定網路號碼的監察有沒有可能再放寬?

答:一定要個化，院方才會准，如果有十個用戶同時在用這條就不會過了，而且這票投出去會比去通訊監察中心還要久，大約五六個工作天這條線才會上，通訊監察中心是馬上上線。

7.問:針對非特定人、甚至犯罪人經常利用的網咖有無特殊通訊監察機制?

答:之前有利用 yahoo (cookie?)，鎖定特別的帳號，只要一上線馬上就可以知道位置，通知我們 IP，就可以知道大概的地方，之前有案子就是都在網咖出沒，後來控了一段時間經過分析找出幾個區域，土城、板橋、樹林一帶，把他用的帳號作即時監控，只要一上線就找到，這種不會丟監察票，因為不是要知道內容，這已經蒐集足夠證據，只是要知道位置，就像通聯記錄。

8.問:如上述回答，犯罪嫌疑人知道自己可能被監控，就去網咖用網路電話，此情形無法監控?

答:根本不用到網咖，只要兩端都是電腦又不用認證，我們就沒辦法了，現在網路通訊的 protocol 太多，連他走哪種都不知道，甚至會加密，攔下來也解不開。

顏警官說明：通訊監察仍是針對犯罪人帳號。又通聯紀錄只能回朔三到六個月，e-mail 申請以後才得紀錄

9.問:我們觀察到美國有不定點監察，不用記載受監察處所或可資識別號碼，幾乎只要記受監察對象，不管用何種方式都可以監察，您覺得可以解決困難嗎?

答:如果針對人不針對特定地點，可是還是要證明是受監察人使用，法院還是開不了票，業者也會迴避。之前有對 imei(手機內碼)做過監察，也被說不能再用這種方式監察，因為用 imei 的話，只要用這手機的 sim 卡都可以監察到，技術可以，但現在也不能做了，因為剛開始可能是對象在用，後來就拍賣賣掉換成毫無相關的人使用，院方認為會侵害到其他人。

10.問:目前是如何填具通訊監察書?

答:我們應該是填申請書，前面會附一個文，加一張申請書和一覽表，然後給地檢署，地檢署會先審，審我們要上線的這些電話是否合乎通訊監察法的要件，如果 OK 沒有跟其他單位相衝突，就會核准再送到院，然後 24 小時內會回覆申請的是否合乎要件。

11.問:接上題，法院或單位內有標準的流程表供參考嗎?

答:沒有，應該是在地檢那有大流程，其實大部分就是我們把申請表提給檢方，檢方審了後提給院方，院方批完大部分是交回檢方再交回我們，這是大流程，細節各法院都會有點差異，例如要先給主任還是先給檢察官，其他基本流程差不多。

12.問:監察票大部分記載何項目，網路部分及電話部分是否不同?

答:不管網路或市話，有號碼就填號碼，沒有號碼像是 yahoo msg 就只能填那條線編號，如果針對到信箱，單純信箱部分可填上 mail address，那這信箱收發

任何信都會 copy 副本給你，如果知道用戶每次都是用這信箱連絡才會這麼做。

13.問:針對網路電話有即時上線監察機制嗎?

答:有門號的話通訊監察中心就可以做，其他就是事後錄下來。

14.問:通訊監察的執行情形是否有人監督?(例如法院)

答:期中要回報告，例如與監察犯罪內容是否相合，(提供格式參考)，如果有不同格式就用法院的格式，不然我們執行單位是沿用通訊監察中心的格式。結束的時候還要再一份報告，書面審查和監察票是否相符，不過會報的應該也都是確有犯罪事實，有時候一案也會衍生出另一案，就留我們需要的或另行啟案調查，或者看檢察官要不要合併，監察範圍只會少不會多。

15.問:實務上有無看網頁有哪些 IP 進來再去追查的執行方式?

