PG10103-0407

網路平台業者紀錄保存規範之研究

受委託者：中華警政研究學會

研究主持人：廖有祿

協同主持人：張維平

研　究　員：蘇莞筑、劉怡汎

研究助理：楊佳蓁

內政部警政署刑事警察局委託研究報告

中華民國 101 年 11 月

（本報告內容及建議，純屬研究小組意見，不代表本機關意見）

目　次

目　次 I

表　次 VII

圖　次 IX

摘　要 XI

一、研究緣起 XI

二、研究方法及過程 XII

三、重要發現 XII

四、主要建議事項 XIII

第一章　緒　論 1

第一節　研究問題與背景 1

一、研究問題 1

二、研究背景 1

第二節　研究動機與目的 7

一、研究動機 7

二、研究目的 8

第三節　研究範圍與限制 11

一、研究範圍 11

二、研究限制 11

第四節　相關名詞定義 12

一、網路 12

二、網路平台業者 12

三、網路平台業者紀錄 15

第二章　文獻回顧 17

第一節　我國現有法規 17

一、網路平台業者紀錄保存規範 17

二、網路平台業者紀錄查詢規範 21
第二節　國內相關研究 23
一、網路平台業者紀錄保存規範 23
二、網路平台業者協助犯罪偵查法制 25
三、網路平台業者協助偵查規範 27
四、網路平台業者法律責任 31
第三節　美國現有法規 37
一、電子通訊隱私法（Electronic Communications Privacy Act, ECPA） 37
二、愛國者法（USA Patriot Act, USAPA） 40
三、愛國者改進與再授權法案（USA Patriot Improvement and Reauthorization Act, 2005） 40
四、犯罪偵查通訊協助法（Communications Assistance for Law Enforcement Act, CALEA） 41
五、外國情報監察法修正案（Foreign Intelligence Surveillance Act Amendments Act, 2008, FISA） 42
第四節　歐盟現有法規 43
一、個人資料保護指令（Directive 95/46/EC） 43
二、電信事業個人資料處理及隱私保護指令（Directive 97/66/EC） 43
三、電子通訊中個人資料處理及隱私保護指令（Directive 2002/58/EC） 44
四、個人通訊資料保存指令（Directive 2006/24/EC 45
五、網路犯罪公約（Cyber-crime Convention） 50
六、歐盟各會員國之國內法規 52
第五節　亞洲現有法規 56
一、日本 56
二、中國大陸 74
三、新加坡 80
第三章　研究設計 87

第一節　研究方法 87
一、文獻探討法 87
二、焦點座談法 87
第二節　研究過程 88
一、國內外相關法規之蒐集彙整 88
二、偵查機關偵辦網路犯罪案件現行作法與所需協助 90
三、網路平台業者現行資料處理作法 91
四、可能修法方向之評估及建議 91
第三節　進行步驟 92
第四節　研究預期成果 93
一、預期成果 93
二、對相關業務之助益 94
第五節　研究分工 96
一、人力配置 96
二、進度管制 96
第四章　資料分析 97
第一節　立法與修法之優缺點比較 97
一、國內學者看法 97
二、本研究認為修法與立法之優缺點 102
第二節　國內現有規範修法建議 106
一、現有法規修訂建議 106
二、採取修法途徑之理由 116
第三節　電磁紀錄之保存項目及期間 119
一、各國現況 119
二、我國現況 120
三、紀錄保存規範之建議 122
四、網路交易定型化契約應記載及不得記載事項指導原則 131
五、小結 138

第四節　保存紀錄之調閱程序、回覆時間及罰則 147
一、我國現行法規 147
二、小結 155
第五章　結論與建議 159
第一節　結論 159
第二節　研究建議 162
一、修法建議 165
二、立法建議 189
附錄一　通訊保障及監察法 201
附錄二　通訊保障及監察法施行細則 207
附錄三　電信法 211
附錄四　第二類電信事業管理規則 213
附錄五　電腦網路內容分級處理辦法（101 年 6 月 13 日廢止） 219
附錄六　兒童及少年福利與權益保障法 221
附錄七　個人資料保護法 225
附錄八　電信事業處理有關機關查詢電信通信紀錄 實施辦法 229
附錄九　電信事業處理有關機關（構）查詢電信使用者資料實施辦法 231
附錄十　第一類電信事業經營者名單暨 其業務項目一覽表 233
附錄十一　第二類電信事業經營者名單暨其許可服務 範圍一覽表 235
附錄十二　美國電子通訊隱私法（Electronic Communications Privacy Act, ECPA） 237

附錄十三　美國愛國者法（USA Patriot Act, USAPA） 239

附錄十四　美國愛國者改進與再授權法案（USA Patriot Improvement and Reauthorization Act, 2005） 241

附錄十五　美國犯罪偵查通訊協助法（Communications Assistance for Law Enforcement Act, CALEA） 243

附錄十六　美國外國情報監察法修正案（Foreign Intelligence Surveillance Act Amendments Act, 2008） 251

附錄十七　歐盟 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data 255

附錄十八　歐盟 Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector 257

附錄十九　歐盟 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector （Directive on privacy and electronic communications） 259

附錄二十　歐盟 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC 261

附錄二十一　歐盟網路犯罪公約（Cyber-crime Convention） 265

附錄二十二　日本刑事訴訟法 269

附錄二十三　日本法務省／通信履歷の電磁的記録の保全要請に関するＱ＆Ａ 271

附錄二十四 日本サイバー犯罪条約（Cybercrime Convention） 273

附錄二十五 日本ハイテク犯罪に対処するための刑事法の整備に関する要綱 279

附錄二十六 日本プロバイダ責任制限法 285

附錄二十七 日本電気通信事業における個人情報に関するガイドライン 289

附錄二十八 日本電気通信事業法 293

附錄三十 日本犯罪捜査のための通信傍受に関する法律 297

附錄三十一 中國大陸互聯網電子公告服務管理規定 305

附錄三十二 中國大陸互聯網信息服務管理辦法 307

附錄三十三 中國大陸計算機信息網絡國際聯網安全保護管理辦法 309

附錄三十四 中華人民共和國計算機信息網絡國際聯網管理暫行規定實施辦法 311

附錄三十五 中國大陸互聯網新聞信息服務管理規定 313

附錄三十六 新加坡濫用電腦法 315

附錄三十七 新加坡電子交易法 319

附錄三十八 新加坡電信法 325

附錄三十九 電信法修正草案條文對照表（摘要） 329

附錄四十 「網路平台業者紀錄保存規範之研究」座談會會議紀錄 333

參考文獻 349

表　次

表 4-1　修法之優缺點 102

表 4-2　立法之優缺點 103

表 4-3　相關法規與主管機關 115

表 4-4　網路平台業者紀錄保存時間及法規修訂建議表 132

表 4-5　網路平台業者紀錄保存時間相關法規及主管機關 134

表 4-6　第二類電信事業管理規則第 27 條修訂建議表 139

圖　次

圖 1-1　電腦網路犯罪發生與破獲統計圖 2

圖 1-2　妨害電腦使用案件發生與破獲統計圖 3

圖 2-1　ISP 免責之立法模式圖 35

圖 3-1　執行進度甘特圖 92

摘　要

關鍵詞：網路犯罪、網際網路平台提供者、紀錄保存規範

近年中華郵政計畫取消限時專送服務，即由於大量的信件改由電子郵件傳送。網際網路的盛行，提供網路使用者更便捷傳遞訊息的方式，也改變了一般民眾傳遞訊息或購物的習慣與商業模式。然另一方面，網際網路平台服務也提供有心人士遂行詐騙與犯罪的空間。警察機關職司犯罪偵查，偵查此類網路侵權或犯罪案件，端賴網際網路平台提供者是否正確保存相關記錄，及保存適當時間。然國內目前對於網路平臺業者保存紀錄未有明確之規範，本研究旨在對於網路平台業者紀錄保存規範提出建議。本研究之研究方法包含文獻探討法與焦點座談法，以了解近期網路及網路平台之發展、各先進國家發展現況、各相關機關及業者意見，最後評估我國未來可能修法或立法方向，提供實務機關研擬相關策略參考。本研究對於各國及國內網際網路平台提供服務記錄保存之現況，有以下幾點重要發現與建議：一、在電信法相關法條以增列定義之方式擴及網際網路的使用及紀錄保存，可解決現有法規對於網際網路平台提供服務記錄保存規範不足之問題；二、修訂電信法相關法條以規範已明確定義之網際網路平台提供者及網際網路平台提供服務紀錄保存所需資訊。三、修訂電信法關於電信事業應辦理資通安全事項之規範，以確保電信事業系統設備、資料及網路之安全，保障民眾通信權益，並保全犯罪證據。四、將「第二類電信事業管理規則」第 27 條現有對於網際網路平台提供服務紀錄保存之規定，作適度修訂可健全網際網路平台提供服務紀錄保存之規定。

一、研究緣起

近年由於網路詐騙與網路侵權事件頻傳，已影響網際網路正常發展與社會治安。警察機關職司犯罪偵查，偵查此類網路侵權或犯罪案件，端賴相關行為是否正確記錄，並保存適當時間，可提供偵查機關依法查詢以協助偵查。網路犯罪偵查需仰賴各網路平臺業者之資料保存，藉此追查出真實犯罪者。然國內目前對於網路平臺業者保存紀錄未有明確之規範，因此律定網路

平臺業者記錄保存之適法性實為重要議題。本研究即在對於網路平台業者紀錄保存規範提出建議，以有效協助偵查犯罪，保障網路業者與消費者之權益，並促進網際網路環境正常發展。

二、研究方法及過程

本研究之研究方法包含文獻探討法與焦點座談法，以了解近期網路及網路平台之發展、各先進國家發展現況、各相關機關及業者意見，最後評估我國未來可能修法或立法方向，提供實務機關研擬相關策略參考。有關本研究之研究方法及過程說明如下：

（一）為了解各國對於網路平台業者紀錄保存相關規範，本計畫以文獻探討法蒐集歐、美、亞等主要國家有關網路平台業者電磁紀錄保存的相關法規，並對照我國現行法規加以比較分析，再參考國內外相關研究結論，透過定期會議研討，比較各種方案的利弊得失，找出適合我國法制的可能修法或立法方向，提供實務機關政策參考。

（二）另為避免本研究之研究結果不切實際，不符合實務機關需求，本計畫以焦點座談法之研究方法邀集偵查網路犯罪的警察單位、協助提供資料的網路平台業者及主管相關法規的目的事業主管機關進行座談，了解業務主管機關的政策立場、偵查單位辦案的實際需求、平台業者的考量方向，找出可行性高且效益彰顯之方案，提供主管機關擬訂修法或立法政策參考。

三、重要發現

本研究經過文獻探討蒐集各國網際網路平台提供服務紀錄保存相關規定，及邀集相關主管機關、網際網路平台提供服務者及警察機關辦理座談，本研究對於各國及國內網際網路平台提供服務紀錄保存之現況，有以下幾點重要發現：

（一）美國與歐盟針對電子通訊之法規已制訂及實行多年，直至 911 恐怖攻擊事件後，乃全面針對網際網路之使用與紀錄等規範有所訂定。而日本「刑事訴訟法」對於發動命令主體、適用對象、保存期間及保存項目等

有較明確之規定。國外有關網際網路平台提供服務法規主要是以歐盟「個人通訊資料保存指令（Directive 2006/24/EC）」及日本「刑事訴訟法」相關規範較具參考價值。

（二）我國目前現有法規已針對通訊監察、電信通信紀錄、電信使用者個人資料及電子郵件等內容，訂定相關規範。依據電信與通訊之同質性，本研究認為在電信法相關法條以增列定義之方式擴及網際網路的使用及紀錄保存，可補充並解決現有法規對於網際網路平台提供服務紀錄保存規範不足之問題。

（三）將網際網路平台提供服務納入「第二類電信事業管理規則」第 27 條，並明確規範網際網路平台提供服務者紀錄保存之規定，為解決目前「第二類電信事業管理規則」對於網際網路平台提供服務者紀錄保存規定未明之可行辦法。

四、主要建議事項

根據研究發現，本研究針對網際網路平台提供服務者紀錄保存與證據保全之規定的法制化，提出下列具體建議。

建議一

(建議事項)中長期建議

主辦機關：行政院

協辦機關：法務部、國家通訊傳播委員會、經濟部、金融監督管理委員會

有關網路平台業者紀錄保存規範之議題，本研究採兩案並陳之做法，先提出採修法方式之六大理由，並針對現有電信法、第二類電信事業管理規則、電信事業處理有關機關查詢電信通信紀錄實施辦法、電信事業處理有關機關(構)查詢電信使用者資料實施辦法、通訊保障及監察法、通訊保障及監察法施行細則等法令內容逐一檢視，列出修改建議之具體條文及理由；後再就制定專法部分，提出具體之建議法規名稱、條文內容及理由，惟國內尚無一專門的網路主管機關，故專法繫屬主管機關之問題，仍有待討論。本研究參考歐盟等有關電信事業資料庫安全與稽核機制（如 ETSC 及 ISO27001），

建議對於相關業者提供服務之系統與資料之證據保全予以規範，以確保偵查機關所取得之犯罪紀錄具有證據能力。

建議二

(建議事項)中長期建議

主辦機關：國家通訊傳播委員會

協辦機關：各目的事業主管機關（視網路張貼文章或傳送訊息所涉業務性質而定）

本研究參考日本刑事訟訴法第 197 條第 3 項之規定及我國通訊保障及監察法第 14 條第 4 項，修訂電信法第 2 條第 1 項第 8 款通信紀錄內容以涵蓋網際網路平台提供服務紀錄保存所需資訊。另本研究引用「電腦網路內容分級處理辦法」（2012 年 6 月 13 日廢止）第 2 條對於網際網路平台提供者之定義，納入電信法第 11 條第 4 項將平台提供者納歸第二類電信事業管理，以便第二類電信事業管理規則、通訊保障及監察法等相關法規在修訂網路平台紀錄保存規範時，對於網際網路平台提供者之定義能有一明確之依據。為提升網路犯罪證據保全，本研究建議增訂電信法第 40-1 條，規範電信事業有關資通安全應辦理事項。

電信法具體修法之建議如下：

(一)電信法第 2 條第 1 項第 8 款「通信紀錄：指電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼或 IP 位址、通信日期、通信起訖時間及其他通信歷程等紀錄，電信系統設備應具有配合提供紀錄之足夠功能。電信號碼係指電話號碼或用戶識別碼。」

(二)增列電信法第 2 條第 1 項第 9 款「九、電腦網路服務提供者：指網際網路接取提供者、網際網路平臺提供者及網際網路內容提供者。」

(三)電信法第 11 條第 4 項「第二類電信事業指第一類電信事業以外之電信事業。其中，網際網路平臺提供者指在網際網路上提供硬體儲存之空間，或利用網際網路建置網站提供資訊發佈及網頁連結服務功能者。」

(四)增訂電信法第 40-1 條：為確保電信事業系統設備、資料及網路之安全，

保障民眾通信權益及保全證據，電信事業應辦理下列事項：

一、建立資通安全管理機制。

二、建立資通安全防護及偵測設施。

三、建立資通安全聯防及資通安全事件之通報、處理、回報等資通安全應變措施。

四、使用經資通安全審驗之資通設備。

另配合修訂「電信事業處理有關機關查詢電信通信紀錄實施辦法」第 2 條第 1 項，及「電信事業處理有關機關（構）查詢電信使用者資料實施辦法」第 4 條第 1 項。

建議三

(建議事項)中長期建議

主辦機關：國家通訊傳播委員會

協辦機關：各目的事業主管機關（視網路張貼文章或傳送訊息所涉業務性質而定）

現行第二類電信事業管理規則第 27 條第二項第三款規定有關留言版、貼圖區或新聞討論群、免費電子郵件信箱、網頁空間線上申請帳號之來源 IP 位址及當時系統時間、電子郵件通信紀錄等，網路接取服務業者(IAP)應予保留以供查詢，然前述之服務應屬網路平台服務，並非網際網路接取服務，建議將第三款(四)、(五)、(六)移至新增之第五款網際網路平台提供服務，再於第五款對於前述網路平台主要之服務與活動及應保存之紀錄項目與期間予以規範。具體修法之建議如下：

(一)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六個月。

(二)電子郵件通信紀錄(含用戶帳號、來源 IP 位址、當時系統時間)應保存六個月。

(三)張貼於電子佈告欄、網路論壇、部落格或其他電子訊息平台之內容來源 IP 位址與當時系統時間應保存六個月。

(四)即時訊息通信紀錄(含用戶帳號、來源 IP 位址、當時系統時間)應保存六個月。

(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)免費留言版、貼圖區、新聞討論群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。

(七)免費電子佈告欄、網路論壇、部落格、即時訊息或其他電子訊息平台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。

建議四

(建議事項)中長期建議

主辦機關：法務部

協辦機關：國家通訊傳播委員會、經濟部、金融監督管理委員會

為使通訊保障及監察法能更符合調閱網路平台紀錄之適用，建議於該法第 5 條第 1 項增訂但書「調閱網路平台紀錄不受前項得發通訊監察書各款罪嫌之限制，惟應符合發動偵查之要件」；及增訂第 12 條第 4 項「調閱網路通信紀錄不受前項監察期間之限制，惟仍不得逾相關網路平台紀錄規範之保存期間。」之規定；並於第 13 條第 1 項增加「電磁紀錄調閱」一項，以使通訊監察之實施方法更為明確。

另通訊保障及監察法施行細則第 26 條第 1 項規定協助執行通訊監察機關之通訊系統設備需求，雖然須設置通訊監察設備之業務種類並不包含網路平台提供者，然本研究亦建議於本項後段增訂「網際網路平台提供者對於通信紀錄之存取，應建置足夠性能之相關設備，以供司法警察機關依法令偵查調閱」之規定，以確實達成其協助犯罪偵查之義務。

建議五

(建議事項)中長期建議

主辦機關：行政院

協辦機關：法務部、國家通訊傳播委員會、經濟部、金融監督管理委員會

如前述修法建議因修法時原法令之主管機關有意見，另可採訂立專法「網際網路平台提供者處理有關機關查詢通訊紀錄及使用者資料實施辦法」，依據行政院「防治網路詐欺專案會議」於 2010 年 9 月 21 日提出網路犯罪防制對策之長期方案，要求各網路平臺業者保存帳戶相關資料至少六個月以上。具體條文如下：

第 1 條（法源依據）

本辦法（以下簡稱本法）依通訊保障及監察法第十四條第二項及電信法第七條第二項規定訂定之。

第 2 條（名詞定義）

本法用詞定義如下：

一、 網際網路平台提供者（以下簡稱平台提供者）：指在網際網路上提供硬體之儲存空間、或利用網際網路建置網站提供資訊發佈及網頁連結服務功能者。

二、 通訊：指利用網路平台設備發送、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。

三、 通訊紀錄：指網路平台使用者使用網路平台服務後，資訊系統所產生之發訊方、受訊方之 IP 位址、通訊日期、通訊起訖時間及其他通訊歷程等紀錄。

四、 使用者資料：指網路平台使用者姓名或名稱、身分證統一編號、地址、用戶識別碼、電子郵件地址、IP 位址等資料，並以用戶申請各項網路平台業務、電子郵件或網路帳號所填列之資料為限。

第 3 條（申請許可及登記）

申請經營網路平台事業，應檢具申請書、事業計畫書及其他相關規定文件，向主管機關申請許可，經依法辦妥公司或商業登記，並取得許可執照後，始得營業。

第 4 條（查詢依據）

有事實足認被告或犯罪嫌疑人之違法行為係透過網路平台為之者，得向平台提供者查詢通訊紀錄。

平台提供者對於通訊紀錄及使用者資料之存取，應建置足夠性能之相關設備，以供司法警察機關依法令偵查調閱。

為確保網路平台系統設備、資料及網路之安全，保障民眾通信權益，平台提供者應辦理下列事項：

一、建立資通安全管理機制。

二、建立資通安全防護及偵測設施。

三、建立資通安全聯防及資通安全事件之通報、處理、回報等資通安全應變措施。

四、使用經資通安全審驗之資通設備。

前項系統設備包括核心網路設備、傳輸網路設備、接取網路設備、網路管理系統設備及其他重要電信設備。

平台提供者處理資通安全事件時，得要求用戶及使用人配合辦理資通安全有關措施；其屬重大資通安全事件者，必要時得暫停或終止服務之一部或全部。

前項之規定意旨，平台提供者應以顯著方式載明於營業規章及服務契約。

平台提供者資通安全管理機制之查核項目與程序、適用之驗證標準與範圍、資通安全之防護與偵測、聯防與應變、重大資通安全事件範圍及其他應遵行事項之管理辦法，由主管機關定之。

主管機關為進行網際網路資通安全聯防，應建置及管理資通安全聯防應變系統。必要時，得指定專責機構建置及管理之。

第一項第四款資通設備應施檢驗項目及其資通安全檢測技術規範，由主管機關訂定公告之。主管機關為資通設備安全檢測需要，應建置及管理資通安全測試樣本資料庫。必要時，得指定專責機構建置及管理之。

前項資通設備之審驗方式與程序、審驗證明之核發、換發、補發與廢止、審驗合格標籤之標貼、印鑄與使用，及審驗業務管理等事項之辦法，由主管機關定之。

第 5 條（保存項目及期間）

平台提供者對於調查或蒐集證據，並依法律程序查詢通訊之有無及其內

容者，應提供之，惟不得逾相關通訊紀錄及使用者資料之規範保存期間。

平台提供者對於第一項通訊紀錄應至少保存期間如下：

一、使用者線上申請帳號：使用者線上申請帳號之來源 IP 位址、當時系統時間、認證之行動電話、電子郵件帳號，平台提供者應至少保存至服務終止後六個月。

二、電子訊息平台網站張貼(傳送)文章(訊息)：使用者帳號、來源 IP 位址、當時系統時間，應保存六個月。

三、線上購物交易：網路買賣用戶之帳號、交易代號、數量、來源 IP 位址、當時系統時間，應保存六個月。

四、線上遊戲虛擬寶物轉移：遊戲玩家轉移虛擬寶物或遊戲幣之遊戲歷程(轉出帳號、遊戲幣、數量、來源 IP 位址、當時系統時間、轉入帳號、遊戲幣、數量)，應保存六個月。

五、網路證券交易：委託人帳號、委託日期時間、證券種類、股數或面額、限價、有效期間、營業員代號、委託方式、來源 IP 位址、當時系統時間，應保存五年。

六、電子銀行交易：交易日期、使用卡號、交易項目、交易金額、交易設備代號、幣別、來源 IP 位址、當時系統時間，應保存五年。

第 6 條（調閱程序）

有關機關查詢通訊紀錄、使用者資料應先考量其必要性、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通訊紀錄或使用者資料查詢單，載明需查詢之通訊紀錄種類、起迄時間、資料用途、使用者姓名及其身分證統一編號、法律依據、案由說明、查詢案號、查詢機關（構）、機關（構）主管、連絡人、連絡電話或傳真機號碼、機關（構）加蓋印信及其首長署名、職章等，送該平台提供者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通訊紀錄或使用者資料查詢單正本。

前項之查詢，經查詢機關與平台提供者雙方認證同意，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通訊紀錄或使用者資料查詢單正本。

第 7 條（受理回覆）

有關機關查詢之通訊紀錄或使用者資料，於平台提供者之保存期限以內者，應予受理並即時提供；已逾網路平台資料保存期限，致無法提供者，平台提供者應書面回覆說明之。

第 8 條（罰責）

有協助執行查詢義務之平台提供者，違反第 7 條之規定者，處以新台幣十萬元以上五十萬元以下罰鍰；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。

ABSTRACT

Keywords: Cybercrime, Internet Platform Provider, Data Retention Regulation

As the Internet becomes a part of our daily lives, criminals are increasingly using it to commit fraud and cybercrime. Law enforcement agencies are responsible for criminal investigation. The investigation of cybercrime cases rely on Internet platform provider(IPP) for the correct logs, and proper retention time. There is no existing law in Taiwan that regulates IPP to keep logs for specific items and time periods. This research is to propose executable regulation about data retention for IPP.

Research methodology in this study included literature reviews and focus groups symposium. Using this two research methods, the researchers understood the current status of data retention in some advanced countries and the suggestions from related organizations in Taiwan. Finally, after assessing our proposed law of the legislation or amendment, this study will provide the research findings and recommendations to relevant authority to elaborate substantive policy reference.

The important findings and recommendations of this research are listed in the followings:

I. increasing items in related articles of current Telecommunications Act can solve the problem of insufficient regulations of data retention for IPP;

II. the amendment of related articles of current Telecommunications Act can clearly define the information need to be kept for IPP;

III adding new article 40-1 of current Telecommunications Act can enhance the security service provided by IPP and ensure the evidence given in court is accurate;

Ⅳ. a moderate amendment of Article 27 of the current "Regulations for Administration on Type II Telecommunications Business" can cover the regulations of data retention for IPP.

第一章　緒　論

第一節　研究問題與背景

一、研究問題

本研究旨在探討「網路平台業者紀錄保存規範」之相關問題，由於現行法規對於網路平台服務業者之紀錄保存規定未明確規範，致網路平台服務業者缺乏規範依循以妥適保存相關紀錄，並影響執法機關對於網路犯罪案件之偵查。另由於網路具跨境特性，本國網路使用者會使用他國網路平台服務業之服務與資源，他國網路使用者亦會使用本國網路平台服務業之服務與資源。本研究希立於國際視野，蒐集、瞭解歐、美、亞等主要國家對於網路平台服務業者之法律責任及相關紀錄保存規範，做為我國制訂相關規範參考。

二、研究背景

（一）網路犯罪案件造成個人與社會之損害龐大

根據資策會調查國內截至 2011 年 12 月底止，我國商用網際網路帳號總數為 2,635 萬，經常上網人口亦達 1,097 萬人[1]。然由於網路人口龐大，其中不免良莠不齊，致使近年網路犯罪頻傳。依據內政部警政署統計 2005 年至 2011 年間，臺灣地區發生的電腦網路犯罪案件各為 24,479 件、22,711 件、29,285 件、26,523 件、26,479 件、17,748 件及 20,016 件；破獲數各為 5,768 件、10,900 件、21,260 件、20,840 件、22,289 件、13,172 件及 9,175 件，如圖 1-1。破獲率從 2005 年不到二成五，上升至 2006 年近五成，至 2008 年近八成，至 2009 年達近八成五，再降至 2010 年近七成五，2011 年為四成六。這些案件以網路詐欺、妨害電腦使用、侵害智慧財產權、妨害名譽、一般妨害風化、違反兒童及少年性交易防制條例、網路賭博等類型居多[2]。其中妨害電腦使用因係觸犯刑法第 36 章妨害電腦使用罪，內政部警政署特將此一犯罪單獨統計，2005 年至 2011 年間，臺灣地區發生的妨害電腦使用案件各為 18,298 件、8,108 件、6,677 件、4,216 件、4,048 件、3,851 件及 8,640 件，

[1] 資料來源：資策會 FIND，網址：http://www.find.org.tw/，上網日期：2012 年 5 月 8 日。
[2] 資料來源：內政部警政署，警政統計通報（101 年第 33 號），2012 年 8 月 15 日。

破獲數各為 654 件、620 件、745 件、865 件、1,168 件、671 件及 517 件，如圖 1-2；破獲率從 2005 年 3.57%，至 2006 年超越一成，至 2008 年超過二成，至 2009 年接近三成，至 2010 年跌至約一成七，再至 2011 年更跌至 5.98%[3]，相對於全般刑案破獲率約為八成，電腦網路犯罪案件破獲率顯然偏低。造成網路犯罪破獲率偏低的原因，網路服務業者（Internet Service Provider, ISP）的紀錄保存不完整為主要原因之一[4]。

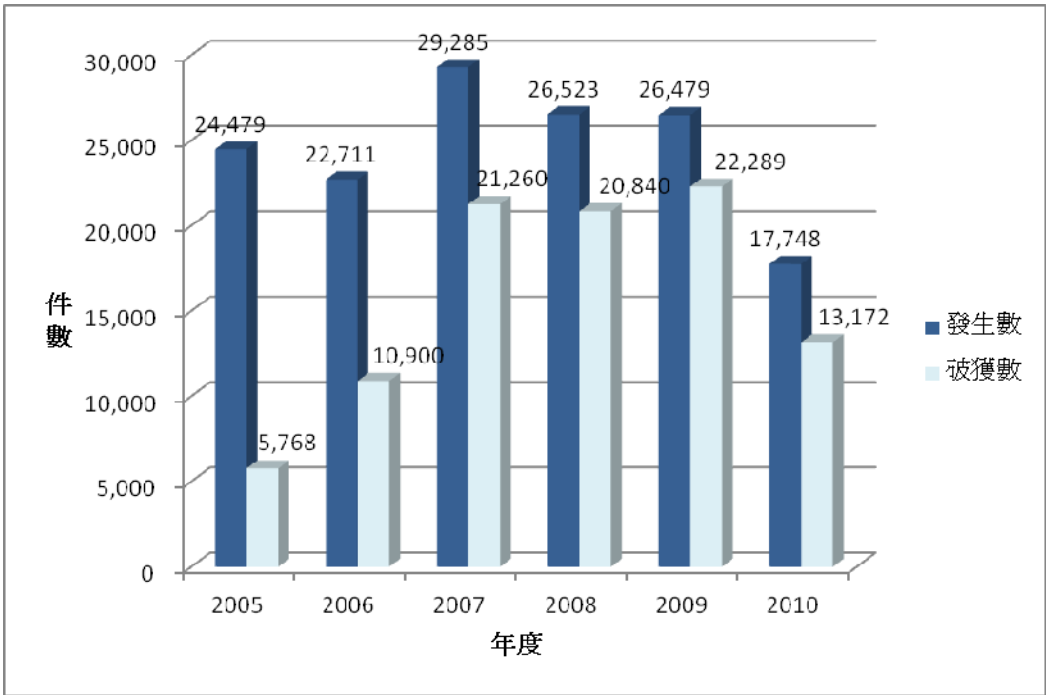


圖 1-1　電腦網路犯罪發生與破獲統計圖

（資料來源：內政部警政署，警政統計通報 101 年第 33 號）

[3] 資料來源：內政部警政署，警政統計通報（101 年第 5 號），2012 年 2 月 1 日。
[4] 章光明、張維平，2005 台灣年鑑—第十一章司法與人權-莫讓網路成為犯罪天堂路，中央通訊社，2005 年。

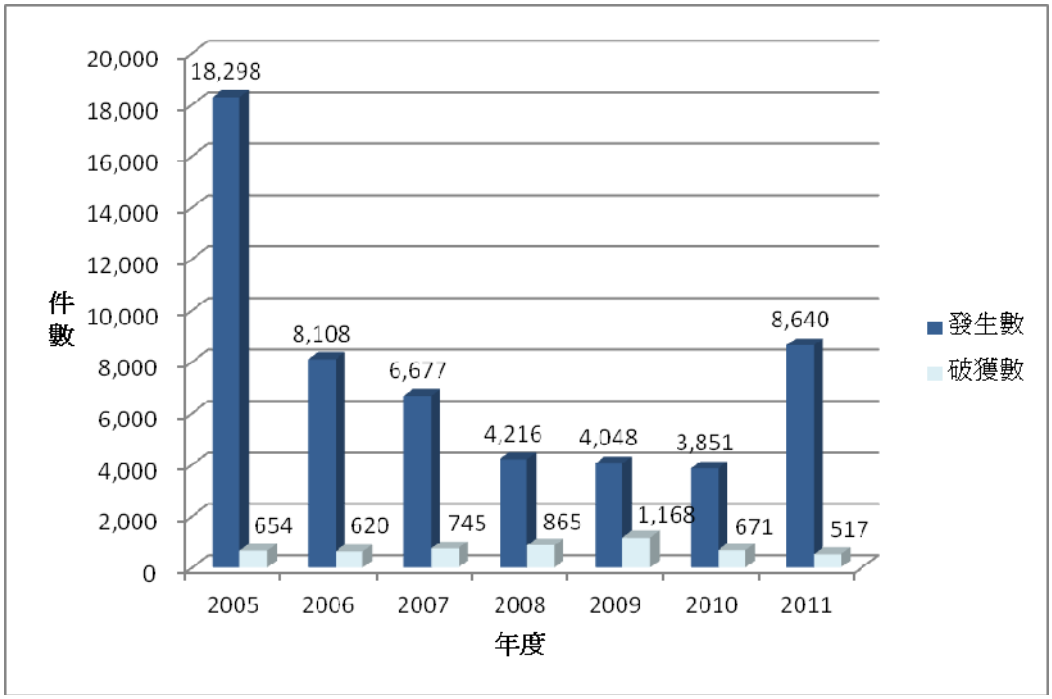


圖 1-2　妨害電腦使用案件發生與破獲統計圖

（資料來源：內政部警政署，警政統計通報 101 年第 5 號）

（二）目前仍欠缺網路通信紀錄資料保留專法

如前所述，造成網路犯罪破獲率偏低的原因，網路服務業者的紀錄保存不完整為主要原因之一[5]。國內網路服務業者包含四類業者：

1、網路接取服務業者（Internet Access Provider, IAP），主要在提供使用者上網之服務，如 Hinet、SeedNet 等。

2、網路內容服務業者（Internet Content Provider, ICP），主要提供網站內容及資訊之服務，如雅虎奇摩等。

3、網路平台服務業者（Internet Platform Provider, IPP），主要提供網站平台服務，如 Hinet、雅虎奇摩等。

4、網路應用服務業者（Application Service Provider, ASP），主要提供應用軟體服務，如金融業務軟體服務或遊戲軟體服務等。

電信法對於這些網路服務業者有相關的規範，然僅對於網路接觸服務業

[5] 章光明、張維平，2005 台灣年鑑—第十一章司法與人權-莫讓網路成為犯罪天堂路，中央通訊社，2005 年。

者的網路紀錄保存規範於「第二類電信事業管理規則」第 27 條：

「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。」

可見，第二類電信事業管理規則對於網路內容服務業者、網路平台服務業者及網路應用服務業者相關紀錄保存並未規範。又「個人資料保護法」已立法通過，如果犯罪者於犯案後要求移除個人資料，業者反而有配合義務；而對於網路業者應保存資料以佐證係故意或過失之外洩行為，已有明文規範，但對於網路平臺之客戶登記資料、交易等稽核紀錄，可用以掌握犯罪者活動、交易情形與登入狀況之資訊，尚未有一套規範機制，任由業者自行安排，因此多數業者常基於營利前提下，摒棄提供安全網路環境，將讓網路犯

罪成為失控的自由，無法掌握犯罪者行蹤。

此外，第二類電信業者目前達約 500 家，提供服務項目多元，包含語音單純轉售服務、網路電話服務、批發轉售服務、公司內部網路通信服務、頻寬轉售服務、語音會議服務、網際網路接取服務、存轉網路服務、存取網路服務、視訊會議服務、數據交換通信服務、付費語音資訊服務、行動轉售服務、行動轉售及加值服務等服務[6]。因此，第二類電信業者的資料保留，除通信紀錄資料外，涵蓋範圍已擴及至電子郵件、瀏覽網頁、社群網站、網路接取、網路電話、即時通訊、電子商務、線上遊戲等網路服務資料，已非以往「通信紀錄」之概念可完全涵蓋。法律規範之架構趕不上資訊發展之速度，導致法律規範密度不足。不論是網路通信紀錄資料保留項目或查詢方式，皆無法與目前實務需求相符，導致網路犯罪問題，實有待深入研究及規範之必要。

由於網路業者對於網路犯罪者之資料留存缺漏、不完整或過短，造成警方在偵查上盲點，且現行網路管理分散數個目的事業主管機關，相關網路管理有多頭馬車之情形，因此行政院「防治網路詐欺專案會議」於 2010 年 9 月 21 日提出網路犯罪防制對策之長期方案，要求各網路平臺業者保存帳戶相關資料(含使用者基本資料、IP 時間及網路交易內容等)至少六個月以上，然由於尚有適法性疑義及相關規範尚未定論，故擬經由本計畫研究其他國家作法與相關文獻內容，並查訪目前實務上之作為及所需協助，以探討相關規範及執行之可能性。

現行針對電信通信紀錄保留、監察，已有「電信法」、「通訊保障及監察法」等規範，在「電信事業處理有關機關查詢電信通信紀錄實施辦法」亦明文規範，其中針對電信通聯紀錄保留應至少三至六個月以上，讓警察機關偵查刑案，以及維持電信秩序具備適法性，另外針對網路接取服務業者(Internet Access Provider，IAP）在「第二類電信事業管理規則」中明訂應配合通訊監察與資料保留六個月的義務。

---

[6] 資料來源：國家通訊傳播委員會，2010 年 8 月 31 日。

反觀目前我國並未有一套規範網路秩序專法，將相關規範制定入法令補充，諸如：刑法增列妨害電腦使用罪章等設計。偵查犯罪亟需相關歷程資料，針對網路平臺業者保存紀錄之規範，我國現行法令並未有條文或相關行政作法研議，但偵查網路犯罪仍需仰賴各網路平臺業者資料保存，藉以追查出真實犯罪者。此概念與本計畫配合警察機關偵查網路犯罪，要求業者須保存資料一定期間之方向一致，以掌握犯罪者行蹤，進而遏止不法牟利之網路犯罪行為。

第二節　研究動機與目的

一、研究動機

如前所述，近年各年電腦網路犯罪案件發生數均多達 2.5 萬件以上，然破獲數僅約 2 萬件，平均破獲率約為六成四，如再檢視其中的妨害電腦使用案件，平均破獲率更低於一成。造成網路犯罪破獲率偏低的原因，網路服務業者的紀錄保存不完整、保留時間或欄位不足為主要原因之一。本研究之研究動機為網路平台服務紀錄保留不完整影響犯罪偵查、查詢網路平台服務業者紀錄須符合個人資料保護法規範、網路平台業者紀錄保存規範應符國際趨勢與世界接軌，茲分述如下：

（一）網路平台服務紀錄保留不完整影響犯罪偵查

我國目前現行雖有「電信法」、「通訊保障及監察法」、「電信事業處理有關機關查詢電信通信紀錄實施辦法」等規範，針對電信通聯紀錄保留應至少 3 至 6 個月以上之義務；及在「第二類電信事業管理規則」中亦明訂網路接取服務業者（IAP）應配合通訊監察與資料保留六個月的義務。惟我國電信法對於網路平台服務業者相關紀錄保存並未規範，又「個人資料保護法」已立法通過，對於網路業者應保存資料以佐證係故意或過失之外洩行為，已有明文規範，但對於網路平臺之客戶登記資料、交易等稽核紀錄（log file），可用以掌握犯罪者活動、交易情形與登入狀況之資訊，尚未有一套規範機制。

（二）查詢網路平台服務業者紀錄須符合個人資料保護法規範

個人資料保護法通過後，執法機關基於犯罪偵查需要查詢網路平台服務業者紀錄，必須符合個人資料保護法規範。網路平台服務業者亦應符合法律規範適當保留網路平台服務紀錄，以協助犯罪偵查。

（三）網路平台業者紀錄保存規範應符國際趨勢與世界接軌

由於網際網路具跨國特性，國內在訂定有關網路平台業者紀錄保存規範，亦應參考各國法規，以符國際趨勢並與世界接軌。

二、研究目的

為能健全整體電子商務發展與有效落實防制新興網路犯罪發生，網路業者律定資料保存之適法性實為重要環節，但亦需考量如何平衡業者私經濟成本與公共利益效益，因此有必要針對近期網路發展及遴選歐、美、亞等先進國家相關規範進行研析，並評估我國未來可能修法方向（例如：建議增修電信法或通訊保障及監察法相關規定），並提供實務機關未來研擬與制定策略之參考。

（一）探討電信監理機制之落實對犯罪偵查之影響

自從電信產業開放競爭後，第二類電信業者或網路加值服務業者如雨後春筍般蓬勃發展，電信業者基於營收考量未過濾客源承攬詐欺話務，間接淪為協助詐欺集團傳送異常話務之共犯。

本研究期能透過現有法律規範探討，瞭解通信紀錄調閱機制與資料保留問題，參酌歐盟、美國及亞洲等主要國家電信主管機關因應數位匯流所帶來衝擊之作法，提出可行之電信監理建議。

（二）探討網路通信紀錄資料保留規範及其面臨之問題

目前網路業者家數眾多且提供服務項目多元，涵蓋層面廣泛。囿於系統儲存效能差異，各家業者網路通信紀錄資料保留參差不齊，間接對執法機關調閱通信紀錄產生衝擊。

本研究期能針對通信紀錄調閱機制與資料保留問題對於犯罪偵查之衝擊部份，探討現行執法機關通信紀錄調閱機制、第一/二類電信業者保留通信紀錄的實際情形及其對執法機關調閱通信紀錄和犯罪偵查之衝擊。參酌歐盟、美國及亞洲等主要國家電信主管機關網路通信紀錄資料保留之作法，研提我國未來網路通信紀錄資料保留之建議，做為相關主管機關研修相關規範之參考。

美國網路通信紀錄資料保留相關法規有 1986 年的「電子通訊隱私法」、1994 年的「犯罪偵查通訊協助法」及 2001 年的「愛國者法」，加諸電子通訊提供者負有協助偵查之責任，包括配合實施通訊監察、提供通信紀錄等。

英國有關網路通信紀錄資料保留規定有 2000 年的「調查權力規制法」[7]。歐盟基於犯罪偵防與恐怖活動之調查目的，於 2006 年通過「個人通訊資料保留指令」強制公用電信事業經營者及網際網路服務提供者留存如發話號碼、用戶身份、某一 IP 位址之用戶身份個人資料，6 個月至 2 年的時間[8]。日本則有「刑事訴訟法」、「犯罪捜査のための通信傍受に関する法律」（犯罪偵查通信監察法）…等相關法令規定。

本研究參考歐盟、美國及亞洲等主要國家相關規範，希能有效協助國內執法機關偵查犯罪，確保網路犯罪案件發生或侵權事件發生後，能從網路平台服務業者所保留之通信紀錄，可以確認使用者帳號與使用紀錄，達可歸責性（accountability）以符合資訊安全要求[9]，保障網路平台服務業者與消費者之權益，以促使網際網路環境正常發展，吸引更多網路服務業者與消費者上網安心交易，促進電子商務更健全更蓬勃發展。

（三）探討網際網路平台服務紀錄或證據保全規範之問題

一件刑案發生犯罪證據在犯罪偵查過程扮演關鍵角色，犯罪證據之正確性不僅影響偵查機關能否將罪犯繩之以法，犯罪證據如不正確可能逮捕錯誤並攸關人權甚鉅。國內現行法規未有，關於網際網路平台服務紀錄保全或證據保全之規範。

本研究參考歐盟等有關電信事業資料庫安全與稽核機制（如 ETSC 及 ISO27001），於研究報告增列網路平台業者證據保全規範建議，確保警察機關可拿到正確有用之資料，並在法庭上具有證據能力。歐盟「個人通訊資料保存指令（Directive 2006/24/EC）」[10]，規定各會員國應確保公共電子通訊服

---

[7] 調查權力規制法（Regulation of Investigatory Powers Act 2000，簡稱 RIPA），資料來源：http://www.homeoffice.gov.uk。

[8] Directive 2006/24/EC of the European Parliament and Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[9] 林祝興、張明信，資訊安全導論，旗標出版公司，2009 年。

[10] 個人通訊資料保存指令（Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending, Directive 2006/24/EC）。