答:這比較沒有用，因為(TBT?)就是單向，不會再用這些 route 回查。法律問題是不是要和科技結合，事實上是把電話和網路分開，單雙向不同技術，如果一直把網路和電話放在一起談不出結果，科技上將來應該是剩網路，不過也會分 circuit network, non-circuit network，事實上不一樣，通保法只有用電話的角度在看，進入下一網路階段，可能就使不上力，二類電信會是更大的問題。美國因為有(MCI?)超級二房東變大房東的案例，法律才被迫進步。

二、通聯資料保存

16.問:內容以外的資訊(通聯記錄)如何取得?網路部份會有上網紀錄(瀏覽過的網頁、做過的交易)嗎?

答:直接發業者，比較不會涉及隱私保護，這部分配合就很 OK，網路都是針對帳號調，調到的資料就是使用哪些服務，電子通訊錄、加的好友，但不會顯示開啟過的網頁，例如使用信箱、交友、部落格的類別服務，明確開了哪個交友檔案就不知道。

顏警官說明:上網紀錄部分因為是以封包方式傳遞訊息，而封包數量龐大，不可能全開

17.問:目前 online game 可以通訊，利用這作犯罪連絡，伺服器會留下和誰對談紀錄，這部分有監察嗎?

答:還是要靠線報，不然也沒注意，目前沒遇過，這部分業者通常比較願意配合。

18.問:接上題，目前對 online game 中和誰對談的紀錄等這類資料，是屬於似通聯紀錄資訊或內容還有爭議，您的看法是如何界定?

答:遊戲中還有對頻、廣播、聊天室，很難界定，聊天室可以調紀錄，不過保留

時間都不長約一星期，要很快就跟業者說哪段時間要留住，(私密頻道也有紀錄，警方要用哪種程序?)user 帳號、何時上線、哪段時間講了什麼話視為電磁紀錄。

19. 問:通聯記錄的部分是否有即時監察機制?(美國有類似制度)

答:資料太大量，沒有這麼做，據所知不只美國，大陸也有這麼做。

三、業者協力義務

20.問: 如果犯罪非屬於通訊監察書上所列，應如何監察？通訊監察實務執行遇有困難的部分?

答:問題可能出在電信業者，而不在法律條文，電信業者是營業單位，要搶市場，像網路電話現在不是要配發 070 開頭的，可是實際上電信為了拓展市場，就偷偷把市內電話門號配在網路電話上，可是 NCC 爭一隻眼閉一隻眼，他們把這門號配到網路上不打緊，但是電話只要帶到有網路的地方都可以打，會形成電話帶到大陸使用，但是打出來還是 02 開頭，網路電話號碼和帳戶對不到，且不需業者到定點裝機，被害人認為這是在台灣為什麼抓不到，實際已在大陸。原本我們對市話是信任度最高的，反而變成比行動電話還難找，因為行動至少還有基地台，甚至有些業者連 IP 都無法提供，像是 so-net giga 等很多都無法做監察，就算我把票給他也無法，嚴格來說能做的只有中華電信一家，(其他能做到但可能是成本問題)，又沒有明確條文規定必須要做。

21.問:接上題，如上述情形該如何使用通訊監察書?

答:會看用戶是哪一家，如果是前述那些填了也是白填，即使法院過了，根本就拿不到資料，投單又會被退回，好像沒有條文可以要求看到通訊監察書一定要做，沒有處罰規定，退回後也只能鼻子摸摸沒辦法，法院又會問票給半年了怎麼什麼東西都沒有，還是業者配合度問題。

22.問:如果僅中華電信可以配合，那填申請書和傳統電話的監察申請書有無不同?例如可能沒有號碼?

答:就監那條線，不是填號碼。

顏警官說明：上網會有上網編號，通訊監察書一定會明確規定被監察者

23.問:接上題，如果通訊監察限於某條特定線，可能會攔到也使用這條網路線的無辜人該怎麼處理?