務提供者及公共通訊網路，至少應遵守有關資料保存之資料安全原則：

（1）保存之資料應與網路上之資料具有相同之品質、安全性與保護程度，亦即資料儲存時之安全性不能低於傳輸時。

（2）應提供資料適當的技術與措施以避免因意外或遭遇非法損壞、非預期損失或竄改，或是未經授權或非法之儲存、處理、存取或洩漏資料。

（3）應提供資料適當的技術與措施，以確保只有特定被授權之人員可進行存取。

（4）除曾被存取並要求留存的資料之外，應在保存期限屆滿即銷毀。

第三節　研究範圍與限制

一、研究範圍

本研究的研究範圍為網路平台業者紀錄保存規範，包含網路平台業者之法律責任、網路平台業者紀錄保存法律依據、網路平台業者紀錄保存項目、保存期間等問題。由於網路服務業者包含網路接取服務業者、網路內容服務業者、網路平台服務業者、及網路應用服務業者等四類業者。本研究範圍不包含網路服務業者中的網路接取服務業者、網路內容服務業者、及網路應用服務業者等業者。

二、研究限制

（一）國內外相關研究文獻少

本研究團隊發現一些國內外對於網路服務業者的規範與相關研究，但對於網路平台服務業者紀錄保存的研究與法規卻付諸闕如，影響本研究需要參考國外如美國、亞洲、歐盟等主要國家的規範與做法。

（二）網路平台服務業者定義不明確

國內法規或 NCC 對於網路平台服務業者缺少明確定義，無法確定網路平台服務業者的對象、家數與經營項目，就難以訂定應保存的紀錄欄位、內容及期間，影響研究之順利進行。

（三）研究時間與經費限制

由於研究時間與經費限制無法全面蒐集世界各國有關網路平台服務業者對於紀錄保存的規範，更由於管道有限，僅能查詢公開在網路的法律規範，無法獲取行政部門的內部規定。

（四）座談對象佔業者比率低

國內網路平台服務業者數目眾多，本研究由於時間及經費限制，僅與數家網路平台業者座談，佔全部業者比率偏低，無法完全反映全部業者的意見，如紀錄的內容、欄位、保留時間，查詢程序與費用等問題。

第四節　相關名詞定義

如前所述，如欠缺明確定義，將影響本研究的推動。本節先針對本研究相關之名詞「網路」、「網路平台業者」、「網路平台業者紀錄」予以定義，為避免各家學者定義不同導致無所適從，本研究原則採行本國法令的定義，以資立法或修法遵循。

一、網路

本研究所稱之「網路」應指一般所稱之「電腦網路」，原「電腦網路內容分級處理辦法」[11]第二條對於「電腦網路」之定義為「指以連線方式擷取網站資訊之開放式應用網際網路」。

二、網路平台業者

網路平台業者又稱為網際網路平台提供者，常見的各類平台服務包含電子佈告欄（Bulletin Board System, BBS）、檔案傳輸協定 （File Transfer Protocol, FTP）、部落格（Blog）、網路論壇（Usenet）、電子郵件（E-mail）、搜尋引擎（Search Engine）、代理伺服器（Proxy Server）、即時訊息（Instant Message）、小額付費[12]。而國內相關法規有定義網路平台業者或相關名詞有「電信法」、「第二類電信事業管理規則」、「電腦網路內容分級處理辦法」與「兒童及少年福利與權益保障法」，茲說明如下：

（一）電信法

第十一條

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。

前項電信機線設備指連接發信端與受信端之網路傳輸設備、與網路傳

[11] 配合「兒童及少年福利與權益保障法」於 100 年 11 月 30 日修正，刪除原第 27 條第 3 項「電腦網路應予分級」之授權規定，國家通訊傳播委員會於 101 年 6 月 13 日以經通傳播字第 10148028630 號令，發布廢止「電腦網路內容分級處理辦法」，但現行法規並無對「電腦網路」加以定義，故仍沿用原「電腦網路內容分級處理辦法」第二條對於「電腦網路」之定義。

[12] 梁隆星，網路業者對網際網路著作權侵權之法律責任—以法律經濟分析為基礎，中原大學財經法律學系碩士論文，2008 年 7 月。

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。

（二）第二類電信事業管理規則

第二條　本規則用詞定義如下：

一、經營者：指經主管機關許可並發給執照經營第二類電信事業者。

二、用戶：指與經營者訂定契約，使用該經營者提供之通信服務者。

三、使用者：指用戶及其他使用經營者提供之通信服務者。

四、第二類電信事業特殊業務：指經營語音單純轉售服務、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。

五、語音單純轉售服務：指經營者以租用電信事業之電路或頻寬連接公眾交換電信網路，提供國際或長途語音服務，或話務轉接服務。

六、網路電話服務：指經營者透過網際網路傳送與接收所提供之語音服務。

七、E.164 用戶號碼網路電話服務：指依國際電信聯合會對電信號碼編定規格書之編號，經營者可利用 E.164 用戶號碼提供之網路電話服務。

八、非 E.164 用戶號碼網路電話服務：指經營者未利用 E.164 用戶號碼所提供之網路電話服務。

九、第二類電信事業一般業務：指第四款以外之第二類電信事業業務。

十、公司內部網路通信服務：指經營者以租用第一類電信事業之電路，並設置節點構成網路，以提供用戶作公司之內部單位、分公司、分支機構及其關係企業間通信之服務。

十一、批發轉售服務：指經營者未租用電信事業之電路或頻寬，以批發方式承購或承租電信事業之電信服務後，並以自己名義向用戶或使用者提供電信服務。

十二、公用電話轉售服務：指經營者以承購或承租電信事業之電信服

務，並設置以投幣、簽帳卡、信用卡或預付卡付費，供公眾使用電話之批發轉售服務。

十三、預付式電話卡轉售服務：指經營者以承購或承租電信事業之電信服務，提供使用者以經由國內撥接電信號碼或密碼構成通話之預付式批發轉售服務。

十四、行動網路業務經營者：指經主管機關特許並發給執照之行動電話業務經營者、第三代行動通信業務經營者、一九〇〇兆赫數位式低功率無線電話經營者及無線寬頻接取業務經營者。

十五、虛擬行動網路服務：指經營者經營行動轉售服務或行動轉售及加值服務。

十六、行動轉售服務：指經營者以批發方式承購或承租行動網路業務經營者之通信服務後，並以自己名義向用戶或使用者提供電信服務。

十七、行動轉售及加值服務：指經營者除經營行動轉售服務外，並設置加值服務之網路元件提供行動通信之加值服務。

經營前項第十七款服務者，如其提供之加值服務包含前項第四款所定之服務者，應另依本規則有關第二類電信事業特殊業務之規定辦理。

（三）電腦網路內容分級處理辦法

電腦網路內容分級處理辦法第二條將電腦網路服務提供者，分為網際網路接取提供者、網際網路平臺提供者及網際網路內容提供者。其中網際網路平臺提供者定義為：指在網際網路上提供硬體之儲存空間、或利用網際網路建置網站提供資訊發佈及網頁連結服務功能者。

（四）兒童及少年福利與權益保障法

2011 年 11 月 30 日公布施行之兒童及少年福利與權益保障法第 46 條第 4 項：前三項所稱網際網路平臺提供者，指提供連線上網後各項網際網路平臺服務，包含在網際網路上提供儲存空間，或利用網際網路建置網站提供資訊、加值服務及網頁連結服務等功能者，本研究原則採行此一定義。

三、網路平台業者紀錄

遍查國內相關法規未有任何法規對於「網路平台業者紀錄」定義，與其相近之定義如「電信法」第二條定義通信紀錄，然該法所定義之「通信紀錄」係指電信使用人使用電信服務所產生之紀錄，與本研究所稱之「網路平台業者紀錄」不同。「網路平台業者紀錄」之紀錄應指「兒童及少年福利與權益保障法」中所稱「網際網路平臺提供者」提供網際網路平臺服務所產生之紀錄。

（一）電信法

電信法第二條定義通信紀錄：指電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼、通信日期、通信起訖時間等紀錄，並以電信系統設備性能可予提供者為原則。電信號碼係指電話號碼或用戶識別碼。

（二）兒童及少年福利與權益保障法

兒童及少年福利與權益保障法第 46 條第 4 項：前三項所稱網際網路平臺提供者，指提供連線上網後各項網際網路平臺服務，包含在網際網路上提供儲存空間，或利用網際網路建置網站提供資訊、加值服務及網頁連結服務等功能者。本研究所稱之「網路平台業者紀錄」係指兒童及少年福利與權益保障法第 46 條第 4 項所指網際網路平臺提供者提供網際網路平臺服務所產生之紀錄，包含在網際網路上提供儲存空間，或利用網際網路建置網站提供資訊、加值服務及網頁連結服務等功能之紀錄。

（三）電信事業處理有關機關查詢電信通信紀錄實施辦法

第二條　本辦法所稱通信紀錄，指電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼、通信日期、通信起迄時間等紀錄，並以電信系統設備性能可予提供者為原則。

前項所稱電信號碼，係指電話號碼或用戶識別碼。

第二章　文獻回顧

第一節　我國現有法規

一、網路平台業者紀錄保存規範

國內現行法規對於網路平台業者紀錄保存未有任何規範，與「網路平台業者」性質接近之電信業者紀錄保存之規範，有通訊保障及監察法、電信法、第二類電信事業管理規則及電信事業處理有關機關查詢電信通信紀錄實施辦法等，相關法條分述如下：

（一）通訊保障及監察法

第三條　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。

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。

第十四條　通訊監察之執行機關及處所，得依聲請機關之聲請定之。法官依職權核發通訊監察書時，由核發人指定之；依第七條規定核發時，亦同。

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。

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；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。

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。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。

第十七條　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。

通訊監察所得資料全部與監察目的無關者，執行機關應即報請檢察官、依職權核發通訊監察書之法官或綜理國家情報工作機關首長許可後銷燬之。

前二項之資料銷燬時，執行機關應紀錄該通訊監察事實，並報請檢察官、依職權核發通訊監察書之法官或綜理國家情報工作機關首長派員在場。

（二）電信法

電信法對於網路服務提供者紀錄保存規範之相關法條有電信法第二條、第十一條，然值得注意的是，電信法的規定，並不適用於所有類型的網際網路服務提供者。一般通稱受電信法規範，需向國家通訊傳播委員會申請第二類電信事業執照的網際網路服務提供者，僅包含提供連線服務與若干提供平台服務者，而對於資訊內容服務之網際網路服務提供者，電信法將無法適用[13]。

第二條　本法用詞定義如下：

一、電信：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。

二、電信設備：指電信所用之機械、器具、線路及其他相關設備。

三、管線基礎設施：指為建設電信網路所需之架空、地下或水底線路、電信引進線、電信用戶設備線路、及各項電信傳輸線路所需之管道、人孔、手孔、塔臺、電桿、配線架、機房及其他附屬或相關設施。

四、電信服務：指利用電信設備所提供之通信服務。

[13]資策會科技法律中心，網際網路服務提供者法律責任與相關法制之研究，行政院經濟建設委員會委託研究，2003 年 12 月，頁 9。

五、電信事業：指經營電信服務供公眾使用之事業。

六、專用電信：指公私機構、團體或國民所設置，專供其本身業務使用之電信。

七、公設專用電信：指政府機關所設置之專用電信。

八、通信紀錄：指電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼、通信日期、通信起訖時間等紀錄，並以電信系統設備性能可予提供者為原則。電信號碼係指電話號碼或用戶識別碼。

第十一條　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。

前項電信機線設備指連接發信端與受信端之網路傳輸設備、與網路傳輸設備形成一體而設置之交換設備、以及二者之附屬設備。

第二類電信事業指第一類電信事業以外之電信事業。

（三）第二類電信事業管理規則

有關第二類電信事業紀錄保存相關規定有第二類電信事業管理規則，該規則第二十三、二十四、二十七條規定如下：

第二十三條　經營公司內部網路通信服務者，應至少保存其用戶基本資料至契約終止後一年。

前項用戶基本資料，包括公司之內部單位、分公司、分支機構及其關係企業之名稱與地址、公司內部關係證明文件、公司內部撥號計畫及用戶與業者網路連接之專線電路編號等。

如用戶之公司內部關係為其關係企業時，經營公司內部網路通信服務者，應檢具用戶名稱、地址及公司內部關係證明文件報請主管機關備查。

第二十四條　經營公司內部網路通信服務者，應登錄及保存連接網路內部節點之專線電路編號、相關路由表及通信紀錄資料。

前項連接網路內部節點之專線電路編號、相關路由表於經營期間內須持續保存，通話紀錄資料應至少保存六個月。

第二十七條　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。

（四）電信事業處理有關機關查詢電信通信紀錄實施辦法

第五條　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、行動通信通信紀錄：最近六個月以內。

前項期限，自受理查詢日回溯起算。

第二類電信事業通信紀錄之保存期限，依第二類電信事業管理規則之規定。

二、網路平台業者紀錄查詢規範

（一）電信事業處理有關機關查詢電信通信紀錄實施辦法

第三條　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，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。

（二）電信事業處理有關機關（構）查詢電信使用者資料實施辦法

第三條　下列情形得依法向電信事業查詢使用者資料：

一、司法機關、監察機關或治安機關因偵查犯罪或調查證據所需者。

二、其他政府機關因執行公權力所需者。

三、與公眾生命安全有關之機關（構）為緊急救助所需者。

依前項第一款、第二款規定查詢者，應敘明其法律依據。

第四條　本辦法所稱使用者資料，指電信使用者姓名或名稱、身分證統一編號、地址、電信號碼等資料，並以用戶申請各項電信業務所填列之資料為限。

前項所稱電信號碼，係指電話號碼或用戶識別碼。

第五條　有關機關（構）查詢使用者資料應備正式公文或電信使用者資料查詢單（格式如附件），載明需查詢之電信號碼或姓名及其身分證統一編號、電信服務種類、法律依據、案由說明、查詢案號、資料用途、查詢機關（構）、機關（構）主管、連絡人、連絡電話或傳真機號碼、機關（構）加蓋印信及其首長署名、職章等，送該電信使用者所屬電信事業指定之受理單位辦理。

對於案由特殊、情況緊急之查詢，得由法官、檢察官或查詢機關（構）之首長或經其授權之主管署名並加蓋職章及連絡人之資料，視同機關（構）正式公文書先傳真之，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使用者資料查詢單正本。

前二項之查詢，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使用者資料查詢單正本。

第二節　國內相關研究

本研究以網路平台業者使用者不法利用行為所衍生之問題，警察機關接獲民眾檢舉不法網站或受理被害民眾報案，需函請網路平台業者揭露不法使用者之用戶資訊，以確認侵權人真實身分，並保障被侵權人行使訴訟之權利[14]，因此網路平台業者需要保留可供警察機關確認侵權人身分之使用紀錄與用戶資訊。茲針對網路平台業者紀錄保存規範、網路平台業者協助犯罪偵查法制、網路平台業者協助偵查規範、網路平台業者法律責任等構面，探討業者法律責任相關議題。

一、網路平台業者紀錄保存規範

有國內研究者將第二類電信所提供之服務態樣區分為（一）有通訊相對人：網路電話服務、簡訊、網路聊天等。（二）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。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，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[15]。

另提出紀錄保存之國外立法例，如：美國電子通訊隱私法（ECPA）關於資料保存之規定，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）；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）。歐盟「資料保存指令」規範：個人通訊資料保存指令（Directive 2006/24/EC）會員國應確保

[14] 張乃文，科技法務透析，談美國對於網站平台提供者揭露用戶資料規範及程序，2008 年 11 月，頁 19-23。

[15] 蘇三榮，網路時代通訊監察與個人資料保護之法制研究，國立交通大學科技法律研究所碩士論文，2009，頁 36。

下列資料之保存：追蹤或辨別通訊來源必要的資料、辨別通訊目的地必要的資料、辨別日期、時間、通訊期間必要的資料、辨別通訊類型必要的資料、辨別使用者通訊設備必要的資料、辨別行動通訊設備方位必要的資料等，但涉及通訊內容的資料則不能根據此指令保存。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[16]。

另有研究指出，我國實務上，電信業者依交通部電信總局訂定之「電信事業處理有關機關查詢電話通話紀錄實施辦法」提供相關機關電話通話紀錄，可查詢機關係指司法機關、監察機關或治安機關，但並不適用於執法者向「網路服務提供者」要求查詢相關通訊資料，亦即現在執法者向網路服務提供者取得任何通訊資料都沒有法律上之依據。因此，建議於刑事訴訟法或通訊保障及監察法中，針對通訊紀錄之取得訂出類似美國電子通訊隱私權法的規範，要求檢察官、司法警察（官）基於刑事偵查目的，應有合理懷疑，並經法官許可，才可向通訊服務提供者取得相關紀錄為宜[17]。該作者建議將現行通訊保障及監察法規範之協助義務機關「電信事業」改為「服務提供者」，將服務性質各異、規模大小不一之各網路服務提供者納入通保法規範之對象，如此做法雖有利於警方犯罪偵查，然而「網路服務提供者」範圍牽涉過廣，是否可行仍有疑義。然就本研究之主題而言，若能將「網路平臺提供者」納入通保法規範之對象，將其保存紀錄協助偵查之義務、及取得相關紀錄之程序…等一併於通保法中增修規範之，亦不失為建議修法方向之一種。

另有研究指出目前網路犯罪偵查普遍遭遇之問題，如：網路通訊協定位址（IP）在國外；網咖、轉址及代理伺服器（Proxy）問題；利用高科技及先進通信設備犯罪、稽核記錄及數位證據保存等問題[18]。在與 ISP 業者訪談結果中，多數意見如下：1.業者如果能夠延長紀錄保存時間，將有助於案件

[16] 蘇三榮，網路時代通訊監察與個人資料保護之法制研究，國立交通大學科技法律研究所碩士論文，2009，頁 79-88。
[17] 謝昆峰，網際網路與刑事偵查，國立臺灣大學法律學研究所碩士論文，2002，頁 141-142。
[18] 陳欽錫，網路犯罪與偵防對策之研究，逢甲大學公共政策研究所碩士論文，2007，頁 61-65。

偵查，惟受訪者均認為延長保存期限之可行性不高，原因是會增加公司營運成本，除非法令硬性規範。2. ISP 業者大都由專人、法務人員辦理有關機關查詢調閱作業，對於警察及其他機構調閱資料，只要條件充足均會配合提供資料查詢。3.稽核紀錄儲存型態各家業者不同，資料建立或管理對於保存期限都會有影響，完善的側錄或記錄設備，一般業者並無意開發或設置先進設備來管理這區塊。4.從案件偵查實務發現，很多網路使用者身分、會員帳號、註冊基本資料虛偽不實或假冒他人個人資料註冊或登入，有關系統服務申請者、會員、註冊帳號（ID）或網域（線路）使用者資料真實（正確）性，警方在獲得這些資料可能對案件一點幫助價值都沒有。5.偵辦網路犯罪經常遭遇的問題是，ISP 業者無法提供警方所需的資料，如代理伺服器問題，犯罪者會利用業者沒有控管機制的途徑，從事犯罪行為[19]。本研究以為就網路平臺提供者（IPP）而言，發信者之 IP 來自國外、網咖或代理伺服器，其於業者處留存之紀錄，若有帳號註冊之真實身分資訊，則前述問題皆可迎刃而解；然而，若准許「匿名」、假身分註冊之情形，即使網路平臺提供者存有發信時間、日期、內容等相關紀錄，亦無法直接追蹤識別發信者身分，必須進一步求助於 ISP 業者之協助，甚或結合其他偵查輔助工具（如：監視器）在犯罪偵查上才有實質助益。

二、網路平台業者協助犯罪偵查法制

由於網路行為具有「凡走過必留下痕跡」的特性，在網路犯罪偵查過程中，包括清查過濾階段之使用者資料或通信紀錄；證據調查階段之實施通訊監察等偵查作為，均須仰賴網路服務提供者提供偵查協助，才能進行後續偵查作為，甚至可以說，網路犯罪偵破與否之關鍵，依存於網路服務提供者能否完全配合。

有國內研究彙整網路業者可提供協助偵查之事項如下：於伺服器主動過濾、攔阻犯罪訊息；發現後主動刪除犯罪資訊；主動保存犯罪訊息並向偵查

[19] 陳欽錫，網路犯罪與偵防對策之研究，逢甲大學公共政策研究所碩士論文，2007，頁151-157。

單位舉報；網路業者亦會儲存 IP、連線時間、傳遞路徑等通信紀錄作為計費及使用者查核帳單之用，可提供偵查之用；業者為確保服務品質，會自動備份通訊內容，或於伺服器主機容量許可下，亦會保留一定期間訊息供使用者查詢過去張貼之內容，顯見業者有儲存資訊之技術與能力；業者可對進行中之犯罪協助實施網路通訊監察及通訊內容解密；業者性質屬第三人搜索，有其協助可加速搜索、扣押之工作；被告對資訊之正確性有質疑時，業者可協助作證[20]。在我國法制規範網路服務提供者協助偵查責任方面有：網路服務停止租用（與用戶簽約）、刪除權（服務條款明定有權刪除會員資訊）、儲存、提供使用者資料及通信紀錄（電信法第 7 條、第二類電信事業管理規則第 27 條之 4、5、個人資料保護法第 20 條、電信事業處理有關機關（構）查詢電信使用者資料實施辦法第 3、4、5 條）、電信業者需有特定網路位址保存跨境連線通信紀錄 90 日之設備及能力（反恐怖行動法草案）、協助實施通訊監察（通訊保障及監察法第 14 條、細則第 21 條）[21]…等。但上述國內電信法、第二類電信事業管理規則、電信事業處理有關機關（構）查詢電信使用者資料實施辦法，其規範之對象－網路業務經營者，係以電信設備為基礎之網際網路連線服務提供者（Internet Access Provider），如：第三代行動通信業務經營者、無線寬頻接取業務經營者等，似乎難謂其涵蓋網際網路平台提供者（Internet Platform Provider）之範疇。

該研究亦指出國內現行法之缺點：規範對象狹隘，第二類電信事業管理規則第 27 條（已辦理公司或商業登記之「經營者」）、通訊保障及監察法第 14 條「電信事業」（含一、二類）及「郵政機關」、所謂「電信事業」無法涵蓋網路服務提供者；侵害隱私權，通訊保障及監察法屬法律位階，但第二類電信事業管理規則屬法規命令，有違反憲法「法律保留原則」之疑義；紀錄儲存時間過短（第二類電信事業管理規則第 27 條）；協助偵查之免責規定不全，通訊保障及監察法第 29 條有規定，電信法、第二類電信事業管理規

[20] 許慈健，網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究，國立交通大學管理學院在職專班碩士論文，2005，頁 101-105。
[21] 許慈健，網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究，國立交通大學管理學院在職專班碩士論文，2005，頁 109-116。

則均未訂定任何免責之規定；不配合之罰責，通訊保障及監察法第 31 條有規定，電信法、第二類電信事業管理規則均未訂有任何處罰規定；行政檢查規定，現行法令均無規定，無法據以督促業者履行相關協助偵查（如：紀錄保存）之義務。[22]因此，提出相關立法建議如下：（一）制定協助偵查專法（網路服務提供者協助偵查法）取代修法，網路服務內容多樣化，經營者可能為非電信業者或個人，無法適用電信法相關法規，專法亦可符合憲法「法律保留原則」。（二）區分不同型態、經營規模之網路服務業者，如：是否為電信事業？營利單位？公司或個人？以決定應負擔之協助偵查義務之高低。[23]

在紀錄保存期間之建議方面，參考美國並未規定通信紀錄的保留期間，而歐盟「隱私及通訊指令」修改 1995 年個人資料保護指令特定條文之適用，對通信紀錄部分，容許各會員國立法要求強制網路服務提供者留存通信紀錄一定期間，而後歐洲議會提出「留存通訊紀錄決定草案」建議歐盟要求各國政府立法強制通訊服務提供者留存所有通訊紀錄，期限從十二個月至二十四個月不等。最後參照我國法務部公佈之電腦犯罪統計分析，顯示各地檢察署偵辦電腦犯罪案件平均結案日數為 52 日做為基準，由於依目前犯罪案件偵查流程，司法警察機關受理網路犯罪之偵查時程約為檢察官偵查日數二倍以上，再加上不易發覺造成延遲報案之特性，因此，該研究建議保留期間應介於六個月以上至十二個月間為宜。[24]

三、網路平台業者協助偵查規範

業者協助義務分別規定於網路犯罪公約第 16 條、第 17 條（保存命令）、第 18 條（提出命令）及第 19 條第 4 項（執行協力義務）。

第 16 條第 1 項要求簽約國應制訂保存命令（保全命令）或其他類似之方式，迅速保全已儲存之電磁紀錄與通訊資料。保存命令係以與特定的偵查

---

[22] 許慈健，網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究，國立交通大學管理學院在職專班碩士論文，2005，頁 120-138。
[23] 許慈健，網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究，國立交通大學管理學院在職專班碩士論文，2005，頁 145-153。
[24] 許慈健，網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究，國立交通大學管理學院在職專班碩士論文，2005，頁 179-180。

有關之已記錄或儲存的電腦資料為對象，並令其不可刪除且須繼續保存。保存命令核發時，資料仍存留在被命令者控制下，之後主管機關再經由搜索扣押或提出命令等程序，從被命令人手中取得資料。為了不對資料持有者造成過大負擔，16 條第 2 項要求各簽約國必須明文規定，保存時間最長不得超過 90 日之期限。而為了顧及國際協力之需求，保存命令之期限亦不得低於 60 日。第 16 條第 3 項則要求各簽約國應制訂守密義務，同時顧及偵查的必要性及被命令者之隱私。

第 17 條第 1 項 a 要求簽約國立法或採取其他措施，不論該通訊係牽涉到一個或多個 ISP 業者，均應確保基於第 16 條迅速保存之通訊資料具有可利用性。目的在使偵查機關可藉由存留在各個 ISP 業者之通訊資料，一個一個還原追蹤犯罪人。具體的執行方法原則上則委由各簽約國決定。此外，由於保存命令核發後，通訊資料尚存於服務提供者手中，偵查機關必須採取搜索扣押或其他類似之方法，否則無法得知其內容，因而亦無法得知該服務提供者是否保有全部相關資料，以及在相關訊息傳輸路徑上，是否仍存有其他服務提供者，因此，17 條第 1 項 b 規定在確認訊息傳輸的路徑上有必要時，即可要求服務提供者將通訊資料的一部分向偵查機關迅速揭示。此時，偵查機關亦必須明確特定應揭示之通訊資料，例如在保存命令中載明「能夠闡明該當通訊涉及其他的服務提供者之通訊資料，應迅速揭示」之要旨[25]。

因為保存命令性質上應屬於任意偵查，因此保存命令之發動僅需偵查機關考量發動的必要性之後，即可要求 ISP 業者保存特定通訊履歷，且不適合附以間接強制。此外，由於保存命令在性質上屬於偵查特定事件之處分，故保全命令無法要求 ISP 業者不論犯罪是否發生，皆應收集全部的通訊履歷並將之保存。此種一般性的保存義務，由於侵害範圍過大，實難作為刑事程序之一環而允許之[26]。實際上，日本在增修刑事法時，亦僅提及業者在接獲命

[25] 陳誌泓，電腦、網路與刑事偵查－以網路犯罪公約於日本法的落實為中心，國立臺灣大學法律學研究所碩士論文，2005 年 7 月，頁 107-109。

[26] 陳誌泓，電腦、網路與刑事偵查－以網路犯罪公約於日本法的落實為中心，國立臺灣大學法律學研究所碩士論文，2005 年 7 月，頁 110-111。（參閱松井茂記，「プライバシーと通信の秘密」，多賀谷一照、松本恒雄編集代表《情報ネットワークの法律実務》，2003 年 3 月収録，頁 4631。）

令處分後，將既有之特定通信歷程繼續保存至多 90 日，並未規定業者必須就全部通信歷程主動予以保存，此與我國第二類電信事業管理規則中訂定之紀錄保存規範不同。日本在刑事法整備綱要第七條，規定了保全要求，就保全之客體而言，僅限於業務上所記錄之特定資料，並非課予相對人一般性保存義務，範圍亦僅限於既存之資料，而不及於將來可得或通訊中的資料。此外，業務上沒有必要而未儲存之資料，以及曾經儲存但已超過業務保存期間而遭刪除之資料，亦不在本條文範圍內。綱要第七條承繼網路公約第 16 條第 3 項之保密要求，但未採行公約第 17 條第 1 項 b 之要求，讓偵查機關得以請求 ISP 業者揭露相關通訊歷程。因此在日本法上，僅能透過偵查機關快速聲請搜索扣押或提出命令之方式，擔保公約之要求[27]。

公約第 18 條「提出命令」之規定，使得偵查機關除了採行搜索扣押等手段外，能選擇另一個侵害性較小的偵查手段，亦可避免偵查機關在搜尋相關電腦資料時浪費時間。另一方面，提出命令對於被命令者（例如 ISP 業者）亦存有利益，有個適切的法律依據以免除其契約責任。註釋書裡載明，偵查機關可命令提出之電腦資料或是使用者資訊，其範圍均僅限於已儲存或已存在之資料，並不包括與將來通訊有關之資料。已刪除或非屬被命令人所有或控制下之資料亦不在本條規範範圍內。提出命令不履行時，可否以其他強制方式擔保其履行？網路犯罪公約本身並未有任何規定，留予各簽約國各自立法形成，因此「僅規定義務，而不設定違反時的間接強制措施」之立法方式，亦不違反公約之要求，且由於被賦予義務者即使拒絕履行義務，事實上也沒有任何權利侵害發生，因此在理論上可認為賦予此義務不須經過令狀主義之檢驗，偵查機關亦可作為課予義務之主體[28]。為了擔保網路犯罪公約第 18 條，日本於刑事法整備綱要第四條，制訂了「附記錄命令之扣押」之新強制處分。在建立提出命令相關法制時，面臨與令狀主義及不自證己罪之可能衝突，採取了較為保守的立法方式，將發動權交由法院行使以符合法官事前審

[27] 陳誌泓，電腦、網路與刑事偵查－以網路犯罪公約於日本法的落實為中心，國立臺灣大學法律學研究所碩士論文，2005 年 7 月，頁 111-112。
[28] 陳誌泓，電腦、網路與刑事偵查－以網路犯罪公約於日本法的落實為中心，國立臺灣大學法律學研究所碩士論文，2005 年 7 月，頁 112-115。

查原則，明訂儲存或印刷之電磁紀錄以符合令狀特定性之要求等[29]。參酌網路犯罪公約及日本法之相關規定，本研究案之未來立法建議，除將重點置於網路平臺業者之紀錄保存規範外，或可將提出命令、不履行命令之罰則及令狀之必要與否…等問題一併納入考量。

有研究者認為，保存命令雖有侵害 ISP 業者之資料處分權，以及使用者之個人資料控制權之虞，但由於前者權利可由國家補償成本後弭平，後者則因偵查機關並未實際取得資料內容，僅要求保存一段時間，因此並非對個人資料控制權的終局性侵害，故可以認為係偵查處分之一種。在明確立法規定保存期限後，可由偵查機關考量緊急性與必要性後，命 ISP 業者等保存之。此外，在違反效果上，由於保存命令僅具任意處分之性質，在允許檢察官審酌要件後即可發動之反面，亦不宜創設違反時之強制效果。因此如被命令人不履行義務時，偵查機關亦僅在具備相當理由等要件後，以搜索扣押之方式進行相關電磁資料之保全[30]，即不必另訂間接強制之規定。又實務界在取得資料時，多數是依照「電信事業處理有關機關查詢電話通話記錄實施辦法」及「電信事業處理有關機關（構）查詢電信使用者資料實施辦法」所規定之程序為之。性質上屬於法規命令，並無法滿足上述法律保留原則及令狀主義之要求。因此，一個規定於刑事訴訟法，且明訂應由法官審核後方可簽發的提出命令制度，對於日益重視隱私權及通訊秘密權的我國，實有慎思其立法之必要[31]。此外，為擔保提出命令之效力，本文認為在相對人不履行提出命令時，允許（檢察官告知後）法院課予相對人一定間接強制之立法方式，較為可採[32]。

---

[29] 陳誌泓，電腦、網路與刑事偵查－以網路犯罪公約於日本法的落實為中心，國立臺灣大學法律學研究所碩士論文，2005 年 7 月，頁 118-119。

[30]陳誌泓，電腦、網路與刑事偵查－以網路犯罪公約於日本法的落實為中心，國立臺灣大學法律學研究所碩士論文，2005 年 7 月，頁 161-162。

[31]陳誌泓，電腦、網路與刑事偵查－以網路犯罪公約於日本法的落實為中心，國立臺灣大學法律學研究所碩士論文，2005 年 7 月，頁 162。

[32]陳誌泓，電腦、網路與刑事偵查－以網路犯罪公約於日本法的落實為中心，國立臺灣大學法律學研究所碩士論文，2005 年 7 月，頁 163。

四、網路平台業者法律責任

網路平台業者為網際網路服務提供者之一，另二類之業者為網路接取提供者（Internet Access Provider）與網路內容提供者（Internet Content Provider）。網際網路服務提供者法律責任之範圍，包括其與使用者間因提供服務本身瑕疵所生責任，以及對網路活動不法行為所生責任。前者係指網際網路服務提供者之瑕疵責任，屬民法契約之債務不履行責任，本屬契約法之責任理論可規制；後者則可區分為網際網路服務業者自己行為不法責任，以及其使用者不法利用行為之責任[33]。

一項由資策會科技法律研究所針對網際網路服務提供者法律責任與相關法制之研究，研究團隊研究結論如下[34]：

（一）應視對傳輸內容控管能力定網際網路服務提供者之責任

我國電信法所規範之電信事業，應以該事業對傳送內容有無控管能力為斷而定其責任，而不問其究為網路接取服務提供者或網路平台服務提供者。

（二）網路廣告責任之要件應以得否知悉作為判斷基準

消費者保護法第 23 條及公平交易法第 21 條第 4 項規定媒體經營者的責任，均以「明知或可得而知」作為主觀要件。此要件具體化言之，即為控制能力與主動之注意。網際網路服務提供者中的網路接取服務提供者（IAP）應排除在媒體經營者的定義外。網路平台服務提供者（IPP），由於涉及入口網站的形象及商業利益考量，常會進行編輯或編排，人為接觸到廣告的內容並為廣告內容當否之判斷，即對不實或引人錯誤廣告或可得而知，顯然較可期待，而較符合消費者保護法第 23 條及公平交易法第 21 條第 4 項之主觀要件。

（三）對負有被動注意義務之網際網路服務提供者，應以對不當資訊之作為義務作為免責要件

---

[33] 資策會科技法律中心，網際網路服務提供者法律責任與相關法制之研究，行政院經濟建設委員會委託研究，2003 年 12 月。

[34] 資策會科技法律中心，網際網路服務提供者法律責任與相關法制之研究，行政院經濟建設委員會委託研究，2003 年 12 月。

要求無法為主動注意之網際網路服務提供者，應著重在對於不當資訊的事後補救，亦即需為被動的注意及負擔一定作為義務較為可行。可參考歐盟電子商務指令第 14 條主要針對主機業者，在一般情形及注意義務下，無法發現傳輸資訊有犯罪情形時，不負法律責任；但在發現或被通知有不當或違法資訊時，仍有儘速移除資訊或阻斷讀取的義務。

（四）避免科予網際網路服務提供者刑事責任

網路平台服務提供者對於其所能控制之網頁內容，除該內容違法且認為網路平台服務提供者有協助之意思外，原則上，網路平台服務提供者如已審查經廣告主管機關核准之證明文件後，應免除其依刑事責任科予幫助犯之可能。

彭賢恩等指出美國「通訊內容端正法」中的第二三０條（CDA§230）澄清了 ISP 業者的定位，使 ISP 業者不必負擔網路言論出版者或發表者的責任，也不需負散布者的責任，美國法院幾乎賦予 ISP 業者完全的免責權。彭賢恩等認為我國並未針對 ISP 業者的責任問題特別進行立法，然而，我國法院似乎受到美國司法實務的影響，傾向賦予 ISP 業者完全的免責權[35]。

學者章忠信指出網路違法或侵權行為範圍廣泛，則關於 ISP 所須承擔之責任，究應分散於電信法規、消費者保護法、刑法、民法、商標法、著作權法等各自領域之法令中規範，抑或集中統一於單一法令中規範，各國各有不同策略。英美法系國家傾向分散式於各別法令中規範，例如美國、澳洲、新加坡，大陸法系國家則多以單一法律集中規範，例如歐盟、德國及日本。章忠信提出美國「通信端正法（The Communications Decency Act）」立法背景、歐盟「電子商務指令（Directive on Electronic Commerce, Directive 2000/31/EC）」，摘述如下[36]：

（一）美國「通信端正法」立法背景

---

[35] 彭賢恩、劉怡靖、彭曉珍，刑法應用於網路誹謗案例之分析，資訊社會研究（11），2006年7月，頁245-273。

[36]章忠信，網路服務提供者著作權侵害責任限制之立法思考與方向，2008 年 8 月號第 347 期，頁 40-41。

美國 1996 年通過「通信端正法」，以遏止網路誹謗或色情內容之散布，該法在第 230 條提供了 ISP 的免責條款[37]，將 ISP 認定為非屬於媒體發行人，以鼓勵 ISP 能對傳輸內容自行發展出監控機制，而不必承擔新聞檢查之責任，希望有利於 ISP 之經營。1995 年的 Religious Technology Center v. Netcom 一案中，法院認為被告 Netcom 經營的 BBS 沒有刪除他人非法轉貼原告 Religious Technology Center 的著作，雖然不構成直接侵害著作權，也沒有從他人非法行為特別獲利，不構成「代理侵害（vicarious infringement）」責任，但一旦被告 Netcom 知悉有侵害著作權的資料，沒有依據原告通知讓這些資料不被接觸到，還是可能應負「輔助侵害（contributory infringement）」責任。美國在 1998 年通過數位千禧年著作權法(Digital Millennium Copyright Act of 1998, DMCA)，在該法案第二章，明定 ISP 的免責條款。該法案規定，只要 ISP 對於侵害的內容無所知悉，未從侵害行為獲有收益、於接獲侵害通知後，立即遵守「通知及取下（notice and takedown）」程序規定，就可以對於他人使用其服務侵害著作權之行為免責。

（二）歐盟「電子商務指令」

歐盟有關 ISP 責任的規定，集中在「電子商務指令」第 12 條至第 15 條，其係適用於各個領域。該指令第 12 條至第 14 條將 ISP 區分為「單純連線（mere conduit）」、「快速存取（caching）」及「資訊儲存（hosting）」三種。在「單純連線」的 ISP 方面，資訊係由第三人所提供，ISP 僅提供使用者連線服務，只要資訊之傳輸非由其發起，對於傳輸內容無從選擇與修改，對傳輸與接收者都不是其決定，此類 ISP 對於內容就不必負責；在「快速存取」方面，只要對於內容沒有修正，遵守接觸資訊之規定，依產業規定更新資訊內容，且一旦知悉該資訊已被原來源處刪除或阻絕，也能立刻予以刪除或阻絕等，此類 ISP 對於內容也不必負責；在「資訊儲存」方面，只要其不知道是違法的資訊或活動，或是從表面上無法知悉是違法的資訊或活動，而在知悉是違法的資訊或活動後，也能立刻予以刪除或阻絕等，此類 ISP 對於內容

[37] "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

也不必負責。

資策會科技法律研究所研究日本「服務提供者責任限制法」之規範，認為日本電信事業法第 2 條第 1 款規定之「電信」係指以有線、無線及其他電磁方式發送、傳輸或接收符號、聲音或影像者。舉凡利用電磁場的通訊行為，如使用銅線、光纖的有線通訊、使用電波的無線區域網路、以及使用雷射或紅外線的通訊均屬之，目前常用之網際網路通訊自亦包括在內。我國之立法，雖有意將電信事業侷限於單純連線提供者，但由於定義之含混，網路平台服務提供者（IPP）於電信法之定位便顯得曖昧不明。依作者之見解，我國電信法所規範之電信事業應以該事業對傳送內容有無控管能力為斷，而不問其究為連線服務提供者或平台服務提供者[38]。

另「電信事業處理有關機關（構）查詢電信使用者資料實施辦法」第 3 條，僅司法機關、監察機關或治安機關因偵查犯罪或調查證據所需者、其他政府機關因執行公權力所需者、與公眾生命安全有關之機關（構）為緊急救助所需者，得敘明其法律依據向電信事業查詢使用者資料。準此，電信業者原則上不負向受侵權人提供使用者資料之義務[39]。此規定與日本「網路服務提供者責任限制法」以受權利侵害者為揭露發信者資訊之請求人顯有不同。

該研究尚依不同的網路媒體經營者，將其責任分為以下 4 種：網路連結服務提供者(IAP)的服務型態與監控內容之能力、網路內容服務提供者(ICP)的責任、經營廣告版面出租業者（IPP）之責任、提供主機出租或代管網頁業者之責任，進而提出 ISP 免責之立法模式如圖 2-1[40]。

另有研究認為，網路平台服務業者之法律責任，應視其對網路服務平台之內容是否具有編輯控制權，而有不同之責任標準，我國法律並無相關立法。美國法院及聯邦法律對於網路服務業者之誹謗責任，曾做出較進步之立

[38]資策會科技法律中心，網際網路服務提供者法律責任與相關法制之研究，行政院經濟建設委員會委託研究，2003 年 12 月。
[39]資策會科技法律中心，網際網路服務提供者法律責任與相關法制之研究，行政院經濟建設委員會委託研究，2003 年 12 月。
[40]資策會科技法律中心，網際網路服務提供者法律責任與相關法制之研究，行政院經濟建設委員會委託研究，2003 年 12 月。

法[41]。通信端正法立法後，美國法認為網路服務業者不應被視為任何資料之出版者或發表者，且規定網路服務業者若基於善意、自動過濾、提供他人科技方法，以限制其認為猥褻、邪惡、淫亂、齷齪、極度暴力、騷擾性或其他令人不悅之言論，不論此言論是否為憲法所保護之範圍，並不應負擔網路使用人違法行為之連帶法律責任。又規定任何與本法相衝突之州法或地方法，均不得成為提起訴訟或課予法律責任之依據[42]。

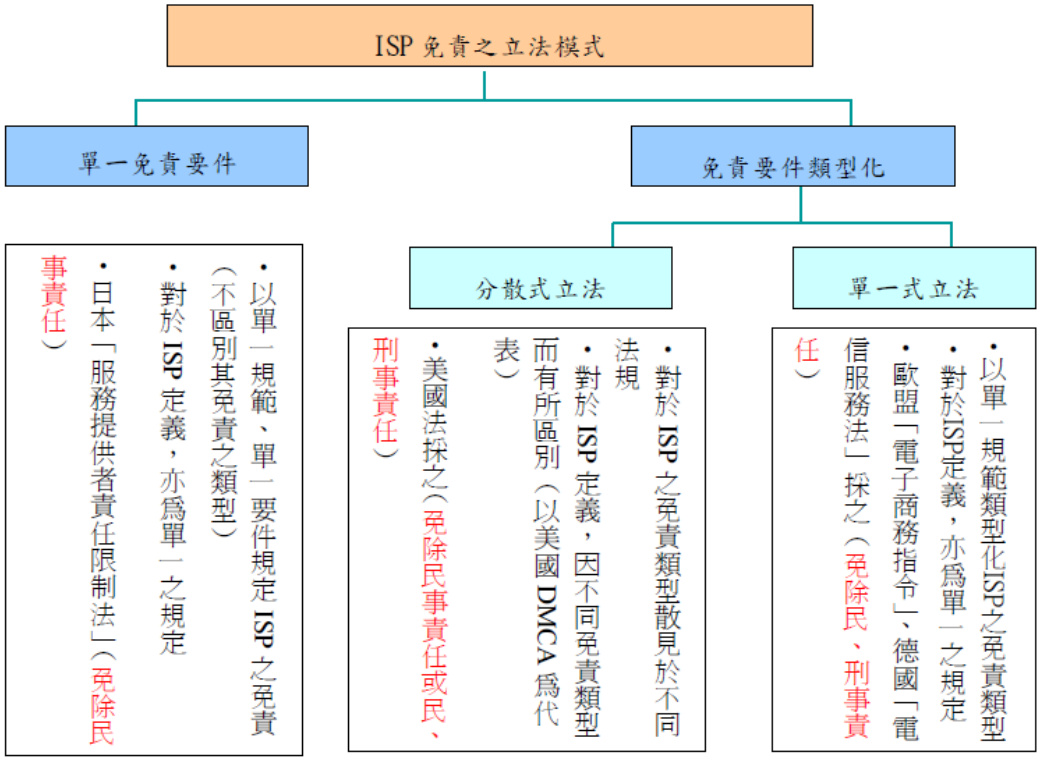


圖 2-1　ISP 免責之立法模式圖

（資料來源：資策會科技法律中心，網際網路服務提供者法律責任與相關法制之研究，行政院經濟建設委員會委託研究，2003 年 12 月）

在我國，網路服務業者對於使用者散佈違法資訊時可為之行為有：1.停止其使用或移除資料（電信法第 8 條第 2 項）。2.提供網路使用者之資料：電信法有相關保密規範；個資法第 20 條亦規定非公務機關對個人資料之利

[41] 黃燦堂，網路犯罪偵查方式與網路服務業者法律責任，國立高雄第一科技大學科技法律研究所碩士論文，2008，頁 134。
[42] 黃燦堂，網路犯罪偵查方式與網路服務業者法律責任，國立高雄第一科技大學科技法律研究所碩士論文，2008，頁 147。

用範圍；公權力機關要求，依電信事業處理有關機關查詢電信通信紀錄實施辦法；網路監聽，依通訊保障及監察法[43]。

經濟部智慧財產局參考各國作法，增訂有效的通知及取下機制，使著作權人於發現網路上有侵害其權利之資訊時，可通知網路服務業者迅速取下該等侵權資訊，避免損害繼續擴大。一旦網路服務業者遵循法律所定程序，快速移除該侵權資料，就網路使用人涉有侵權行為之部分，可主張不負連帶損害賠償責任。並提供網路使用人「回復通知」之機制，若其認為自己有合法權利使用被移除之資料時，可檢具回復通知文件，要求網路服務業者回復，也可向發錯通知的權利人請求損害賠償，以維護自身權益。而網路服務業者移除侵權資訊之行為，對著作權人及網路使用人均可不負賠償責任[44]。

[43] 黃燦堂，網路犯罪偵查方式與網路服務業者法律責任，國立高雄第一科技大學科技法律研究所碩士論文，2008，頁 148-155。
[44] 黃燦堂，網路犯罪偵查方式與網路服務業者法律責任，國立高雄第一科技大學科技法律研究所碩士論文，2008，頁 162-163。

第三節　美國現有法規

一、電子通訊隱私法（Electronic Communications Privacy Act, ECPA）

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「犯罪防制及街頭安全綜合法」（The Omnibus Crime Control and Safe Street Act）之第 3 篇的第 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」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，因此前開法案對新興的「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，美國國會議員感受到來自業界與民間自由團體，要求正視新科技為社會帶來衝擊的壓力，國會「科技評估辦公室（Office of Technology Assessment)」提出報告，表示執法機構利用「許多在電子監視科技的革新技術，違反憲法與法律保護，使得目前有些地帶無法受到法律保護，以抵擋新的監視技術」，而逐漸關心政府與私人團體侵入個人隱私權的問題[45]。有鑑於此，遂將「電子通訊」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」(Wire and Electronic Communications Interception and Interception of Oral Communications)，而此部法律稱為「電子通訊隱私法」(Electronic Communications Privacy Act, ECPA)，修正後之得進行通訊監察的客體包括「有線通訊」、「口頭對話」及「電子通訊」等三種類型。

美國通訊監察法規範的通訊，僅限於傳送中的通訊（communication in

[45] 呂雅文，探討通訊隱私範圍之變遷-以美國、德國和台灣法規為例，國立中正大學電訊傳播研究所碩士論文，2000 年 6 月。

transmission）。至於儲存中的通訊則是由「電子通訊隱私法」之第 121 章「有線通訊、電子通訊儲存與交易紀錄之存取」（Stored Wire and Electronic Communications and Transactional Records Access）來規範。

根據「電子通訊隱私法」,「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」[46],「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」[47]。「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，其全部或部份藉由電信設備、無線電、電磁、光電子或光學系統進行的任何傳遞」。但電子通訊並不包括下列通訊：任何有線或口頭通訊、任何透過只具音頻系統的傳呼裝置發出的通訊以及任何由追蹤裝置發出的通訊[48]。「電子通訊服務」指任何能提供用戶傳送或接收有線或電子通訊之服務[49]。「電子儲存」指伴隨於有線或電子通訊傳輸的過程，所產生之有線或電子通訊的暫時性與中繼性儲存，以及基於電子通訊服務備援之目的，所為的電子通訊儲存[50]。

進一步探討美國政府機關要求電子通訊服務提供者，關於提供客戶的通訊或紀錄之相關規範，其中明訂政府機關須依犯罪偵查程序規定，取得具有司法管轄權的法院所核發之搜索票後，方得要求電子通訊服務提供者，提供

---

[46] ECPA §2510（4）"intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.