答:必需要特定用戶的，像大廈共用那種法院就會比較謹慎了，法院發票就在把關，就像 cable 數十用戶就不可能監察，cable 要到機房，現在 cable 也不會監，除非可以濾出來源，(濾的過程也是全部抓下來，發現不是 source 就丟掉，只是誰來監督?)所以目前 cable 都不會做監察，針對傳統電話線像是 hi-net

seed-net ADSL 才上線。

24.問:如果要特定到只有此用戶在用，就只有限於在家裡的情形，無線網路或公共場所該如何申請?

答:目前如此，無線網路如果是 3.5G，通訊監察中心是說可以測錄到，wi-fi 就沒辦法，但是登錄時要認證，所以應該也可以，看業者要不配合，因為以前網路是個三不管地帶，後來才指定 NCC。

台北市刑警大隊 訪談記錄	
訪 談 時 間：97 年 12 月 25 日 13 時 00 分至 14 時 30 分止	
訪 談 地 點：台北市刑大八樓資訊室	出 席 人 數：3 人
受 訪 者：鄭國隆 警官	訪 問 者：王煌玄、蘇三榮

一、通訊監察程序規範

1.問：針對網路通訊監察的流程

答：做過四件，我的網路監察指的是接網路線，還不包括語音轉售的監察，因為三四年前大家也不知道什麼是語音轉售，大家看到那電話號碼就覺得很奇怪，怎麼會是一家公司去申請，和信的門號大家都在用，以前的做事先取得權力時間，去和二類公司調號碼是哪一隻，取得這一隻以後，在看有沒有監察機制，通常是沒有，比較能做的是 E-mail，聽說也是收到監票後幫你去信箱看，不是真正的監察，真正的監察應該是第三人也不知內容。

E-mail 要先查到帳號，然後確定是什麼方式申請，例如 CABEBL，可能就要去查裝機地址，配給他的信箱是哪一隻，然後再向檢察官申請，通常我們遇到的方式，都不是很一致的回覆你，還要去和它裡面燒光碟，另外取得機房接線，接的方式都不太一樣，現在有機台，以前要說幾月幾號、哪一條用戶、編號，監票給他，有的是回光碟，光碟沒有用他們的電腦開還開不起來，要用特殊軟體，如果有訊息的話，文字又不完整，URL 又不是很清楚的 URL，以前網路監察差不多就是這樣，監察的部份最基礎就是要調 E-mail 的信，你就是為了看他的內容才會去申請監票

ISR 部份比較少，一張通聯裡面有 ISR 資料，會下給受話方，以前監票好請，聽一聽不是可以換，今天聽一聽是語音轉售的話就去聽他的線，如果二類電信業者沒有衡量好電信監察機制的話，他就不敢去偷這條線了，聽受話方對話內容都一樣。VOIP 曾遇到我們去機房裝的時候，他們說沒開放，所以 VOIP 的部份比較沒有做，

2.問：現在申請監察票是哪種案件比較多

答：如果依照通保法就要五年以上重罪，或其他所列特別案件，那我的部分都是槍枝，之前在分局還有詐欺

3.問：那有無遇到有需要通訊監察的罪名而通保法未列?

答：應該是說有這樣的案件很多，但都開放就太浮濫了，例如竊盜，以被害利益來說可能超過詐欺，但刑法上並無分級，所以很可惜，所以你知道哪些地方可以銷贓，也不能聽，那種東西他們不是面對面講就是用辦公室電話講，所以我相信外勤人員應該會講竊盜，但是反過來說竊盜都可以聽這樣的案件

就太多了，汽車竊盜要怎麼抓，不能聽，他一定是用別的案子，例如毒品，聽到竊盜再另外啟案偵查，所以你常會掛別的案子聽，這樣的案件只有誰能做，例如說調查局，一定是把人力放在毒品上，要是聽到別的案子，也沒有人力去做，我認為通保法已經規範的很好了，我相信他們也想過竊盜的問題，但是現在要減少監察量的情形會背道而馳，就法制來說，可以被害標的的價值，去判斷是不是可以實施通訊監察，應該要區分為重大或是銷贓

4.問：所以理論上所有刑事案件都可以用通訊監察的方式偵辦?

答：我認為應該是，但是被害價值並沒有明顯的區分，我們今天太侷限於罪名，例如駭客案、個資的部份沒有其他技巧能力，就是只能透過分析再分析，沒有監察，除非另起詐騙的案子，不然無法監察

5.問：網路監察票和一般監察票填寫由不同?例如識別的特徵

答：我等一下可以列印一個案子裡面有電話和網路還有 E-mail 有三種，E-mail 包含在網路上面，這傢伙跑去網咖，所以我又監了 E-mail，如果你要取得這三個，電話不用講，網路線就要另外在監察書寫到用戶號碼，通信地址、使用者名稱，通常我還附上犯罪事由，每次登錄的時間長度，中華電信給他的 IP 是什麼，附件證明他的確常用這條網路線，他上過什麼地方，不然我監他的線都沒封包就沒什麼好監，Email 就要知道是那家業者，可能是一類中華電信，或是非屬一二類的雅虎，知道這些以後，長期登入的次數，都從哪些 IP 進去，登入的服務有什麼，申請 mail 帳號留下的資料。

我們不監 IP，例如亞太是用號碼當標的，在這電話上所有 ADSL(非語音)都監察，除非監察書中有說含本線語音，就算他固定 IP，我還是要查申請人的編號，還以編號為主，附帶和檢察官說他的地址，甚至於繳費方式，申請人是誰，有無前科，網路申請人和我其他被監察人的關係，受監察處所就寫裝機地址，ISR 無受監察處所就沒填，那一欄附註原因，實務上監票就是用戶、號碼不一定要位址，網路就有了，裝機地址甚至會是先問中華電信要設在哪裡的機房，因為事實上是去機房監那條線，應該不用考慮到位址，就寫這支電話的持有申請人是誰，其他的都可以援引通保法規定，要位址的話例如無線網路就蠻難的，ISR 的話就一般一類一樣，VOIP 是公司的話就寫地點，沒有也沒辦法填，Email 就到哪都可以上，應該沒辦法受限於地點。

6.問:如果網路監察會寫出網路編號，這些線通常是家裡的線還是哪裡的線?

答:我監察過的都是 ADSL，所以都是個人裝機，之前有針對過無線網路的部份做過訪談，還包含 3G，概念都是一樣的，有線就填有線，3G 就是填帳單上的電話號碼，WI-FI 可能就會寫客戶編號，因為要儲值是用客戶編號。

7.問:是否限於個人用戶使用，監察票才會過

答:如果你查出這個 VOIP 是否屬於公司所有，你勢必就只能填那個公司，除非你有法知道這個時間是哪台分機在用的話，那當然就寫，不過大概沒法通過吧，你沒辦法在法制上細分到很細當時是哪一支電話打的。給號碼和時間也不知道是誰。

8.問:如果一條網路線有多人使用?沒辦法特定只有某個人使用，法院會准許這樣的監察票嗎?