[47] ECPA §2510 （1） "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception （including the use of such connection in a switching station） furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications for communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication.

[48] ECPA §2510（12） "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include: *（A）* any wire or oral communication; *（B）* any communication made through a tone-only paging device; or *（C）* any communication from a tracking device.

[49] ECPA §2510（15） "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications.

[50] ECPA §2510 （17） "electronic storage" means: *（A）* any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and *（B）* any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

其電子通訊系統中最近 180 天內，電子儲存之有線或電子通訊紀錄[51]。擬要求電子通訊服務提供者提供之電子儲存通訊內容為 180 天以前者，若持有法院核發之搜索票即可要求提供，但若僅取得行政授權之傳票或法院命令，則須於事前通知用戶或客戶[52]。

政府機關要求提供有關電子通訊用戶或客戶之相關資訊（不包含實質通訊內容），可藉由法院核發之搜索票、法院命令、取得用戶或客戶之同意以及基於調查電話推銷詐欺所提交之正式書面資料，寫明參與詐騙之用戶或客戶的姓名、地址及營業地點等方式[53]。而政府機關不須先行通知電子通訊之用戶或客戶[54]，可要求其提供之紀錄，包括：

（一）用戶或客戶之姓名；

（二）用戶或客戶之地址；

（三）本地與長途電話通信之紀錄；

（四）使用的服務類型與使用時間長短；

---

[51] ECPA §2703 （a） A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure （or, in the case of a State court, issued using State warrant procedures） by a court of competent jurisdiction.

[52] ECPA §2703 （b）（A） without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure （or, in the case of a State court, issued using State warrant procedures） by a court of competent jurisdiction; or （B） with prior notice from the governmental entity to the subscriber or customer if the governmental entity: （i） uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or （ii） obtains a court order for such disclosure.

[53] ECPA §2703 （c）（1） A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service （not including the contents of communications） only when the governmental entity: （A） obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure（or, in the case of a State court, issued using State warrant procedures） by a court of competent jurisdiction; （B） obtains a court order for such disclosure under subsection （d） of this section; （C） has the consent of the subscriber or customer to such disclosure; （D） submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing.

[54] ECPA §2703 （c）（3） A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

（五）足以識別用戶身分之辨識號碼或電話號碼；

（六）政府機關利用行政授權之傳票所要求提供之用戶或客戶付費資訊。

二、愛國者法（USA Patriot Act, USAPA）

在歷經 911 恐怖攻擊事件後，美國國會於 2001 年 10 月 25 日通過「愛國者法」，並由美國總統布希於 2001 年 10 月 26 日簽署通過，該法案總計修正「通訊監察法」、「電子通訊隱私法」、「電腦詐欺及濫用法」、「外國情報調查法」、「Pen Register 與 Trap and Trace 裝置法」[55]、「洗錢法」及「移民法」等超過 15 個不同的法案。

愛國者法案增加「電子通訊隱私法」U.S.C§2703（c），所列舉的政府機關有權要求提供之個人資料項目，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，含括在增修規定的資訊包括以撥接或計時制 ADSL 上網時，ISP 隨機暫時分配予客戶使用的網路位址、客戶付費的信用卡號碼與銀行帳戶以及登入之次數與期間的紀錄[56]，透過這些資訊與客戶個人資料或其他通訊資料，可以更確定受調查人的身份。

三、愛國者改進與再授權法案（USA Patriot Improvement and Reauthorization Act, 2005）

美國聯邦司法部下設之國家安全司，即是為因應愛國者改進與再授權法案而設置，目的在結合司法部刑事司原有之反恐怖主義與反間諜科，結合情報局於「外國情報監察法」（Foreign Intelligence Surveillance Act）之專長，

---

[55] ECPA 的第三篇禁止監視記錄器（Pen Register）與／或追蹤裝置（Trap And Trace）在未有搜索票下，去記錄傳遞有線或電子通訊的過程中之通話、路由、定位、訊號資訊。

[56] ECPA §2703 （c）（2） A provider of electronic communication service or remote computing service shall disclose to a governmental entity the: （A） name; （B） address; （C） local and long distance telephone connection records, or records of session times and durations; （D） length of service （including start date） and types of service utilized; （E） telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and （F） means and source of payment for such service （including any credit card or bank account number）, of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena.

負責處理該部所有國家安全任務[57]。

四、犯罪偵查通訊協助法（Communications Assistance for Law Enforcement Act, CALEA）[58]

美國社會原本認為未經法院命令而獲取私人通訊資料，是明顯的濫權行為，但自從 1994 年世貿中心的恐怖攻擊事件以來，一股擔心恐怖組織犯罪猖獗的氣氛，造成社會上態度的轉變。聯邦調查局與司法部都在國會表達他們擔心缺乏監控恐怖分子的能力，於是國會立即於 1994 年 10 月通過「犯罪偵查通訊協助法」，確保獲得法院授權進行通訊監察的執法機構，在通訊科技日新月異之際，依然有能力去進行電子通訊的截聽[59]。

該法案規範電信業者負有協助執行法律的責任及要求電信業者設計或修改系統，以確保合法授權的電子調查得以達到其目的。換言之，依據「犯罪偵查通訊協助法」，電信業者在有法院命令或合法授權實施通訊監察的情形下，必須具備確保其裝置、設備或服務具有如下之功能：讓政府能迅速截取電信業者提供給用戶服務範圍內之有線及電子通訊內容；讓政府能迅速取得在電子通訊傳輸期間所合理取得之電話識別資料或從屬於通訊之電話識別資料；傳送已截取的電子通訊內容及電話識別資料給政府；在最小侵害用戶電信服務之條件下，協助執行已授權之截取通訊及取得電話識別資料。

在補償業者方面，本法案規定司法部長須在可運用的預算內，提供通訊業者一定的經費用以執行本法，惟「犯罪偵查通訊協助法」規範對象僅為電信業者，至於資訊服務業者、私人網路業者、長途網路通信業者等類型之業者，則非屬「犯罪偵查通訊協助法」之規範對象。

---

[57] 楊崇森，美國聯邦司法部之組織與功能，法學講座，軍法專刊，第 56 卷第 4 期，頁 240，2010 年 8 月。

[58] 犯罪偵查通訊協助法（Communication Assistance for Law Enforcement Act, CALEA）：1994 年 10 月美國國會，基於保護人民及國土安全及偵查機關在面對快速進步的通訊科技時代，仍能保存執行電子調查的法律能力等等考量，而制訂通過之法規。

[59] 呂雅文，探討通訊隱私範圍之變遷-以美國、德國和台灣法規為例，國立中正大學電訊傳播研究所碩士論文，2000 年 6 月。

五、外國情報監察法修正案（Foreign Intelligence Surveillance Act Amendments Act, 2008, FISA）

本法案是由美國國會制訂的一部關於反恐怖活動、反間諜活動、情報收集活動以及秘密司法程序的一部基本法，對電子監控、物理性搜查、通訊紀錄與通訊追蹤、使用商務紀錄等秘密調查手段進行了全面規定。該法案以國家安全目的為前提，提供一個反制外國力量介入的法律規範，以規範通訊監察事項，但只規範有線傳播的截聽問題，並未涵蓋有線和無線通訊傳播[60]。

而修正法案則擴大美國國家安全局和其他情報機構對可疑間諜和恐怖分子進行監聽的權限，並保護與布希政府合作進行未獲法院許可監聽的電話公司，免於侵犯隱私之訴訟。九一一恐怖攻擊後，布希政府對可疑恐怖分子進行未經法院許可的秘密監聽，當時包括 AT&T、Verizon Communications 等電信公司，因協助政府而面臨四十多樁侵犯隱私權的訴訟，一旦確認後將面臨高達數十億元的賠償損失。FISA 修正案通過後，一併赦免這些電信公司，已繫屬在法院的訴訟也將一併被駁回。

[60]呂雅文，探討通訊隱私範圍之變遷-以美國、德國和台灣法規為例，國立中正大學電訊傳播研究所碩士論文，2000 年 6 月。

第四節　歐盟現有法規

歐洲各國的電信自由化推動腳步，直至歐盟 1987 年發表「電信自由化綠皮書」後，陸續制訂各項法律規範俾使歐盟內各國成員逐步朝向實施電信自由化。尤其 2004 年 3 月 11 日在西班牙馬德里發生火車爆炸案的恐怖攻擊事件[61]，遂促使歐盟各國更為重視電子通訊資料的保存議題，相關草案也同時應運而生[62]。

一、個人資料保護指令（Directive 95/46/EC）[63]

歐盟規定各會員國應基於保護自然人之基本權與自由等主張，尤其針對個人資料處理過程中之隱私權保障，因此於 1995 年通過「個人資料保護指令」，並指示蒐集而來的個人資料均須加以保護，以防止意外或非法之破壞、損失及修改，以及未經授權之公開或存取。

該指令之基本原則含括「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」，而其中關於資料當事人則另有「接觸權利」、「更正刪除或封存個人資料」以及「反對權利」等規範。

二、電信事業個人資料處理及隱私保護指令（Directive 97/66/EC）[64]

有鑑於公共電信服務對使用者之個人資料及隱私權更應予以尊重，且 Directive 95/46/EC 並未明確規範適用對象，因此本指令特別強調針對公共電信網路所提供之公共電信服務使用者，尤其是透過整合服務數位網路（Integrated Services Digital Network, ISDN）與公共數位行動網路（Public

---

[61] 參閱網址：http://zh.wikipedia.org/wiki/%E9%A9%AC%E5%BE%B7%E9%87%8C%E4%B8%89%E4%B8%80%E4%B8%80%E7%88%86%E7%82%B8%E6%A1%88。最後瀏覽日期：2012 年 6 月 6 日。

[62] Stephen S., European parliament says ‘No!’ to member states’ data retention proposals, Computer law & security report, Vol. 21, pp.279-280, 2005.

[63] 個人資料保護指令（Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive 95/46/EC）。

[64] 電信事業個人資料處理及隱私保護指令（Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the processing of personal data and the protection of privacy in the telecommunications sector, Directive 97/66/EC）。

digital mobile networks）所進行之通訊，其個人資料之處理與隱私權保障所須遵循之規範。

關於本指令，較特殊之議題包括：

（一）本指令要求公共電信服務提供者，應採取適當之技術方法防衛其所提供服務之安全。

（二）要求歐盟各會員國必須確保公共電信網路及公共電信服務之通訊秘密。

（三）用戶及使用者關於通話之紀錄應於通話結束時即予消除。

（四）必須提供發話方免費方式以就個別之通話得以除去來電顯示。

（五）必須確保用戶有權停止來自第三方之通話自動轉接。

三、電子通訊中個人資料處理及隱私保護指令（Directive 2002/58/EC）[65]

歐洲議會與歐盟理事會於2002年7月通過本指令，以取代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有別於傳統通訊結構，且為廣大範圍的電子通訊服務提供一個共同及全球性的基礎設施。以網際網路提供公共使用之電子通訊服務，雖為用戶提供一個新的可能性，但也同時對其個人資料和隱私產生新的風險，特別是網際網路上之個人資料與隱私權的保護相關議題。有鑑於此，針對公共通訊網路，特別是日益增強之用戶個人資料自動儲存與處理能力部分，提供法律上、管制政策上與技術上的特別規定，以使得法人與自然人之基本權利及自由能獲得妥善的保護。

除一方面要求保障個人資料之通訊機密，另一方面儘可能使用最少個人

---

[65] 電子通訊中個人資料處理及隱私保護指令（Directive 2002/58/EC of the European Parliament and of the Council, Concerning the processing of personal data and the protection of privacy in the electronic communications sector, Directive 2002/58/EC）。

資料來提供服務，並積極要求各會員國、相關服務提供者及相關主管機關，應該共同合作與開發，將數位化或原始資料與個人資料處理之利用，限制在最小必要範圍內之相關技術。又對於防止未經批准之訊息及與之相連接的資料內容，其通路、公共通訊網路或公共電子通訊服務所為之訊息傳遞機密，指令亦要求各會員國應採取一定的保護措施。

指令中特別提到須列入保護之通訊紀錄，包括位置資料（Location data）與流量資料（Traffic data），位置資料可藉由使用者所使用之終端設備，對照出所在位置的經緯度及海拔高度以判別行進路線與相關地理資訊，亦可利用網路單元細胞（Network cell）之紀錄得知時間相關資訊[66]。流量資料則包含路由數據、連線期間、連線時間及通訊流量等資料[67]。

四、個人通訊資料保存指令（Directive 2006/24/EC）[68]

本指令立法目的是為規範公共通訊網路產生或傳輸的資料之保存責任，確保資料可供各會員國國內法定義下的重大犯罪調查、偵查及起訴目的之運用，適用範圍為法人及自然人的位置資料與流量資料，以及可用以辨認出用戶或登記用戶身分之相關資料，但不包含電子通訊實質內容之保存[69]，針對資料保存之相關規範詳列如下：

（一）保存資料之內容[70]

---

[66] Directive 2002/58/EC（14）Location data may refer to the latitude, .longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.

[67] Directive 2002/58/EC （15） A communication may include any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication. Traffic data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission. Traffic data may, inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network.

[68] 個人通訊資料保存指令（Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending, Directive 2006/24/EC）。

[69] Directive 2006/24/EC, Article 1.

[70] Directive 2006/24/EC, Article 5.

1、追蹤或辨別通訊來源之必要資料

（1）固定網路的電話或行動電話

A、電話號碼

B、用戶或登記用戶之姓名與地址

（2）網路存取、電子郵件及網路電話

A、分配之使用者帳號（ID）

B、利用公共電話網路進行通訊時所分配之使用者帳號與電話號碼

C、通訊時分配之 IP 位址、使用者帳號或電話號碼其使用的用戶或登記用戶之名字與地址

2、辨別通訊目的地之必要資料

（1）固定網路的電話或行動電話

A、撥出或接收之電話號碼，包含如轉接等附加服務中所記錄的電話號碼

B、用戶或登記用戶之名字與地址

（2）電子郵件及網路電話

A、預期接收網路電話之使用者帳號或電話號碼

B、預期接收通訊之使用者帳號以及用戶或登記用戶之姓名與地址

3、辨別通訊日期、時間與期間之必要資料

（1）固定網路的電話與手機之通訊日期與通訊起迄時間

（2）網路存取、電子郵件及網路電話

A、特定時區中網路存取服務之登入及登出日期與時間、分配之固定或浮動 IP 位址以及用戶或登記用戶之使用者帳號

B、特定時區中電子郵件或網路電話之登入與登出的日期及時間

4、辨別通訊類型之必要資料

（1）固定網路的電話與行動電話所使用之電信服務

（2）電子郵件與網路電話所使用之網路服務

5、辨別使用者通訊設備之必要資料

（1）固定網路的電話所撥出與接收之電話號碼

（2）行動電話

A、撥出與接收之電話號碼

B、撥號方國際行動電話識別碼（IMSI）

C、撥號方國際行動設備識別碼（IMEI）

D、接收方國際行動用戶識別碼

E、接收方國際行動設備識別碼

F、預付之匿名服務其第一次啟用之日期、時間與所在方位

（1）網路接取、電子郵件與網路電話

A、撥號方之電話號碼

B、數位用戶迴路或其他原始通訊終端

6、辨別行動通訊設備方位之必要資料

（1）通訊起始之方位標識（基地台識別碼）

（2）通訊期間藉由方位標識以辨別之地理位置並予以保存之通訊資料

（二）保存資料之期限

會員國應確保規範中所須保存之資料其保存期限至少六個月，但不得超過自通訊日期起之兩年[71]。

Taylor（2006）曾針對資料保存期限之訂定進行探究，原先委員會建議各會員國之資料保存期限為一年，而透過 IP 進行之通訊則建議保存六個月，但委員會在評估各會員國之國內立法情形後，發現各會員國關於資料保存所訂定之期限，範圍自三個月至四年不等，如此大的差異性與委員會原先期望於歐盟訂定統一範圍之保存期限之初衷有違，因此最後明確於 Directive 2006/24/EC 中訂定資料保存之期限範圍。

（三）資料保護與安全[72]

在不違背 Directive 95/46/EC 與 Directive 2002/58/EC 之前提下，各會員國應確保公共電子通訊服務提供者及公共通訊網路，至少應遵守有關資料保存之資料安全原則：

---

[71] Directive 2006/24/EC, Article 6.
[72] Directive 2006/24/EC, Article 7.

1、保存之資料應與網路上之資料具有相同之品質、安全性與保護程度，亦即資料儲存時之安全性不能低於傳輸時。

2、應提供資料適當的技術與措施以避免因意外或遭遇非法損壞、非預期損失或竄改，或是未經授權或非法之儲存、處理、存取或洩漏資料。

3、應提供資料適當的技術與措施，以確保只有特定被授權之人員可進行存取。

4、除曾被存取並要求留存的資料之外，應在保存期限屆滿即銷毀。

（四）保存資料之儲存要求[73]

各會員國應確保上述保存資料之內容或其他相關必要資訊，須在主管機關要求提供時無任何延誤地立即提供。

（五）監督機關[74]

1、每一會員國應指派一個以上的主管機關，負責監督保存資料之保護與安全。

2、負責監督之主管機關於執行監督時具有完全獨立性。

（六）補救、責任與制裁[75]

1、各會員國應採取必要措施以確保實行 Directive 95/46/EC 第三章，針對法律上的補救、責任與義務及制裁等相關規範[76]：

（1）補救

A、在不違反任何行政程序之前提下，會員國應提供每個人有司法救濟之權利，以處理國家的法律適用相關問題。

（2）責任與義務

A、各會員國應提供每個人有因非法資料處理程序，或不符合該指令所列之任何規範而遭受損失時，有權對其損失要求賠償。

B、被要求賠償之主管機關可證明此損害非其責任或非因其而致生，可

[73] Directive 2006/24/EC, Article 8.
[74] Directive 2006/24/EC, Article 9.
[75] Directive 2006/24/EC, Article 13.
[76] Directive 95/46/EC, Article 22, 23& 24.

一部或全部豁免賠償責任。

（1）制裁

A、各會員國應採取適當措施以確保全面實施本指令的規定，並應依據本指令特別針對侵犯規範的情況實施制裁。

B、各會員國尤其應採取有效、合比例原則及勸戒的行政罰或刑罰，不允許任何有意違反本指令的資料傳輸或轉移行為，並應加以處罰。

（七）會員國國內立法[77]

1、各會員國應立即告知相關委員會，最遲於 2007 年 9 月 15 日前訂定相符於本指令之法案，發布立法之內容亦應相符本指令。

2、各會員國應與其國會充分溝通，確保主要法條內文涵蓋本指令的內容。

3、各會員國得於 2009 年 3 月 15 日前，暫緩實施本指令中網路存取、電子郵件及網路電話的通訊資料保存相關規範。任一會員國預計實施本指令之前，應通知理事會與委員會聲明公告，並刊登於歐盟之官方期刊。

（八）適用準則

蘇三榮[78]與邱佩俞[79]皆有針對網路通訊紀錄資料保存適用準則部分，歸納資料保存事務委員會（Data Protection Working Party）所提出之保護措施，以補充該指令在資料處理充分性及特定性之不足，委員會並建議各會員國應參考如下標準：

1、須有特定之目的

主管機關要求提供個人資料之目的須明確，若是依據指令所規範是針對「重大犯罪」之調查、偵查與起訴，則應予以釐清「重大犯罪」一詞。

2、要求提供資料之限制

要求提供個人資料之主管機關，限於有權執行犯罪調查、偵查與起訴之

---

[77] Directive 2006/24/EC, Article 15.

[78] 蘇三榮，網路時代通訊監察與個人資料保護之法制研究，國立交通大學科技法律研究所碩士論文，2009。

[79]邱佩俞，電信詐欺犯罪運作歷程及其查緝因應策略之研究，中央警察大學犯罪防治研究所博士論文，2011 年 12 月。

機關，並應對民眾公告該等機關之名單，且調閱資料之紀錄應呈報予監督機關以發揮監督效果。

3、資料調閱之必要性

資料之調閱須依循必要性原則並詳列清單，如清單異動，則應採嚴格必要性原則檢視。

4、探查資料之限度

以犯罪調查、偵查與起訴為目的所調閱之資料，不得對該資料進行前述目的以外之探查，以維護民眾行動自由與使用通訊之權利，不因犯罪嫌疑而受影響。

5、司法或獨立機關之檢驗與監督機制

個人資料之調閱是以個案方式進行，且須由特定機關為之並受監督機關之檢驗，因此，調閱資料之機關應詳列特定目的之個案需求及調閱範圍。

6、業者保存資料目的之限制

業者保存客戶資料時，除因應主管機關之特定需求外，不得以其他理由進行資料之不當留存。

7、資料保存系統之區隔

因應主管機關需求而用以保存資料之系統，應與業者自行以商業為目的而進行之資料儲存系統有所區隔。

8、資料保存之安全性

該指令應更進一步對於資料保存之要求訂定規範，並要求業者對於技術與組織上的安全措施，訂定依循之最低標準。

五、網路犯罪公約（Cyber-crime Convention）

網路犯罪公約是於 2001 年 11 月由歐洲理事會的 26 個歐盟成員國，以及美國、加拿大、日本和南非等 30 個國家的政府官員，於布達佩斯所共同簽署的國際公約，自此《網路犯罪公約》成為全世界第一部針對網路犯罪行為所制訂的國際公約。而其制定的目標之一，是期望國際間對於網路犯罪的立法有一致共同的參考標的，也希望國際間在進行網路犯罪偵查時有此國際

公約予以支持，而得以有效進行國際合作。

網路犯罪公約除序言外，本文分為四個章節，共計 48 個條文。序言是說明公約的功能與目標；第一章為術語的使用，即是對網路犯罪涉及的術語進行名詞定義，其中包括有電腦系統（computer system）、電腦資料（computer data）、服務提供者（service provider）與流量資料（traffic data）等都有明確之定義；第二章為國家法律層面上的措施，包括有刑事實體法、刑事程序法和管轄權三個部分，其目的為規範各簽約國於各國國內應採取的措施，且在程序法部分規定有關電子證據調查的特殊程序法制度，其中值得注意的是在規範非法擷取之行為方面，公約要求各國應立法明訂相關犯罪行為並予以處罰；第三章為國際合作，包括一般原則和特殊規定兩部分，在一般原則中包含規範引渡及相互合作等相關問題，而特殊規定則係有關電腦證據取得之面向，簽約國應建立一周七天且一天二十四小時皆能聯絡的合作機制網路，各國亦要對於相關人員加強訓練，並配予必要的裝備以配合各國合作事項的進行；第四章為最後條款，主要規定公約的簽署、生效、加入、區域應用、公約的效力、聲明、聯邦條款、保留、保留的法律地位與撤回、修訂、爭端處理、締約方大會以及公約的退出與通告等事項[80]。

參閱許慈健[81]之整理，網路犯罪公約中協助網路犯罪偵查主要規定於第二章，其中要求服務提供者應配合協助之事項如下：

（一）應迅速保存、儲存及提供電腦中之相關資料；

（二）應迅速儲存及揭露部分之通訊紀錄；

（三）協助執行搜索及扣押；

（四）協助即時收集通訊紀錄；

（五）協助擷取通訊內容資料。

---

[80] 參閱網址：
http://zh.wikipedia.org/wiki/%E7%B6%B2%E8%B7%AF%E7%8A%AF%E7%BD%AA%E5%85%AC%E7%B4%84。最後瀏覽日期：2012 年 5 月 2 日。

[81] 許慈健，網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究，國立交通大學管理學院在職專班碩士論文，2005，頁 101-105。

依網路犯罪公約之規定，其適用之規範主體為「服務提供者」（service provider），其定義係指「提供用戶有能力經由電腦系統進行通訊之任何公共或私人機構」[82]，因此所謂網路服務提供者，並不限於電信業者。

六、歐盟各會員國之國內法規

（一）英國

英國並未有針對資料保存期限之相關立法，僅有一般性原則是關於服務提供者不再需要帳單之類的流量資料後，即須立即銷毀不得保存，儘管如此，英國在 2001 年的〝反恐、犯罪與安全法案〞（Anti-terrorism, Crime and Security Act of 2001）訂定後，便推出一套自願保存資料的系統（The system of voluntary data retention）。根據該法案，通訊服務提供者須以維護國家安全及直接或間接與國家安全有關之預防、偵查或起訴犯罪為目的，而進行通訊資料之保存，此亦為提供者與內政部之自願協議。而另一個關於收購與洩漏上述規範須保存之通訊資料的修訂草案，也已經於英國正式公告。

（二）比利時

根據比利時的法規，電子通訊服務提供者或網路提供者（包含經銷商），應保存流量資料與使用者身分辨識資料一至三年。然而，比利時皇家法令所規範之一些特定議題所致生的強制力，足以導致資料保存相關立法無法執行。因此，皇家法令應定義確切之資料保存期限，以及在何種情況下，提供者須註記與保存前述之通訊資料，這樣的做法將有助於犯罪行為的調查與起訴、行使追蹤惡意呼叫之緊急服務，及使電信專員反查詢出不當使用電子通訊服務與網路的特定人士身分。

（三）愛爾蘭

愛爾蘭明文規定固定線路或行動電話之通訊資料須保存三年，但並未適用於實質通訊內容與網路資料之保存。愛爾蘭國內刑法於 2005 年之法案，

---

[82] Cyber-crime Convention, Article 1. "Any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and any other entity that processes or stores computer data on behalf of such communication service or users of such service."

針對通訊服務提供者以預防、調查、偵查或起訴犯罪（包括恐怖份子犯罪）以及維護國家安全為目的，根據 1993 年的郵件封包與通訊資訊規範法案，於 2005 年所訂定關於保存通訊資料（包括流量資料與位置資料）之相關規範法案，此亦保障避免擴張指定法官與投訴裁判之職權，而造成保存資料的濫權。

2005 年的法案賦予愛爾蘭國家警察一個完整的法定職權，可要求服務提供者保存資料三年，並因應特定目的而予以提供，但是資料保護專員的意見限縮保存期限為六個月。

（四）義大利

義大利於歐盟已有一個限制資料保存期限之政策，根據資料保護法規，應授權提供者能處理流量資料並保存不得超過六個月，特別嚴格針對用戶帳單與連線費用，一旦帳單有爭議或要求付款時可提供證據。不過，此法規亦有因帳單與連線費用之外的其他目的而須保存流量資料之相關規範。

依據該法規第 132 條所示：「電信流量資料，包含未接來電之資料，應由服務提供者保存二十四個月。」用以偵查與防制罪犯，而電子通訊流量資料，不含括通訊實質內容，應由服務提供者為履行相同目的而保存資料六個月。電信流量資料之保存期限應僅延長至四十八個月，而電子通訊流量資料應保存上限為一年，以因應偵查與防制組織犯罪之目的，包括網路犯罪與犯罪組織（黑手黨類型）所犯之罪行，或者由敵對國家之公民所提供的服務。

2005 年 7 月 27 日，義大利政府發佈「對抗國際恐怖主義之緊急措施」，並於 2005 年 7 月 31 日轉為正式立法，規範所有的公共通訊網路與電子通訊服務中之電信與電子通訊流量資料，須由服務提供者保存直至 2007 年 12 月 31 日，其中網際網路提供者應保存所有的資料至少六個月，有必要之情形得再延長六個月。

（五）德國

德國並未有以執法為目的而保存流量資料之正式立法，該國電信法於 2004 年修法時就已否決流量資料之保存提案，其否決之理由乃認為流量資

料屬於通信保密之範疇，且亦有洩漏個人資料之可能。德國資料保存與言論自由聯邦委員會表示，公共流量資料之保存，等同於對所有使用者之監視作為，此並不符合基本民主原則，而當討論到資料保存指令，委員會亦指出將確保採取對公民產生最低影響的作為，並實現於德國的法制系統中。因此，資料保存期限應限縮至最少六個月，從而滿足現存允許保存帳單資料之期限，但保存資料之義務並未含括撥號不成功之紀錄。

（六）法國

資料保存等議題在法國遭到強烈反對，部分社會主義與共產主義小組之成員提出一項反恐怖主義法草案，該法案內容提及資料保存之立法，憲法委員會則質疑此項立法給予內政事務過大的權力。然而，經過一段漫長時間的協商，2006 年 1 月 23 日法國關於打擊及反抗恐怖主義之法案（2006-64），包括安全與邊境管制等議題終於納入立法。法國第一個資料保存規範頒布於日常安全法（the Law Regarding Daily Safety, 25 Nov. 2001）第 29 條，該法條歷經多次法規修訂，包括上述關於打擊及反抗恐怖主義之法案，並正式於電子通訊法第 34-1 條及第 34-1-1 條完成修法。

相關之修法有利於警察單位進行通訊之監視，並允許其獲得由電信營運商（telephone operators）、ISP 業者及網咖業者（Internet cafes）提供之通訊資料，修法內容明文規定 ISP 業者、網咖業者、託管服務提供商（hosting providers）及營運商應專門針對恐怖活動之犯罪嫌疑人的調查動作，彼此傳達流量資料、來電號碼與 IP 位址等資料，而行動電話營運商與網咖業者將被要求保存客戶連線紀錄長達一年。根據法國資料保護局（French Data Protection Authority）表示，該項修法被認為是「為因應嚴重威脅而採取之特殊措施」。

2006 年 3 月 26 日法國第 2006-358 號法令關於電子通訊資料之保存已正式發布，網路與電信營運商應保存相關資料長達一年，同時這些資料能提供司法當局及警察單位處理運用。該法令詳列須保存之資料，包含用以識別用戶之資料、通訊終端使用之設備、通訊之接收者、通訊日期、通訊時間及期間、使用者使用之額外服務以及電信服務供應商之通訊來源與通訊位置。法

國網路接取服務業者協會（The French Association of Internet Access and Service Providers）於 2006 年 3 月 28 日宣布將於行政法院對上述法令提出質疑，依據其所聲明之內容，表示雖然法令規定須支付為因應執法機關之要求所衍生之費用，但在個別情況下，並不包含已具體規定為保存資料而施加於提供者的一般成本。

第五節　亞洲現有法規

一、日本

以下就日本紀錄保存之各相關法規，包括刑事訴訟法、電信事業法、特定電信服務提供者之損害賠償責任限制及發信者資訊揭露法、電信事業對個人資訊保護準則及犯罪偵查之通信監察法等分別說明。

（一）刑事訴訟法

1、立法源起

隨著資訊技術領域、電腦網路的迅速發展，伴隨而來的網路犯罪問題亦日益嚴重，意識到國際間協調合作為有效防制網路犯罪之重要方法，歐洲理事會有了一項共同認知－必須作成具法律拘束力之國際文書，因此，1997年歐洲理事會設置了「網路犯罪專家委員會」，開始著手條約制定作業，2001年經歐洲理事會部長委員會通過，同年 11 月 23 日於匈牙利的布達佩斯舉行簽署典禮，日本亦簽署條約。身為締約國之一，日本外務省於 2004 年 2 月作成「網路犯罪公約」譯文及其說明書，並經國會承認，於同年 7 月 1 日生效，為達成必須擔負之義務與其宣示之內容[83]，日本國內開始展開一連串修法行動，包括有線電氣通信法、刑法，及有關兒童買春與兒童色情等行為之處罰、兒童保護等相關法律之部分修正案，陸續於日本國會中提出。

---

[83]參閱日本外務省網頁 http://www.mofa.go.jp/mofaj/index.html ，有關外務省＼外交政策＼條約項下之刊載，標題「サイバー犯罪に関する条約説明書」，平成 16 年 7 月 1 日生效。

＊第一大項第 3 小項－基於締結條約，日本須擔負之義務概要如下：

（1）將違法連接電腦系統、違法監聽電腦資訊、製造電腦病毒、連接兒童色情的電腦系統等行為，定為犯罪行為，並設定相關之裁判權。

（2）國內權限當局，應針對已儲存電腦資訊之迅速保全、搜索、扣押及提出命令、通信紀錄之即時蒐集、通信內容之監聽，採取必要之立法及其他措施。

（3）促進電腦相關刑事程序、犯罪人引渡等國際合作。

＊第一大項第 5 小項－日本宣示

本條約以尊重締約國國內事務之觀點，承認對部分規定之實施課予適當追加要件、不適用之部分予以保留等宣示事項。日本宣示內容概要如下：

（1）將對於電腦系統之違法連接（第二條）及電腦資訊之違法監聽（第三條）以國內法之犯罪定之時，課予追加之要件。

（2）除以提供或公然陳列為目的而持有及保管兒童色情者之國內法犯罪外，不為國內法犯罪之兒童色情保有者。

（3）描寫兒童姿態之色情（含得辨認為實在描寫兒童姿態之情形）視為本條約中之兒童色情。（第九條）

日本法務省亦於2003年4月14日，於原有法制審議委員會下新設「科技犯罪小組」（ハイテク犯罪関係部会），經八次會議審議研修，於2003年9月10日提出「處理科技犯罪之刑事法律修正概要」，在2004年2月20日向國會提出修正案之「犯罪國際化、組織化對策以及針對情報處理技術提升之刑法等部分條文修正概要」中，提出有關刑事訴訟法「電磁紀錄儲存媒體證據保全程序」之修正概要，包括：與電腦經網路連結儲存媒體之複製、附紀錄命令之扣押、搜索扣押電磁紀錄之儲存媒體的執行方法、對接受電磁紀錄儲存媒體扣押者之協助命令、命令保全處分、不法作成電磁紀錄之沒收…等項目[84]，而對於網路業者紀錄保存之相關規範亦見其中。

「因應資訊處理技術提升之刑法部分修正案」（情報処理の高度化等に対処するための刑法等の一部を改正する法律案）2011年4月1日於國會提出，同年6月17日通過，6月24日公布，並分二階段施行：有關罰則整備相關部分（一部分除外）於同年7月14日開始施行；有關程序法整備相關部分（包含上述刑事訴訟法六大項目增修條文），自公布日起一年內以行政命令訂定之[85]。

2、相關條文

日本刑事訴訟法第197條增修條文載明：「檢察官、檢察事務官或司法警察官，於認為有扣押或紀錄指令附帶扣押之必要時，對於提供電信設備以為他人通信之用之業者，或為了自己的業務媒介不特定或多數人通信而架設電信設備者，特別指定該業務上紀錄之通信來源、目的、日期時間及其他通信歷程（通信履歷）[86]之必要者，得以書面要求於30日期間內不得刪除。在此情形下，如認為相關電磁紀錄扣押或紀錄指令附帶扣押不必要時，應取消相關要求」（第197條第3項）。「有特殊必要時，要求不可刪除之期間，在

[84] 林裕順，電磁紀錄之證據保全－檢討日本代表性判例的啟示，法令月刊，第58卷第10期，頁1325-1326，2007年10月。

[85] 參閱日本法務省網站：http://www.moj.go.jp/index.html，トップページ ＼所管法令等 ＼ 国会提出法案など ＼ 国会提出主要法案第177回国会（常会）項下之刊載，標題「情報処理の高度化等に対処するための刑法等の一部を改正する法律案」。

[86] 日本原文為「通信履歷」，本文譯為「通信歷程」，係指除通信內容以外之相關事項紀錄，具體而言，即為通信來源、目的、日期時間等一般稱為log之紀錄，故電子郵件本文、通信內容等不適用之。

不超過 30 日範圍內得延長之，但最長不得超過 60 日」(第 197 條第 4 項)。

此保全處分之制定，乃依循網路犯罪公約第 16 條第 1 項「各簽約國應立法或採取其他必要措施，在有合理根據相信電腦資料特別容易滅失或遭竄改時，使主管機關得以命令或他法迅速保存該特定電腦資料（包括通訊資料)」之規定，提出保全處分時，相關電磁紀錄仍保存於該通信服務提供者控制之下，須經由搜索扣押或提出命令等程序方可取得。訂定通信歷程保全處分制度之必要，原因在於電腦網路犯罪具匿名性，在追查犯罪人過程中，通信歷程之電磁紀錄扮演著極為重要的角色，但在一般情況下，這些紀錄大多在短時間內即遭刪除，等到取得令狀實施扣押時早就為時已晚。因此，日前在日本偵查實務上，對於偵查上必要之通信歷程電磁紀錄，在依令狀實施扣押之前，就會要求通信服務提供者遵守保全義務，不可予以刪除，但是像這種任意請求保全的情形，攸關當事人之權益，仍應在法律上有明確之依據，方能符合民眾之期待。

保全處分的主體為檢察官、檢察事務官或司法警察官。保全處分之要件，為對於相關通信歷程之電磁紀錄，認為有扣押或紀錄指令附帶扣押必要之情況下。保全處分的對象有二，一是提供電信設備以為他人通信之用的業者，如：電信公司、電信服務提供者…等；另一是為了自己的業務媒介不特定或多數人通信而架設電信設備者，如：架設區域網路（LAN）公司、公務機關、大專院校…等。保全處分之標的物，係指上述二種處分對象在業務上已記錄之通信來源、目的地、日期時間及其他通信歷程之電磁紀錄，亦即非業務相關或命令保全處分時尚未存在之紀錄，不在保全處分之標的範圍內。本法所指「通信歷程」為通信內容除外之其他通信相關資訊，除了法條中例示之通信來源、目的地、日期時間外，尚包括其他通信歷程如：通信協定（Protocol)的種類、電子郵件的檔案大小…等。但像是電子郵件檔頭(Head)資訊中的「Subject（主題)」，是電子郵件傳送者使用電子郵件軟體而作成、記錄之資訊，非屬電信業者業務上之紀錄，因此，不可作為保全處分之標的物。至於如何識別哪些電磁紀錄是「必要者」呢？識別的方法，視案件內容、偵查的進度狀況，所必要之通信歷程種類也會有所差異，在日本，一般的呈