答:語音的部分可能只有 VOIP 會有這樣的問題，就單純的網路部份，ISR 勢必要和二類電信查到真正號碼，email 網路的部分是一條網路線的話，會有其他用戶同時使用，全家人上網都抓的下來，監票上就要寫得很清楚，今天監察的網路線可能用戶有誰，我會去查他的人口，再用身分證號碼去向比較大家的網路服務業者查出有哪些 mail，可是以前可以，現在不能這樣反查，所以變成 data retention 的問題，我們沒有限定規範可以提供反查的話，那我就不讓你營利，那我就給你發還，必須要限制這些二類業者，或是你廣義的二類電信業者，能夠反查，你不給我反查我如何在監察時確保人權？不給我反查我怎麼知道他是誰？在同一條網路上會有誰？舉例給你聽我怎麼做，我們一條網路線上不是會有編號嗎，這段編號在這區間會有每次上的浮動 IP，如果有人登入代表這時段有人使用，那他就一個 IP，而且有時間，在他上網期間用了很多服務，他上了 UI、email、IM，甚至其他 ICP 給他的服務，各種服務一旦有認證機制，也就是要輸入 account 的話，ID 密碼就有驗證的問題，申請 ID 就必須要有個人的資料，必須要能讓我從這個人資料裡知道 ID 是什麼，或是給你 IP 給你時間，這個 IP 有沒在你們的服務去登入過，哪些 service，這個 service 的帳號是什麼，所以我就這麼做，假設這戶有很多人，我要監察一個，那個人是改造槍枝的，他的妹妹他老婆都不要，那我就先只調這條 ADSL 網路線，一段區間的所有 IP，這些 IP 和時間再向其他的例如雅虎露天 pchome 蕃薯藤調這些 IP 這些時間有無帳號登入的紀錄，就發現可能是犯嫌的妹妹或老婆登入的，那我就把他排除掉啦，監察的時候要跟法官說只監犯嫌的某個 mail，雖然整條網路線，但是我監查這條網路線上使用犯嫌帳號所進行的網路活動，其他人帳號排除不予監察。

9.問:所以會先確認誰是誰？那排除這動作事實上已經在監察這條線?

答:沒有監察，是在監察前，都是 retention 而已，只是調資料，我還沒做到內容，廣義的二類電信業者例如雅虎就不給你這麼做，因為你沒有規範他嘛，不讓你 IP 反查，這麼說一個架構要使用網路必須要有 service，要有 access、IP，三個是惺惺相惜，有 email 可不可以取得 account，可以阿，從 account 可不可以取得 IP 和 service，可以阿，但是現在業者都是只給你正向查詢，只能從 account 取得 IP 連的 service，不能反向，那這樣我怎麼排除，例如陳進興透過他小孩身分證號碼去取得 mail 帳號和軍火商連絡，如果我不透過

全家人身分證號碼去洗這些帳號的話，怎麼取得帳號，所以這是 retention 上就有缺失啦，沒有 retention 這些資料，而且沒有法律授權我們可以調，他一定有但不要幫你作，你沒有用法律規範他們必須有義務做這些 retention 而且提供給司法警察機關的話，他才不理你，但事實上當然他們會認為說我用某個 IP 去洗這段時間所有帳號，會有很多和案件無關的帳號，他們會認為這樣侵犯人權，但是事實上如果我們為了取締不法打擊犯罪，勢必會干涉到無關的人，但是法律上本來就賦予我們這種特許權，我們是警察，一定在辦案的過程中，這社會是公開的，一定會牽扯到其他人，但是他不是我歸責非難的標的，只是我經過而已，所以我的部分如果我要監察某一個對象，要很明確的我只是要監察他，在那之前可能我已經聽過電話了，知道他太太和妹妹和案子毫無相關，只是我們監察可能會監察到他們，所以 retention 一定要有，但是 retention 之外還要能夠反求，(Q:民眾擔心的是遇到比較不好的警察，所以要的是一個監察機制，在過程中即時你有機會碰到，但是與犯罪無關的，誰來監督丟掉這東西?)美國不就這麼做嗎？美國甚至聽到與案件無關的就不能聽了，但我們沒要求那麼嚴格，因為已經是道德約定俗成才有法律，所以既然法律都已形成了，何必去管道德的問題，他們會擔心道德的問題，可是法律是道德約定俗成才有法律，當然會有人不法，難道因噎廢食嗎，所以有些業者就很奇怪，怕有人亂查。

例如雅虎發生詐騙，民眾報案，很多需要雅虎配合他不配合，那我就沒辦法偵查，破案率就降低。

10.問:所以是在過濾的時候你就會看到聽到很多帳號的內容或是？

答:過濾期間只會看到帳號，沒辦法看內容

11.問:這樣怎麼確定誰是目標?

答:所以我說你要 retention 而且要可以反向，舉我剛才的例子，某個監察對象和他太太妹妹，我要排除掉監查過程中監到他們，必須要先知道他們有什麼帳號，那如果這帳號本身有身分驗證稽核，準確度很高的話，如果用他太太妹妹的身分證字號，身分證號碼屬於個人資料但非機密，或許我們警方可以取得，查有沒有申請這些資料，如果驗證機制有準的話，確認某幾個帳號是他太太或妹妹。

12.問:網路監察的過濾和一般傳統電話監察過濾是一樣作法嗎

答:電話監察其實一樣過濾，不管你的票據，一類不管是 2G3G 你一定要過濾過，才有辦法監察，依照現在的法制，甚至你要透過其他方式去確認現在監察這支電話的準確性，這些方式不一定合法，可能必須透過線民，第三人蒐集資料，警執法給我們的權限，去確認電話號碼是不是這個人，然後再調機子來看，因為有時候機子就真的不是這個你要監察，如果你調的用戶和持機人不

同，被監察人不一樣那就人頭，你怎麼證明你現在監察的對象使用這支號碼，很難，所以有時候你要透過其他迂迴的方式去確認，所以不管是一二類的監察，都一定要有過濾行為，不能有太廣泛的偵查。

13.問:一般這過濾大概要花多久的時間？

答:很長，看案情，緊急上線的話就要透過檢察官的幫忙，以一類電信來舉例，你要馬上緊急上線，要取得 cell ID，緊急上線的目的是要取得資料，而不是取得一支電話，所以緊急上線在我們警察機關內規，是要重大案件才可以，緊急上線有兩種，一種是取得 cell ID，他會用很多路線的 cell 去取得裏面有交集的號碼，這是一種，另外一種是我今天反查，現場發生了反查，就是有一個電話號碼適用某一個人，我要知道他現在的行蹤，那就會有他的電話了，或是由他的身分資料去反查出電話，馬上做緊急上線。你剛說緊急的情況下要怎麼過濾，緊急的情況你還是找 cell，就用 cell 過濾，你還是必須透過反查，縱然是 cell ID 的部分的話，也有無線的問題，一定有監視器，用案發地案發時間當時的 cell 是哪個，這樣還是有過濾，大致上你還要一般的過濾，絕對不能想接哪個就接哪個，很難，現在法制也不太可能。

14.問:經過過濾後，確定帳號，監察的時候有無可能會牽涉到其他不相關的帳號？

答:如果是針對帳號的話，除非這帳號有很多用戶使用，可是今天你很難非難警方說我去確認這帳號現在是誰在使用，因為他是掛在同一個帳號上面，我又沒在電腦前裝監視器，怎麼知道現在是誰在用，當你還沒監察的時候，你根本也看不到他的內容，先生在用講話的對象是他公司同事，太太在用可能是他的家人，從內 容可以看出誰在用，都是同一支帳號同一支電話，你必須要看到內容，如果還沒監察一定看不到內容，除非你喬裝誰和他談，所以你沒辦法非難，如果我今天監的是帳號，已經是很細的，已經可以個化，原則上不會牽涉到其他帳號。

15.問:網路電話監察是要和業者調還是可以即時監察？

答:大部分都要去機房裝，因為我相信現在沒有二類業者可以提供假設是雅虎即時通在使用他們網路服務下的封包，應該是沒辦法，可以抓得下來，但是如果你沒有透過即時通給你的編碼方式，也沒辦法去取得，也沒辦法破解。

16.問:到機房裝抓下來的封包要如何解碼？

答:所以刑事警察局才會去蒐集各種的解碼的方式，沒有到每家，但是應該可以涵蓋到百分之八九十，很強了，除了 google 的好像不行，google 也有 google 通。其他我相信都可以，今天只要取到監票，我們刑事警察局也是蠻利害的，他們也是想辦法弄到一個主機讓你去裝，裝完他幫你解好，以前我們請二類電信做，就是燒光碟的那種方式，他沒辦法解碼，技術上一定可行，可是他