現方式舉例如「○年○月○日至○月○日，由郵件地址○○○○收發信件的電子郵件通信歷程（收發日期、來源或目的郵件地址）」。

以通信秘密權利保障的觀點來看，雖然通信歷程是通信秘密保障的範圍，但是，一旦有人利用電信實施犯罪，確保通信歷程存在以追蹤識別犯罪人是相對重要的，因此，要求通信服務提供者「迅速保全」相關通信歷程仍是必要的。且保全處分對象僅限於通信服務提供者「業務上」已記錄之通信歷程，不能過度要求通信服務提供者保存該通信歷程、不得向偵查機關揭露該通信歷程，即使保全處分對象不願履行保全義務，實際上並不會有任何權利侵害發生，也沒有相關之罰則規定，故不會造成不當制約通信秘密之情形，所以，保全處分非必定需要法官核發之令狀，亦無違反法律保障通信秘密之規定，假如保全處分必須依據法官核發之令狀，則申請核發令狀之事前準備工作所耗費之時日，反而可能影響「迅速保全」的要求。

除了迅速保全之外，迅速搜索扣押亦甚為重要。犯罪人在使用網路過程中常會牽涉到數個不同之通信服務提供者，每一個都可能擁有犯罪相關通信的來源與目的之關鍵性資訊，為了確認該服務提供者保有全部相關資料，以及在相關通信傳輸路徑中是否仍存有其他服務提供者，並且能保全所有通信服務提供者持有之相關通信紀錄，網路犯罪公約特別制訂了第 17 條第 1 項之規定[87]。惟條文上並未要求各簽約國均須發出帶有部分揭露效果之保全命令，只要能夠確保具備實效性之履行（例如：迅速要求全體揭露）亦為本條所許。因此，日本為符合本條之要求，除新增保全處分外，並未採行第 17 條第 1 項 b「帶有一部分揭露之保全處分」的規定，而以迅速執行有令狀之搜索扣押或揭露命令代替之[88]。

在法律效力方面，保全處分對其對象賦予法律上保全通信歷程電磁紀錄

---

[87] 網路犯罪公約第 17 條第 1 項規定：a.不論該訊息傳輸牽涉到一個或多個服務提供者，皆應確保該迅速保存之通訊資料具有可利用性。b. 確保對簽約國之主管機關或主管機關指定之人迅速揭露足夠數量之通訊資料，使簽約國得以識別服務提供者及其訊息傳輸之路徑。

[88] 陳誌泓，電腦、網路與刑事偵查－以網路犯罪公約於日本法的落實為中心，國立臺灣大學法律學研究所碩士論文，2005 年 7 月，頁 109 註 124（參照山田利行，「サイバー犯罪に関する条約の概要」，法律のひろば，2004 年 7 月，頁 49）。

之義務。換句話說，通信事業者依保全處分而繼續保存通信歷程，係基於法令義務之履行，該當日本個人資料保護法（個人情報の保護に関する法律）第 16 條第 3 項第 1 款「基於法令者」[89]，或電信事業者對個人資訊保護準則（電気通信事業における個人情報保護に関するガイドライン）第 10 條第 2 項第 1 款「基於法令應予保存時」之規定。只不過，在沒有相關罰則規定之情形下，假如遇到保全處分對象不願配合時，只得迅速執行扣押及紀錄指令附帶扣押以為因應。

保全期間訂有不可逾 30 日，有特殊必要時得延長之規定，其延長之次數不限，但單次延長期間應在 30 日範圍內，且延長之總日數不得逾 60 日，亦即保全期間之上限為 90 日。此期間之訂定主要係遵從網路犯罪公約第 16 條第 2 項之規定[90]，且考量日本實務上，偵查機關於扣押相關通信歷程之電磁紀錄前，多會事先與通信服務提供者連絡，雖可視個案偵查需要而調整期間，但一般多會在二個月內扣押完畢，因此訂出 90 天之保全期間上限。且為避免造成通信服務提供者之負擔，在延長期間上亦有附加條件，不管是第一次延長，或是第二次、後續之延長，都須符合「有特殊必要時」之要件，也就是說，這項延長期間之決定，係因對該通信歷程之電磁紀錄進行扣押或紀錄指令附帶扣押有困難，為了確保日後之扣押或紀錄指令附帶扣押順利進行，而有延長其保全期間之高度必要，方符合保全處分延長之條件。另外，保全期間達上限後，亦不允許對同一通信歷程之電磁紀錄重新提出保全處分，否則，如此無限期的保全處分，反而淪為對保全處分對象之過分要求，本法一再強調之「迅速保全」便毫無意義了。同時，對於該電磁紀錄於認為已無必要扣押或紀錄指令附帶扣押時，偵查機關即有義務取消保全處分，值得注意的是，本法規定保全處分應以書面為之，但保全處分之延長期間或取消則未有明確規範，不以書面為之亦可。

---

[89] 該條規定，個人資訊處理業者未事先取得本人之同意，不得作超過為達特定使用目的所需範圍之個人資訊之處理，但基於法令者不適用之。完整法條請參閱附錄。

[90] 網路犯罪公約第 16 條第 2 項規定，締約國應立法或採取其他必要措施，要求特定人在必要時間（最多 90 天）內，保存及維持其所有或控制之特定電腦資料之完整性，使主管機關得揭露該資料。完整法條請參閱附錄。

另外，依循網路犯罪公約第 16 條第 3 項規定「各簽約國應立法或採取必要措施，對於命其保存電腦資料之人，在其內國法所規定一定時間內，課予其保持秘密之義務」，日本於刑事訴訟法第 197 條第 5 項增修條文規定「依第 2 項或第 3 項之要求情形，必要時，得要求不得擅自洩漏相關事項。」該第 2 項之偵查相關事項詢問[91]及第 3 項之保全處分，性質上均屬偵查之初期階段工作，大多要求應秘密進行，否則可能因洩漏相關事項而造成偵查上之阻礙，因此，要求保全處分對象對保全處分相關事項擔負法律上之保密義務有必要。同時，由於法律明確規定該保密義務，當電信服務提供者之使用者詢問保全處分等相關事項時，即可依此不予回答。但應注意，本項以「必要時」為要件，如果像是嫌犯已落網之情形，即無要求保密之必要了。此外，所謂「不得擅自洩漏相關事項」即「無正當理由」不得洩漏之意，若有保全處分之情形，在業務上須向內部報告，即屬正當理由向他人洩漏，與保密義務不相違背。當保密期間經過或相關事項已不具秘密性，不必要繼續保密時，即可解除保密之義務。不過，即使保全處分對象違反保密義務，亦無相關罰則規定，在立法上或有不足。

網路犯罪公約第 18 條[92]之「提出命令」規定，亦可視為日本延續保全處分，制定「附紀錄命令之扣押」之參考依據；所謂「附紀錄命令之扣押」係指命令電磁紀錄之保管者或其他具備利用權限者，將必要之電磁紀錄儲存或印刷於電磁媒體後，扣押該當紀錄媒體[93]。讓偵查機關在實施保全處分後，除了採行搜索扣押等手段之外，能選擇另一侵害性較小之手段取得偵查上必要之相關通信歷程之電磁紀錄，同時也提供了通信服務提供者一個法律上之依據，使其於提供犯罪偵查協助時能無後顧之憂。但提出命令不履行時，是否須施以其他間接強制措施？網路犯罪公約則無任何規定，留予各簽約國立

---

[91] 日本刑事訴訟法第 197 條第 2 項規定：「關於偵查，得詢問公務機關或公私團體，要求其提出必要事項之報告」。

[92] 網路犯罪公約第 18 條第 1 項，規定簽約國應採取必要之立法或其他措施，授權主管機關對其領域範圍內之人，命其提出其所有或在其控制下儲存於電腦系統或電腦儲存媒介中之特定電腦資料；對在締約國領域範圍內提供服務之服務提供者，命其提供其所有或在其控制下與該服務相關之使用者資訊。詳細條文內容如附錄。

[93] 參閱日本刑事訴訟法第 99 條之 2 增修條文，詳見附錄。

法空間，如此是否意謂著默許「僅規定義務，不設定違反義務之間接強制措施」之立法方式？既然不履行提出義務不會造成任何權利侵害，則偵查機關亦可為發動命令之主體，非必定須經過令狀主義之檢驗[94]。換句話說，依循網路犯罪公約之規定，自命令通信服務提供者保全犯罪相關通信歷程之電磁紀錄或使用者資訊至提出該等紀錄、資訊，均非必定需要令狀方可執行，在日本檢警雙偵查主體之體制下，即可自行發動該命令。然而，日本在建立「提出命令」相關法制時，仍然採取了較為保守之立法方式，將附紀錄命令之扣押之發動權交由法院行使，以符合令狀主義之原則[95]。

日本刑事訟訴法值得我國參考部分，在於其第 197 條規定之保全處分對象，除了一般提供電信設備以為他人通信之用之經營事業者（如：電信公司、電信服務提供者…等）之外，尚涵蓋「基於自己業務需要媒介不特定或多數人通信而架設電信設備者」，如：架設區域網路的公司、公務機關、大專院校等。我國目前在犯罪偵查上調閱相關電信通信紀錄及使用者資料，均係依「電信法」第 7 條第 2 項、「電信事業處理有關機關查詢電信通信紀錄實施辦法」及「電信事業處理有關機關（構）查詢電信使用者資訊實施辦法」，暫且不論相關紀錄保存期間為多少，單就依法可向其查詢紀錄之對象，我國就僅侷限於「電信事業」，亦即「電信法」第 2 條第 1 項第 5 款所定義之「經營電信服務供公眾使用之事業」，以公司組織型態或為商業登記者為限，條件較為嚴格，適用範圍相對狹猶，難以涵蓋本研究「網路服務平臺業者」之全數對象。反觀日本法之規範對象，除一般電信事業經營者外，另加入「基於自己業務需要媒介不特定或多數人通信而架設電信設備者」，範圍擴及未達「經營者」標準之其他小規模電信服務業者、公務機關、學術網路、教育單位電算中心及其他非以營利為目的之服務提供者，似乎較符合本研究對於「網路服務平臺業者」範圍之期待，值得我國立法之參考。

日本在犯罪偵查上屬雙偵查主體，警方亦具備偵查權，可為保全處分之

---

[94] 陳誌泓，電腦、網路與刑事偵查－以網路犯罪公約於日本法的落實為中心，國立臺灣大學法律學研究所碩士論文，2005 年 7 月，頁 112-115。

[95] 日本刑事訴訟法第 218 條第 1 項增修條文規定：「檢察官、檢察事務官或司法警察，於實施犯罪偵查之必要時，得依法官核發之令狀，行使附紀錄命令之扣押」。

主體，確保已存在之犯罪相關電磁紀錄得以繼續留存至多 90 日之期間，以待法官核發令狀作進一步之搜索扣押或附紀錄命令扣押之程序。而我國係以檢察機關為偵查主體，但在實務上，從受理案件至展開初步階段之偵查蒐證工作大多由警察機關任之，與日本偵查體制有異，因此，如何制定出適合我國之相關規範，尚有待討論。惟不可否認，若能朝「網路紀錄主動保存一定期間」之立法方向著手，讓警方於偵查初期階段即可確定相關電磁紀錄證據尚存在與否，且會繼續留存多久，對犯罪偵查工作必有所助益。例如：警方欲取得犯罪嫌疑人於 2012 年 2 月 14 日在某 BBS 站留言販賣毒品之來源 IP 位址資訊，而假設我國法律有明文規定網路平臺提供者應保存使用者之來源 IP 位址至少 6 個月之期間，則偵查人員即可確定該紀錄於 2012 年 8 月 13 日前不會遭到刪除，以利其掌握時效取得並分析運用相關紀錄，追查犯罪嫌疑人身分。

（二）電信事業法（電気通信事業法）

本法第 2 條定義各相關名詞如下：所謂「電信」指以有線、無線及其他電磁方式發送、傳輸或接收符號、聲音或影像者。範圍相當廣泛，舉凡利用電磁媒介的通訊行為，諸如使用銅線、光纖之有線通訊、使用電波之無線區域網路、及使用雷射或紅外線之通訊均屬之，目前常用之網際網路通訊自亦包括在內[96]。「電信設備」係指電信所用之機械、器具、線路及其他電氣設備。舉凡終端機、伺服器、交換機、有線電視電纜線等以有線或無線方式相互結合，以提供電信通訊的個別設備均屬之[97]。本研究以為，日本刑事訴訟法第 197 條增修條文所述之電信設備應係採本項定義。「電信服務」指使用電信設備媒介他人通信、及其他提供電信設備供他人通信之服務。「電信事業」指應他人需要而提供電信服務之事業。「電信業者」指經營電信事業，辦理本法第 9 條之登記及依第 16 條第 1 項規定提出報告者。此處所指應提出報告之電信業者，規範於電信事業報告規則[98]（電気通信事業報告規則）

[96] 資策會，網際網路服務提供者法律責任與相關法制之研究，2003，頁 84。
[97] 資策會，網際網路服務提供者法律責任與相關法制之研究，2003，頁 85。
[98] 最終改正：平成 24 年 4 月 27 日総務省令第 42 号。
http://law.e-gov.go.jp/htmldata/S63/S63F04001000046.html

第 1 條第 2 項中，亦即日本「電信事業」所涵蓋之種類範圍，經營項目包含：中繼電話、IP 電話、FMC 服務、網路連線服務、FTTH 接取服務、DSL 接取服務、FWA 接取服務、CATV 接取服務、行動電話 PHS 端末網路連線服務、行動電話 PHS 封包通信接取服務、3.9G 行動電話端末網路連線服務、3.9G 行動電話封包通信接取服務、BWA 接取服務、公眾無線 LAN 接取服務、IP-VPN 服務、廣域乙太網路服務及國際電話等。

電信事業從業人員的工作既然與通信相關，可能探知他人隱私秘密之機會也相對增加，因此，該法第 4 條載明保密義務「任何人對於有關電信業者處理中之通信秘密，不得侵害之。從事電信事業之工作人員，於任職期間，因處理電信業者之相關通信，而得知他人秘密者，應保密之，於退職後亦同」，以保障相關電信用戶之通信秘密權利，若要提供通信等個人資訊予第三人，必須遵從法律之明確規範為宜。

（三）ISP 責任限制法（プロバイダ責任制限法[99]）

全名為「特定電信服務提供者之損害賠償責任限制及發信者資訊揭露法」（特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律），本法於 2001 年 11 月通過、2002 年 5 月施行，旨在規定因特定電信流通資訊造成權利侵害時，特定電信服務提供者之損害賠償責任限制及請求揭露發信者資訊之權利，以民事上權利受侵害之個人為對象。本法第 2 條定義所謂「特定電信」係以不特定人為電信發送之接收者，例如：網站、電子佈告欄等即是，但像廣播等以公眾為接收目的之發送，或電話等一對一之通信方式則不在此「特定電信」範圍內。所謂「特定電信服務提供者」係指以特定電信設備媒介他人通信，或其他提供特定電信設備以為他人通信之用者，指網路的管理、營運者，也包含典型的電信業者，但因不以營利目的為限，故典型電信業者以外之服務提供者，不論個人、團體、學校或地方自治團體，均亦包含在內。就本研究之主角「網路平臺業者」而言，在定義上不若日本特定電信服務提供者範圍如此寬廣，但既屬我國第二類電信

[99] 參閱日本「プロバイダ責任制限法 関連情報 Web サイト」網站，http://www.isplaw.jp/。

事業，則有「第二類電信事業管理規則」第 27 條「已辦理公司或商業登記之經營者」之條件限制，惟常見之網路平臺提供者類型如：FTP 站、網路論壇、BBS 站…等，多無商業登記，若直接於「第二類電信事業管理規則」中增修網路平臺提供者紀錄保存之規定，恐將無法規範到多數 IPP 類型，如此修法便毫無意義。反之，若對「條件」不加限制，舉凡個人或企業、是否以營利為目的者（如：教育用之免費服務平台）皆涵蓋其中，要求其行使網路紀錄保存之義務，必會發生執行上之困難，是否可行，仍有待討論。另外，本法所指「發信者」係指在特定電信服務提供者所用之特定電信設備的紀錄媒體上紀錄資訊、或在該特定電信設備的發送裝置輸入資訊者，合先敘明。

什麼樣的情況才符合向特定電信服務提供者請求揭露發信者資訊的資格呢？本法第 4 條第 1 項載明因特定電信資訊之流通而使自身權利遭受侵害者，須符合二種情形，方能對該特定電信服務提供者請求揭露其保存之相關侵害權利之發信者資料，一為因侵害資訊之流通，顯有侵害該請求揭露者之權利時；二為請求揭露者為了行使損害賠償請求權或有其他正當理由，有揭露發信者資料之必要時。符合以上二要件，權利受侵害人方可向特定電信服務提供者請求揭露該發信人之資訊。

發信者資訊究係包含哪些項目？2002 年 5 月 22 日，日本總務省發布「訂定特定電信服務提供者之損害賠償責任之限制及發信者資訊揭露法第 4 條第 1 項省令」[100]，並經 2011 年 9 月 15 日總務省令第 128 號修正，明訂發信者資訊項目共計 7 項，包含：發信者及其他相關侵害資訊傳送者[101]之姓名、住址、電子郵件地址、侵害資訊之相關 IP 位址、由相關行動電話末端裝置或 PHS 端末裝置連接網路服務發布侵害資訊之使用者識別符號、相關 SIM 卡識別碼中由該服務傳送者、經特定電信設備傳送侵害資訊之年、月、日及時間等。以提供遭受權利侵害者得以識別發信者為何人，並進一步行使損害

[100] 參閱日本總務省網頁 http://www.soumu.go.jp/，有關所管法令等／電気通信事業項下之刊載，標題「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律第四条第一項の発信者情報を定める省令（平成 14 年総務省令 57）」，最終改正：平成 23 年 9 月 15 日総務省令第 128 号。

[101] 當發信者使用所屬企業、學校的通信端末設備發送資訊的情況下，該企業、學校等即所謂「其他相關侵害資訊傳送者」。參閱「プロバイダ責任制限法」逐條解說，頁 27。

賠償請求權。但必須了解的是，特定電信服務提供者在實際運作時，尚有不同屬性之分類，如同我國網路服務提供者亦細分為網路接取提供者（IAP）、網路平臺提供者（IPP）及網路內容提供者（ICP）一樣。就有日本律師表示，主張被害者（遭受權利侵害者）請求特定電信服務提供者揭露資訊可能有兩階段之情形，第一階段大多先向佈告欄或聊天室等的網站管理者請求揭露發信者資訊，但這些管理者並不知道發信者的全部資訊，只知道發信者在網站上留下的稽核紀錄（log）等部分資訊，可提供的資訊有限，難以看出可識別個人的資訊。但經由 log 分析也可能得知發信者 IP 位址等資訊，進行推斷發信者係經由哪個通信事業者連線到佈告欄網站留言。此類業者基於商業目的（如：費用索取），會較網站管理者保有更多發信者正確的姓名、地址等資訊，且亦屬上述侵害資訊流通時之部分通信媒介，因此於第二階段，再向相關連線服務提供者請求揭露發信者資訊[102]。亦即第一階段先向網路平臺提供者（IPP）提出揭露請求，第二階段再向網路接取提供者（IAP）提出揭露請求，方可取得可供識別之發信者資訊。本研究目的雖非在協助主張被害者順利取得發信者資訊，以進行相關損害賠償訴訟，與日本 ISP 責任限制法有異，但研究對象既為「網路平臺提供者」，在要求紀錄保存時亦可能遭遇同樣問題，例如：「匿名」電子佈告欄之服務提供者，既未要求發信者「具名」，自然不會保有姓名、帳號、住所、聯絡方式、電子郵件等註冊資訊，僅能就發送訊息之日期、時間、內容、連線來源 IP 等紀錄加以保存，故偵查機關若為犯罪偵查需要，要求網路平臺提供者保存紀錄，紀錄項目亦將受限於其業務上、技術上所能提供之資訊，欲深入追查犯罪嫌疑人身分，最終仍有賴網路接取提供者（IAP）配合提供。至於網路平臺提供者保存相關紀錄後，偵查機關尚可能面臨發信者透過代理伺服器連線、連線伺服器在國外…等無法據以追查 IP 使用者等問題，則不在本研究討論範圍內。

在資訊保存方面，日本雖對於發信者可揭露之資訊項目有明白規範，但

[102] 參閱日本ベルマン法務事務所網站 http://www.cyber-eraser.jp/，TOP＼IP 開示請求項下，標題「発信者情報開示の現行法の問題点 日本弁護士連合会 壇俊光 先生 」。上網日期：2012 年 5 月 24 日。

並沒有賦予特定電信服務提供者保存發信者資訊之義務，從適當管理個人資訊的觀點來看，更要求特定電信服務提供者於沒有保存之必要時，應儘速刪除發信者個人資訊，相關保存期間及電信事業者提供發信者個人資訊予第三人之規定，詳見於總務省「電気通信事業における個人情報保護に関するガイドライン」（電信事業對個人資訊保護準則）中。

（四）電信事業者對個人資訊保護準則（電気通信事業における個人情報に関するガイドライン）

關於個人資訊保存期間之規範，本準則第 10 條前段即載明電信事業者處理個人資訊時，以於使用目的必要範圍內訂定保存期間為原則，例如：通信歷程紀錄之保存期間，可依提供服務的種類、收費方式、通信歷程的項目等，由各家電信事業者自行設定。另同條後段規定，該保存期間經過後或該使用目的達成後，應立即刪除該個人資訊。目前，日本特定電信服務提供者對於通信 log 保存期間，大多為三個月（也有公司是保存一個月以內）[103]，所以，若因民事案件須向特定電信服務提供者請求揭露 IP 等資訊時，也只得儘可能在三個月內迅速進行請求揭露之程序，以保障自身權益。

但原則中也有例外，在日本「電信事業對個人資訊保護準則」第 10 條第 2 項即規定資訊保存期間之例外情形，包括：（一）基於法令規定應予保存者。（二）經本人同意者。（三）電信事業者為遂行業務，於必要限度內認為有保存個人資訊之需要，有相當理由不予刪除者，例如：過去曾滯納費用而停權之用戶資訊，認為仍有必要保存至契約解除後。（四）有特別理由不予刪除者，如：特定個人資訊變成刑事案件之證據，經偵查機關請求先予保存之情形等。電信事業者如果認為有符合前述四種情形之一，即可於保存期間經過後或使用目的達成後，仍保存該個人資料不予刪除。

此外，基於個人資訊保護，該準則第 15 條在將個人資訊提供予第三人方面亦有明確之規範限制，非事先經本人同意，電信事業者不得提供個人資

[103] 參閱日本ベルマン法務事務所網站 http://www.cyber-eraser.jp/，於 TOP＼IP 開示請求項下，標題「発信者情報開示の現行法の問題点 日本弁護士連合会 壇俊光先生」，上網日期：2012 年 5 月 24 日。

訊予第三人，但下列四種情形除外：（一）基於法令者。（二）為保護個人生命、身體或財產之必要，且取得本人同意有困難者。（三）為提升公共衛生或促進兒童健全發展，有特殊必要，且取得本人同意有困難者。（四）國家機關、地方公共團體或其他受委託者，對於遂行法令規定事務有協助必要，且取得本人同意有妨礙該事務遂行之虞者。例如：依法官核發令狀執行搜索、扣押等強制處分之情形、法律上具有詢問權限之詢問情形[104]…等均屬之，可不事先經本人同意而提供相關個人資訊予第三人。又電信事業者雖可因應當事人請求停止提供可識別之個人資訊予第三人，但如將第三人之使用目的、提供資訊項目及提供方法等事項事先通知本人或使本人處於容易知悉之情況下，仍可提供該個人資訊予第三人[105]。但有關通信秘密之保護，通信事業者仍應遵守電氣通信事業法第 4 條之規定，對於業務處理而取得之通信內容不得侵害，且不論在職中或離職後均應保守他人通信之秘密。

電信事業者因業務用途而取得之資訊，除發信者資訊外，尚有通信歷程、使用明細、欠款資訊…等。其中，通信歷程是通信的構成要件，亦是本研究探討之重點。通信歷程受電信事業法第 4 條第 1 項通信秘密的保護，因此，記錄通信歷程亦可說是對通信秘密的侵害，依準則第 23 條第 1 項規定，電信事業者得記錄之通信歷程（指使用者使用電信的日期、時間，該通信對方使用者之通信內容以外之相關通信資訊），以罰款、通信費用請求、申訴處理、防止不當利用及其他業務遂行必要情形者為限。亦即，電信事業者基於業務用途須作成使用明細，據以請求費用，會記錄通信歷程並加以保存，這是身為債權人的電信事業者的權利，即使用戶不同意，電信事業者仍可在必要的限度內記錄並保存通信歷程，此種正當業務行為是被允許的。但若是為了追蹤、識別發信者而分析通信歷程，則屬業務遂行目的外之運用，牽涉到通信秘密之侵害，因此必須具備阻卻違法事由，否則不得對外提供。同條

[104] 日本刑事訴訟法第 197 條第 2 項規定：「關於偵查，得詢問公務機關或公私團體，要求其提出必要事項之報告。」即屬之。

[105] 一般而言，電信事業者提供用戶的個人資訊給第三人的情形，通常在契約條款中均會敘明，用戶等於在簽約的同時業已同意，但還是認為通知本人並取得同意是較符合期望的。參閱「電気通信事業における個人情報保護に関するガイドラインの解説」（平成 16 年總務省告示第 695 號，最終改正平成 23 年總務省告示第 465 號），頁 24。

第 2 項即規定，除經使用者同意、依法官核發令狀、符合正當防衛或緊急避難等阻卻違法事由等三種情形外，不得將通信歷程提供給他人。例如：因應法律上有詢問權限者之詢問而提供通信歷程，未必提供行為之阻卻違法性，因此原則上應認為此提供行為不適當。又如：當自家公司遭受大量宣傳廣告郵件攻擊、癱瘓電腦系統，使公司網路服務受到威脅時，基於正當防衛自己或他人權利，即可允許將相關通信歷程（發信者的 IP 位址及時間戳記）提供給發信來源的所屬電信事業者[106]，不受紀錄提供之限制。

由此觀之，日本已然將通信歷程納入個人資料保護的範疇之內，並規範了將通信歷程提供給他人之要件。然而，「通信歷程」與「姓名、地址」等資訊，應置於同一標準上考量嗎？又應受到同樣程度之保護嗎？我國於 2010 年 5 月 26 日修正通過之「個人資料保護法」[107]，對姓名、地址等個人資料之適用自無疑義，惟通信歷程係指通信來源 IP、目的 IP、日期、時間及其他通信內容以外之相關通信資訊（即一般所稱之 log），依該法第 2 條第 1 項第 1 款之定義，個人資料係指「自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料」，則「通信歷程」之適用與否不免產生爭議。

所謂 IP 位址（Internet Protocol Address）係一種主機編址的方式，網際網路在傳送資料時皆係透過 IP 位址進行辨識，將資料傳送到目的位址以完成通訊。任何一台電腦要連線到網際網路均會有一組獨立且不重複的 IP 位址；又 IP 位址區分為浮動式及固定式兩種，一般個人上網大多係由 ISP 業者分配一個臨時的浮動式 IP，需透過 ISP 業者查詢比對其配發紀錄與用戶資料，方能識別該用戶為何人。關於通信歷程是否屬個人資料，各國看法不一，例如歐盟、瑞典、瑞士等國採肯定說；德國、愛爾蘭、法國等國採否定說；

---

[106] 參閱「電気通信事業における個人情報保護に関するガイドラインの解説」，頁 39。

[107] 原「電腦處理個人資料保護法」，新法修正公布之全文施行日期，由行政院定之，但現行條文第 19～22、43 條之刪除，自公布日施行。

香港、英國則採折衷說。國內某學者亦較支持否定說或折衷說，理由如下：依新法中「得以直接或間接方式識別該個人之資料」之定義，IP 位址本身為一組數字，一般人無法「直接」識別出特定個人；再者，所謂「間接」依個人資料保護法施行細則修正草案第 3 條之規定，係指僅以該資料不能識別，須與其他資料對照、組合、連結等，始能識別該特定個人者。但查詢困難、需耗費過鉅或耗時過久始能識別該特定個人者，不在此限。IP 位址雖可透過 ISP 業者之查詢比對而得知特定用戶資料，以「間接」識別出特定個人，但對一般民眾而言，仍屬無法識別之個人資料，又 ISP 業者查詢得知之特定用戶資料亦非必定等同於電腦前之實際操作者，綜上，IP 位址無論直接或間接均無法識別出特定個人，應非屬個人資料之一種[108]，其他通信歷程如日期、時間…等紀錄，自亦排除於個人資料保護之範疇外。因此，本研究在探討網路平臺提供者之紀錄保存規範時，針對各保存紀錄之項目於個人資料保護法之適用與否、紀錄查詢是否須經過「令狀主義」之檢驗，實有討論之空間。

（五）犯罪偵查之通信監察法（犯罪捜査のための通信傍受に関する法律[109]）

本法之制定，乃日本政府鑒於組織犯罪嚴重危害社會安定，對於數人共謀實施組織殺人、非法買賣藥品及槍枝等重大犯罪，如不對犯人間之聯絡電話及其他通信實施監聽，查明案件真相顯有困難之情形將逐漸增加，因此，乃增訂刑事訴訟法第 222 條之 2[110]作為通信監察強制處分之依據，並於平成 11（1999）年 8 月 18 日通過第 137 號之「犯罪偵查之通信監察法」，經平成 11 年 12 月以第 160 號法律案修正後，於平成 12（2000）年 8 月 15 日開始實施。條文中明確規範通訊監察之要件、程序及其他必要事項，以期在犯罪偵查之同時，不會對當事人造成通信秘密之不當侵害。

相關名詞之定義規定於本法第 2 條，所謂「通信」係指其傳送途徑的全

---

[108] 張靜婕，凡走過必留下 IP，淺談 IP 位址是否係屬個資法之個人資料，2011 年 12 月 19 日發表，參閱達文西個資暨高科技法律事務所網站 http://www.davinci.idv.tw/。

[109] 最終改正：平成23年6月24日法律第74号。
日文「傍受」為監聽之意，本文參考我國通訊保障及監察法，將其譯為「監察」。

[110] 日本刑事訴訟法第二百二十二条の二：「通信の当事者のいずれの同意も得ないで電気通信の傍受を行う強制の処分については、別に法律で定めるところによる。」

部或一部分為有線（以有線以外方式，傳送電波或其他電磁波，或用於接收而附屬之有線設備除外），或於傳送途徑裝設有交換設備之電話及其他電信。因此，不僅電話，其他如傳真、電腦之通信等均可為本法監聽之對象，惟成為監聽對象之電話、電子郵件等，在令狀上應載明特定之電話號碼或電子郵件地址等，方允許實施監聽[111]。所謂「監聽」係指為探知他人正在進行之通信內容，未經該通信當事人任何一方之同意，而予以接收之行為。因此，有國內研究以為，日本監聽通信之對象並不包括「通信紀錄」與「已儲存的電子郵件」，因為二者已非「正在進行之通信」，已然屬搜索扣押之範疇，在案件尚未釐清之偵查階段即施以搜索扣押，有違程序正義，故不涵括於監聽通信之對象中[112]。所謂「通信事業者等」係指使用電信之設備（以下稱『電信設備』）媒介他人通信、提供電信設備以為他人通信之用之事業經營者，及其他基於自身業務需要，而設置電信設備以媒介不特定或多數人通信者。

在我國，關於網路通信之監察是否一體適用於「通訊保障及監察法」之疑義，本研究採肯定之立場。雖然，網路與傳統電話通信在傳輸方式上有顯著差異：傳統電話資料交換之方式係採電路交換（Circuit Switch）系統，於發話端與受話端通話時，會建立一條專屬線路供雙方使用，頻寬不與他人共享；而網際網路則採封包交換（Packet Switch）系統，網路提供通信之平台供大家共用，不專屬任一使用者，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，實施網路監聽時，可能會截收到監察對象以外之人的通訊[113]。但網路既符合我國電信法第 2 條「電信」之定義[114]，

---

[111] 參閱日本法務省網站：http://www.moj.go.jp/，トップページ＼法務省の概要＼各組織の説明＼内部部局＼刑事局＼過去の国会提出法律案（平成 10 年 3 月から平成 18 年 2 月までに提出されたもの）項下之刊載，標題「犯罪捜査のための通信傍受に関する法律案 Q&A」Q6，上網日期：2012 年 6 月 2 日。

[112]許慈健，網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究，國立交通大學管理學院在職專班碩士論文，2005。

[113] 陳信郎，資訊隱私權保障與網路犯罪通訊監察法制，國立政治大學法律學研究所碩士論文，2004 年 8 月，頁 106。

[114] 我國電信法第 2 條第 1 項第 1 款：「電信：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。」又同項第 2 款：「電信設備：指電信所用之機械、器具、線路及其他相關設備」，故網路通訊設備亦屬電信設備。

則通訊保障及監察法第 3 條所稱通訊－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－自當包含網路在內，故網路通訊在我國「通訊保障及監察法」之適用上，應無疑義。

有關日本通信監察之要件，規定於本法第 3 條中，該條第 1 項即載明檢察官及司法警察於犯罪偵查時，認為犯罪嫌疑人之通信內容與該犯罪之實行、準備或湮滅證據等事後措施相關之策劃、指示及犯行相互聯絡有關，且以其他方法查明犯罪嫌疑人或犯罪事實顯有困難時，方得向法官聲請核發通信監察令狀。而犯罪行為亦限縮於藥物、偷渡、槍砲、組織殺人等重大犯罪[115]，或同條第 1 項第 3 款為準備前述犯罪而犯之死刑、無期徒刑、2 年以上有期徒刑或監禁之罪，並以超過 2 人之數人共謀一罪為要件，以上該當犯罪嫌疑之要件，可謂明確地限縮了通信監察可運用之範圍。

---

[115] 該法附表所列得實施通信監察之犯罪如下：

一、大麻管理法（昭和23年第124號法律）第24條（栽培、輸入等）或第24條之2（持有、轉讓等）之罪。

二、興奮劑管理法（昭和26年第252號法律）第41條（輸入等）或第41條之2（持有、轉讓等）之罪，同法第41條之3第1項第3款（輸入興奮劑原料等）或第4款（製造興奮劑原料）之罪或與該等犯罪相關之同條第2項（以營利為目的輸入興奮劑原料等）之罪或未遂之罪，或同法第41條之4第1項第3款（持有興奮劑原料）或第4款（轉讓興奮劑原料等）之罪或與該等犯罪相關之同條第2項（以營利為目的持有、轉讓興奮劑原料等）之罪或未遂之罪。

三、出入境管理及難民認定法（昭和26年第319號政令）第74條（使集體偷渡者非法入境之行為等）、第74條之2（運送集體偷渡者）或第74條之4（收容集體偷渡者等）之罪。

四、麻醉藥品及精神藥品管理法（昭和28年第14號法律）第64條（輸入海洛因等）、第64條之2（轉讓、持有海洛因等）、第65條（輸入海洛因等以外之麻醉藥品等）、第66條（轉讓、持有海洛因等以外之麻醉藥品等）、第66條之3（輸入精神藥品等）或第66條之4（轉讓精神藥品等）之罪。

五、武器等製造法（昭和28年第145號法律）第31條（未經許可製造槍砲）、第31條之2（未經許可製造彈藥）或第31條之3第1款（未經許可製造槍砲及彈藥以外之武器）之罪。

六、鴉片法（昭和29年第71號法律）第51條（種植罌粟、輸入鴉片等）或第52條（轉讓、持有鴉片等）之罪。

七、持有槍砲、刀械管理法（昭和33 年第6號法律）第31條至第31條之4（發射、輸入、持有、轉讓手槍等）、第31條之7至第31條之9（輸入、持有、轉讓手槍子彈等）、第31條之11第1項第2款（輸入手槍零件）或第2項（未遂罪）或第31條之16第1項第2款（持有手槍零件）或第3款（轉讓手槍零件等）或第2 項（未遂罪）之罪。

八、關於國際合作下防止助長限制藥物之不當行為之麻醉藥品及精神藥品管理法等特例法律（平成3年第94號法律）第5條（以非法輸入為職業等）之罪。

九、處罰組織犯罪及規定犯罪收益法律（平成11年第136號法律）第3條第1項第7款所列之罪相關之同條（組織殺人等）之罪或其未遂之罪。

此外，依本法第 3 條第 1 項後段之規定，須針對犯罪嫌疑人基於與通信事業者之契約而使用之電話號碼、其他識別發信來源與目的之號碼符號等特定通信方式，或足以懷疑用於犯罪關聯通信之特定通信方式，始得實施通信監察，但與犯罪無關之通信除外。實施通信監察的範圍與內容必須與該偵辦之犯罪有關，偵辦機關在聲請通信監察時，必須表明對犯罪嫌疑人實施通信監察之將來某一特定時點，足以懷疑存在有該犯罪之相關資訊，例如犯罪嫌疑人事前約定會在將來某特定時點進行該犯罪之相關通信，且該約定至今並無變更之情事發生等證據。且偵查單位必須有充分理由表示該通信設備為此犯罪嫌疑人用於該犯罪之聯絡，方可對其施以通信監察，若為第三人傳送給嫌疑人之電子郵件或傳真，即不包括在內[116]。

值得注意的是，在確定犯罪嫌疑人與該偵查中之犯罪行為相關聯，准予核發通信監察令狀後，日本通信監察法另有對通信監察之內容判斷是否符合令狀上所載明「應監察通信」之規定，依本法第 13 條，檢察官或司法警察對於其通信內容是否該當應監察通信不明顯時，得於必要之最小限度範圍內先施予監聽[117]，以決定是否繼續對其實施監察。但特殊情形如：使用外語通信、暗號及其他內容無法即時復原之方式所為之通信，檢警人員為了能了解該通信內容，即可實施全部監聽，以迅速判斷該通信內容是否與該犯罪有關。

在通信監察令狀之聲請與核發方面，依本法第 4 條規定，得聲請通信監察令狀之主體，限於檢察總長指定之檢察官，或由國家公安委員會、都道府縣公安委員會指定之警視以上警察官、厚生勞動大臣指定之麻藥取締官及海上保安廳長官指定之海上保安官為限。法官受理該監聽聲請，如認為有理由時，得核發通信監察令狀，並定以 10 日內之通訊監察期間，必要時，得於 10 日期間內延長之，但通信監察總日數不可超過 30 日；且法官核發通訊監察令狀時，得就通訊監察之實施，附加適當條件。相較於美國、英國、德國、

---

[116] 呂寧莉，日本通信監察之實施要件及實施現況，檢察新論，第 5 期，2009 年 1 月，頁 300。

[117] 此最小程度監聽之實施方式為「點監聽」（spot monitoring），該機器可預先設定段點監聽的間隔時間，時間一到機器就會自動切斷電源，過一段時間機器會再度啟動，如此進行反覆、短時間之監聽。參閱呂寧莉，日本通信監察之實施要件及實施現況，檢察新論，第 5 期，2009 年 1 月，頁 301。

法國、加拿大、義大利等先進國家之通信監察相關法律，日本在核發通信監察令狀上，係以有「充分理由」為要件，不論在犯罪種類之限定、犯罪之嫌疑等逮捕要件、監聽期間及延長規定…等，均較其他國家更為嚴格[118]，以避免公權力濫用，使憲法保障之秘密通信權形同空殼。

本法第 11 條規定了通信事業者之協助義務，偵查人員於實施監聽時，得要求通信事業者協助裝設相關之監聽設備，或提供其他必要之協助，通信事業者除非有正當理由，否則不得拒絕。此乃因通信監聽工作係在令狀上記載之監聽場所實施，通常為日本電信電話株式會社（Nippon Telegraph and Telephone Corporation, NTT）等通信事業者的設備，而相關設備的操作及技術，若無業者內部技術人員從旁協助，偵查人員要順利執行監聽工作恐有困難。此外，偵查機關執行通信監聽，目的在打擊不法、端正社會風氣，通信事業者若無正當理由，不得拒絕之。

日本為防止執法機關濫權、違法監聽，於本法第 29 條明訂相關報告與公布規定，希望能藉此減輕民眾之疑慮。該條載明政府每年應就偵查機關偵辦通信監察案件之相關內容，向國會提出報告並公布之，內容包括：監聽令狀之聲請及核發件數、罪名、監聽對象通信方式之種類、監聽期間、監聽通話次數與該等案件逮捕人數…等。但罪名公開有礙偵查之進行時，可俟障礙原因消滅後，再行公布。此一規定，讓國會代替全民有效監督政府行動，使偵查機關在執行通信監察上，能更為審慎、嚴謹，又能無礙於打擊犯罪之任務遂行，值得我國參考。

二、中國大陸

近年來，網際網路帶來許多商機，對中國經濟發展有正面幫助，然而，網際網路普及造成信息得以快速流通，使得政府控制輿論的工作出現一個缺口。中國官方和學者擔心境內外敵對團體可能利用網際網路散布批評當局的言論，進而危及國家安全與政局隱定[119]。因此，近年來開始加強對網路活動

[118] 例如：美國聯邦法之通信監察規定，初次監聽期間為 30 日內，得於 30 日內期間延長之，且延長次數不限。日本之規定明顯嚴格許多。

[119] 寇健文，中共對網路資訊傳播的政治控制，問題與研究，第 40 卷第 2 期，2001 年 3、4

的控制，自 1995 年起，頒布了一連串與網際網路訊息傳播有關之法規及行政命令，從上網傳播的信息內容、電子出版物、國際聯網的安全與管理、登載新聞業務的管理等方面來管制網路訊息的傳播。「互聯網電子公告服務管理規定」第 9 條列出了 9 種不得在電子公告服務系統中發佈之信息：

（一）反對憲法所確定的基本原則者；

（二）危害國家安全，洩露國家秘密，顛覆國家政權，破壞國家統一者；

（三）損害國家榮譽和利益者；

（四）煽動民族仇恨、民族歧視，破壞民族團結者；

（五）破壞國家宗教政策，宣揚邪教和封建迷信者；

（六）散佈謠言，擾亂社會秩序，破壞社會穩定者；

（七）散佈淫穢、色情、賭博、暴力、兇殺、恐怖或者教唆犯罪者；

（八）侮辱或者誹謗他人，侵害他人合法權益者；

（九）含有法律、行政法規禁止的其他內容者；

上述禁止發佈之內容在「互聯網信息服務管理辦法」第 15 條、「計算機信息網絡國際聯網安全保護管理辦法」第 5 條、「互聯網新聞信息服務管理規定」第 19 條、「互聯網站從事登載新聞業務管理暫行規定」第 13 條均有類似規定，政治性考量因素即佔有半數以上，顯示中國政府有心掌控網友所能接觸之網路信息內容，以確保輿論主控權、穩定政權。

若發現被禁止上網的信息或是國家機密，中國要求所有網路服務提供者和上網用戶必須妥善處理－停止傳輸或刪除違法信息，防止這些信息擴散、保存相關紀錄、主動報告主管機關部門、配合有關單位查緝違法犯罪行為[120]。

（一）互聯網電子公告服務管理規定[121]