敢不敢這麼做有沒有人幫你作是一回事。雅虎和 msn 的編譯方式都很簡單，大部分適用這兩者，少數用 skype。

17.問:網路封包都是先抓下來再進行過濾嗎

答:網路線上一定是全抓下來，但是之前有能力先排除的就先排除，是看到這帳號不是你要的不去看他，當然業者如果到這麼強，監某條網路線，這條網路線是用某些 account 我才要，你有本事就這樣做，我當然可以接受。通常是全部抓下來到警方這邊選擇要看不看，如果業者可以事前幫我過濾好，當然是沒問題，但是他有那麼厲害嗎，那表示業者很強可以看到所有帳號，法制單位要相信業者還是相信警察。

18.問:如果要全部抓下來是不是只特定線才可？網咖或公司的情形?

答:只有網路線，個化到某人，公司網咖不特定量太多，監察不會過，也不能授權給警方這麼做。一個房東向二類電信業者買一個網路線，給各戶使用，我不知道哪一戶，我申請某一段，可能監察量到 10%就已經知道是誰了，就只要監察那戶就好了

19.問:對象跑出家門外做通訊，就比較難監察到?

答:所以我剛說除了 2G3G、家用電話、ADSL 以外，還要去監他們使用的 account，這樣他到別地方用才可以個化到他

20.問:通訊監察的監督機制有沒要向誰報告？報告內容？

答:定期向指揮檢察官和開票給你的法官報告，一個月報告兩次，期中期末，就是現行的通保法規範，其他就沒有了，其他就是你自己單位裏面的公務倫理報告機制。報告內容就是我現在聽到哪裡聽到什麼東西，有沒有必要下一次通訊監察終止前再針對某一項目減縮或擴張監查內容，俗稱的擴監。我們和檢察官報告，檢察官和法官報告，檢察官那麼多案子沒辦法實質參與監察，但是要把帶子結果給他，有權力去聽，但他不可能每個案子都聽，他可以調，可以請他的事務官去聽，他有辦法監督，考量當時能力可不可以做，考量對受指揮單位的信任感。

二、通聯資料保存

21.問:網路上通聯紀錄調取的部分，主要調哪種類資料？

答:像 skype，就必須知道哪個國家打進來、接線的 IP、本國受話的電話、期間，現在 skype 還有給 payment access。但是沒有辦法給電話號碼查誰曾打過，還是要給他帳號，但是 2G3G 可以給受話方，查有哪些發號方聯繫過，調受話方的雙向通聯紀錄，可以知道發號方有誰，網路電話 VoIP 我是不知道，

ISR 應該是可以。

22.問:通常調這些通聯資料的目的是在過濾之用或是偵查？

答:過濾就是偵查，有些案子沒辦法通訊監察，我們就只能透過調 CDR 來去解決這些問題，不然案子都不用破了，還是要有其他方式偵辦

23.問:上網紀錄通常是要向誰調？調怎樣的記錄？

答:向有提供這樣的服務的業者調，調的方式絕大部分是正向，用 ID、時間，請他給我們這個 files,比較深一點的反向,提供 IP,中華電信可以給你到 URL,seednet 可能就不行，如果就有通聯性質的話，現在比較能做到就是中華電信，像雅虎所謂的通聯就只給你 email 申請人資料和 email local files，但是寄給誰不知道，所以這不算通聯。所以 email 的部分通聯幾乎是沒有，必須要作監察,沒有辦法透過 email 通聯知道和誰聯繫。相信科技上是可行，可是業者認為沒有法律規定可以給你，這法理好像怪怪的，到底是規範可以給你什麼，還是規範不可以給你什麼。比較像有通聯概念的就是中華電信多給你一個他上線的 URL，但是線上寄信給誰也不知，這是一類電信也沒辦法給你的，比較健全的 hinet 也沒辦法給你。