信息產業部於 2000 年 10 月 8 日發布本項規定。所謂「電子公告服務」依第 2 條第 2 項「指在互聯網上以電子佈告欄、電子白板、電子論壇、網路

月，頁 40。

[120] 寇健文，中共對網路資訊傳播的政治控制，問題與研究，第 40 卷第 2 期，2001 年 3、4 月，頁 46。

[121] 參閱中華人民共和國工業和信息化部網站 http://www.miit.gov.cn/n11293472/index.html，政策法規司項下，標題「互联网电子公告服务管理规定」，上網日期：2012 年 10 月 1 日。

聊天室、留言板等交互形式，為上網用戶提供信息發佈條件的行為」。適用對象為中華人民共和國境內開展電子公告服務和利用電子公告發佈信息者。凡從事互聯網信息服務，擬開展電子公告服務者，應依本規定向相關單位專案申請或專項備案。另外，為方便中國官方追蹤違法上網行為，更明訂電子公告服務提供者紀錄保存之相關規定如下：第 13 條規定「電子公告服務提供者發現其電子公告服務系統中出現明顯屬於本辦法第 9 條所列的信息內容之一者，應當立即刪除，保存有關紀錄，並向國家有關機關報告」。第 14 條「電子公告服務提供者應當記錄在電子公告服務系統中發佈的信息內容及其發佈時間、互聯網地址或者域名。記錄備份應當保存 60 日，並在國家有關機關依法查詢時，予以提供」，此項規定給予電子公告服務提供者義務，對於系統中之某些特定項目紀錄（包括信息內容），無論發生違法情形與否均應事先保存 60 日，以供國家有關機關查詢。此外，第 15 條規定「互聯網接入服務提供者應當記錄上網用戶的上網時間、用戶帳號、互聯網地址或者域名、主叫電話號碼等信息，記錄備份應保存 60 日，並在國家有關機關依法查詢時，予以提供。」此規定係在規範「接入服務提供者」對於上網用戶之上網基本資料予以保存 60 日，以供國家有關機關查詢。上述第 13、14、15 條規定之義務未能履行者，依「互聯網信息服務管理辦法」第 21 條及第 23 條之規定處罰。

（二）互聯網信息服務管理辦法[122]

中國互聯網絡信息中心於 2000 年 9 月 25 日發佈本辦法。第 2 條第 2 項定義「互聯網信息服務」係指「通過互聯網向上網用戶提供信息的服務活動」，分為經營性及非經營性兩類：「經營性互聯網信息服務」指通過互聯網向上網用戶有償提供信息或網頁製作等服務活動；而「非經營性互聯網信息服務」係指通過互聯網向上網用戶無償提供具有公開性、共享性信息之服務活動」。本辦法網路信息保存規範訂於第 14 條「從事新聞、出版以及電子公

[122] 參閱「中國互聯網絡訊息中心」網站，http://www.cnnic.net.cn/首頁／國家域名安全中心／政策法規項下，標題「互联网信息服务管理办法》（国务院令第 292 号）」，上網日期：2012 年 10 月 1 日。

告等服務項目的互聯網信息服務提供者，應當記錄提供之信息內容及其發布時間、互聯網地址或者域名；互聯網接入服務提供者應紀錄上網用戶之上網時間、用戶帳號、互聯網地址或者域名、主叫電話號碼等信息」；同條第 2 項「互聯網信息服務提供者和互聯網接入服務提供者之紀錄備份應保存 60 日，並在國家有關機關依法查詢時，予以提供」。明白指出應保存信息紀錄（含信息內容）者為從事新聞、出版以及電子公告等服務項目之互聯網信息服務提供者，以及互聯網接入服務提供者；且保存期間為 60 日，於國家有關機關依法查詢時應予提供，但未規定以違法信息為保存之前提要件。第 16 條亦有規定「互聯網信息服務提供者發現其網站傳輸之信息明顯屬於本辦法第 15 條所列內容之一者，應立即停止傳輸，保存有關紀錄，並向國家有關機關報告」，亦即，不論經營性或非經營性之互聯網信息服務提供者，於其網站內發現有反對憲法所確定之基本原則者；危害國家安全，洩露國家秘密，顛覆國家政權，破壞國家統一者；損害國家榮譽和利益者；煽動民族仇恨、民族歧視，破壞民族團結者；破壞國家宗教政策，宣揚邪教和封建迷信者；散布謠言，擾亂社會秩序，破壞社會穩定者；散布淫穢、色情、賭博、暴力、兇殺、恐怖或教唆犯罪者；侮辱或誹謗他人，侵害他人合法權益者；有法律、行政法規禁止的其他內容者…等 9 大項信息之一者，即有保存有關紀錄之義務，然本條規定係在互聯網信息服務提供者發生違法信息後，始啟動保存之動作，與本辦法第 14 條非以違法信息為前提之紀錄保存規範有別。

此外，本辦法第 21 條及第 22 條訂有未履行義務之罰則，第 21 條規定「未履行本辦法第 14 條規定之義務者，由省、自治區、直轄市電信管理機構責令改正；情節嚴重者，責令停業整頓或暫時關閉網站」。第 23 條規定「違反本辦法第 16 條規定之義務者，由省、自治區、直轄市電信管理機構責令改正；情節嚴重者，對經營性互聯網信息服務提供者，由發證機關吊銷經營許可證，對非經營性互聯網信息服務提供者，由備案機關責令關閉網站」。違反「互聯網電子公告服務管理規定」第 13 條、第 14 條及第 15 條者，亦依本辦法上述兩項罰則規定處罰。

（三）計算機信息網絡國際聯網安全保護管理辦法[123]

公安部於 1997 年 12 月 30 日發布實施，並由公安部計算機管理監察機構負責計算機信息網絡國際聯網的安全保護管理工作。其服務提供者之協助義務於第 8 條規定，從事國際聯網業務之單位和個人應接受公安機關之安全監督、檢查和指導，如實向公安機關提供有關安全保護之信息、資料及數據文件，協助公安機關查處通過國際聯網之計算機信息網絡的違法犯罪行為。以及第 10 條規定互聯單位、接入單位及使用計算機信息網絡國際聯網的法人和其他組織應當履行七項安全保護職責，包括：負責本網絡之安全保護管理工作，建立健全安全保護管理制度；落實安全保護技術措施，保障本網絡之運行安全和信息安全；負責對本網絡用戶之安全教育和培訓；對委託發布信息的單位和個人進行登記，並對所提供的信息內容按照本辦法第 5 條進行審核；建立計算機信息網絡電子公告系統之用戶登記和信息管理制度；發現有本辦法第 4 條、第 5 條、第 6 條、第 7 條所列情形之一者，應當保留有關原始紀錄，並在 24 小時內向當地公安機關報告；按照國家有關規定，刪除本網絡中含有本辦法第 5 條內容的地址、目錄或者關閉服務器。保留有關原始紀錄即為安全保護職責其中一項，於發現有本辦法第 4 條、第 5 條、第 6 條、第 7 條所列情形之一時，互聯單位、接入單位及使用計算機信息網絡國際聯網的法人和其他組織即發動保留紀錄之義務，主動向公安機關報告，以協助查處國際聯網之違法犯罪行為，維護公共秩序及社會安定。

（四）中華人民共和國計算機信息網絡國際聯網管理暫行規定實施辦法[124]

中國大陸為防止境外網路信息無限制的進入境內，影響輿論、有礙政權穩定，由國務院信息化工作領導小組於 1998 年 2 月 13 日發佈本辦法，嚴格規定中國本地與境外網站的聯結活動。本辦法第 7 條即規定「我國境內的計

123 參閱中華人民共和國公安部網站 http://www.mps.gov.cn/n16/index.html，首頁 ／信息公開／法律法規／ 公安部令／信息網络安全管理項下，標題「计算机信息网络国际联网安全保护管理办法（公安部令第 33 号）」，上網日期：2012 年 10 月 1 日。

124 參閱中國百科網網站 http://www.chinabaike.com/，中央法規／部委規章及文件／協調和臨時機構項下，標題「中华人民共和国计算机信息网络国际联网管理暂行规定实施办法」，上網日期：2012 年 9 月 5 日。

算機信息網絡直接進行國際聯網，必須使用郵電部國家公用電信網提供的國際出入口信道」。第 12 條亦有「個人、法人和其他組織用戶使用的計算機或者計算機信息網絡必須通過接入網絡進行國際聯網，不得以其他方式進行國際聯網」之規定，以有效掌握境內與境外網站間之信息流通。在本辦法第 19 條第 1 項亦訂有信息保存之規定「國際出入口信道提供單位、互聯單位和接入單位應當保存與其服務相關的所有信息資料；在國務院信息化工作領導小組辦公室和有關主管部門進行檢查時，應當及時提供有關信息資料」。因此，國際間之相關網路信息流通之資料，國際出入口信道提供單位、互聯單位和接入單位等 3 個單位，均有保存、提供之義務。

（五）互聯網新聞信息服務管理規定[125]

2005 年 9 月 25 日，國務院新聞辦公室、信息產業部聯合發布本項規定，目的在於規範互聯網新聞信息服務，滿足公眾對互聯網新聞信息之需求，維護國家安全與公共利益，保護互聯網新聞信息服務單位之合法權益，促進互聯網新聞信息服務健康、有序發展。所謂「互聯網新聞信息服務」於第 2 條第 3 項明訂「包含通過互聯網登載新聞信息、提供時政類電子公告服務和向公眾發送時政類通訊信息」。並將互聯網新聞信息服務單位分為以下三類：

1、新聞單位設立的登載超出本單位已刊登播發的新聞信息、提供時政類電子公告服務、向公眾發送時政類通訊信息的互聯網新聞信息服務單位；

2、非新聞單位設立的轉載新聞信息、提供時政類電子公告服務、向公眾發送時政類通訊信息的互聯網新聞信息服務單位；

3、新聞單位設立的登載本單位已刊登播發的新聞信息的互聯網新聞信息服務單位。在互聯網相關紀錄保存方面，第 20 條規定「互聯網新聞信息服務單位應建立新聞信息內容管理責任制度。不得登載、發送含有違反本規定第 3 條第 1 項、第 19 條規定內容之新聞信息；發現提供之時政類電子公告服務中含有違反本規定第 3 條第 1 項、第 19 條規定內容者，應立即刪除，保存有關紀錄，並於有關部門依法查詢時予以提供」。並

[125] 參閱中國互聯網絡信息中心網站 http://www1.cnnic.cn/，首頁／政策法規／2005 年／正文項下，標題「互聯網新聞信息服務管理規定」，上網日期：2012 年 10 月 1 日。

於第 21 條規定「互聯網新聞信息服務單位應記錄所登載、發送之新聞信息內容及其時間、互聯網地址，記錄備份應至少保存 60 日，並於有關部門依法查詢時予以提供」。亦即，前述三類互聯網新聞信息服務單位，於發現所提供之時政類電子公告服務中含有違法信息內容後，應立即保存相關紀錄，並依法提供有關部門查詢之用；再者，對其所登載、發送之信息內容、時間、網址，不論含有違法信息與否，均應保存至少 60 日以備有關部門查詢時提供之。對於保存紀錄之單位、項目、期間、要件均有明確規範。

此外，本規定第 23 條亦有針對國務院新聞辦公室和省、自治區、直轄市人民政府新聞辦公室作出規範，在對互聯網新聞信息服務進行監督時，發現登載、發送之新聞信息或提供之時政類電子公告服務中含有違反第 3 條第 1 項、第 19 條規定內容者，應通知互聯網新聞信息服務單位立即刪除、保存有關紀錄，並於有關部門依法查詢時予以提供。

三、新加坡

（一）現狀概述

新加坡政府於 2005 年提出智慧國度（An Intelligent Nation 2015, iN 2015）的願景，主管機關資訊通信發展管理局（Info-Communications Development Authority of Singapore，IDA）為吸引外資參與新加坡資通訊市場，制定了自由及公平競爭規則，期望透過良性的市場競爭，能確保新加坡消費者權益，也期望透過這種合作模式，讓新加坡資通訊產業與國際市場接軌。同時，資訊通信發展管理局也正積極打造新世代國家資通訊基礎建設（Next Generation National Infocomm Infrastructure），率先採用眾多新技術的計畫並繼續提升資訊通信基礎設施，至 2015 年新加坡將擁有世界最完善的寬頻網路，並能提供 1Gbps 甚至更高速的網路連線。

根據新加坡資訊通信發展管理局統計，2009 年資訊通信產業總營收超過 627 億星元（499 億美元），較 2008 年增長 8.0%，其中 36%的收入來自國內市場，64%來自出口業務。通信產業年產值占整體營收 14%，約為 88 億星元（70 億美元），較 2009 年的 87 億星元有微幅成長。截至 2010 年 12 月，

新加坡的固定電話家庭覆蓋率達 102.9%，行動電話覆蓋率為 143.6%，家庭寬頻覆蓋率為 190.8%。

此外，根據 BMI （Business Monitor International）的統計調查顯示，新加坡資訊通信市場的發展在亞太區域高居第二名（僅次日本），行動通訊覆蓋率在 2011 年超過 150%，其中，新加坡最大電信業者 SingTel 仍穩居市場龍頭，市占率為 44.3%，儘管面對其他兩大本土同業，包括 Starhub 及 M1 的挑戰，仍擁有高達 59%的網路覆蓋率[126]。

（二）網際網路管理

新加坡政府投入鉅資建立科技基礎設施，為網路經濟與傳統經濟的融合創造有利的環境，新經濟的發展使新加坡國家競爭力更為提升，新加坡連續七年世界排名第二。鑒於網際網路的迅速發展，新加坡在 1994 年 10 月 1 日成立新加坡廣播管理局（The Singapore Broadcasting Authority，簡稱 SBA）負責管理，並於 1996 年 7 月 11 日宣布對網際網路實行管制。2003 年 1 月，新加坡廣播管理局、電影與出版物管理局（The Films and Publications Department）、新加坡電影委員會（Singapore Film Commission）三個機關合併為新加坡傳媒發展局（Media Development Authority，簡稱 MDA）。因此，目前傳媒發展局為新加坡網際網路的主管機關。

新加坡傳媒發展局的網際網路管理框架主要依據《廣播法（分類許可證）》（2001），依照這一制度，網際網路服務提供商（ISP）和網際網路內容提供商（ICP）只要在傳媒發展局登記，便被視為自動獲得經營執照。新加坡政府於 1996 年 7 月 15 日頒布“網際網路管理法規”，也稱為分類許可證制度（Class License Scheme），另“網際網路操作規則”（Internet Code of Practice）是分類許可證制度的補充，這二項法令都是為了鼓勵網路業者能負責任地使用網路媒體。該二項法律對於網路傳播內容方面的規定，形成了新加坡網路“自我調節式管理”的基礎，即新加坡傳媒發展局所稱的“平衡的、輕度的”管理，分別說明如下：

[126]經濟部投資業務處，新加坡投資環境簡介，經濟部投資業務處，2011。

1、對網路服務商的分類管理[127]

根據 2001 年 10 月 10 日修訂的《分類許可證制》的規定，網際網路服務提供商（ISP），必須在傳媒發展局登記。對其管理分為三類：網際網路接取服務提供商（Internet Access Service Provider，簡稱 IAP），定點網路服務轉售商（Localised Internet Service Reseller）、非定點網路服務轉售商（Non-localised Internet Service Reseller）[128]。網際網路接取服務提供商（IAP）是指新加坡三大接取服務提供商，即新加坡網（SingNet）、太平洋網（Pacific Internet）和星樞網（Starhub Internet）；定點網路服務轉售商具體指在網路咖啡屋、圖書館、社區服務中心和學校等地向公眾提供網際網路服務的服務提供商；非定點網路服務轉售商是指從網際網路接取服務商處獲得網際網路連接，然後轉售給公眾的網路服務者，如“新加坡網路服務”和“國家計算機系統”。

而網際網路內容提供商（ICP），無須專門註冊，但以下情況必須註冊：

（1）在新加坡註冊的政治團體通過網際網路以 WWW 方式提供網頁者。

（2）在 WWW 上參與有關新加坡的政治和宗教討論的用戶團體或新聞組。

（3）為政治目的或宗教目的而提供網頁的個人，以及由廣管局通知其註冊者。

（4）通過網際網路在新加坡銷售的報紙，由廣管局通知其註冊者。

傳媒發展局指出，註冊是為了加強和明確使用網路的責任，在不違反法律規定和不破壞社會和睦的前提下，政治和宗教團體可以自由討論。與一般的執照審批制不同，申請網路經營者依《分類許可制》自動發放執照，網站只要在傳媒發展局登記，便可直接獲得經營執照。登記後的網站自覺根據《網際網路操作規則》，自主判斷並管理其網頁內容。

2、網路提供商的責任與免責[129]

---

[127] Internet Regulatory Framework, http://www.mda.gov.sg/Policies/PoliciesandContentGuidelines/Internet/Pages/InternetRegulatoryFramework.aspx, Accessed Date: 09/01/2012.

[128] 陳曉寧主編，廣播電視新媒介政策法規研究：國外法規與評介研究（第 1 版），北京：中國法制出版社，2001，第 90-91 頁。

[129] Media Development Authority, Internet Code of Practice,

網際網路服務提供商和內容提供商之所以要求在傳媒發展局註冊登記，主要原因是要防止和及時地清除網上出現的有害信息。網際網路接取服務商（IAP）根據傳媒發展局提供的“黑名單”禁止用戶連接或屏蔽相關網站。網路服務商不僅要訂閱經過傳媒發展局審查同意的新聞組，而且要刪除包含有害信息的新聞組或文章。網際網路接取服務商必須在傳媒發展局同意的基礎上建立用戶守則，保存用戶訪問的有害信息的站點記錄。同時，網際網路接取服務提供商（IAP）有義務幫助傳媒發展局管理進入這些被禁止的網站。

而有關網路運營商之責任要求，規範於《分類許可證制度》概述部分第五條：傳媒發展局不可能隨時主動地監視網際網路，查處有害信息站點。因此要求信息服務提供者按廣管局的指示關閉有害站點。對於那些預定服務項目，如新聞組（newsgroup）服務，要求各 ISP 按照廣管局的內容指導原則對服務內容進行檢查。第六條：由於網際網路的站點數量眾多，並且變化很大，要想在網際網路接取服務商（IAP）這一層次上進行完全的控制是不可能的。廣管局鼓勵其他 ISP 在各自的網路內部進一步的控制，以對網際網路接取服務商（IAP）的控制進行補充。”（新加坡廣播管理局網際網路管理法規，1996）為了減輕網際網路服務和內容提供商的顧慮和負擔，《網際網路操作規則》規定了服務和內容提供商的免責條款[130]：

（1）如果網路接取服務提供商或轉售商在接到傳媒發展局的通知後，按要求關閉了含有“禁止內容”的網頁鏈接，即可免責。

（2）如果網路接取服務提供商或轉售商按照傳媒發展局的要求取消訂閱那些含有“禁止”內容的新聞組，即可免責。

（3）關於私人討論區與公共展示區

A、對基於網路服務而建立的私人討論區（如聊天室），只要保證不設定“禁止內容”範圍內的話題，即可免責。

---

http://www.mda.gov.sg/Licences/Pages/IntSCPCLicence.aspx, Accessed Date: 09/01/2012.

[130] Media Development Authority （MDA）, The Schedule: Internet Code of Practice.Broadcasting Act （Chapter 28, Section 3）.

B、對基於網路服務而建立的公共展示區（如 BBS 系統），只要在日常編輯、檢查的過程中關閉了含有“禁止內容”的鏈接，即可免責。

（4）網路內容提供商必須按照傳媒發展局的要求，關閉含有“禁止內容”的網頁。

（三）有關網路與電子商務的法規

關於網路對立法的影響，新加坡採取的策略是求取政府管制、行業自律和教育消費者三者的綜合平衡，既保障國家凝聚力和價值認同，又為網路和電子商務的發展留有足夠空間。立法是新加坡政府營造矽谷環境的重要前瞻政策。

資訊網路安全與電子交易規則是影響電子商務發展的根本問題，規則形成後需要法律保護，而制約資訊安全並不完全是靠技術，管理問題在某種程度上更重要，而強化管理則依靠法律，新加坡的方式正是依法管理、措施配套。新加坡除制訂了電子交易法、成立了電子證書認證中心外，還建立解決電子商務糾紛的初級法庭採用最新科技的電子法庭（e－Court）、交互法庭（i－Court）、和電子內堂（e－Chamber）解決電子糾紛。

就資訊通信、網路和電子商務而言，有關的主要法規、業務指南分述如下：

1、資訊安全方面

網路無國界，政府部門必須有安全可靠的電腦系統來防止駭客侵入政府系統，也有保安系統防止在傳送電子郵件重要檔案時洩密，設有安全設施掃描、偵測和消滅病毒等。網路的運用必須架構在可靠、穩定、安全的基礎上，才能有 e 化服務，制訂法律和技術指南就是其保障，避免打擊電子商務和使金融秩序大亂。

（1）濫用電腦法（Computer Misuse Act l998）；

1998 年 6 月 30 日通過濫用電腦（修正）法，以處理日益嚴重的電腦犯罪和造成的嚴重後果。修正法案明列三項有關非法進入電腦系統的新罪名：

A、干預或阻礙合法使用的行為；

B、在授權和未經授權的情況下，進入電腦系統犯案；

C、將進入網路的密碼透露以非法獲利和使別人受損失。

（2）資訊安全指南（Security Guidelines for Information Technology）；

（3）電子認證安全指南（Security Guidelines for Certification of Authorities）。

2、電子商務方面

新加坡電子交易法於 1998 年 7 月制定，為電子交易提供了一個法律構架（相關法律如下），政府隨之推出了電子商業總藍圖，不久電子證書認證中心成立，這些皆為推動電子商業，並期使新加坡成為安全和值得信賴的國際商業樞紐的目標而努力。新加坡政府發展電子商務必須確保認證中心發出的數位憑證可獲各國承認並有效解決電子商務糾紛。

（1）電子交易法（Electronic Transactions Act, 1999）；

（2）電子交易執法指南（Legal Guide to the Electronic Transactions Act）；

（3）電子交易（認證）條例（Electronic Transactions（Certification of Authorities）Regulations 1999）；

（4）電子證書指南（Guidelines for Preparing Certification Practice Statement）；

（5）電子認證安全指南（Security Guidelines for Certification of Authorities）。

3、資訊通信與傳媒方面

新加坡資訊通信與傳媒方面的分工是廣播管理局負責管理傳播內容，而資訊電信發展局負責基礎設施建設和非傳播內容的技術管制。政府的角色和作用概括如下：充分發揮互聯網的作用；維護社會價值觀和種族和諧；鼓勵業者和社群自我管制；鼓勵更多的公眾參與；扮演促進者角色。

有關新加坡資訊通信與傳媒方面相關的法律如下：

（1）資訊通信發展管理局法（Info-comm Development of Authority of S’pore Act 1999）；

（2）電信法（Telecommunication Act l999）：

新的電信法涉及到處理電信、資訊科技和廣播業結合後所產生的法律和管制問題。

（3）新加坡廣播管理局法（297 章：互聯網執業準則）（The Singapore

Broadcasting Authority Act（Chapter 297:The Schedule Internet Code of Practice）：

關注以下三類網頁：色情、暴力、種族主義和宗教極端主義。

（4）新加坡廣播管理局互聯網政策指南（Industry Guidelines on the Singapore Broadcasting Authority Internet Policy）：

政府、業者及公眾共同監督互聯網，政府採取較放鬆的管制結構。

第三章　研究設計

第一節　研究方法

一、文獻探討法

本研究蒐集歐、美、亞等先進國家有關網路平台業者電磁紀錄保存的相關法規，並對照我國現行法規加以比較分析，再參考國內外相關研究結論，透過定期會議研討，比較各種方案的利弊得失，找出適合我國法制的可能修法或立法方向，提供實務機關政策參考。

二、焦點座談法

為避免政策建議不切實際，不符合實務機關需求，本研究邀集偵查網路犯罪的警察單位、協助提供資料的網路平台業者及主管相關法規的目的事業主管機關進行座談，了解偵查單位辦案的實際需求及平台業者的成本考量，找出可行性高且效益彰顯之方案，供主管機關擬訂修法或立法政策參考（附錄四十）。

第二節　研究過程

一、國內外相關法規之蒐集彙整

（一）我國相關法規

１、通訊保障及監察法（含施行細則）（附錄一、二）

２、電信法（附錄三）

３、個人資料保護法（附錄七）

４、第二類電信事業管理規則（附錄四）

５、電信事業處理有關機關查詢電信通信紀錄實施辦法（附錄八）

６、電信事業處理有關機關（構）查詢電信使用者資料實施辦法（附錄九）

７、電腦網路內容分級處理辦法（廢止）（附錄五）

８、兒童及少年福利與權益保障法（附錄六）

９、第一類電信事業經營者名單暨其業務項目一覽表（附錄十）

１０、第二類電信事業經營者名單暨其許可服務範圍一覽表（附錄十一）

１１、電信法修正草案條文對照表（摘要）（附錄三十九）

（二）日本相關法規

１、刑事訴訟法（附錄二十二）

２、電信事業法（電気通信事業法）（附錄二十八）

３、ISP 責任限制法（プロバイダ責任制限法）：全名「特定電信服務提供者之損害賠償責任限制及發信者資訊揭露法」（特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律）（附錄二十六）

４、電信事業者對個人資訊保護準則（電気通信事業における個人情報保護に関するガイドライン）（附錄二十七）

５、犯罪偵查之通信監察法（犯罪捜査のための通信傍受に関する法律）（附錄三十）

６、網路犯罪公約（サイバー犯罪条約）（附錄二十四）

（三）中國大陸相關法規

1、互聯網電子公告服務管理規定（附錄三十一）

2、互聯網信息服務管理辦法（附錄三十二）

3、計算機信息網絡國際聯網安全保護管理辦法（附錄三十三）

4、中華人民共和國計算機信息網絡國際聯網管理暫行規定實施辦法（附錄三十四）

5、互聯網新聞信息服務管理規定（附錄三十五）

（四）新加坡相關法規

1、濫用電腦法（附錄三十六）

2、電子交易法（附錄三十七）

3、電信法（附錄三十八）

（五）美國相關法規

1、電子通訊隱私法（Electronic Communications Privacy Act, ECPA）（附錄十二）

2、愛國者法（USA Patriot Act, USAPA）（附錄十三）

3、愛國者改進與再授權法案（USA Patriot Improvement and Reauthorization Act, 2005）（附錄十四）

4、犯罪偵查通訊協助法（Communications Assistance for Law Enforcement Act, CALEA）（附錄十五）

5、外國情報監察法修正案（Foreign Intelligence Surveillance Act Amendments Act, 2008）（附錄十六）

（六）歐盟相關法規

1、個人資料保護指令（Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive 95/46/EC）（附錄十七）

2、電信事業個人資料處理及隱私保護指令（Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning

the processing of personal data and the protection of privacy in the telecommunications sector, Directive 97/66/EC）（附錄十八）

3、電子通訊中個人資料處理及隱私保護指令（Directive 2002/58/EC of the European Parliament and of the Council, Concerning the processing of personal data and the protection of privacy in the electronic communications sector, Directive 2002/58/EC）（附錄十九）

4、個人通訊資料保存指令（Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending, Directive 2006/24/EC）（附錄二十）

5、網路犯罪公約（Cyber-crime Convention）（附錄二十一）

（七）英國相關法規：反恐、犯罪與安全法案（Anti-terrorism, Crime and Security Act of 2001）

（八）義大利相關法規：對抗國際恐怖主義之緊急措施（with Urgent Measures to Fight International Terrorism）

（九）法國相關法規：日常安全法（the Law Regarding Daily Safety, 25 Nov. 2001）

二、偵查機關偵辦網路犯罪案件現行作法與所需協助

針對國內博碩士論文、期刊論文、警察機關相關公文、刊物及政府部門研究計畫進行資料搜尋，藉以瞭解國內警察機關偵查犯罪之現行作法，以及目前遭遇之狀況與困境，並根據因應而生的法案修訂或政策調整，檢討其適法性及建議可能之修法方向。

本研究亦安排與警察機關之偵查、資訊單位人員進行座談，同步蒐集相關資訊以獲取更為實際之現行作法檢討建議，以避免學術理論與實務操作無法契合之矛盾現象發生。

三、網路平台業者現行資料處理作法

歸納目前國內主要網路平台業者之種類，以及網路犯罪發生之主要族群及犯罪方式，以釐清研究對象與範圍，並統整管理相關業者之目的事業主管機關，及目前對其適用之法令規範，才有助於瞭解適法性不足之處及可能之修法方向。

同時針對相關網路平台業者進行座談，根據座談紀錄，在兼顧業者私經濟成本及公共利益之雙重考量下，研擬網路平台業者最可能配合之法規修正方向，並符合社會大眾合理之法律保障期待。

四、可能修法方向之評估及建議

政策之執行或是法規之修訂，均可能對適用對象造成極大的影響，尤其是犯罪偵查機關在執行職務之適法性，更是攸關合法與非法之認定標準，倘若偵查機關無法合法獲得有效之刑事證據，則提請檢察官起訴的可能性將銳減，同時亦會打擊警方士氣，甚至喪失民眾對警察機關之信賴，更讓不法份子逍遙法外、牟取暴利。

因此本研究最主要之目的，即是吸取國外先進國家在此領域之相關法規及實務經驗，並配合與偵查機關、網路平台業者及目的事業主管機關之焦點座談結論，以評估出可行性最高，且較為社會大眾所能接受的可能修法方向，在介於學術理論與實務操作之平衡桿上，尋求雙贏之最佳建議。

第三節　進行步驟

研究期程預計於 101 年 4 月 1 日起至 11 月 30 日前完成，共計八個月，並以書面研究報告作為結案（分別於 7 月 31 日及 11 月 30 日前提出期中及期末報告）。研究報告內容概以緒論（研究背景、目的與方法）、國內外電磁紀錄保存法規說明（國內電磁紀錄保存相關法規、遭遇問題現況與國外網路平台業者紀錄保存相關法規說明）、研究內容（主管機關與法規制度研析、立法原則之探討、優缺點研析）以及結論與建議（執行進度如圖 3-1）。

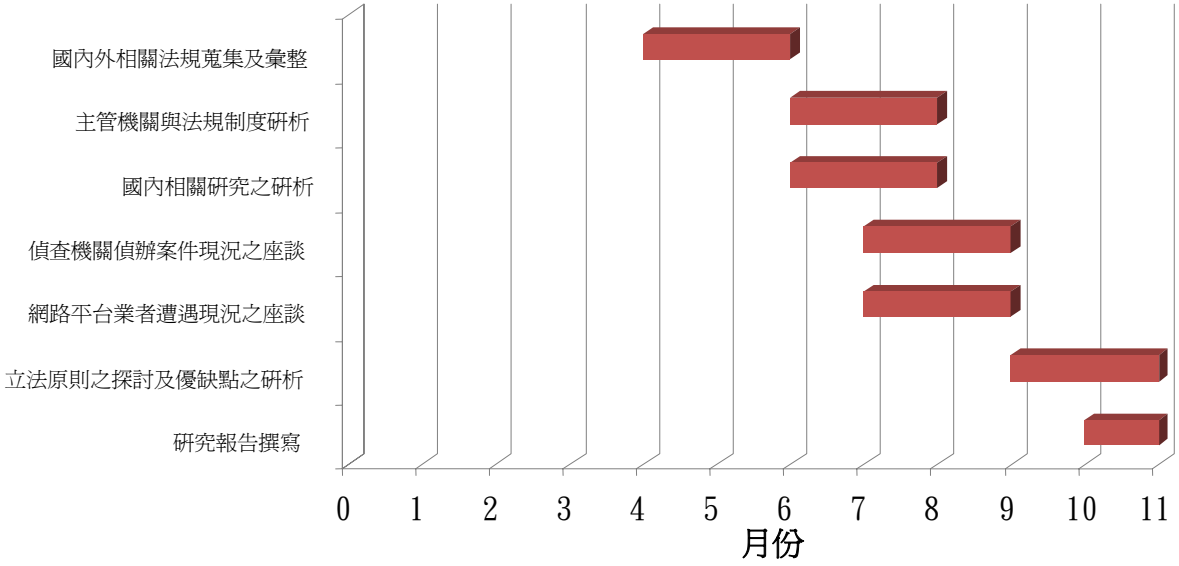


圖 3-1　執行進度甘特圖

（資料來源：本研究繪製）

第四節　研究預期成果

一、預期成果

針對近期網路發展及歐美亞等主要國家相關規範，評估我國未來修法時，在網路平臺業者保存紀錄之相關規範的參考建議：

（一）保存項目

我國「通訊保障及監察法」中監察標的為：

1、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。

2、郵件及書信。

3、言論及談話。

「第二類電信事業管理規則」第 27 條亦有明訂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，應提供之電信通信紀錄項目，如：語音單純轉售服務通信紀錄、網路電話服務通信紀錄、網際網路接取服務紀錄…等。因此，針對網路平台上的活動內容應保存之項目如：用戶登記註冊資料、各項買賣、轉帳交易等稽核紀錄…等，亦有明確訂定之需要。

（二）保存期間

我國「第二類電信事業管理規則」第 27 條即明定相關電信通信紀錄應至少保存期間，例如：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；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；電子郵件通信紀錄應保存一個月；用戶資料更應至少保存至服務契約終止後一年…等。因此，亦應在符合「比例原則」之情況下，規範網路平台業者針對特定紀錄項目保存合理而足夠之期間，以期達到刑案偵查及嚇阻犯罪之目的。

（三）其他

是否需建立專法或增列法條於相關法律規範中；如需建立專法，將於研究報告中提出建議條文以供參考。另業者若未配合提供紀錄，是否應列罰則

來規範業者。另參考歐盟等有關電信事業資料庫安全與稽核機制（如 ETSC 及 ISO27001），於研究報告增列網路平台業者證據保全規範建議，確保警察機關可拿到正確有用之資料，並在法庭上具有證據能力。其他如：用戶註冊網站時是否有登錄真實身分之義務、資料紀錄申請調閱及核發之程序、紀錄輸出格式是否統一、偵查人員對於調閱資料之運用與保密、調查結束後通知被調閱人之義務、資料保存及銷毀之義務…等，亦納入探討議題。

上述分別有關網路平臺業者、網路用戶、偵查人員等規範事項，皆為必須妥善研究訂定之細目，畢竟網路平台上之活動紀錄攸關民眾隱私權益，務必嚴謹而周全，才能保障合法，又讓非法之徒無所循形。

二、對相關業務之助益

（一）於法有據，方可堅定偵查網路犯罪時調閱相關網路紀錄之適法性。

執法機關為了維護社會秩序，常常必須採取干預、侵入性之手段，面對傳統犯罪如此，面對新興的網路犯罪亦同，正當網路功能（例如：遊戲、購物、網路銀行…等）加速發展之際，維護個人隱私和權益的觀念亦日漸普及，執法程序稍有疏漏，即可能遭輿論撻伐，甚至導致偵查結果付之一炬。因此，更需要國家、法律給予強而有力的支持，一旦相關法令確立，執法人員在網路犯罪偵查、證據蒐集時方可更加堅定信心，不必擔憂游走於法律邊緣、承擔風險。

（二）明確規範網路平臺業者應配合之事項（如：保存紀錄之設備規格、資料項目、保存期間、輸出格式…等）

不僅可避免業者因私經濟利益考量而枉顧網路治安環境，亦可使業者在積極配合國家政策意願下能有所依從，用最少的成本花費達到最大的效益，不致像無頭蒼蠅般對協助維護網路秩序及公共利益之需求各自解讀，反而保存過多不必要或對網路犯罪偵查無助益之資訊，導致效果事倍功半。

（三）縮短偵查時間、掌握時效、迅速破案。

犯罪偵查如同一場和時間的賽跑，除了偵查人員必須具備縝密細心之特質，證據蒐集更是將罪犯繩之以法的關鍵所在。網路世界凡走過必留下痕

跡，犯罪過程必定有跡可尋，立法規範網路平台業者保存相關紀錄，即能提供偵查人員便捷之管道以取得犯罪證據、或是在調查過程研判案情上有所助益，縮短偵查時間，迅速釐清疑點、確立偵查方向、取得犯罪證據，進而逮捕嫌犯，毋須受限於網路犯罪紀錄之缺漏不足、無法取得或不及取得，而被迫放棄調查或停滯不前、錯失破案契機。

第五節　研究分工

一、人力配置

姓　名	類　別	研究分工	詳細說明
廖有祿	計畫主持人	計畫規劃及督導	規劃研究方向、定期召開會議、掌握及回報研究進度、負責研究報告撰寫
張維平	協同主持人	計畫執行	國內、新加坡相關法規及研究蒐集整理、彙整相關資料、綜整期中及期末報告
蘇莞筑	研究助理	訪談相關單位	國外（日本、中國大陸）相關法規蒐集整理、辦理與偵查機關及網路平台業者座談、協助研究報告撰寫
劉怡汎	研究助理	相關資料蒐集	國外（歐美）相關網路規範之資料蒐集彙整、研析目前法規制度之優缺點、協助研究報告撰寫
楊佳蓁	研究助理	處理行政事務	公文撰擬、耗材採購及經費核銷、處理本研究案之相關行政事務

二、進度管制

本研究案為掌握進度，於計畫期程開始，定期（二周）召開會議，除了解各研究成員資料蒐集情形外，並律定後續進度要求，了解目前遭遇之困難及謀求解決方法，而在期中及期末報告繳交前，分配工作範圍，並統一寫作格式俾利彙整，會議結束後立即作成紀錄，除讓各研究成員確實了解分派工作外，亦將會議紀錄傳送委託單位，使其掌握研究進度，並從中發覺有無方向偏誤，提供修正建議。

第四章　資料分析

本研究首先蒐集歐、美、亞等主要國家有關網路平台業者電磁紀錄保存的法規，再檢視我國相關法規，經由綜合分析，本章首先比較立法與修法之優、缺點，再提出國內現有規範修法建議，包括：電磁紀錄的保存項目、保存期間、調閱程序、回覆時間及罰則，分別說明如下。

第一節　立法與修法之優缺點比較

一、國內學者看法

（一）主張制定專法學者之看法：

1、制定專法之優點：

（1）網路服務內容多樣化，經營者可能為非電信業者或個人，無法適用電信法相關法規，故建議制定協助偵查專法（如：網路服務提供者協助偵查法）取代修法，專法亦可符合憲法「法律保留原則」[131]。

（2）訊息傳遞，附著之媒體，如無線電波、電信電纜、有線電視同軸電纜、衛星、光纖等，其物理上特性，截然不同。欲對物理上特性大不相同之各類媒體，予以千篇一律之統一規範，在法律技術上，幾殆無可能，因此各國現制，通信法皆針對媒體類別、媒體特性，應用不同之規範原理，分設不同之法律規範，此即「通信依媒體類別規範原則」[132]。而網路時代之通信法規體系，應超越媒體類別之思考模式，視參與者（如網路服務提供者、使用者等）於該電信過程中之角色，統一架構網際網路法令架構，建立總則性質之法令規範，再就具特殊性之電信市場行為或現象，另訂特別法令規範，始符合科技法律之性質[133]。

2、修法之缺點：

（1）國內現行法規範對象狹隘，第二類電信事業管理規則第 27 條（已辦理

---

[131] 許慈健，網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究，國立交通大學管理學院在職專班碩士論文，2005，頁 145-153。

[132] 陳銘祥，網際網路之規範上定位－從通信之法規體系談起，經社法制論叢，第 24 期，1999 年 7 月，頁 78。

[133] 包國祥，電信法令之分析－依電信媒介各別訂定規範管理模式之檢討，律師雜誌，第 285 期，2003 年 6 月，頁 98。

公司或商業登記之「經營者」)、通訊保障及監察法第 14 條「電信事業」（含一、二類）及「郵政機關」，所謂「電信事業」無法涵蓋網路服務提供者[134]。法規範主體（第二類電信事業、電信事業）既已無法符合網路平台業者之主題，則修訂該法規之內容亦可能產生適用之疑慮。

（2）目前我國法制規範網路服務提供者協助偵查責任方面有：網路服務停止租用（與用戶簽約)、刪除權（服務條款明定有權刪除會員資訊)、儲存、提供使用者資料及通信紀錄（電信法第 7 條、第二類電信事業管理規則第 27 條之 4、5、個人資料保護法第 20 條、電信事業處理有關機關（構）查詢電信使用者資料實施辦法第 3、4、5 條)、電信業者需有特定網路位址保存跨境連線通信紀錄 90 日之設備及能力（反恐怖行動法草案)、協助實施通訊監察（通訊保障及監察法第 14 條、施行細則第 21 條）[135]…等。然而，其規範之對象為網路業務經營者，係以電信設備為基礎之網際網路接取服務提供者（Internet Access Provider)，如：第三代行動通信業務經營者、無線寬頻接取業務經營者等，若直接於上述法規修訂，難謂其涵蓋網路平台提供者（Internet Platform Provider）之範疇。

（3）有國內研究者將第二類電信所提供之服務態樣區分為：

A、有通訊相對人：網路電話服務、簡訊、網路聊天等。

B、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。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，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[136]。以 IPP 類型觀之，電子商務網站、電子交易平台及電子訊息平台等三大類型，即囊括有通訊相對人

[134] 許慈健，網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究，國立交通大學管理學院在職專班碩士論文，2005，頁 120-138。

[135] 許慈健，網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究，國立交通大學管理學院在職專班碩士論文，2005，頁 109-116。

[136] 蘇三榮，網路時代通訊監察與個人資料保護之法制研究，國立交通大學科技法律研究所碩士論文，2009，頁 36。

及無通訊相對人之通訊模式，前者尚無適用之疑慮，惟後者（如：網路銀行、搜尋引擎）則有通訊保障及監察法適用之疑義，如此，則直接於該法中增修 IPP 之紀錄保存規範，難免不妥。

（4）國內一有關網路服務提供者法律責任之研究於探討立法模式時指出，「分散式立法」可由各自主管的行政機關，依職權提出修正草案，於行政院院會審查通過後，送立法院審議。然站在網際網路服務提供者的角度而言，其所傳輸或儲存的資訊內容各式各樣，涉及的權利、法益各有不同，不同法領域內的不同免責要件，如採分散式立法，如各主管機關未進行整合考量，而分別訂定相關規範，將有可能導致規定差異甚大的情形，恐將對網際網路服務提供者於經營上造成困擾[137]。本研究牽涉數個法規亦有各自之主管機關，分別針對不同領域修訂相關規範而未加整合的話，難保不會發生類似情形。

（二）主張修法學者之看法：

1、修法之優點：

（1）以美國為例，在 1984 年國會通過「非法存取電腦設備及電腦詐欺濫用法案」之後，事實上依據此項法律起訴判決的數量並不多，其主要原因之一就是許多電腦犯罪仍可以用其他罪名追訴[138]。可見，並無必要動輒制定特別法，部份在解釋上有困難之條文，可以修訂法律方式加以因應。

（2）有研究指出，我國實務上，電信業者依交通部電信總局訂定之「電信事業處理有關機關查詢電信通信紀錄實施辦法」提供相關機關電話通話紀錄，可查詢機關係指司法機關、監察機關或治安機關，但並不適用於執法者向「網路服務提供者」要求查詢相關通訊資料，亦即現在執法者向網路服務提供者取得任何通訊資料都沒有法律上之依據。因此，建議於刑事訴訟法或通訊保障及監察法中，針對通訊紀錄之取得訂出類似美國「電子通訊隱私權法」的規範，要求檢察官、司法警察（官）基於刑

---

[137] 資策會科技法律中心，網際網路服務提供者法律責任與相關法制之研究，行政院經濟建設委員會委託研究，2003 年 12 月，頁 162。

[138] Xan Raskin & Jeannie Schaldach-Paiva（1996）, Computer Crimes, American Criminal Law Review, vol.33（3）, p.555.

事偵查目的，應有合理懷疑，並經法官許可，才可向通訊服務提供者取得相關紀錄為宜[139]。該作者建議將現行通訊保障及監察法規範之協助義務機關「電信事業」改為「服務提供者」，將服務性質各異、規模大小不一之各網路服務提供者納入通保法規範之對象，如此做法雖有利於警方犯罪偵查，然而「網路服務提供者」範圍牽涉過廣，是否可行仍有疑義。然就本研究之主題而言，若能將「網路平臺提供者」納入通保法規範之對象，將其保存紀錄協助偵查之義務、取得相關紀錄之程序…等一併於通保法中增修規範之，亦不失為建議修法方向之一種。

（3）實務界在取得資料時，多數是依照「電信事業處理有關機關查詢電信通信記錄實施辦法」及「電信事業處理有關機關（構）查詢電信使用者資料實施辦法」所規定之程序為之。性質上屬於法規命令，並無法滿足上述法律保留原則及令狀主義之要求。因此，一個規定於刑事訴訟法，且明訂應由法官審核後方可簽發的提出命令制度，對於日益重視隱私權及通訊秘密權的我國，實有慎思其立法之必要[140]。此外，為擔保提出命令之效力，在相對人不履行提出命令時，允許（檢察官告知後）法院課予相對人一定間接強制之立法方式，較為可採[141]。亦即，該作者主張對IPP 保存紀錄之「提出命令」制度及罰則修訂於刑事訴訟法中，取代現行之「電信事業處理有關機關查詢電話通話記錄實施辦法」及「電信事業處理有關機關（構）查詢電信使用者資料實施辦法」規定，方可顧及國人之隱私權及通訊秘密權。

（4）資策會科技法律研究所研究日本「服務提供者責任限制法」之規範，認為日本電信事業法第 2 條第 1 款規定之「電信」係指以有線、無線及其他電磁方式發送、傳輸或接收符號、聲音或影像者。舉凡利用電磁場的通訊行為，如使用銅線、光纖的有線通訊、使用電波的無線區域網路、

---

[139] 謝昆峰，網際網路與刑事偵查，國立臺灣大學法律學研究所碩士論文，2002，頁 141-142。

[140]陳誌泓，電腦、網路與刑事偵查－以網路犯罪公約於日本法的落實為中心，國立臺灣大學法律學研究所碩士論文，2005 年 7 月，頁 162。

[141]陳誌泓，電腦、網路與刑事偵查－以網路犯罪公約於日本法的落實為中心，國立臺灣大學法律學研究所碩士論文，2005 年 7 月，頁 163。

以及使用雷射或紅外線的通訊均屬之，目前常用之網際網路通訊自亦包括在內。我國之立法，雖有意將電信事業侷限於單純連線提供者，但由於定義之含混，網路平台服務提供者（IPP）於電信法之定位便顯得曖昧不明[142]。若依此見，可將日本電信事業法「電信」的定義做為本研究修法之參考，或直接就「電信法」第 2 條「電信」之定義修訂，將網路平台業者包含在內；或將 IPP 新增至「電信法」第 2 條名詞定義中，以使其適用「電信法」、「第二類電信事業管理規則」及「通訊保障及監察法」之規範，將需變動修訂之幅度降至最低。

（5）有學者表示，實體世界的法律已經有相當比例的成熟度，但這也不是一蹴可幾，同樣地，對於網路虛擬世界，可以隨著發展，觀察哪些行為比較嚴重，需要列入管制。未來若制定類似「優質網路社會基本法」的專法，應屬宣示性的母法，代表政府重視網路社會秩序，而目前做法則是修訂現有法律以因應網路發展[143]。

（6）法務部檢察司檢察官邱智宏曾表示，詐欺及妨害名譽等傳統類型犯罪行為，不會因為轉移至虛擬網路平台進行而改變犯罪構成要件，原有刑法條文仍然適用，因此，對人民權益影響重大的犯罪行為，目前都在法律規範範疇內，沒有必要額外訂立網路使用規則[144]。

2、制定專法之缺點：

（1）立法委員葉宜津認為，網路發展快速且多元化，無法以一部專法框住現在與未來的網路行為，且過去也已針對電腦犯罪行為修正刑法，不建議再設專法[145]。

（2）有國內律師指出，當前電信市場主要可分為六大部門：市內電信、長途及國際電話、衛星通信、行動通信以及網際網路資訊等業務，各業務間之硬體設施、網路互連義務以及規範重點均存差異。電信市場發展迅速，倘針對電信類別而以法律分別制訂規範，衡諸當前立法效率，緩不

[142]資策會科技法律中心，網際網路服務提供者法律責任與相關法制之研究，行政院經濟建設委員會委託研究，2003 年 12 月。
[143] 陳慧真，網路交通安全，中時電子報第 2009、10 期，2009。
[144] 陳慧真，網路交通安全，中時電子報第 2009、10 期，2009。
[145] 陳慧真，網路交通安全，中時電子報第 200910 期，2009。

濟急，此在電信、廣播或資訊業匯流之今日，亦屬不可行之規範方式[146]。

（3）法務部檢察司檢察官邱智宏表示，現行法律對網路業者的管理行為沒有規範，業者的自律程度全憑良心，若要制定網路專法，重點應放在網路業者的管理上，但制定有其困難，因為國內沒有單一網路主管機關，網路業者的營運態樣也複雜多變，制定專法的時程可能趕不上變化。建議應就各主管機關對網路上的業務範圍來做調整，如網路金融業務屬行政院金融監督管理委員會主管、電子商務部分屬經濟部商業司主管，各目的事業主管機關可針對業務範圍內的網路新興行為，分別修訂現有法律或管理規則[147]。

二、本研究認為修法與立法之優缺點

以下分別列舉修法之優缺點（表 4-1）及立法之優缺點（表 4-2）。

表 4-1　修法之優缺點

優點	1. 可隨時代與科技的發展，適時增訂現有法規，以維持法之適應性，與時俱進，避免動輒立法導致特別法多如牛毛之情況發生。例如：日本即是將通信歷程之保全規定增修於刑事訴訟法中，以維持刑法之完整性與適應性，而非訂定專法。 2. 國內各相關法規幾乎皆依附著「電信法」而生，如「第二類電信事業管理規則」、「通訊保障及監察法」、「電信事業處理有關機關查詢電信通信紀錄實施辦法」及「電信事業處理有關機關（構）查詢電信使用者資料實施辦法」，如果能在「電信法」中增列 IPP 定義，並將「網路平台業者紀錄」修訂囊括於「通信紀錄」範圍內，則其他相關法規依循即可，不需有過大幅度之修改。 3. 「通訊保障及監察法」中相關令狀之聲請、核發、延長、結束通知、報告義務、資料留存及銷毀、保密義務、洩漏之賠償、罰則、

[146] 包國祥，電信法令之分析－依電信媒介各別訂定規範管理模式之檢討，法律雜誌第 285 期，2003 年 6 月，頁 94。
[147] 陳慧真，網路交通安全，中時電子報第 200910 期，2009。

	協助義務…等均已有明文之規定，網路平台紀錄查詢若能直接套用，僅須修訂少部分條文即可使相關規範具備完整性。 4. 承上，未來通保法若能針對網路平台提供紀錄查詢有完整之規範，日後司法警察機關即可以此為法源依據查詢網路平台相關紀錄，無須再依「電信事業處理有關機關查詢電信通信紀錄實施辦法」，不僅法源位階提升，亦可將該辦法排除在修法範圍之外。 5. 許多傳統犯罪類型不會因為轉移至虛擬網路平台進行而改變犯罪構成要件，原有刑法條文仍然適用，沒有必要額外訂立專法。
缺點	1. 並非修訂單一法規即可，凡相關之法規如：通訊保障及監察法、電信法、第二類電信事業管理規則、電信事業處理有關機關(構)查詢電信使用者資料實施辦法…等，均應一併修訂。 2. 各個相關法規之主管機關各不相同，各自修訂可能會產生標準不一、相互矛盾之情形。 3. 網路紀錄保存與提供事涉個人資料保護及隱私權侵害問題，但第二類電信事業管理規則、電信事業處理有關機關（構）查詢電信使用者資料實施辦法、電信事業處理有關機關查詢電話通話紀錄實施辦法…等屬法規命令，有違反憲法「法律保留原則」之疑義。 4. 網路平台業者紀錄保存期間、保密義務、資訊安全責任、罰則、司法警察機關欲查詢調閱之程序、業者之配合義務、監理工作…等，散見於不同法令規範中，顯得凌亂無章。 5. 網路平台紀錄（如：來源 IP 位址、時間）與現行「通訊保障及監察法」所稱之「通訊實質內容」性質有別，侵犯人民隱私權之程度難以併論，於同一法規中做相同規範並不恰當。

（資料來源：本研究整理）

表 4-2　立法之優缺點

優點	1. 我國目前未有一套完整規範網路秩序專法，但偵查網路犯罪亟需仰賴各網路平台業者資料保存，藉以追查犯罪者行蹤，遏止不法之網路犯罪行為發生。歐盟「個人通訊資料保存指令(Directive

	2006/24/EC）[148]」即是一套規範通訊資料保存的專法，其立法目的在規範公共通訊網路產生或傳輸的資料之保存責任，確保資料可供各會員國國內法定義下的重大犯罪調查、偵查及起訴目的之運用，與本研究之目的相符，其規範內容不僅包括資料保存的項目（包括追蹤或辨別通訊來源之必要資料、辨別通訊目的地之必要資料、辨別通訊日期、時間與期間之必要資料、辨別通訊類型之必要資料、辨別使用者通訊設備之必要資料、辨別行動通訊設備方位之必要資料）及保存期間，更擴及資料保護與安全、保存資料之提供要求、監督機關、補救、責任與制裁、適用準則…等。 2. 另外，該資料保存委員會亦提出補充準則，包括：主管機關要求提供個人資料之目的須明確、要求提供個人資料限於有權執行犯罪調查、偵查與起訴之機關、必要性原則、不得對該資料進行犯罪調查、偵查與起訴等目的以外之探查、司法或獨立機關之檢驗與監督機制、業者保存資料目的之限制、保存資料之系統應與業者以商業目的進行之資料儲存系統有所區隔、資料保存之安全性…等內容，使規範詳盡充分且具整體性，足以一法完整規範網路平台業者紀錄保存之全數細節。
缺點	1. 採取立法模式，就必須面對「何者為主管機關」之問題，而何者為主管機關則須視法規條文內容及規範目的而定。目前與本研究案探討主題性質較相近之「第二類電信事業管理規則」，目的在於健全電信發展、保障通信安全及維護使用者權益，主管機關為國家通訊傳播委員會；但本研究目的為有效協助執法機關犯罪偵查，確保網路犯罪或侵權事件發生後，網路紀錄得以達到可歸責性，與「通訊保障及監察法」之確保國家安全、維持社會秩序之目的較為接近，其主管機關則為法務部，日後將如何決定主管機

[148] 個人通訊資料保存指令（Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending, Directive 2006/24/EC）。

	關，尚有討論空間。(參見表 4-3) 2. 國內沒有單一網路主管機關，網路業者的營運態樣也複雜多變，制定專法的時程可能趕不上時代、科技的變化。

（資料來源：本研究整理）

第二節　國內現有規範修法建議

綜合第一節所述，立法與修法各有利弊，唯本研究依國內法制，建議採修法為宜，以下針對現有法規提出修訂建議，並列舉為何採取修法之理由。

一、現有法規修訂建議

（一）電信法

1、日本電信事業法第 2 條電信之定義，係指以有線、無線及其他電磁方式發送、傳輸或接收符號、聲音或影像者[149]。範圍相當廣泛，舉凡利用電磁媒介的通訊行為，諸如使用銅線、光纖之有線通訊、使用電波之無線區域網路、及使用雷射或紅外線之通訊均屬之，目前常用之網際網路通訊自亦包括在內[150]。我國電信法第 2 條第 1 項第 1 款定義電信為「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」，與日本電信事業法之定義雷同，故本研究以為網際網路通訊為我國電信法所稱電信之一種，當無疑義。另外，日本「特定電信服務提供者之損害賠償責任限制及發信者資訊揭露法」第 2 條中，特定電信一詞係指「以不特定人為電信發送之接收者」，例如：留言版、電子佈告欄等即是，雖亦屬 IPP 類型，惟僅包含電子商務網站、電子金融平台與電子訊息平台等三大類之一部分，故亦不採用日本「特定電信」之用法，沿用我國電信法之定義即可，但仍建議於第 2 條第 9 款增列「電腦網路服務提供者」之定義，以使網路服務提供者於電信法之適用更為清楚明確。

2、國內法規關於「網路平臺提供者」之定義，可參考「電腦網路分級處理辦法」第 2 條條文，雖然該法業於 2012 年 6 月 13 日發布廢止，但「兒童及少年福利與權益保障法」第 46 條第 4 項定義中「提供連線上網後」等字樣，恐有遭不當解釋而限縮為 IAP 之虞，相較之下，「電腦網路分

[149] 日本「電気通信事業法」第 2 條第 1 項第 1 款「電気通信，有線、無線その他の電磁的方式により、符号、音響又は影像を送り、伝え、又は受けることをいう」。
[150] 資策會，網際網路服務提供者法律責任與相關法制之研究，2003，頁 84。

級處理辦法」第 2 條之定義顯然較佳且適用範圍較大，故建議採用「電腦網路分級處理辦法」之定義，並將其修訂於電信法第 11 條第 4 項中，將網路平臺提供者納歸第二類電信事業，以便第二類電信事業管理規則、通訊保障及監察法等相關法規在修訂網路平台紀錄保存規範時，對於網路平台業者之定義能有一明確之依據。

3、我國電信法第 2 條第 1 項第 8 款定義通信紀錄為「電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼、通信日期、通信起訖時間等紀錄，並以電信系統設備性能可予提供者為原則」。就網路犯罪偵查的角度而言，通信紀錄若僅侷限於發信方、受信方之電信號碼、通信日期、起訖時間等紀錄，似乎有所不足，建議增列「發信方（受信方）之 IP 位址」；並可參考日本刑事訟訴法第 197 條第 3 項之規定，保存項目除了通信來源、目的、時間日期外，並加入「其他通信歷程」一項，以含括通信內容以外之相關 log 紀錄。另該款後段之「以電信系統設備性能可予提供者為原則」亦建議修訂，避免業者以設備性能不足為由拒絕給予協助，此部分修法可參考國內通訊保障及監察法規定，第 14 條第 4 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」，進一步訂出適用於網路平台業者建置紀錄保存設備之規範，以確保業者在硬體設備方面有足夠建置能力，確實達成保存網路相關紀錄之義務。

4、歐盟「個人通訊資料保存指令（Directive 2006/24/EC）」[151]，規定各會員國應確保公共電子通訊服務提供者及公共通訊網路，至少應遵守有關資料保存之資料安全原則：

（1）保存之資料應與網路上之資料具有相同之品質、安全性與保護程度，亦即資料儲存時之安全性不能低於傳輸時。

（2）應提供資料適當的技術與措施以避免因意外或遭遇非法損壞、非預期

[151] 個人通訊資料保存指令（Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending, Directive 2006/24/EC）。

損失或竄改，或是未經授權或非法之儲存、處理、存取或洩漏資料。

（3）應提供資料適當的技術與措施，以確保只有特定被授權之人員可進行存取。

（4）除曾被存取並要求留存的資料之外，應在保存期限屆滿即銷毀。

上述內容可供參考加入本法「資通安全」相關規範中，以對保存之紀錄有更完善之安全機制，並確保警察機關可取得正確有用之資料，在法庭上具有證據能力。

國家通訊傳播委員會現刻正修訂電信法，亦將「資通安全」規範新增至該法第 56 條。本研究建議採用國家通訊傳播委員會 101 年 7 月 30 日函報行政院審查電信法修正草案版本，該版本草案第 56 條變更為現行電信法增訂之第 40-1 條，該條內容如下[152]：

第 40-1 條　為確保電信事業系統設備、資料及網路之安全，保障民眾通信權益，電信事業應辦理下列事項：

一、建立資通安全管理機制。

二、建立資通安全防護及偵測設施。

三、建立資通安全聯防及資通安全事件之通報、處理、回報等資通安全應變措施。

四、使用經資通安全審驗之資通設備。

前項系統設備包括核心網路設備、傳輸網路設備、接取網路設備、網路管理系統設備及其他重要電信設備。

電信事業處理資通安全事件時，得要求用戶及使用人配合辦理資通安全有關措施；其屬重大資通安全事件者，必要時得暫停或終止服務之一部或全部。

前項之規定意旨，電信事業應以顯著方式載明於營業規章及服務契約。

電信事業資通安全管理機制之查核項目與程序、適用之驗證標準與範

[152] 資料來源：國家通訊傳播委員會 101 年 7 月 30 日函報行政院審查電信法修正草案版本。

圍、資通安全之防護與偵測、聯防與應變、重大資通安全事件範圍及其他應遵行事項之管理辦法，由主管機關定之。

主管機關為進行網際網路資通安全聯防，應建置及管理資通安全聯防應變系統。必要時，得指定專責機構建置及管理之。

第一項第四款資通設備應施檢驗項目及其資通安全檢測技術規範，由主管機關訂定公告之。主管機關為資通設備安全檢測需要，應建置及管理資通安全測試樣本資料庫。必要時，得指定專責機構建置及管理之。

前項資通設備之審驗方式與程序、審驗證明之核發、換發、補發與廢止、審驗合格標籤之標貼、印鑄與使用，及審驗業務管理等事項之辦法，由主管機關定之。

（二）第二類電信事業管理規則

1、第 27 條第 1 項規定「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」。而所謂「經營者」，依同法第 2 條之定義，係指「經主管機關許可並發給執照經營第二類電信事業者」；另第 4 條第 1 項亦載明「申請經營第二類電信事業，應檢具申請書、事業計畫書及其他相關規定文件，向主管機關申請許可，經依法辦妥公司或商業登記，並取得許可執照後，始得營業」。惟常見之網路平臺提供者類型如：FTP 站、網路論壇…等，並非均有商業登記，此「經營者」之條件限制恐將無法規範到部分網路平台業者類型；然而，若不加條件限制，舉凡個人或企業、是否以營利為目的者（如：教育用之免費服務平台）皆涵蓋其中，要求其行使網路平台紀錄保存之義務，又有過度擴張公權力行使範圍之虞，必定會產生執行上之困難。因此，建議保留原有規範，要求「依法辦理公司或商業登記」之網路平台業者於營利之同時，亦須擔負提供網路平台紀錄之義務。

2、第 27 條第 3 項訂有若干「網際網路接取服務」應保存之項目及期間，如：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；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；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…等。然而，規定之客體既為「網際網路接取服務」，即表示有關留言版、貼圖區或新聞討論群、免費電子郵件信箱、網頁空間線上申請帳號之來源 IP 位址及當時系統時間、電子郵件通信紀錄…等，IAP 應予保留以供查詢，但上述資料 IAP 有辦法提供嗎？實際上，IAP 只提供網路接取連線之服務，根本無從得知用戶連線上網後去了哪些網站？或做了什麼行為？可供調閱查詢 IP、時間、留信版帳號的對象，應該是該網路平台 IPP 架設伺服器之網管人員。例如：欲追查某留言版信息之來源 IP 及時間，向 HINET 是查詢不到的，而是先向該留言版的網管人員取得 IP 及時間後，再向 HINET 查詢該用戶的真實身分資料。因此，本條內容似乎部分與標題「網際網路接取服務」不相符，建議將「（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。」等屬 IPP 之服務項目刪除。

3、承上，國內雖無單一網路主管機關，網路業者的營運態樣也複雜多變，如網路金融業務屬行政院金融監督管理委員會主管、電子商務部分屬經濟部商業司主管，但營運態樣不同、業務性質差異，應不影響網路紀錄之保存工作，本研究案以犯罪偵查之目的為主要考量，即使各網路平台分屬不同主管機關，針對紀錄保存的部分，仍可集中於單一法規加以規範，因此，建議於第 27 條第 3 項下直接增列第 5 款「網際網路平台服務提供」，列出較詳盡之各種網路平台業者類型及其保存項目、保存期間，以更符合本研究之目標。

4、日本在 2011 年 6 月通過「因應資訊處理技術提升之刑法部分修正案」（情報処理の高度化等に対処するための刑法等の一部を改正する法律案）後，於增修之刑事訴訟法第 197 條中，亦僅提及業者在接獲命令處分後，將既有之特定通信歷程繼續保存至多 90 日，並未規定業者必須就全部通信歷程主動予以保存，此與我國第二類電信事業管理規則中

訂定之紀錄保存規範不同。日本的做法可能會面臨「要什麼沒什麼」的窘境，業者大可聲稱在接到保全命令時，該紀錄已刪除，無法提供，因此不考慮將日本刑事訴訟法紀錄保存之規範納入我國參考。

（三）電信事業處理有關機關查詢電信通信紀錄實施辦法

第 2 條有關本辦法所稱通信紀錄，引用電信法第 2 條第 1 項第 8 款之定義，其修訂亦應以電信法為標準，以求法規之一致性。

（四）電信事業處理有關機關（構）查詢電信使用者資料實施辦法

1、第 4 條第 1 項規定「本辦法所稱使用者資料，指電信使用者姓名或名稱、身分證統一編號、地址、電信號碼等資料，並以用戶申請各項電信業務所填列之資料為限」，同條第 2 項「前項所稱電信號碼，係指電話號碼或用戶識別碼」。參考日本總務省發布之「訂定特定電信服務提供者之損害賠償責任之限制及發信者資訊揭露法第 4 條第 1 項省令」[153]，明訂發信者資訊項目共計 7 項，包含：發信者及其他相關侵害資訊傳送者[154]之姓名、住址、電子郵件地址、侵害資訊之相關 IP 位址、由相關行動電話末端裝置或 PHS 端末裝置連接網路服務發布侵害資訊之使用者識別符號、相關 SIM 卡識別碼中由該服務傳送者、經特定電信設備傳送侵害資訊之年、月、日及時間等。因為日本規範上述發信者資訊係由「特定電信服務提供者」揭露之，因此，提供的資料即為特定電信（如：BBS、留言版）使用者資料項目。考量現行在偵查網路犯罪工作上，除網路申裝時所填寫之用戶資料外，於線上申請註冊電子郵件或網路帳號時，亦會留下使用者資料，因此，建議於現行規範中針對缺漏之資料項目參考日本法進行補充修訂，以期規範能更臻完備。

2、本辦法第 3 條規定，僅司法機關、監察機關或治安機關因偵查犯罪或調

[153] 參閱日本總務省網頁 http://www.soumu.go.jp/，有關所管法令等／電気通信事業項下之刊載，標題「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律第四条第一項の発信者情報を定める省令（平成 14 年総務省令 57）」，最終改正：平成 23 年 9 月 15 日総務省令第 128 号。

[154] 當發信者使用所屬企業、學校的通信端末設備發送資訊的情況下，該企業、學校等即所謂「其他相關侵害資訊傳送者」。參閱「プロバイダ責任制限法」逐條解說，頁 27。

查證據所需者、其他政府機關因執行公權力所需者、與公眾生命安全有關之機關（構）為緊急救助所需者，得敘明其法律依據向電信事業查詢使用者資料。準此，電信業者原則上不負向受侵權人提供使用者資料之義務[155]。此規定與日本「網路服務提供者責任限制法」以受權利侵害者為揭露發信者資訊之請求人顯有不同。本研究係以網路平台業者提供保存之紀錄以協助犯罪偵查為出發點，而非供受侵權人提出損害賠償、維護自身權益之用，故不參考該日本法之做法。

（五）通訊保障及監察法

1、第 3 條第 1 項「通訊」定義之一為「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」，同條第 2 項規定「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」。就「調閱網路平台紀錄」角度觀之，是否有修訂之必要？此處所謂電信設備因本法無相關定義，故本研究引自電信法第 2 條電信設備之定義「指電信所用之機械、器具、線路及其他相關設備」，其中所謂電信，依國內研究對日本電信事業法之解讀，復以我國電信法與日本法定義之雷同，推論網際網路通訊亦屬電信之一種[156]。是故，偵查機關在調閱網路通信紀錄之適用上，該網路通信紀錄即在「通訊」涵蓋範圍內，暫無修訂之必要。參考美國「電子通訊隱私法」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」等三種類型，其中「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，其全部或部份藉由電信設備、無線電、電磁、光電子或光學系統進行的任何傳遞」；另該法第 121 章「有線通訊、電子通訊儲存與交易紀錄之存取」之規範中，「電子儲存」指伴隨於有線或電子通訊傳輸的過程，所產生之有線或電子通訊的暫時性與中繼性儲存，以及基於電子通訊服務備援之目的，所為的電子通訊儲存[157]。此定

[155]資策會科技法律中心，網際網路服務提供者法律責任與相關法制之研究，行政院經濟建設委員會委託研究，2003 年 12 月。

[156] 資策會，網際網路服務提供者法律責任與相關法制之研究，2003，頁 84。

[157] ECPA §2510 （17） "electronic storage" means: （A） any temporary, intermediate storage

義似乎更貼近本研究之「網路平台紀錄」，足供參考。

2、第 5 條第 1 項臚列符合聲請通訊監察的罪嫌，並以「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」為構成要件，是否為因應網路犯罪類型而有增修之必要？例如：違反刑法公然侮辱罪、社會秩序維護法…等。但其造成危害之嚴重性與原有之「通訊保障及監察法」訂定之罪嫌顯有差異，若無明確區隔，恐大大擴張通訊監察之範圍，侵犯國民隱私權，有違比例原則。考量現行通保法監察之客體為「通訊內容」，而本研究探討之對象僅為「網路通信紀錄」，侵犯個人隱私之程度較輕，因此，建議在請求調閱網路通信紀錄時，可不必限定如此嚴格之犯罪類型，改以較寬鬆之要件取代之，亦即調閱網路通信紀錄不受本條第 1 項規範之限制，僅需符合一般發動偵查[158]之要件，且係以網路平台為犯罪工具或犯罪場所者即可。

3、第 11 條規定通訊監察書應記載事項包括：案由及涉嫌觸犯之法條、監察對象、監察通訊種類及號碼等足資識別之特徵、受監察處所、監察理由、監察期間及方法、聲請機關、執行機關、建置機關等 9 個項目。可適用於網路平台紀錄調閱，毋須修訂。例如：監察之通訊種類即為「網路紀錄調閱」並註記網路帳號、E-mial、IP 等識別資訊；受監察處所為該網路平台業者；執行機關為偵查犯罪機關。惟在監察方法[159]部分，為符合司法警察機關調閱網路平台紀錄之適用，建議併於通保法第 13 條中修訂。

4、第 12 條規定違反該法第 5 條、第 6 條之通訊監察期間，每次不得逾 30 日，第 7 條之通訊監察期間，每次不得逾一年，及有繼續監察必要之延

---

of a wire or electronic communication incidental to the electronic transmission thereof; and （B） any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

[158] 刑事訴訟法第 228 條規定，檢察官因告訴、告發、自首或其他情事知有犯罪嫌疑者，應即開始偵查。前項偵查，檢察官得限期命檢察事務官、司法警察官或司法警察調查犯罪情形及蒐集證據，並提出報告。

[159] 有關「通訊監察管制資料登記簿」之「監察所得資料種類、數量」欄位，除現有之錄音帶、光碟、譯文及通聯（含簡訊）外，亦建議增加「網路通信紀錄（不含通信內容）」之選項，以配合通訊保障及監察法第 13 條監察方法之修訂。

長規定。但網路犯罪類型廣泛且罪刑輕重不一，如：刑法第 310 條誹謗罪，處一年以下有期徒刑、拘役或五百元以下罰金[160]；刑法第 339 條詐欺罪，處五年以下有期徒刑、拘役或科或併科一千元以下罰金[161]；槍砲彈藥刀械管制條例第 7 條，最高可處死刑或無期徒刑，併科新臺幣五千萬元以下罰金[162]。同樣為可能透過網路平台而實施之犯罪行為，刑責輕重卻是天壤之別。而且，實務上，調閱網路平台紀錄之期間，需視案情複雜程度及調閱目的而定，短則 1 日，長則數個月，實在難以明確規範調閱時間以多久為宜，因此，建議由偵查機關自行勘酌案情需要，於網路平台紀錄相關規範保存期間內申請之，而不受本條 30 日監察期間之限制。

5、第 13 條第 1 項規定通訊監察之方法，以「截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法為之」。實務上聲請網路監察時，監察方法多以「其他」類表示之，而本研究探討網路紀錄調閱，則須由網路平台業者儲存相關通信紀錄，雖亦可採用原條文「其他類似之必要方法」作概括性之規定，但若增例「電磁紀錄調閱」1 項，可較為清楚明確，惟仍建議保留「其他類似之必要方法」之規定，以因應未來通訊技術之發展擴張。

（六）通訊保障及監察法施行細則

第 21 條第 1 項「電信事業為協助執行通訊監察，應將電信線路以專線

---

160 刑法第 310 條「意圖散布於眾，而指摘或傳述足以毀損他人名譽之事者，為誹謗罪，處一年以下有期徒刑、拘役或五百元以下罰金。
散布文字、圖畫犯前項之罪者，處二年以下有期徒刑、拘役或一千元以下罰金。」

161 刑法第 339 條「意圖為自己或第三人不法之所有，以詐術使人將本人或第三人之物交付者，處五年以下有期徒刑、拘役或科或併科一千元以下罰金。
以前項方法得財產上不法之利益或使第三人得之者，亦同。」

162 槍砲彈藥刀械管制條例第 7 條「未經許可，製造、販賣或運輸火砲、肩射武器、機關槍、衝鋒槍、卡柄槍、自動步槍、普通步槍、馬槍、手槍或各類砲彈、炸彈、爆裂物者，處無期徒刑或七年以上有期徒刑，併科新臺幣三千萬元以下罰金。
未經許可，轉讓、出租或出借前項所列槍砲、彈藥者，處無期徒刑或五年以上有期徒刑，併科新臺幣一千萬元以下罰金。
意圖供自己或他人犯罪之用，而犯前二項之罪者，處死刑或無期徒刑；處徒刑者，併科新臺幣五千萬元以下罰金。
未經許可，持有、寄藏或意圖販賣而陳列第一項所列槍砲、彈藥者，處五年以上有期徒刑，併科新臺幣一千萬元以下罰金。」

接至建置機關監察機房。但專線不敷使用或無法在監察機房內實施時，執行機關得請求建置機關與電信事業協商後，派員進入電信機房附設之監錄場所執行」；同條第 3 項「第一項發生專線不敷使用情形時，電信事業應依執行機關或建置機關之需求，儘速擴增軟、硬體設施」；第 24 條第 3 項「電信事業之通訊系統應具有可立即以線路調撥執行通訊監察之功能；線路調撥後執行通訊監察所需之器材，由建置機關或執行機關自備」。考量網路平台業者屬性不同於傳統電信，且規模大小迥異，僅係單純提供偵查機關網路通信紀錄，是否有必要符合上述之規定？檢視第 26 條第 6 項之規定「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」。國家通訊傳播委員會於 2006 年 10 月 14 日公告第二類電信事業須設置通訊監察設備之業務種類如下：一、非 E.164 用戶號碼網路電話服務（不含不透過業者 VoIP Gateway 直接於網際網路間互相傳輸語音者）。二、E.164 用戶號碼網路電話服務。三、語音單純轉售服務。四、由網際網路接取服務經營者附加提供之電子郵件服務[163]。換言之，網路平台業者如未兼營上述服務，則無須設置通訊監察設備，自當無上述法規之適用，惟針對網路平台業者相關服務項目之紀錄，建議仍應規範其建置足夠性能之相關設備，以供司法機關依法令偵查調閱網路平台紀錄。

表 4-3　相關法規與主管機關

修訂法規	主管機關
電信法[164]	行政院／國家通訊傳播委員會
第二類電信事業管理規則	行政院／國家通訊傳播委員會
電信事業處理有關機關（構）	行政院／國家通訊傳播委員會

[163] 參閱國家通訊傳播委員會網站 http://www.ncc.gov.tw/ ，首頁／民眾服務／公告訊息／一般公告項下，標題「公告第二類電信事業須設置通訊監察設備之業務種類」，上網日期：2012 年 9 月 19 日。

[164] 該法第 3 條明訂，電信事業之主管機關為交通部，為監督、輔導電信事業並辦理電信監理，設電信總局。

修訂法規	主管機關
查詢電信使用者資料實施辦法	
電信事業處理有關機關查詢電信通信紀錄實施辦法	行政院／國家通訊傳播委員會
通訊保障及監察法	行政院／法務部
通訊保障及監察法施行細則	行政院／法務部＆司法院
個人資料保護法	行政院／法務部
個人資料保護法施行細則	行政院／法務部

（資料來源：本研究整理）

二、採取修法途徑之理由

考量諸多制定專法與修法的優、缺點後，本研究以為，網路平台業者紀錄保存之相關規範，仍應以修訂現有法規之方式較符合我國現有的法制環境，其理由如下：

（一）一昧制訂新法，將難以維持舊有法規之適應性

法律規範之腳步永遠落後於科技產品之創新，我國現有之相關法令規範已多達 8 種（如表 4-3 所示），若再為了規範「網路平台業者之紀錄保存」單一目的而制定專法，恐導致特別法多如牛毛之情況發生，而且，面臨科技潮流的推進，難保原有法規能永久適用而不被淘汰。倒不如順應時勢，修訂現有法規，以維持法規之適應性及完整性。日本將通信歷程之保全規定增修於刑事訴訟法中，便是最佳的例子。

（二）於電信法中增修「網路平台業者」定義，可降低附屬法規修改幅度

國內各相關法令規範如：第二類電信事業管理規則、通訊保障及監察法、電信事業處理有關機關查詢電信通信紀錄實施辦法、電信事業處理有關機關（構）查詢電信使用者資料實施辦法…等，幾乎皆依附著「電信法」而生，而電信法第 2 條第 1 款對「電信」之定義甚廣，除固定通信、行動通信、

衛星通信等有線、無線通信外，亦包括以數位訊息傳送文字符號語音及影像之網際網路在內[165]，因此，若能在電信法中明確增列「網路平台業者」之定義，則「通信紀錄」自然包括網路平台業者所儲存之相關紀錄，如此一來，其他附屬法規便可依循引用，不必要有過大幅度之修改。

（三）「通訊保障及監察法」程序規範完整，增訂網路紀錄查詢程序較易

建議修訂之一的「通訊保障及監察法」中，有關令狀之聲請、核發、延長、結束通知、報告義務、資料留存及銷毀、保密義務、洩漏之賠償、罰則、業者協助義務…等均已有明確而完整之規定，有關網路平台之紀錄查詢若能直接套用，僅須修訂少部分條文即可使相關規範具備完整性。雖然網路平台紀錄（如：來源 IP 位址、時間、註冊資料）與現行「通訊保障及監察法」所稱之「通訊實質內容」性質有別，侵犯人民隱私權之程度難以併論，且得聲請法院核發通訊監察書之犯罪要件、查詢期間之規定尚有待討論，但若能以增訂專門條款之方式修法，在考量比例原則的情況下，將「網路紀錄查詢」與「通訊內容監聽」做一明確區別，亦可無損人民隱私權之保障。此外，未來通訊保障及監察法若能針對網路平台提供紀錄查詢有完整而嚴謹之規範，日後司法警察機關即可依此為法源依據來查詢網路平台相關紀錄，無須再依「電信事業處理有關機關查詢電信通信紀錄實施辦法」，不僅法源位階提升，亦可將該辦法排除在修法範圍之外。

（四）成立修法統籌單位，解決不同主管機關問題

雖然各個相關法規之主管機關各不相同，各自修訂可能會產生標準不一、相互矛盾之情形，然而，若能成立一專門之審議單位擔任統籌角色，邀集各相關主管機關共同參與研擬修法事宜，問題即可迎刃而解。以日本為例，在簽署「網路犯罪公約」後，法務省於 2003 年在法制審議委員會下新設「科技犯罪小組」，針對犯罪國際化、組織化對策以及情報處理技術提升來研修相關法律，並於 2011 年提出「因應資訊處理技術提升之刑法部分修正案」，

[165] 包國祥，電信法令之分析－依電信媒介各別訂定規範管理模式之檢討，律師雜誌，第 285 期，2003 年 6 月，頁 92。

在網路犯罪相關整備法中，一共修訂了刑法、刑事訴訟法、組織犯罪處罰及犯罪收益限制法（組織的な犯罪の処罰及び犯罪収益の規制等に関する法律）、刑事案件第三人所有物沒收程序緊急處理法（刑事事件における第三者所有物の没収手続に関する応急措置法）、國際偵查合作法（国際捜査共助等に関する法律）、禁止不法接取行為法（不正アクセス行為の禁止等に関する法律）[166]…等多個法律。此外，亦可免於制定專法後尚須面臨的主管機關之難題。

（五）法規命令經明確授權，符合法律保留原則

法律保留原則，為憲法第 23 條所宣示之法律原則，係指行政機關為行政行為須有法律授權，積極要求行政機關之行為必須有法律依據，不得任意自為。司法警察機關為犯罪偵查之目的，要求網路平台業者保存並提供相關紀錄之作為，事涉個人資料保護及隱私權侵害問題，本研究欲針對相關法規進行修訂，當然須考量法律保留問題，雖然通訊保障及監察法施行細則、第二類電信事業管理規則、電信事業處理有關機關（構）查詢電信使用者資料實施辦法、電信事業處理有關機關查詢電話通話紀錄實施辦法…等屬法規命令，但若能在電信法、通訊保障及監察法中授權規範，即無違反法律保留原則之疑慮。

（六）修法集中兩大方向，對業者不致產生困擾

雖然非訂立專法，網路平台業者紀錄保存及其他相關規範如：保存項目、保存期限、保密義務、資訊安全責任、罰則、司法警察機關查詢調閱之程序、結束通知、洩漏賠償、業者協助義務、監理機制…等，必須規範在不同法令之中，對業者難免造成困擾。然而，本研究僅將修法方向分為兩大部分，一係於「第二類電信事業管理規則」中增訂網路平台業者類型、紀錄保存項目、保存期間；二則是於「通訊保障及監察法」中增訂網路紀錄查詢程序及其他如回復時間、保密、協助義務、資料留存及銷毀、洩漏之賠償、監

[166] 參閱日本法務省網站：http://www.moj.go.jp/index.html，トップページ＼所管法令等＼国会提出法案など＼国会提出主要法案第 177 回国会（常会）項下之刊載，標題「情報処理の高度化等に対処するための刑法等の一部を改正する法律案」。

理機制及罰則…等規定。其他「電信法」、「電信事業處理有關機關（構）查詢電信使用者資料實施辦法」等法規多為定義上之小幅修正，不會有規範過於分散、雜亂無章之感，業者在遵循相關規範時應不致產生過多困擾。

第三節　電磁紀錄之保存項目及期間

一、各國現況

目前世界各國並未有專法對於「網路平台業者紀錄保存」加以規範，美國相關法規散在「電子通訊隱私法（ECPA）」及「著作權法」等法當中。歐盟方面相關法規主要是「個人通訊資料保存指令（Directive 2006/24/EC）」，其中英國訂有「保留通訊資料規範」（The Retention of Communications Data Code of Practice），亦為規範通訊或通話資料最長可以保留期間。日本方面針對電信設備通信紀錄，在刑事訴訟法予以相關規範。各國現有之通訊或電信紀錄保存之法規，皆非針對「網路平台業者紀錄保存」之規範。以下茲就歐、美、日等國現況說明，再就我國「網路平台業者紀錄保存」提出建議。

美國警方多年來在偵查兒童色情罪案件遭遇取得網路使用者紀錄之困境之後，National Sheriffs' Association 反映此一問題認為：電信業者對於客戶資料保留期間的限制和不一致，阻礙了警方調查兒童色情罪犯的能力；並要求：網路業者保留客戶 IP address 至少 18 個月[167]。美國執法機關亦要求網際網路業者保留相關紀錄以利偵查兒童色情網站，在修訂中的 Protecting Children From Internet Pornographers Act of 2011，規定：電子通訊供應商應至少保留一年足以辨識用戶的 IP Address 或用戶資訊[168]。

歐洲理事會「個人通訊資料保存指令（Directive 2006/24/EC）」要求會員國應確保規範中所須保存之資料其保存期限至少六個月，但不得超過自通訊日期起之兩年，這項法律對歐洲執法機關在對抗反恐及重大犯罪是重要的工具。電信業者需要保留在歐洲境內的固網或行動電信通話，不論是接收或

---

[167] CNET, Police: Internet providers must keep user logs, CNET, July 11, 2011, http://news.cnet.com.

[168] H. R. 1981, To amend title 18, United States Code, with respect to child pornography and child exploitation offenses,in the House of Representatives, May 25, 2011.

是撥出，都要記錄通話的時間，還有其他可以追蹤至通話者的身分。在網際網路方面，業者必須保留用戶上線的時間、IP address、保留 E-mail、VOIP 等訊息，惟通訊的內容不予記錄[169]。其中英國在 2003 年所訂" The Retention of Communications Data Code of Practice"規定通訊或通話資料最長可以保留時間[170,171]：

（一）用戶資料：1 年

（二）用戶上線記錄：6 個月

（三）電子郵件通聯記錄：6 個月

（四）通聯記錄：1 年

（五）SMS, EMS and MMS 等簡訊資料：6 個月

（六）網路活動記錄：4 天

日本方面相關法規列在刑事訴訟法第 197 條增修條文：檢察官、檢察事務官或司法警察官，對於提供電信設備通信紀錄之通信來源、目的、日期時間及其他通信歷程（通信履歷），可以要求保留 30 至 90 日。

二、我國現況

我國目前未有專法規範網路平台業者紀錄保存之規定，與「網路平台業者」性質接近之電信業者紀錄保存的規範有通訊保障及監察法、電信法、第二類電信事業管理規則及電信事業處理有關機關查詢電信通信紀錄實施辦法。關於連線記錄保存規定於第二類電信事業管理規則，但僅規範網路連線服務者 （Internet Access Provider, IAP）。另我國著作權法第六章之一網路服務提供者之民事免責事由，將網路服務提供者分為連線服務提供者、快速存取服務提供者、及資訊儲存服務提供者，其中資訊儲存服務提供者較為接近網路平台業者，但亦未規範相關紀錄保存時間。

---

[169] CNET News.com, Europe passes tough new data retention laws, December 14, 2005, http://news.cnet.com/Europe-passes-tough-new-data-retention-laws/2100-7350_3-5995089.html
[170] Watson Hall Ltd, UK data retention requirements, Watson Hall Ltd, 2009.
[171] IT & Communications Community, A review by InTechnology of legislation and regulation concerning data storage in the UK and Europe, http://www.intechnology.co.uk/.