24.問:上網紀錄是和電信業者或是其他網路服務提供者調取

答:3G 沒有 IP，就要向電信業者調，網站就向網路公司調，或是有些二類電信業者不是有架站部分嗎，提供空間給你，你就要向這些電信業者要這個網站申請人資料。

25.問:上述資料可以到多詳細？

答:買那網站空間當然是越簡便越有好處，要很多資料誰要去申請那網站，同業有那麼多好申請的，又不是免費，幹嘛要那麼辛苦，資料不多啦，通常也不會有驗證，最多就是付費和留電話聯繫那一段，剩下就沒有。只要一個傳真申請單匯款給業者，就可以改出去的號碼改成地檢署的號碼，他只要錢而已，後來被刑事局抓，就查到真的有一張申請表傳真的，還不是正本，在某段時間把我們的出現號碼都弄成地檢署的號碼。他們會認為這是業務，哪知道什麼東西。

三、業者協力義務

26.問:現在有業者提供反向查詢給警方嗎?

答:只有受規範的一二類電信業者才有，通常只有一類電信，二類電信很多還沒有,還有受一類電信規範的 IAP 通常會有,我不知道他有沒規範在二類電信，因為很多家搞不清楚，類似這樣，或是 so-net，用身分證字號去查他們會給我，速度快與否，IAP 通常會給，IPP、ICP 通常是正向，那部份很好的會給

反向，還可以幫你交叉，查出這個帳號就是和哪個帳號一起，是同一個人使用的

27.問:有遇到法律上業者應該要給資料卻遭到困難的情形？

答:因為目前能夠作的都是從刑事警察局的平台上抓的，基本上平台上可以 work 的東西，他都要給我，那都沒問題，他有錢賺，我們能下的也就是行政局給我們的網站平台上那些參數，所以目前沒有遇過要的是他不能提供的。今天只能針對他有的、開放給警方調閱的，刑事局選單裡有的我才能調，其他不行，暫時還好啦，以一類電信的機制是蠻充分的。

28.問：其他業者配合問題

答：剛剛和顏警務聯繫，我們在 ICC、ICP 這些的通訊監察或是 DATA，其實就和二類電信一樣的問題，它們不屬於第二類電信條例，但事實上現在它們和二類電信差不多，例如雅虎廣義上是但不受法律侷限，它們理論上是要去申請，可是並沒有強迫，所以調紀錄有難度，大部分問題不在一二類電信，他們都有法源可約束，可以透過光碟調記錄，非一二類電信都很調皮，他們也不是外商，但是在台灣要申請營利事業登記。所我們最大的困難是在非一二類電信的 ISP 提供網路服務業者，ISP 有分很多種，有 ICP、IPP 等，但他們不屬於二類電信業者。

29.問:那有沒其他通訊監察調資料或其他問題？

答:通訊監察我覺得已經很強了，主要還是在歸類哪些是二類電信，就是說應該是提供二類電信服務的業者沒有明確規範在二類電信裏面，所以他們不用去遵守法規，也沒罰則。高興給你就給你，不高興給你就不給你，所以真正有問題的不是現在規範的二類電信業者的 data retention，他的 data retention 還是有很多問題，你看大部份的二類電信業者的 retention 時間還是不夠長，那再來就是說監察機制不是那麼完整，如果要你幫他做監察平台那很好嘛，那要付出很多成本而且又太多家，另外就是他的規模性很容易出問題。但是我覺得最大問題還是在非一二類電信業者，根本就沒有規則可管，所以問題應該是在非一二類電信業者但是卻提供電信服務、資料傳輸等各種營業項目很像，資本額更大，賺的錢更多，用戶更多，那為什麼一個資本額三十萬的二類電信業者就要作監察，什麼都要配合刑事局和 NCC，動不動還要被罰錢，當然二類電信業者 retention 還是很重要，大概是這樣。