本研究將依據電子商務型態及網路使用者之網路活動將網路平台業者區分為電子商務網站、電子金融平台、及電子訊息平台三類[172]：

（一）電子商務網站：

１、線上即時交易

整個交易過程都在網路線上完成，消費者於線上付款購物，並於線上即時取得商品。適合這種交易方式的物品皆為電子化數位資料，可直接透過網路下載，包含線上影音下載網站（音樂、電影、VOD 隨選視訊系統）、軟體下載網站、網路遊戲、電子書下載網站、線上資料庫、線上圖書館、P2P 網站、APP 下載網站、手機鈴聲下載網站、雲端服務網站（含基礎設施服務、平台服務、和軟體服務）[173]等。

２、線上購物交易

線上購物交易之商品無法在網路線上進行，必須透過其他管道取得購買的商品，例如郵局、快遞業者送貨到府，或配銷到住家附近的便利商店。包含網路拍賣網站、線上購物（書、比薩、CD 等）、網路旅行社、網路購票（機票、高鐵、台鐵）等。

（二）電子金融平台：

電子金融平台在網路上提供金融相關服務，如電子銀行、網路 ATM、網路銀行（信用卡、電子票證）、網路證券、小額付費等。

（三）電子訊息平台：

電子訊息平台在網路上提供訊息交換、傳遞之服務，如 BBS、留言版、貼圖網站、部落格、網路論壇、電子郵件、代理伺服器、即時訊息（MSN、Skype 等）、臉書等。

---

[172] 范錚強、侯永昌、范懿文、李世材，資訊管理導論，旗標出版，2006。

[173] 鐘嘉德，高天助，楊嘉栩，雲端運算與產業發展，研考雙月刊第 34 卷第 4 期，2010 年 8 月，頁 20-31。

三、紀錄保存規範之建議

本研究將網路使用者在前述電子商務網站、電子金融平台、及電子訊息平台等三類網路平台上的主要活動區分為線上申請帳號、線上遊戲虛擬寶物及遊戲幣轉移、網路下單、電子銀行交易、網路張貼文章、線上購物交易，並針對這些活動所涉資料欄位，參考歐美各國規定與做法、及國內相關法規如網際網路等電子式交易型態交易資料保存規範、商業會計法、經濟部工業局線上遊戲定型化契約範本第十四條遊戲歷程之保存與查詢、電子票證發行管理條例等，建議增列或修訂相關法規，如表 4-4、表 4-5。

（一）電子訊息平台張貼文章：

1、留言版、貼圖區或新聞討論群張貼文章、圖片

使用者於電子訊息平台網站之留言版、貼圖區或新聞討論群張貼文章、圖片等，留言版、貼圖區或新聞討論群對於張貼文章、圖片之使用者，保存其來源 IP 位址、當時系統時間。

（1）相關法規：

第二類電信事業管理規則第二十七條第三項第三款（四）規定：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。

（2）建議：

A、第二類電信事業管理規則第二十七條第三項係規範「網際網路接取服務」，然該項第三款內之留言版、貼圖區或新聞討論群，係屬於「網路平台服務」，並非「網際網路接取服務」。建議將原第二十七條第三項第三款（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，移至第二類電信事業管理規則第二十七條新增之第二項第五款網路平台服務（一）：「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六個月。」

B、第二類電信事業管理規則第二十七條：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六個月。

１、電子郵件傳送訊息

使用者利用電子郵件傳送訊息，電子郵件伺服器對於使用者電子郵件通信紀錄應保存其來源 IP 位址、當時系統時間。

（1）相關法規：

第二類電信事業管理規則第二十七條第三項第三款（六）規定：電子郵件通信紀錄應保存一個月。

（2）建議：

A、第二類電信事業管理規則第二十七條第三項係規範「網際網路接取服務」，然該項第三款（六）「電子郵件」，係屬於「網路平台服務」，並非「網際網路接取服務」。建議將原第二十七條第三項第三款（六）規定：電子郵件通信紀錄應保存一個月，移至第二類電信事業管理規則第二十七條新增之第二項第五款網路平台服務（二）：「電子郵件通信紀錄（含用戶帳號、來源 IP 位址、當時系統時間）應保存六個月。」

B、第二類電信事業管理規則第二十七條新增之第二項第五款網路平台服務（二）：「電子郵件通信紀錄（含用戶帳號、來源 IP 位址、當時系統時間）應保存六個月。」

２、其他電子訊息平台張貼文章或傳送訊息

除前述留言版、貼圖區、新聞討論群及電子郵件外，其他與留言版、貼圖區、新聞討論群及電子郵件類似的電子訊息平台有電子佈告欄、部落格、網路論壇、即時訊息（MSN、Skype 等）、臉書等。其中部落格、臉書與留言版、貼圖區相似；電子佈告欄、網路論壇與新聞討論群性質及功能近似；即時訊息（MSN、Skype 等）與電子郵件類似，應一併規範。

（1）其他電子訊息平台張貼文章

比照第二類電信事業管理規則第二十七條第三項第三款（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」之規範，對於使用者於與類似留言版、貼圖區或新聞討論群之電子佈告欄、網路論壇、部落格等其他電子訊息平台張貼文章、圖片，亦應保存其來源 IP 位址、當時系統時間。

A、相關法規：

第二類電信事業管理規則第二十七條第三項第三款（四）規定：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。

B、建議：

第二類電信事業管理規則第二十七條新增之第二項第五款網路平台服務（三）:「張貼於電子佈告欄、網路論壇、部落格或其他電子訊息平台之內容來源 IP 位址與當時系統時間應保存六個月。」

（1）其他電子訊息平台傳送訊息

比照第二類電信事業管理規則第二十七條第三項第三款（六）「電子郵件通信紀錄應保存一個月」之規範，對於使用者於與電子郵件類似之即時訊息（如 MSN、Skype）等其他電子訊息平台傳送訊息，應保存其來源 IP 位址、當時系統時間。

A、相關法規：

第二類電信事業管理規則第二十七條第三項第三款（六）規定：電子郵件通信紀錄應保存一個月。

B、建議：

第二類電信事業管理規則第二十七條新增之第二項第五款網路平台服務（四）:「即時訊息通信紀錄（含用戶帳號、來源 IP 位址、當時系統時間）應保存六個月。」

３、主管機關：

（1）電信事業主管機關：國家通訊傳播委員會。

（2）其他事業主管機關：視網路張貼文章或傳送訊息所涉業務性質而定。

（二）線上申請帳號：

所有網路使用者在網路進行任何活動之前均需先申請該網站帳號，如電子郵件、貼圖區、留言版、新聞討論群、即時訊息、臉書等，使用者申請帳號時需輸入基本資料如姓名、身分證號、生日、地址、電子郵件、聯絡電話，部分網站需經過電子郵件或行動電話認證，方能啟動申請帳號。網站經過電子郵件或行動電話認證，將使用者所輸入之基本資料及申請者上線 IP、上線系統時間記錄於資料庫。

1、免費電子郵件信箱及網頁空間：

（1）相關法規：

第二類電信事業管理規則第二十七條第三項第三款（五）規定：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。

（2）建議：

第二類電信事業管理規則第二十七條第三項係規範「網際網路接取服務」，然該項第四款內之免費電子郵件信箱及網頁空間，係屬於「網路平台服務」，並非「網際網路接取服務」。建議將原第二十七條第三項第三款（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，移至第二類電信事業管理規則第二十七條新增之第二項第五款網路平台服務（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。」

2、免費留言版、貼圖區及新聞討論群：

比照第二類電信事業管理規則第二十七條第三項第三款（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」之規定，使用者於留言版、貼圖區、新聞討論群，亦應保存使用者線上申請帳號時之來源 IP 位址及當時系統時間。

（1）相關法規：

第二類電信事業管理規則第二十七條第三項第三款（五）規定：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。

（2）建議：

第二類電信事業管理規則第二十七條第三項第三款（五）規定：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。該規定僅規範免費電子郵件信箱及網頁空間線上申請帳號時應保存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，對於同款留言版、貼圖區、新聞討論群並未規範。建議第二類電信事業管理規則第二十七條增列第二項第五款網路平台服務（六）:「免費留言版、貼圖區、新聞討論群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。」

３、其他電子訊息平臺：

比照第二類電信事業管理規則第二十七條第三項第三款（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」之規定，使用者於類似之電子佈告欄、部落格、網路論壇、即時訊息（MSN、Skype 等）、臉書等電子訊息平台，亦應保存使用者線上申請帳號時之來源 IP 位址及當時系統時間。

（1）相關法規：

第二類電信事業管理規則第二十七條第三項第三款（五）規定：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。

（2）建議：

第二類電信事業管理規則第二十七條第三項第三款（五）規定：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。該規定僅規範免費電子郵件信箱及網頁空間線上申請帳號時應保存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，對於同款留言版、貼圖區、新聞討論群，及其他類似之電子佈告欄、部落格、網路論壇、即時訊息（MSN、Skype 等）、臉書等電子訊息平台並未規範。建議第二類電信事業管理規則第二十七條增列第二項第五款網路平台服務（七）:「免費電子佈告欄、網路論壇、部落格、即時訊息或其他電子訊息平台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。」

4、主管機關：

（1）電信事業主管機關：國家通訊傳播委員會。

（2）其他事業主管機關：視網路張貼文章或傳送訊息所涉業務性質而定。

（三）線上遊戲虛擬寶物轉移：

線上遊戲網站記錄遊戲玩家轉移虛擬寶物或遊戲幣之遊戲歷程，包含轉出帳號、遊戲幣、數量、來源 IP 位址、當時系統時間、轉入帳號、遊戲幣、數量。

1、相關法規：

（1）經濟部工業局線上遊戲定型化契約範本第十四條遊戲歷程之保存與查詢：乙方應保存甲方之個人遊戲歷程紀錄，且保存期間為____日（不得低於三十日），以供甲方查詢。

（2）建議：

A、遊戲玩家轉移虛擬寶物或遊戲幣之遊戲歷程(轉出帳號、遊戲幣、數量、來源 IP 位址、當時系統時間、轉入帳號、遊戲幣、數量)，應保存六個月。

B、建議修訂經濟部工業局線上遊戲定型化契約範本第十四條遊戲歷程之保存與查詢：乙方應保存甲方之個人遊戲歷程紀錄，且保存期間為____日（不得低於六個月），以供甲方查詢。

2、主管機關：經濟部工業局

（四）網路下單：

網路下單網站記錄用戶下單紀錄如委託人帳號、委託日期時間、證券種類、股數或面額、限價、有效期間、營業員代號、委託方式、來源 IP、當時系統時間。

1、相關法規：

（1）證券經紀商受託買賣有價證券製作委託書買賣報告書及對帳單應行記載事項準則第 12 條：以電子式交易型態 （IC 卡、網際網路等） 委託買賣者，證券商免製作、代填委託書，惟仍應即時製作留存買賣委託

之相關書面紀錄憑核，並需每日經相關主管簽章後至少留存二個月。前項相關書面紀錄，其內容應包含委託人帳號、委託日期時間、證券種類、股數或面額、限價、有效期間、營業員代號、委託方式等，並須依時序別之方式為之。

（2）證券商帳表憑證保存年限表：

A、委託書（成交部分）五年。

B、證券商依據商業會計法第四十條及商業使用電子方式處理會計資料辦法規定，以電子方式處理會計資料者，其會計報告之日報、月報、會計簿籍及業務憑證之買賣報告書、交割憑單、買賣回報單、成交回報單等均得以媒體方式儲存，惟應依規定格式及需求列印。證券商未依商業會計法第四十條及商業使用電子方式處理會計資料辦法規定，以電子方式處理會計資料者，其業務憑證之買賣報告書、交割憑單、買賣回報單、成交回報單亦得以媒體方式保存，並應依規定格式及需求列印。至媒體保存年限應依本表所列各帳表憑證保存年限規定辦理，如其他有關法令對各項資料保存期限有較長規定者，應依各該法令辦理。

（3）網際網路等電子式交易型態交易資料保存規範二：對客戶經由網際網路等電子式交易型態所為之交易委託及查詢，其電腦稽核紀錄（log）應至少保留五年，但買賣委託有爭議者，應保留至爭議消除為止。

（4）商業會計法第 38 條：各項會計憑證，除應永久保存或有關未結會計事項者外，應於年度決算程序辦理終了後，至少保存五年。

（5）商業使用電子方式處理會計資料辦法第 9 條：資料儲存媒體內所儲存之各項會計憑證，除應永久保存或有關未結會計事項者外，應於年度決算程序辦理終了後，至少保存五年。

（6）建議：現有法規「證券經紀商受託買賣有價證券製作委託書買賣報告書及對帳單應行記載事項準則」、「證券商帳表憑證保存年限表」、「網際網路等電子式交易型態交易資料保存規範」、「商業會計法」、及「商業使用電子方式處理會計資料辦法」已有明確規範，無需再增修訂其他法規。

2、主管機關：金融監督管理委員會

（五）電子銀行交易：

電子銀行網站記錄用戶網路銀行交易紀錄包含交易日期、使用卡號、交易項目、交易金額、交易設備代號、幣別、來源 IP 位址、當時系統時間。

1、相關法規：

（1）電子票證發行管理條例第 22 條：發行機構發行電子票證應保存持卡人交易帳款明細資料，並至少保存五年。前項明細資料應充分揭露交易日期、使用卡號、交易項目、交易金額、交易設備代號及幣別等項目。

（2）建議：現有法規「電子票證發行管理條例」已有明確規範，無需再增修訂其他法規。

2、主管機關：金融監督管理委員會

（六）線上購物交易：

線上購物網站記錄網路買賣用戶之帳號、交易代號、數量、來源 IP 位址、當時系統時間。

1、相關法規：

（1）電子簽章法

（2）電子簽章法施行細則

（3）網路交易定型化契約應記載及不得記載事項指導原則（如下）

（4）建議：於「網路交易定型化契約應記載及不得記載事項指導原則」第六點個人資料安全維護義務增列第二項線上購物網站記錄網路買賣用戶之帳號、交易代號、數量、來源 IP 位址、當時系統時間，應保存六個月。

2、主管機關：

（1）電子商務主管機關：經濟部商業司

（2）其他事業主管機關：視線上購物商品所涉業務性質而定，如：

A、盜版光碟：經濟部智慧財產局

B、仿冒商品：經濟部智慧財產局

C、個人資料：法務部

D、藥品：衛生署

E、保育類動物：農委會

網路交易定型化契約應記載及不得記載事項指導原則

（一）應記載事項

第一點　個人資料保護原則

個人資料之蒐集、處理及利用，應尊重消費者之權益，並取得消費者同意，依誠實及信用方法為之，不得逾越契約特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

第二點　依請求答覆查詢、供閱覽個人資料等義務企業經營者應依消費者之請求，就其保有消費者之個人資料檔案，答覆查詢、提供閱覽或製給複製本。

前項請求，消費者得提出可資確認之身分證明文件申請；委託他人代為申請者，另應提出可資確認之身分證明。

查詢或請求閱覽個人資料或製給複製本者，企業經營者得酌收合理費用。

第三點　維護個人資料正確性義務

企業經營者為維護個人資料之正確，應依消費者之請求即時更正或補充之。

個人資料正確性有爭議者，企業經營者應即時停止該筆資料之處理及利用或採取其他保護措施。

第四點　契約目的消失或期限屆滿時個人資料之處理

處理個人資料之契約目的消失或期限屆滿時，企業經營者應停止處理及利用該資料。但經當事人書面同意者，不在此限。

第五點　個人資料處理請求之期限

企業經營者受理消費者就其個人資料之查詢、閱覽、刪除製給複製本、停止處理及利用等請求，應於三十日內處理之。其未能於該期間內處理者，應將其原因以書面通知消費者。

第六點　個人資料安全維護義務

企業經營者對個人資料之存取均應建立識別碼、通行碼之管理制度，並加設資料存取控制。

個人資料檔案，應指定專人依相關法令辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏，並應定期不定期稽核其檔案管理情形。

表 4-4　網路平台業者紀錄保存時間及法規修訂建議表

網路活動/事件	保留欄位、項目	保留時間	網路平台業者型態	適用法規
留言版、貼圖區或新聞討論群張貼文章、圖片	來源 IP 位址、當時系統時間	六個月	留言版、貼圖區或新聞討論群	第二類電信事業管理規則第二十七條
電子郵件傳送訊息	來源 IP 位址、當時系統時間	六個月	電子郵件	第二類電信事業管理規則第二十七條
其他電子訊息平台張貼文章	來源 IP 位址、當時系統時間	六個月	電子佈告欄、網路論壇、部落格等其他電子訊息平台	第二類電信事業管理規則第二十七條
其他電子訊息平台傳送訊息	來源 IP 位址、當時系統時間	六個月	即時訊息（如 MSN、Skype）等其他電子訊息平台	第二類電信事業管理規則第二十七條
免費電子郵件信箱及網頁空間線上申請帳號	來源 IP 位址、當時系統時間	六個月	電子郵件信箱、網頁空間	第二類電信事業管理規則第二十七條
免費留言版、貼圖區、新聞討	來源 IP 位址、當時系統時間	六個月	留言版、貼圖區、新聞討論群	第二類電信事業管理規則第二十七條

論群線上申請帳號				
免費電子佈告欄、網路論壇、部落格、即時訊息或其他電子訊息平台線上申請帳號	來源 IP 位址、當時系統時間	六個月	電子佈告欄、網路論壇、部落格、即時訊息或其他電子訊息平台	第二類電信事業管理規則第二十七條
線上遊戲虛擬寶物、遊戲幣轉移	遊戲歷程（轉出帳號、遊戲幣、數量、來源 IP 位址、當時系統時間、轉入帳號、遊戲幣、數量）	六個月	線上遊戲網站	經濟部工業局線上遊戲定型化契約範本第十四條遊戲歷程之保存與查詢
網路下單	委託人帳號、委託日期時間、證券種類、股數或面額、限價、有效期間、營業員代號、委託方式、來源 IP 位址、當時系統時間	五年	電子金融平台	網際網路等電子式交易型態交易資料保存規範、證券經紀商受託買賣有價證券製作委託書買賣報告書及對帳單應行記載事項準則第 12

				條、證券商帳表憑證保存年限表、商業會計法第 38 條、商業使用電子方式處理會計資料辦法第 9 條
電子銀行交易	交易日期、使用卡號、交易項目、交易金額、交易設備代號、幣別、來源 IP 位址、當時系統時間	五年	電子金融平台	電子票證發行管理條例第 22 條、商業會計法第 38 條、商業使用電子方式處理會計資料辦法第 9 條
線上購物交易	帳號、交易代號、數量、來源 IP 位址、當時系統時間	六個月	線上購物交易網站	電子簽章法

（資料來源：本研究整理）

表 4-5　網路平台業者紀錄保存時間相關法規及主管機關

網路活動／事件	適用法規	主管機關
網路張貼文章（含電子佈告欄、網路論壇、部落格等其他電	第二類電信事業管理規則第二十七條：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。	1. 電信事業主管機關：國家通訊傳播委員會。 2. 其他目的事業主

子訊息平台）		管機關：視網路張貼文章所涉業務性質而定
線上申請帳號之個人資料（含免費電子郵件信箱、網頁空間、留言版、貼圖區、新聞討論群、電子佈告欄、網路論壇、部落格、即時訊息或其他電子訊息平台等）	第二類電信事業管理規則第二十七條第三項第三款（五）規定：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。	電信事業主管機關：國家通訊傳播委員會
線上遊戲虛擬寶物、遊戲幣轉移	經濟部工業局線上遊戲定型化契約範本第十四條遊戲歷程之保存與查詢：乙方應保存甲方之個人遊戲歷程紀錄，且保存期間為____日（不得低於三十日），以供甲方查詢。	經濟部工業局
網路下單	網際網路等電子式交易型態交易資料保存規範二：對客戶經由網際網路等電子式交易型態所為之交易委託及查詢，其電腦稽核紀錄（log）應至少保留五年，但買賣委託有爭議者，應保留至爭議消除為止。證券經紀商受託買賣有價證券製作委託書買賣報告	金融監督管理委員會

	書及對帳單應行記載事項準則第12 條：以電子式交易型態 （IC卡、網際網路等） 委託買賣者，證券商免製作、代填委託書，惟仍應即時製作留存買賣委託之相關書面紀錄憑核，並需每日經相關主管簽章後至少留存二個月。 前項相關書面紀錄，其內容應包含委託人帳號、委託日期時間、證券種類、股數或面額、限價、有效期間、營業員代號、委託方式等，並須依時序別之方式為之。 證券商帳表憑證保存年限表：委託書（成交部分）五年。 證券商依據商業會計法第四十條及商業使用電子方式處理會計資料辦法規定，以電子方式處理會計資料者，其會計報告之日報、月報、會計簿籍及業務憑證之買賣報告書、交割憑單、買賣回報單、成交回報單等均得以媒體方式儲存，惟應依規定格式及需求列印。證券商未依商業會計法第四十條及商業使用電子方式處理會計資料辦法規定，以電子方式處理會計資料者，其業務憑證之買賣報告書、交割憑單、買賣回報單、成交回報單亦得以媒體方式保存，並應依規定格式及需求	

	列印。至媒體保存年限應依本表所列各帳表憑證保存年限規定辦理，如其他有關法令對各項資料保存期限有較長規定者，應依各該法令辦理。 商業會計法第 38 條：各項會計憑證，除應永久保存或有關未結會計事項者外，應於年度決算程序辦理終了後，至少保存五年。 商業使用電子方式處理會計資料辦法第 9 條：資料儲存媒體內所儲存之各項會計憑證，除應永久保存或有關未結會計事項者外，應於年度決算程序辦理終了後，至少保存五年。	
電子銀行交易	電子票證發行管理條例第 22 條：發行機構發行電子票證應保存持卡人交易帳款明細資料，並至少保存五年。前項明細資料應充分揭露交易日期、使用卡號、交易項目、交易金額、交易設備代號及幣別等項目。	金融監督管理委員會
線上購物交易	電子簽章法 電子簽章法施行細則 網路交易定型化契約應記載及不得記載事項指導原則	1. 電子商務主管機關：經濟部商業司 2. 其他目的事業主管機關：視線上購物商品所涉業

		務性質而定，如： (1) 盜版光碟：經濟部智慧財產局 (2) 仿冒商品：經濟部智慧財產局 (3) 個人資料：法務部 (4) 藥品：衛生署 (5) 保育類動物：農委會

（資料來源：本研究整理）

五、小結

綜上，各國現有之通訊或電信紀錄保存之法規，皆非針對「網路平台業者紀錄保存」之規範，且並未規範相關業者平時有保存相關紀錄之義務，均在執法機關認為有必要之情況下，在一定程序下要求業者開始保存通訊或電信紀錄，並對於保存期間有明確規範。我國目前未有專法規範網路平台業者紀錄保存之規定，本研究將網路平台業者區分為電子商務網站、電子金融平台、及電子訊息平台三類，再將該三類網路平台上的主要活動區分為線上申請帳號、線上遊戲虛擬寶物、遊戲幣轉移、網路下單、電子銀行交易、網路張貼文章、線上購物交易，並彙整這些活動所涉資料之相關法規及主管機關。

本研究認為修訂「第二類電信事業管理規則」第 27 條第 2 項內容，將現有規範第 1 款的語音單純轉售服務、第 2 款網路電話服務、第 3 款網際網路接取服務、及第 4 款虛擬行動網路服務，增加第 5 款網路平台服務。並將第三款網際網路接取服務包含撥接、非固接式非對稱性數位用戶迴路（ADSL）、纜線數據機、留言版(貼圖區或新聞討論群)、免費電子郵件信箱(網頁空間)、及電子郵件等項服務中，應屬網路平台服務的留言版(貼圖區或

新聞討論群)、免費電子郵件信箱(網頁空間)、及電子郵件等項服務，整合於第 5 款網路平台服務內。再於第 5 款對於前述本網路平台主要之服務與活動及應保存之紀錄項目與時間予以規範(如表 4-6)，當可解決目前對於「網路平台業者紀錄保存」規範不明之問題。其他有關線上遊戲虛擬寶物及遊戲幣轉移、網路下單、電子銀行交易、線上購物交易等網路活動，均各有業務主管機關如經濟部工業局、經濟部商業司與金融監督管理委員會，並皆有現行法規予以規範，無需大幅修增訂其他法規。建議由各相關主關機關本於職權檢視現行相關法規，做必要之局部修訂相關法規(如表 4-4)，以健全網路平台服務紀錄保存之規範。

表 4-6　第二類電信事業管理規則第 27 條修訂建議表

第二類電信事業管理規則第 27 條		
現行條文	**修訂建議**	**修訂理由**
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。	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。	本條第二項第三款規定之客體為「網際網路接取服務」，即表示有關留言版、貼圖區或新聞討論群、免費電子郵件信箱、網頁空間線上申請帳號之來源 IP 位址及當時系統時間、電子郵件通信紀錄等，網路接取服務業者（IAP）應予保留以供查詢，但前述之服務應屬網路平台服務，並非網際網路接取服務，建議將： （四）張貼於留言版、貼圖區或新聞討論群之內容

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。	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。~~	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。 等三款刪除，併入新增之第五款網路平台服務。原因為提供網際網路接取服務之 IAP，無從得知用戶連線上網後之動向，對於用戶在留言版、貼圖區、新聞討論群張貼內容，或線上申請電子信箱及網頁空間之帳號，IAP 並無法保存相關 IP、時間及電子郵件通信紀錄。因此，本條內容似乎部分與標題「網際網路接取服務」不相符，建議將（四）至（六）款等屬 IPP 之服務項目刪除。而各網路平台雖分屬不同主管機關（如：網路金融業務屬行政院金融監督管理委員會主管、電子商務屬經濟部商業司主管），但

（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。	四、虛擬行動網路服務通信紀錄應保存六個月。 五、網路平台服務： (一) 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六個月。 (二) 電子郵件通信紀錄（含用戶帳號、來源 IP 位址、當時系統時間）應保存六個月。 (三) 張貼於電子佈告欄、網路論壇、部落格或其他電子訊息平台之內容來源 IP 位址與當時系統時間應保存六個月。 (四) 即時訊息通信紀錄（含用戶帳號、來源 IP 位址、當時系統時間）應保存六個月。 (五) 免費電子郵件信箱及網頁空間線上申	營運態樣不同、業務性質差異，應不影響網路紀錄之保存工作，仍可集中於單一法規訂定紀錄保存規定，因此，建議於第 27 條第 3 項增列第 5 款「網路平台服務」，列出較詳盡之各種網路平台業者類型及其保存項目、保存期間，以更符合本研究之目標。 一、建議新增第二項第五款網路平台服務，參考第二項第一至第四項，將使用者在網路上常使用之服務，及應保存之紀錄項目與時間予以規範。 二、第二類電信事業管理規則第二十七條第三項係規範「網際網路接取服務」，然該項第三款內之留言版、貼圖區或新聞討論群，係屬於「網路平台服務」，並非「網際網路接取服務」。建議將原第二十七條第三項第三款（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

	請帳號時之來源 IP 位址及當時系統時間應保存六個月。 (六) 免費留言版、貼圖區、新聞討論群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。 (七) 免費電子佈告欄、網路論壇、部落格、即時訊息或其他電子訊息平台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。	三個月，移至第二類電信事業管理規則第二十七條新增之第二項第五款網路平台服務（一）:「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六個月。」。 三、第二類電信事業管理規則第二十七條第三項係規範「網際網路接取服務」，然該項第三款（六）「電子郵件」，係屬於「網路平台服務」，並非「網際網路接取服務」。建議將原第二十七條第三項第三款（六）規定：電子郵件通信紀錄應保存一個月，移至第二類電信事業管理規則第二十七條新增之第二項第五款網路平台服務（二）:「電子郵件通信紀錄（含用戶帳號、來源 IP 位址、當時系統時間）應保存六個月。」 四、比照第二類電信事業管理規則第二十七條第三項第三款（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」之規範，對於使用者於與類似留言版、貼圖區或新聞討論群之電子佈告欄、網路論壇、部落格等其他電子訊息平台張貼文章、圖片，亦應保存其來源 IP 位址、當時系統時間。建議第二類電信事業管理規則第二十七條新增之第二項第五款網路平台服務（三）:「張貼於電子佈告欄、網路論壇、部落格或其他電子訊息平台之內容來源 IP 位址與當時系統時間應保存六個月。」五、比照第二類電信事業管理規則第二十七條第三項第三款（六）「電子郵件通信紀錄應保存一個月」之規範，對於使用者於與電子郵件類似之即時訊息（如 MSN、Skype）等其他電子訊息平台傳送訊息，應保存其來源 IP 位址、當時系統時間。建議

		第二類電信事業管理規則第二十七條新增之第二項第五款網路平台服務（四）:「即時訊息通信紀錄（含用戶帳號、來源 IP 位址、當時系統時間）應保存六個月。」。 六、第二類電信事業管理規則第二十七條第三項係規範「網際網路接取服務」，然該項第四款內之免費電子郵件信箱及網頁空間，係屬於「網路平台服務」，並非「網際網路接取服務」。建議將原第二十七條第三項第三款（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，移至第二類電信事業管理規則第二十七條新增之第二項第五款網路平台服務（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。」 七、比照第二類電信事業

		管理規則第二十七條第三項第三款（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」之規定，使用者於留言版、貼圖區、新聞討論群，亦應保存使用者線上申請帳號時之來源 IP 位址及當時系統時間。建議建議第二類電信事業管理規則第二十七條增列第二項第五款網路平台服務（六）:「免費留言版、貼圖區、新聞討論群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。」 八、比照第二類電信事業管理規則第二十七條第三項第三款（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」之規定，使用者於類似之電子佈告欄、部落格、網路論壇、即時訊息（MSN、Skype 等）、臉

		書等電子訊息平台，亦應保存使用者線上申請帳號時之來源 IP 位址及當時系統時間。建議第二類電信事業管理規則第二十七條增列第二項第五款網路平台服務（七）:「免費電子佈告欄、網路論壇、部落格、即時訊息或其他電子訊息平台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。」 九、主管機關： (1) 電信事業主管機關:國家通訊傳播委員會。 (2) 其他事業主管機關:視網路張貼文章或傳送訊息所涉業務性質而定。

（資料來源：本研究整理）

第四節　保存紀錄之調閱程序、回覆時間及罰則

本節主要藉由我國現行法規，探討執法單位針對網路平台業者保存紀錄之調閱程序、要求之回覆時間以及相關罰則，但由於網際網路之盛行與普及未若有線及無線通訊行之有年，因此我國相關的法律規範係以通訊監察方面較為完整，本節即以通訊監察相關法規之執行程序、回覆時間與罰則作為引導，最後再總結本研究之建議方向。

一、我國現行法規

（一）通訊監察相關法規

針對通訊保障及監察法分別探討其執行、協助及罰則，關於通訊監察之執行，係以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法為之。在執行通訊監察時，除了經依法處置者外，並應維持通訊之暢通（通訊保障及監察法第十三條）。通訊監察之執行，除了依據法律規定另予處置者外，不得阻礙該通訊之暢通，以維護人民之基本權益。通訊保障及監察法主要立法保障之項目如下（第三條）[174]：

1、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。

2、郵件及書信。

3、言論及談話。

網際網路之盛行與普及未若有線及無線通訊行之有年，但其具有相似之本質及功能提供，因此執法單位在執行網路保存紀錄之調閱程序時，亦應確保維持通訊之暢通，並不得阻礙人民通訊之自由為首要目標。

在通訊監察之協助方面，依據通訊保障及監察法第十四條第二項之規定，電信事業及郵政機關（構）有協助執行通訊監察之義務，其通訊系統應具有配合執行監察之功能。協助執行通訊監察之電信事業、郵政機關（構）

[174] 徐智明，通訊監察之保障與規範，國立中正大學法律學研究所碩士論文，2004，頁61-63。

於執行後，得請求執行機關支付必要之費用。其費額由交通部會同內政部、國防部及法務部定之。按電信事業及郵政機關（構）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。

網路服務提供者包含網路接取提供者（Internet Access Provider）、網路平台提供者（Internet Platform Provider）與網路內容提供者（Internet Content Provider），在我國法制規範網路服務提供者協助偵查責任方面有：網路服務停止租用（與用戶簽約）、刪除權（服務條款明定有權刪除會員資訊）、刪除義務（原電腦網路內容分級處理辦法第 8 條，但法位階僅屬法規命令）、儲存、提供使用者資料及通信紀錄（電信法第 7 條、第二類電信事業管理規則第 27 條之 4、5、個人資料保護法第 20 條、電信事業處理有關機關（構）查詢電信使用者資料實施辦法第 3、4、5 條）、電信業者需有特定網路位址保存跨境連線通信紀錄 90 日之設備及能力（反恐怖行動法草案）、協助實施通訊監察（通訊保障及監察法第 14 條、細則第 21 條）[175]…等。但上述之相關法規僅止於闡明網路業者之協助偵查責任，並未詳列對於執法單位要求提供相關紀錄時，網路平台業者必須回覆之時間限制，若現行法規對此無任何約束力，將有礙於犯罪偵查之進行，甚至影響國家與人民之安危甚鉅。

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，則對於這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。

[175] 許慈健，網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究，國立交通大學管理學院在職專班碩士論文，2005，頁 109-116。

相較於網際網路服務提供者，除以電信設備為基礎之網際網路接取服務提供者（IAP）外，尚有第三代行動通信業者經營者、無線寬頻接取業務經營者等分類，可謂難以完全概括網路平台業者之範疇。此外，對於網路保存紀錄之儲存平台，亦因服務階段之不同而分存於不同平台，倘若執法單位需要某特定對象之保存紀錄，勢必要先確認其應接洽之平台業者，以避免因執法單位之誤投而有所延誤，進而影響案件偵辦之時效性。是故，網路保存紀錄之回覆時間，並不適宜以詳細之時數或日數訂定，建議可朝向多次通知後限期回覆仍不願配合，再處以連續罰鍰或撤銷其特許或許可，才能對於案件偵辦之時效性有實質上之助益。

（二）電信通信紀錄相關法規

國內於探討資訊隱私權保障與網路犯罪通訊監察法制之研究[176]，指出在刑事偵查中，透過通信紀錄的取得可以得知通訊工具的使用人曾經和哪些人進行通訊、通訊時間有多長，甚至透過訊號的來源還可以得知其所在地，因此具有相當的重要性。所謂「通信紀錄」，除了比較常見的電話通話紀錄外，在網路世界中，還包括網路撥接電話號碼、使用者本身的 IP 位置、所登入主機的 IP 位置、瀏覽的網頁及滯留時間等。

電信法第七條規定：「電信事業或其服務人員對於電信之有無及其內容，應嚴守秘密，退職人員，亦同。前項依法律規定查詢者不適用之。」因此，所謂「法律規定」的內容，便是重要的課題。過去我國實務上關於調閱電信通信紀錄的依據，係依照交通部電信總局所制定的「電信事業處理有關查詢電信通信紀錄實施辦法」來規範，本辦法性質上係行政機關自行制定的職權命令。由於本辦法只針對電話通話紀錄，並不適用於執法者向網路服務提供者要求查詢相關通訊資料，而且本辦法在位階上僅屬職權命令，不符合法律保留原則。因此，為符合行政程序法的要求，電信法第七條第二項遂增訂本辦法的法源依據[177]，另為配合網路世界的趨勢，擴大本辦法的適用範

[176] 陳信郎，資訊隱私權保障與網路犯罪通訊監察法制，國立政治大學法律學研究所碩士論文，2004，頁 99-102。

[177] 行政程序法第一百七十四條之一：「本法施行前，行政機關依中央法規標準法第七條訂

圍，本辦法乃於 2002 年 12 月 26 日修正為「電信事業處理有關機關查詢電信通信紀錄實施辦法」。依本辦法規定，所謂通信紀錄是指：電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼、通信日期、通信起迄時間等紀錄，並以電信系統設備性能可予提供者為原則。前項所稱電信號碼，係指電話號碼或用戶識別碼（第二條）。至於查詢程序的要件為：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，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、聯絡人、聯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（第三條）。

由上可知，我國有關通信紀錄的取得形式上雖以法規命令的方式，符合了法律保留原則的要求，並就可查詢的機關、查詢要件以及查詢應符合的程序有所規定。但對於相關資料的查詢並沒有一個機關加以監控，也沒有一個較嚴密的審查標準，由於政府對於電信業者有許可執照與管理監督的權力，因此只要執法者依上述程序提出查詢要求，電信業者便會給予相關電信紀錄。

（三）調閱電信使用者個人資料相關法規

關於調閱電信使用者個人資料之相關法規，在申請電信服務之際，電信業者都會要求申請人提供個人資料，其中包括了姓名、住址乃至於身份證統一編號、職業、財務資料等等不一而足，這些資料對於執法者進行刑事偵查作為時具有一定的價值，因為在刑事偵查的過程中，單純取得特定的電話號

定之命令，須以法律規定或以法律明列其授權依據者，應於本法施行後二年內，以法律規定或以法律明列其授權依據後修正或訂定；逾期失效。」

碼、IP 位址乃至於通話紀錄，都只能知道所使用的通訊工具，尚未能鎖定通訊工具的使用者，因此，除了電話號碼等相關通訊工具的號碼外，必須和這些工具的所有人或使用人身份識別相結合，才是可利用的資訊。

實務上犯罪偵查機關向電信業者要求提供使用者的基本資料，係依據「電信事業處理有關機關（構）查詢電信使用者資料實施辦法」。本辦法原為交通部電信總局所制定的職權命令，但與「電信事業處理有關機關查詢電信通信紀錄實施辦法」一樣，配合行政程序法的要求，於電信法第七條第二項增訂其法源依據。依本辦法，有權調閱使用者資料的機關如下（第三條）：

１、司法機關、監察機關或治安機關因偵查犯罪或調查證據所需者。

２、其他政府機關因執行公權力所需者。

３、與公眾生命安全有關之機關（構）為緊急救助所需者。

而所謂使用者資料，指電信使用者姓名或名稱、身份證統一編號、地址、電信號碼等資料，並以用戶申請各項電信業務所填列之資料為限。前項所稱電信號碼，係指電話號碼或用戶識別碼（第四條）。查詢的程序為：有關機關（構）查詢使用者資料應備正式公文或電信使用者資料查詢單，載明需查詢之電信號碼或姓名及其身份證統一編號、電信服務種類、法律依據、案由說明、查詢案號、資料用途、查詢機關（構）、機關（構）主管、聯絡人、聯絡電話或傳真機號碼、機關（構）加蓋印信及其首長署名、職章等，送該電信使用者所屬電信事業指定之受理單位辦理。對於案由特殊、情況緊急之查詢，得由法官、檢察官或查詢機關（構）首長或經其授權之主管署名並加蓋職章及聯絡人之資料，視同機關（構）正式公文書先傳真之，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使用者資料查詢單正本。前二項之查詢，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使用者資料查詢單正本（第五條）[178]。

本辦法與取得通信紀錄一樣，性質上都僅屬法規命令，而且對於調閱個

[178] 陳信郎，資訊隱私權保障與網路犯罪通訊監察法制，國立政治大學法律學研究所碩士論文，2004，頁 102-103。

人資料缺乏一個較嚴密的審查標準，僅籠統的規定因偵查犯罪或調查證據所需即可調閱，因此，我國有關個人資料保護的一般性法律——個人資料保護法即擔負起這樣的責任。該法的立法目的是為了規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用（第一條）。另要求對於個人資料之收集或利用，應尊重當事人之權益，對個人資料之蒐集、處理或利用，必須要有特定目的，且原則上只能在該特定目的必要範圍內為之（第六條）。就規範的內容而言，個人資料保護法主要可以分為二大部分，也就是對「公務機關」的規範以及對「非公務機關」的規範。依本法第三條第七、八款規定，所謂「公務機關」，指依法行使公權力之中央或地方機關，而「非公務機關」則羅列如下：

１、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。

２、醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業。

３、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。已經指定者，包括臺北市產物、人壽保險商業同業公會、期貨業、中華民國產物保險商業同業公會及中華民國人壽保險商業同業公會、財團法人臺灣更生保護會等。至於未被列舉，又沒有經指定者，就不在本法規範圍內。

電信業者在本法係屬於「非公務機關」，因此，對於個人資料的蒐集或處理，只有在其取得個人資料的特定目的範圍內才能使用，不得任意移作他用或任意給予他人。若執法者在沒有法律依據的情況下，向電信業者要求提供個人相關資料，電信業者不得給予（第十九條）。但是，在個人資料保護法第二十條另訂有除外規定，在有下列情形之一者，得為特定目的外之利用：

１、法律明文規定。

２、為增進公共利益。

３、為免除當事人之生命、身體、自由或財產上的急迫危險。

４、為防止他人權益之重大危害。

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

6、當事人書面同意者。

2 至 4 款之公益事項的除外規定看似合理，但內容仍過於模糊，且就調閱的程序亦未有規定，略嫌不足。最重要的是第六種事由，即經當事人書面同意，依我國電信業務營業規章範本中，皆加入「電信使用人同意在符合個人資料保護法第二十條及相關法令規定下，司法機關、監察機關或治安機關因偵查犯罪或調查證據所需者而查詢時，電信業者得提供個人資料」的條款，如此意味著只要司法機關、監察機關或治安機關因偵查犯罪或調查證據所需要而查詢，電信業者提供相關個人資料便不需要受到個人資料保護法的限制。

「電信事業處理有關機關（構）查詢電信使用者資料實施辦法」雖規定可查詢的機關種類、查詢要件以及查詢程序，但是目前刑事訴訟法相關法規似乎沒有任何法律給予執法者查詢個人資料的查詢程序，因此，未來修法方向可在刑事訴訟法增訂相關規定，並就調閱個人資料規定核發機關（法官或及於檢察官）及審查標準（比照搜索、扣押或較寬鬆的標準）為制定方向[179]。

（四）調閱電子郵件相關法規

監聽特定 E-mail 帳號的目的有二，一為藉由特定郵件的通聯紀錄，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份；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。

1、調閱特定 E-mail 帳號使用者身份資料[180]

由於檢警調單位監聽目的在瞭解犯罪嫌疑人的身份資料，目前實務上主要是透過「電信事業處理有關機關查詢電信通信紀錄實施辦法」，由檢警調單位出具公文向網路服務業者調取特定電子郵件的通信號碼，即電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼、通信日期、

[179] 陳信郎，資訊隱私權保障與網路犯罪通訊監察法制，國立政治大學法律學研究所碩士論文，2004，頁 103-105。

[180] 陳信郎，資訊隱私權保障與網路犯罪通訊監察法制，國立政治大學法律學研究所碩士論文，2004，頁 108-109。

通信起迄時間等紀錄。另外，亦可依「電信事業處理有關機關（構）查詢電信使用者資料實施辦法」的規定，向網路服務業者調閱特定 E-mail 帳號使用者的身份資料。不過，上開通信紀錄係以電信系統設備可予提供者為原則，因此若網路服務業者未儲存通信紀錄時，則無法調閱。

２、監看特定 E-mail 郵件內容[181]

若檢警調單位需要監看特定郵件內容時，由於涉及「截收」及「開拆」通訊內容，則必須符合通訊保障及監察法的規定，先向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。但儲存於執法人員電腦中的電子郵件，並無進行加密，僅係透過執法人員進入電腦的帳號及密碼加以保護。

３、未經閱讀的 E-mail 之調閱[182]

若電磁紀錄未經犯罪嫌疑人開啟或瀏覽，且現在網路服務業者持有中時（如 webmail 尚未讀取）者，雖然該通訊形式上已經存在，然而犯罪嫌疑人既未讀取，如檢警調單位在讀取前即向網路服務業者調閱時，實質上仍應認為屬於即時通訊的截取，而應適用通訊保障及監察法規定。此由我國通訊保障及監察法第三條將利用電信設備「儲存」符號、文字、影像、聲音或其他信息之有線及無線電信納入本法所保障的「通訊」範圍（第三條第一項第一款），因此，有關未經讀取且現在網路服務提供業者持有之網路儲存資料的取得，即應適用通訊保障及監察法之規定，始為正確[183]。其原因乃是多數網

[181] 陳信郎，資訊隱私權保障與網路犯罪通訊監察法制，國立政治大學法律學研究所碩士論文，2004，頁 108-109。

[182] 陳信郎，資訊隱私權保障與網路犯罪通訊監察法制，國立政治大學法律學研究所碩士論文，2004，頁 113-114。

[183] 但有認為由於取得儲存資料係針對過去所發生通訊行為所作的監控，不需比照即時通訊適用通訊保障及監察法之規定，此時可適用刑事訴訟法第一百三十五條有關郵件扣押之規定，將電子郵件解釋為「文書」，而適用刑事訴訟法。惟刑事訴訟法第一百三十五條所稱之郵件文書，應係指具有實體性質之文書而言，除非儲存資料係儲存在特定磁片中而可

路儲存資料雖已儲存在網路服務提供業者的伺服器主機中，但使用者大多尚未開啟，為保障個人資訊隱私權，實有將此種類型比照即時通訊的截取，適用法律要件程序最為嚴格的通訊保障及監察法。

不過上述的看法並未為我國實務所採，對於未經閱讀的電子郵件，實務上仍與處理已經閱讀的電子郵件一樣，適用刑事訴訟法第一百三十五條第一項之規定，以搜索扣押方式為之。但這樣的做法忽略即時通訊的截取與搜索扣押之區分，使得通訊保障及監察法之規定形同具文。

二、小結

綜上所述，有權限向網路服務業者調閱保存紀錄之執法單位，包含司法機關、監察機關及治安機關，且於執行調閱程序時，應以維持網路服務及通訊之暢通為首要目標，針對所能要求調閱之保存紀錄，亦應以網路服務提供業者之系統設備所能提供者為限，但若因偵查犯罪與調查證據所需者，網路服務提供業者因協助執行所加裝之相關軟硬體設備，其必要之支出費用，在實施調閱程序結束後，自得向執行機關請求支付。

我國法制規範網路服務提供者有協助偵查之責任，包括儲存、提供使用者資料及通信紀錄之義務，但卻未明文規範調閱資料之回覆時間，參考通訊保障及監察法，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（第三十一條）。但反觀網路保存紀錄之儲存平台，因服務階段之不同而分存於不同平台，而網路相關犯罪之偵查作為，往往具有相當時效性之需求，因此若執法單位未待確認調閱資料之確切平台，即以網路服務提供者未即時回覆為理由，而處以罰鍰，則可預見相關業者之反彈與違背協助義務之情事。

由於政府對於電信業者有許可執照與管理監督的權力，故執法機關實施

為搜索扣押之客體外，倘若該網路儲存資料僅單純儲存於服務業務提供業者伺服器主機時，仍應適用通訊保障及監察法。

調閱保存紀錄時，若網路服務提供者違反其協助之義務時，應以明文限期提供為原則，若經通知限期遵行而仍未予以理會，或是未提出任何異議表明其非指定之保存紀錄儲存平台，自得準用通訊保障及監察法第三十一條相關罰則。此外，該法第五條第一項亦明文規定，本法適用於執行通訊監察之規定如下：「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。一、最輕本刑為三年以上有期徒刑之罪。二至十五、觸及刑法、貪污治罪條例、懲治走私條例、藥事法、證券交易法、期貨交易法、槍砲彈藥刀械管制條例、公職人員選舉罷免法、農會法、漁會法、兒童及少年性交易防制條例、洗錢防制法、組織犯罪防制條例及陸海空軍刑法等法規」，然網路相關犯罪不若通訊監察多涉及三年以上有期徒刑之刑事案件，是故，本研究建議於該法條中增列但書，若違法行為是以透過網路平台所完成，並觸及刑事案件成立之構成要件，經執法機關之判定足認有調閱保存紀錄之必要者，即符合網路紀錄調閱之要件。

至於網路保存紀錄之調閱程序，我國現行針對通訊監察、電信通信紀錄之調閱、調閱電信使用者個人資料以及調閱電子郵件等相關法令規範，均是以正式公文或專屬之查詢單，載明需要查詢之資料後，送交所屬電信事業指定之受理單位辦理。是故網路保存紀錄之調閱程序，亦得以正式公文及專屬之調閱單比照辦理，惟網路犯罪之偵查多具情況緊急與急迫性，因此為掌握時效性，應另得由法官、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，限於一定期限內提供保存紀錄，或是提出異議表明其非指定之保存紀錄儲存平台，否則即得準用通訊保障及監察法第三十一條處以罰鍰。

目前現行法制尚無法針對網路保存紀錄之調閱，施以較有強制力之令狀強制處分，乃由於相關法規主要是規定電信行政事項，並不適合就相關內容規範，未來，在有關保存紀錄的取得上，可以考慮由通訊保障及監察法或刑事訴訟法加以規定，包括核發網路保存紀錄的主體（法官或及於檢察官）、

審查程序（比照搜索、扣押或監聽抑或另立較寬鬆的審查標準）等。

第五章　結論與建議

第一節　結論

關於網路平台業者紀錄保存規範之議題，國內學者與相關研究均對修訂現有法規或制定專法提出不同之看法，主張制定專法者認為，網路服務多樣化無法適用電信法相關法規；電信法規範主體難謂其涵蓋網路平台提供者，直接修訂恐有適用上之疑慮；制定專法可符合憲法「法律保留原則」；統一架構網際網路法令，建立總則性質之規範，再就特殊市場行為另訂特別規範，始符合科技法律之性質；各相關主管機關若未進行整合而分別修訂主管規範，恐產生差異及困擾。另一方面，主張修法者則認為，許多電腦犯罪屬傳統犯罪類型，不因轉移至網路平台而改變其構成要件，故無必要動輒制定特別法；實體世界法律已有相當成熟度，對於網路虛擬世界之行為，目前仍以修訂現有法律以因應網路發展為宜；建議於刑事訴訟法或通訊保障及監察法中，針對通訊紀錄之取得訂出類似美國「電子通訊隱私權法」的規範；目前實務上查詢紀錄之依據僅為「法規命令」位階，建議於刑事訴訟法修訂，方可顧及隱私權及通訊秘密權；國內無單一網路主管機關，網路營運態樣複雜多變，制定專法可能趕不上變化，建議就各目的事業主管機關業務範圍內之網路新興行為，分別修訂現有法律或管理規則。

本研究認為，修訂現有法規之優點在於：可與時俱進，維持法之適應性，避免特別法多如牛毛之情況；從母法「電信法」之定義著手修訂，其他附屬法規即不需有過大幅度之修改；通保法之程序完備，調閱網路平台紀錄規範若直接套用，僅須修訂少部分條文即可，亦可提升法源位階。惟缺點為：須一併修訂多部法令；各相關主管機關各自修訂恐生標準不一、相互矛盾之情形；網路紀錄保存與提供事涉個人資料保護及隱私權侵害問題，部分相關法規位階不足；相關規範散見於不同法令中，易顯凌亂無章；網路平台紀錄與「通訊實質內容」侵犯人民隱私權之程度難以併論，同於「通訊保障及監察法」中規範恐不恰當。另一方面，制定專法有其優點：國內目前缺乏一套完整規範網路秩序專法，或可參考歐盟「個人通訊資料保存指令（Directive 2006/24/EC）」，且該資料保存委員會亦提出補充準則，規範詳盡而具整體

性，足以涵蓋網路平台業者紀錄保存之全數細節。惟缺點在於必須考量涉及多個主管機關中，制定專法後「何者為主管機關」之問題；加上網路營運態樣複雜多變，制定專法恐不及時代、科技的進步。

綜合上述分析，本研究提出採修法途徑之六大理由，包括：一昧制訂新法，將難以維持舊有法規之適應性；於電信法中增修「網路平台業者」定義，可降低附屬法規修改幅度；「通訊保障及監察法」程序規範完整，增訂網路紀錄查詢程序較易；成立修法統籌單位，解決不同主管機關問題；法規命令經明確授權，符合法律保留原則；修法集中兩大方向，對業者不致產生困擾。並且針對現有電信法、第二類電信事業管理規則、電信事業處理有關機關查詢電信通信紀錄實施辦法、電信事業處理有關機關（構）查詢電信使用者資料實施辦法、通訊保障及監察法、通訊保障及監察法施行細則等法令內容逐一檢視，列出建議修改之條文及理由，以作為日後修法之參考。

美國與歐盟針對電子通訊之法規已制訂及實行多年，直至 911 恐怖攻擊事件後，乃全面針對網際網路之使用與紀錄等規範有所訂定。而日本「刑事訴訟法」對於發動命令主體、適用對象、保存期間及保存項目等有較明確之規定。國外有關網際網路平台提供服務法規主要是以歐盟「個人通訊資料保存指令（Directive 2006/24/EC）」及日本「刑事訴訟法」相關規範較具參考價值。

我國目前現有法規已針對通訊監察、電信通信紀錄、電信使用者個人資料及電子郵件等內容，訂定相關規範。依據電信與通訊之同質性，本研究認為在電信法相關法條以增列定義之方式擴及網際網路的使用及紀錄保存，可補充並解決現有法規對於網際網路平台提供服務記錄保存規範不足之問題。

將網際網路平台提供服務納入「第二類電信事業管理規則」第 27 條，並明確規範網際網路平台提供服務者紀錄保存之規定，為解決目前「第二類電信事業管理規則」對於網際網路平台提供服務者紀錄保存規定未明之可行辦法。

我國於通訊保障及監察法之相關規範訂定完善，包括聲請通訊監察之程

序、通訊監察期間之規定以及相關罰則等，已供治安單位於偵辦案件所需時有法源依據，有鑑於此，本研究主要目的即是欲以修訂現有法規或是設立專法等方式，擬定網路通訊紀錄之調閱程序、回覆時間與罰則等具體規範。

參閱我國相關法令規範，網路保存紀錄之調閱程序，以「電信事業處理有關機關查詢電信通信紀錄實施辦法」第 3 條之規範最為明確適用，另外，「電信事業處理有關機關（構）查詢電信使用者資料實施辦法」第 5 條之規範，亦適用於查詢所調閱之網路保存紀錄的使用者資料之程序。而本研究已針對網路紀錄保存機制作說明，其具有分階段存取之特性，因此上述之調閱程序，建議應給予受調閱之機關（構）限期提出異議之權利，以表明其非該筆保存紀錄之存取者，否則在超過所限期間後即可採取必要處罰。

相關罰則之訂定，在以修訂現有法規為前提之考量下，本研究擬採「通訊保障及監察法」第 31 條之規範，因為對於治安單位偵辦案件之必要性與急迫性而論，通訊監察與網路保存紀錄之調閱，均具有提供偵查方向及突破案情之重要貢獻，故其適用相同程度之罰則並未有超乎比例原則的疑慮。在調閱程序之發動要件上，通訊監察之聲請要件顯然受該法之嚴格限定，但是因偵辦案件而需要調閱網路保存紀錄之犯罪行為可能較為輕微，若按照該法第 5 條之要件始得以申請調閱，勢必在偵查作為上將難以施展，故建議於該法條增列但書，惟應符合發動偵查之要件，且違法行為係透過網路平台為之者，即得進行調閱之程序。

第二節　研究建議

本研究為多方收集偵查實務單位與網路平台業者之意見，於研究期程中召開座談會，針對網路保存紀錄之議題進行討論，若以修訂現有法規為主要作法，將引致法規主管機關之爭議，且因應「個人資料保護法」之施行，為避免當事人主張依據該法而刪除犯罪人個資之情事發生，故建議亦可採取設立專法之方式加以規範，以保障網路保存紀錄之留存及執法機關之執法依據。

為使網路平台提供之紀錄能更符合實務上犯罪偵查之需求，而建議於電信法中明確定義「網際網路平台提供者」，通信紀錄之定義中亦加入 IP 位址及其他通信歷程，並要求相關電信系統設備應具有配合提供紀錄之足夠功能。但對第二類電信事業管理規則中，「向主管機關申請許可，經依法辦妥公司或商業登記，並取得許可執照」之適用對象限制不加修改，以免過度擴張公權力。對於網路平台使用者資料之查詢，建議於現有「電信事業處理有關機關（構）查詢電信使用者資料實施辦法」之使用者資料規定中，新增用戶申請電子郵件或網路帳號所填寫之資料，查詢資料項目亦新增電子郵件及 IP 位址二項，而查詢方式則沿用原條文，以公文送交為原則，緊急時得以檢察/警察機關首長電話或公文傳真為輔，足以適用，不需修改。

網路平台通信紀錄調閱期間之規定，雖建議於通訊保障及監察法中修訂，然紀錄調閱與通訊內容監察性質迥異，侵犯民眾隱私權之程度亦較輕微，故建議可不受原條文監察期間之限制，僅需在不逾越相關網路平台紀錄規範之保存期間範圍內即可。另外，取得網路平台紀錄之方法，非為該法規定之截收、監聽、錄音、錄影、攝影、開拆、檢查、影印其中之一，故建議增修「電磁紀錄調閱」一詞，以符合相關紀錄取得之方式。有關設備建置之要求，因取得方式及內涵不同，建議網際網路平台提供者不須設置通訊監察設備，惟對於通信紀錄之存取，仍應建置足夠性能之相關設備，以供司法機關依法令偵查調閱。

有關網路平台業者紀錄保存規範之議題，本研究採兩案並陳之做法，先提出採修法方式之六大理由，並針對現有電信法、第二類電信事業管理規

則、電信事業處理有關機關查詢電信通信紀錄實施辦法、電信事業處理有關機關（構）查詢電信使用者資料實施辦法、通訊保障及監察法、通訊保障及監察法施行細則等法令內容逐一檢視，列出建議修改之具體條文及理由；後再就制定專法部分，提出具體之建議法規名稱、條文內容及理由，惟國內尚無一專門的網路主管機關，故專法繫屬主管機關之問題，仍有待討論。

本研究參考日本刑事訟訴法第 197 條第 3 項之規定及我國通訊保障及監察法第 14 條第 4 項，修訂電信法第 2 條第 1 項第 8 款通信紀錄內容以涵蓋網際網路平台提供服務記錄保存所需資訊。另本研究引用「電腦網路內容分級處理辦法」（2012 年 6 月 13 日廢止）第 2 條對於網際網路平台提供者之定義，納入電信法第 11 條第 4 項將平台提供者納歸第二類電信事業管理，以便第二類電信事業管理規則、通訊保障及監察法等相關法規在修訂網路平台紀錄保存規範時，對於網際網路平台提供者之定義能有一明確之依據。為提升網路犯罪證據保全，本研究建議增訂電信法第 40-1 條，規範電信事業有關資通安全應辦理事項。電信法具體修法之建議如下：

１、電信法第 2 條第 1 項第 8 款通信紀錄

指電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼或 IP 位址、通信日期、通信起訖時間及其他通信歷程等紀錄，電信系統設備應具有配合提供紀錄之足夠功能。電信號碼係指電話號碼或用戶識別碼。

２、增列電信法第 2 條第 1 項第 9 款電腦網路服務提供者

指網際網路接取提供者、網際網路平台提供者及網際網路內容提供者。

３、電信法第 11 條第 4 項第二類電信事業指第一類電信事業以外之電信事業。

其中，網際網路平臺提供者指在網際網路上提供硬體儲存之空間、或利用網際網路建置網站提供資訊發佈及網頁連結服務功能者。

４、增訂電信法第 40-1 條：為確保電信事業系統設備、資料及網路之安全，保障民眾通信權益，並確保犯罪證據，規範電信事業應辦理資通安全事

項。

現行第二類電信事業管理規則第 27 條第二項第三款規定有關留言版、貼圖區或新聞討論群、免費電子郵件信箱、網頁空間線上申請帳號之來源 IP 位址及當時系統時間、電子郵件通信紀錄等，網際網路接取服務業者（IAP）應予保留以供查詢，然前述之服務應屬網路平台服務，並非網路接取服務，建議將第三款（四）、（五）、（六）移至新增之第五款網際網路平台提供服務，再於第五款對於前述本網路平台主要之服務與活動及應保存之紀錄項目與期間予以規範。具體修法之建議如下：

1、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六個月。

2、電子郵件通信紀錄（含用戶帳號、來源 IP 位址、當時系統時間）應保存六個月。

3、張貼於電子佈告欄、網路論壇、部落格或其他電子訊息平台之內容來源 IP 位址與當時系統時間應保存六個月。

4、即時訊息通信紀錄（含用戶帳號、來源 IP 位址、當時系統時間）應保存六個月。

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、免費留言版、貼圖區、新聞討論群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。

7、免費電子佈告欄、網路論壇、部落格、即時訊息或其他電子訊息平台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。

針對網路保存紀錄之調閱依據，載明有事實足認被告或犯罪嫌疑人之違法行為係透過網路平台為之者，得向平台提供者查詢之，而調閱程序則參考前述之實施辦法執行，回覆時間部分，以平台提供者之保存期限為界，保存期限內應予受理並即時提供，已逾保存期限以書面回覆說明之。若經通知限期遵行而仍未予以理會，或是未提出任何異議表明其非指定之保存紀錄儲存平台，自得準用原「通訊保障及監察法」第 31 條相關罰則，但既已設立專法劃分網路保存紀錄之調閱與通訊監察之法規，擬將原罰鍰額度減至 1/5，

且載明以影響犯罪偵查情形嚴重者為限，即賦予治安機關行政裁量之彈性空間，違反者得處以新台幣十萬元以上五十萬元以下罰鍰，以為罰則。

一、修法建議

根據第四章第二節本研究建議採取修法之理由，提出修法建議如下（加底線為新增條文，刪除部分加~~雙刪除線~~），其中電信法、第二類電信事業管理規則、電信事業處理有關機關查詢電信通信紀錄實施辦法、電信事業處理有關機關（構）查詢電信使用者資料實施辦法之主管機關為國家通訊傳播委員會；而通訊保障及監察法、通訊保障及監察法施行細則之主管機關為法務部。

（一）電信法

現行條文	修訂建議	修訂理由
第 2 條第 1 項第 8 款 通信紀錄：指電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼、通信日期、通信起訖時間等紀錄，並以電信系統設備性能可予提供者為原則。電信號碼係指電話號碼或用戶識別碼。	通信紀錄：指電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼或 IP 位址、通信日期、通信起訖時間及其他通信歷程等紀錄，電信系統設備應具有配合提供紀錄之足夠功能。~~並以電信系統設備性能可予提供者為原則。~~電信號碼係指電話號碼或用戶識別碼。	就犯罪偵查角度而言，通信紀錄若僅侷限於發信方、受信方之電信號碼、通信日期、起訖時間等紀錄，似乎有所不足，建議增列「發信方、受信方之 IP 位址」；並參考日本刑事訟訴法第 197 條第 3 項之規定，保存項目除了通信來源、目的、時間日期外，加入「其他通信歷程」乙項，以含括通信內容以外之相關 log 紀錄。 為避免業者以設備性能

		不足為由拒絕提供協助，後段之「以電信系統設備性能可予提供者為原則」部分參考國內通訊保障及監察法第14條第4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」，進一步訂出適用於網路平台業者建置紀錄保存設備之規範，以確保業者在硬體設備方面有足夠建置能力，確實達成保存網路相關紀錄之義務。
無	**<u>增列第2條第1項第9款</u>** <u>九、電腦網路服務提供者：指網際網路接取提供者、網際網路平臺提供者及網際網路內容提供者。</u>	為求網路服務提供者於電信法之適用更為清楚明確，建議在電信法中明列其定義，內容則參考前「電腦網路內容分級處理辦法」（2012年6月13日廢止）第2條對電腦網路服務提供者之定義。
第11條第4項 第二類電信事業指第一	第二類電信事業指第一類電信事業以外之電信	雖然「電腦網路分級處理辦法」業於2012年6

類電信事業以外之電信事業。	事業。其中，網際網路平臺提供者指在網際網路上提供硬體之儲存空間，或利用網際網路建置網站提供資訊發佈及網頁連結服務功能者。	月 13 日廢止，然「兒童及少年福利與權益保障法」第 46 條第 4 項之定義中「提供連線上網後」等字樣，恐有遭不當解釋而限縮為 IAP 之虞，相較之下，「電腦網路分級處理辦法」第 2 條之定義顯然較佳且適用範圍較大，故本研究建議採用該辦法對於「網際網路平臺提供者」之定義，並將其納歸第二類電信事業管理，以便第二類電信事業管理規則、通訊保障及監察法等相關法規在修訂網路平台紀錄保存規範時，對於網際網路平台提供者之定義能有一明確之依據。
第40-1條 為確保電信事業系統設備、資料及網路之安全，保障民眾通信權益，電信事業應辦理下列事項： 一、建立資通安全管理機制。		一、本條新增。 二、近年來由於網際網路蓬勃發展及電子商務之普及應用，電信事業利用其通訊系統，結合網際網路傳送訊息、影像或聲音。然網路之便利性，亦引發頻繁之資

二、建立資通安全防護及偵測設施。 三、建立資通安全聯防及資通安全事件之通報、處理、回報等資通安全應變措施。 四、使用經資通安全審驗之資通設備。 前項系統設備包括核心網路設備、傳輸網路設備、接取網路設備、網路管理系統設備及其他重要電信設備。 電信事業處理資通安全事件時，得要求用戶及使用人配合辦理資通安全有關措施；其屬重大資通安全事件者，必要時得暫停或終止服務之一部或全部。 前項之規定意旨，電信事業應以顯著方式載明於營業規章及服務契約。 電信事業資通安全管理機制之查核項目與程序、適用之驗證標準與範圍、資通安全之防護與偵測、聯防與應變、		安事件及日新月異之攻擊手法。我國政府機關（構）自民國九十年起已推動資訊安全管理制度，並獲致一定之成果。為達資通安全防護全面化，對民眾隱私保護影響重大之電信事業亦應建立資通安全管理機制，另為強化電信事業資通安全之防護能力，防禦日益頻繁之資安事件發生，電信事業應建立適當之資通安全防護及偵測設施，蒐集所屬網段遭受惡意程式或殭屍電腦之攻擊行為，以防堵任何資通安全之漏洞與弱點，降低資安所造成之威脅，並為架構我國整體資通基礎設施之資安防護網，爰訂定第一項。 三、說明系統設備之範圍，爰訂定第二項。 四、為即時應變資安事件，降低對整體網路之傷害，爰於第三項明定電信事業處理資通安全

重大資通安全事件範圍及其他應遵行事項之管理辦法，由主管機關定之。 主管機關為進行網際網路資通安全聯防，應建置及管理資通安全聯防應變系統。必要時，得指定專責機構建置及管理之。 第一項第四款資通設備應施檢驗項目及其資通安全檢測技術規範，由主管機關訂定公告之。 主管機關為資通設備安全檢測需要，應建置及管理資通安全測試樣本資料庫。必要時，得指定專責機構建置及管理之。 前項資通設備之審驗方式與程序、審驗證明之核發、換發、補發與廢止、審驗合格標籤之標貼、印鑄與使用，及審驗業務管理等事項之辦法，由主管機關定之。		事件，得要求使用電信人配合辦理有關措施，且遇重大資通安全事件發生時，得暫停或終止服務之一部或全部。 五、為使第三項之要求具有明確性，爰於第四項明定應載明於電信事業之營業規章及服務契約中，並應以顯著方式呈現。 六、第五項授權主管機關訂定管理辦法規範之。 七、為與政府、教育及學術等網路進行網際網路資通安全聯防，主管機關應建置及管理資通安全聯防應變系統，且本系統需要配置足夠之技術人員以對資通安全事件進行蒐集、分析、分享、匯入、審核、通報、回報等工作，並適時擴充系統功能，亟須由專責機構之專業技術人員協助維運，爰參照水污染防治法、空氣污染防制法、海洋污染防

		治法等規定，授權主管機關於必要時，得指定專責機構建置與管理本系統，爰於第六項明定之。 八、第七項授權主管機關訂定資通安全檢測技術規範。為提供檢測實驗室資通安全測試樣本，需建置測試樣本資料庫，考量該資料庫具高度敏感，並應隨時做樣本蒐集與更新，亟須由專責機構之專業技術人員協助維運，爰參照水污染防治法、空氣污染防制法、海洋污染防治法等規定，授權主管機關於必要時，得指定專責機構建置與管理本系統。 九、第八項授權主管機關訂定審驗辦法。

（二）第二類電信事業管理規則

現行條文	修訂建議	修訂理由
第 4 條第 1 項 申請經營第二類電信事業，應檢具申請書、事	原條文不變	常見之網際網路平台提供者類型如：FTP 站、網路論壇…等，並非均

業計畫書及其他相關規定文件，向主管機關申請許可，經依法辦妥公司或商業登記，並取得許可執照後，始得營業。		有商業登記，此「經營者」之條件限制恐將無法規範到部分網際網路平台提供者類型；然而，若不加條件限制，舉凡個人或企業、是否以營利為目的者（如：教育用之免費服務平台）皆涵蓋其中，要求其行使網路平台紀錄保存之義務，又有過度擴張公權力行使範圍之虞，必定會產生執行上之困難。因此，建議保留原有規範，要求「依法辦理公司或商業登記」之網際網路平台提供者於營利之同時，亦須擔負提供網路平台紀錄之義務。
第 27 條 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	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	本條第二項第三款規定之客體為「網際網路接取服務」，即表示有關留言版、貼圖區或新聞討論群、免費電子郵件信箱、網頁空間線上申請帳號之來源 IP 位址及當時系統時間、電子郵件通信紀錄等，網路接取

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	： 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~~	服務業者（IAP）應予保留以供查詢，但前述之服務應屬網際網路平台提供服務，並非網際網路接取服務，建議將： （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。 等三款刪除，併入新增之第五款網路平台服務。原因為提供網際網路接取服務之IAP，無從得知用戶連線上網後之動向，對於用戶在留言版、貼圖區、新聞討論群張貼內容，或線上申請電子信箱及網頁空間之帳號，IAP 並無法保存相關IP、時間及電子郵件通信紀錄。因此，

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。	~~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。 五、網際網路平台提供服務： （一）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六個月。 （二）電子郵件通信紀錄（含用戶帳號、來源IP位址、當時系統時間）應保存六個月。 （三）張貼於電子佈告欄、網路論壇、部落格或其他電子訊息平台之內容來源IP位址與當時系統時間應保存六個月。 （四）即時訊息通信紀錄（含用戶帳號、來源IP位址、當時系統時間）應保存六個月。 （五）免費電子郵件信	本條內容似乎部分與標題「網際網路接取服務」不相符，建議將（四）至（六）款等屬IPP之服務項目刪除。 而各網路平台雖分屬不同主管機關（如：網路金融業務屬行政院金融監督管理委員會主管、電子商務屬經濟部商業司主管），但營運態樣不同、業務性質差異，應不影響網路紀錄之保存工作，仍可集中於單一法規訂定紀錄保存規定，因此，建議於第27條第3項增列第5款「網際網路平台提供服務」，列出較詳盡之各種網際網路平台提供者類型及其保存項目、保存期間，以更符合本研究之目標。 一、建議新增第二項第五款網際網路平台提供服務，參考第二項第一至第四項，將使用者在網路上常使用之服務，及應保存之紀錄項目與

	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）免費留言版、貼圖區、新聞討論群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。 （七）免費電子佈告欄、網路論壇、部落格、即時訊息或其他電子訊息平台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。	時間予以規範。 二、第二類電信事業管理規則第二十七條第二項係規範「網際網路接取服務」，然該項第三款內之留言版、貼圖區或新聞討論群，係屬於「網路平台服務」，並非「網際網路接取服務」。建議將原第二十七條第二項第三款（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，移至第二類電信事業管理規則第二十七條新增之第二項第五款網路平台服務（一）:「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六個月。」。 三、第二類電信事業管理規則第二十七條第二項係規範「網際網路接取服務」，然該項第三款（六）「電子郵件」，係屬於「網路平台服務」，

		並非「網際網路接取服務」。建議將原第二十七條第二項第三款（六）規定：電子郵件通信紀錄應保存一個月，移至第二類電信事業管理規則第二十七條新增之第二項第五款網路平台服務（二):「電子郵件通信紀錄（含用戶帳號、來源 IP 位址、當時系統時間）應保存六個月。」 四、比照第二類電信事業管理規則第二十七條第二項第三款（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」之規範，對於使用者於與類似留言版、貼圖區或新聞討論群之電子佈告欄、網路論壇、部落格等其他電子訊息平台張貼文章、圖片，亦應保存其來源 IP 位址、當時系統時間。建議第二類電信事業管理規則第二十七

		條新增之第二項第五款網路平台服務（三）:「張貼於電子佈告欄、網路論壇、部落格或其他電子訊息平台之內容來源 IP 位址與當時系統時間應保存六個月。」 五、比照第二類電信事業管理規則第二十七條第二項第三款（六）「電子郵件通信紀錄應保存一個月」之規範，對於使用者於與電子郵件類似之即時訊息（如 MSN、Skype）等其他電子訊息平台傳送訊息，應保存其來源 IP 位址、當時系統時間。建議第二類電信事業管理規則第二十七條新增之第二項第五款網路平台服務（四）:「即時訊息通信紀錄（含用戶帳號、來源 IP 位址、當時系統時間）應保存六個月。」。 六、第二類電信事業管理規則第二十七條第二項係規範「網際網路接取服務」，然該項第四款

		內之免費電子郵件信箱及網頁空間，係屬於「網際網路平台提供服務」，並非「網際網路接取服務」。建議將原第二十七條第二項第三款（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，移至第二類電信事業管理規則第二十七條新增之第二項第五款網路平台服務（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。」 七、比照第二類電信事業管理規則第二十七條第二項第三款（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」之規定，使用者於留言版、貼圖區、新聞討論群，亦應保存使用者線

		上申請帳號時之來源 IP 位址及當時系統時間。建議建議第二類電信事業管理規則第二十七條增列第二項第五款網路平台服務（六）:「免費留言版、貼圖區、新聞討論群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。」 八、比照第二類電信事業管理規則第二十七條第二項第三款（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」之規定，使用者於類似之電子佈告欄、部落格、網路論壇、即時訊息（MSN、Skype 等）、臉書等電子訊息平台，亦應保存使用者線上申請帳號時之來源 IP 位址及當時系統時間。建議第二類電信事業管理規則第二十七條增列第二項第五款網路平台服務

		（七）:「免費電子佈告欄、網路論壇、部落格、即時訊息或其他電子訊息平台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。」 九、主管機關： （一）電信事業主管機關：國家通訊傳播委員會。 （二）其他事業主管機關：視網路張貼文章或傳送訊息所涉業務性質而定。

（三）電信事業處理有關機關查詢電信通信紀錄實施辦法

現行條文	修訂建議	修訂理由
第 2 條第 1 項 本辦法所稱通信紀錄，指電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼、通信日期、通信起迄時間等紀錄，並以電信系統設備性能可予提供者為原則。	本辦法所稱通信紀錄，指電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼或 IP 位址、通信日期、通信起訖時間及其他通信歷程等紀錄，電信系統設備應具有配合提供紀錄之足夠功能。~~並以電信系統設備性能可予提供者為原則~~	本條係引用電信法第 2 條第 1 項第 8 款「通信紀錄」之定義，其修訂亦應以電信法為標準，以求法規之一致性。

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	原條文不變	查詢網路保存紀錄援用電信事業處理有關機關查詢電信通信紀錄實施辦法之程序，以公文送交查詢為原則，緊急時得以檢察/警察機關首長電話或公文傳真為輔，並於三日內補具正式公文或調閱單正本。

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 有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，電信事業應書面回覆說明之。	原條文不變	網路保存紀錄之儲存平台，因服務階段之不同而分存於不同平台，若待執法單位確認調閱之確切平台則可能造成案件偵辦之延宕，是故，限期業者提供保存紀錄，或限期提出異議，否則準用違反協助監察義務之現行罰則。即限期各平台業者以提供為原則，若經通知限期遵行而仍未予以理會，或是未提出任何異議表明其非指定之保存紀錄儲存平台，自得準用通訊保障及監察法第三十一條相關罰則。

（四）電信事業處理有關機關（構）查詢電信使用者資料實施辦法

現行條文	修訂建議	修訂理由
第 4 條 本辦法所稱使用者資料	本辦法所稱使用者資料，指電信使用者姓名或	參考日本總務省發布之「訂定特定電信服務提

，指電信使用者姓名或名稱、身分證統一編號、地址、電信號碼等資料，並以用戶申請各項電信業務所填列之資料為限。 前項所稱電信號碼，係指電話號碼或用戶識別碼。	名稱、身分證統一編號、地址、電信號碼、電子郵件地址、IP 位址等資料，並以用戶申請各項電信業務、電子郵件或網路帳號所填列之資料為限。 前項所稱電信號碼，係指電話號碼或用戶識別碼。	供者之損害賠償責任之限制及發信者資訊揭露法第 4 條第 1 項省令」，明訂發信者資訊項目共計 7 項，包含：發信者及其他相關侵害資訊傳送者之姓名、住址、電子郵件地址、侵害資訊之相關 IP 位址、由相關行動電話末端裝置或 PHS 端末裝置連接網路服務發布侵害資訊之使用者識別符號、相關 SIM 卡識別碼中由該服務傳送者、經特定電信設備傳送侵害資訊之年、月、日及時間等。因為日本規範上述發信者資訊係由「特定電信服務提供者」揭露之，因此，提供的資料即為特定電信（如：BBS、留言版）使用者資料項目。考量現行在偵查網路犯罪工作上，除網路申裝時所填寫之用戶資料外，於線上申請註冊電子郵件或網路帳號時，亦會留下使用者資料，

		因此，建議於現行規範中針對缺漏之資料項目參考日本法進行補充修訂，以期規範能更臻完備。
第 5 條 有關機關（構）查詢使用者資料應備正式公文或電信使用者資料查詢單（格式如附件），載明需查詢之電信號碼或姓名及其身分證統一編號、電信服務種類、法律依據、案由說明、查詢案號、資料用途、查詢機關（構）、機關（構）主管、連絡人、連絡電話或傳真機號碼、機關（構）加蓋印信及其首長署名、職章等，送該電信使用者所屬電信事業指定之受理單位辦理。 對於案由特殊、情況緊急之查詢，得由法官、檢察官或查詢機關（構）之首長或經其授權之主管署名並加蓋職章及連絡人之資料，視同機	原條文不變	查詢網路使用者紀錄援用電信事業處理有關機關（構）查詢電信使用者資料實施辦法之程序，以公文送交查詢為原則，緊急時得以檢察/警察機關首長電話或公文傳真為輔，並於三日內補具正式公文或調閱單正本。

關（構）正式公文書先傳真之，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使用者資料查詢單正本。 前二項之查詢，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使用者資料查詢單正本。		

（五）通訊保障及監察法

現行條文	修訂建議	修訂理由
第 3 條第 1 項 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。	原條文不變	所謂電信設備因本法無相關定義，故本研究引自電信法第 2 條電信設備之定義「指電信所用之機械、器具、線路及其他相關設備」，其中所謂電信，依國內研究對日本電信事業法之解讀，復以我國電信法與日本法定義之雷同，推論網際網路通訊亦屬電信之一種。是故，偵查機關在調閱網路通信紀

		錄之適用上，該網路通信紀錄即在「通訊」涵蓋範圍內，暫無修訂之必要。
第 5 條第 1 項 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： 一、　最輕本刑為三年以上有期徒刑之罪。 （以下省略）	新增第 5 條第 1 項但書 調閱網路平台紀錄不受前項得發通訊監察書各款罪嫌之限制，惟應符合發動偵查之要件。	通訊保障及監察法第 5 條第 1 項以「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」為聲請通訊監察之構成要件。考量通訊保障及監察法之監察客體為「通訊內容」，而「網路通信紀錄」並非通訊內容，侵犯個人隱私之程度較輕，因此，可不必限定如此嚴格之犯罪類型，改以較寬鬆之要件取代之，亦即調閱網路通信紀錄不受本條第 1 項規範之限制，僅需符合一般發動偵查之要件（刑事訴訟法第 228 條），且係以網路平台為犯罪工具或犯罪場所者即可。 網路相關犯罪不若通訊

		監察多涉及三年以上有期徒刑之刑事案件，是故，建議於條文中增列但書以供執行機關評估符合網路通信紀錄調閱之要件與法源依據。
第 11 條第 1 項 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。	原條文不變	現行通訊監察書記載事項可適用於網路平台紀錄調閱，毋須修訂。惟監察方法部分，為符合司法警察機關調閱網路平台紀錄之需求，須連帶修訂第 13 條，以為適用。 註:「通訊監察管制資料登記簿」之「監察所得資料種類、數量」欄位，除現有之錄音帶、光碟、譯文及通聯（含簡訊）外，亦建議增加「網路通信紀錄（不含通信內容）」之選項，以配合第 13 條之修訂。
第 12 條第 1 項 第 5 條、第 6 條之通訊監察期間，每次不得逾三十日，第 7 條之通訊監察期間，每次不得逾	新增第 12 條第 4 項 調閱網路通信紀錄不受前項監察期間之限制，惟仍不得逾相關網路平台紀錄規範之保存期間。	網路犯罪類型廣泛且罪刑輕重不一，同樣為透過網路平台而實施之犯罪行為，刑責輕重卻有天壤之別。且實務上，

一年；其有繼續監察之必要者，應附具體理由，至遲於期間屆滿之二日前，提出聲請。		調閱網路平台紀錄之期間，視案情複雜程度及調閱目的而有所不同，短則 1 日，長則數個月，實在難以明確規範。因此，建議由偵查機關自行斟酌案情需要，於網路平台紀錄相關規範保存期間內申請之，而不受本條 30 日監察期間之限制。
第 13 條第 1 項 通訊監察以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法為之。但不得於私人住宅裝置竊聽器、錄影設備或其他監察器材。	通訊監察以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印、電磁紀錄調閱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。	實務上聲請網路監察時，監察方法多以「其他」類表示之，而本研究探討網路紀錄調閱，則須由網路平台提供者「儲存」相關通信紀錄，雖亦可採用原條文「其他類似之必要方法」作概括性之規定，但若增列「電磁紀錄調閱」1 項，可較為清楚明確，惟仍建議保留「其他類似之必要方法」之規定，以因應未來通訊技術之發展擴張。
第 31 條 有協助執行通訊監察義	原條文不變	網路通信紀錄之資料儲存，因服務階段之不同

務之電信事業及郵政機關（構），違反第十四條第二項之規定者，由交通部處以新台幣五十萬元以上二百五十萬元以下罰鍰；經通知限期遵行而仍不遵行者，按日連續處罰，並得撤銷其特許或許可。		而分存於不同平台，若待執法單位確認調閱之確切平台，則可能造成案件偵辦之延宕，是故，限期業者提供保存紀錄，或限期提出異議，否則準用違反協助監察義務之現行罰則。即限期各平台業者以提供為原則，若經通知限期遵行而仍未予以理會，或是未提出任何異議表明其非指定之保存紀錄儲存平台，自得準用通訊保障及監察法第三十一條相關罰則。

（六）通訊保障及監察法施行細則

現行條文	修訂建議	修訂理由
第 26 條第 1 項 本法第 14 條第 2 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、	本法第 14 條第 2 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	第 26 條第 6 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」。國家通訊傳播委員會於 2006 年 10 月 14 日公告第二類電信事業

電力及相關介接設備及本施行細則所定之其他配合事項。	本施行細則所定之其他配合事項。另網際網路平台提供者對於通信紀錄之存取，應建置足夠性能之相關設備，以供司法警察機關依法令偵查調閱。	須設置通訊監察設備之業務種類如下：一、非E.164用戶號碼網路電話服務（不含不透過業者VoIP Gateway直接於網際網路間互相傳輸語音者）。二、E.164用戶號碼網路電話服務。三、語音單純轉售服務。四、由網際網路接取服務經營者附加提供之電子郵件服務。換言之，網際網路平台提供者如未兼營上述服務，則無須設置通訊監察設備，自當亦無第21條第1項、第3項及第24條第3項之適用，惟針對網際網路平台提供者之服務項目，仍應規範其建置足夠性能之相關設備。

二、立法建議

如前述修法建議因修法時原法令之主管機關有意見，另可採訂立專法「網際網路平台提供者處理有關機關查詢通訊紀錄及使用者資料實施辦法」（具體條文如下），依據行政院「防治網路詐欺專案會議」於2010年9月21日提出網路犯罪防制對策之長期方案，要求各網路平臺業者保存帳戶相關資料至少六個月以上，建議由行政院召集相關部會研商，解決主管機關爭

議，唯此種方式有其缺點，詳見第四章第一節說明。

立法建議	立法理由
第 1 條（法源依據） 本辦法（以下簡稱本法）依通訊保障及監察法第十四條第二項及電信法第七條第二項規定訂定之。	建議配合增修通訊保障及監察法第十四條第二項： 電信事業、電腦網路服務提供者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。 建議配合修訂電信法第七條： 電信事業、電腦網路服務提供者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。 另建議配合增修電信法第二條第九款： 九、電腦網路服務提供者：指網際網路接取提供者、網際網路平台提供者及網際網路內容提供者。
第 2 條（名詞定義） 本法用詞定義如下： 一、 網際網路平台提供者(以下簡稱平台提供者)：指在網際網路上提供硬體之儲存空間、或利用網際網路建置網站提供資訊發佈	一、雖然「電腦網路分級處理辦法」業於 2012 年 6 月 13 日發布廢止，但「兒童及少年福利與權益保障法」第 46 條第 4 項定義中「提供連線上網後」之字樣，恐有遭不當解釋而限縮為 IAP 之虞，相

及網頁連結服務功能者。 二、 通訊：指利用網路平台設備發送、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。 三、 通訊紀錄：指網路平台使用者使用網路平台服務後，資訊系統所產生之發訊方、受訊方之 IP 位址、通訊日期、通訊起訖時間及其他通訊歷程等紀錄。 四、 使用者資料：指網路平台使用者姓名或名稱、身分證統一編號、地址、用戶識別碼、電子郵件地址、IP 位址等資料，並以用戶申請各項網路平台業務、電子郵件或網路帳號所填列之資料為限。	較之下，「電腦網路分級處理辦法」第 2 條之定義顯然較佳且適用範圍較大，故本研究仍引用該辦法之定義，以便本法規在訂立網路平台紀錄保存規範時，對於網際網路平台提供者之定義能有一明確之依據。 二、引用通訊保障及監察法第三條第十二項針對通訊之定義，另依國內研究對日本電信事業法之解讀，復以我國電信法與日本法定義之雷同，推論網際網路通訊亦屬電信之一種。是故，偵查機關在調閱網路通訊紀錄之適用上，該網路通訊紀錄即在「通訊」涵蓋範圍內。 三、參考電信法第二條第一項第十八款針對通信紀錄之定義，另就犯罪偵查角度而言，通訊紀錄若僅侷限於發訊方、受訊方之電信號碼、通訊日期、起訖時間等紀錄，似乎有所不足，建議增列「發訊方之 IP 位址」；並參考日本刑事訟訴法第 197 條第 3 項之規定，保存項目除了通訊來源、目的、時間日期外，加入「其他通訊歷程」乙項，以含括通訊內容以外之相關 log 紀錄。

	四、參考日本總務省發布之「訂定特定電信服務提供者之損害賠償責任之限制及發信者資訊揭露法第4條第1項省令」，明訂發信者資訊項目共計7項，包含：發信者及其他相關侵害資訊傳送者之姓名、住址、電子郵件地址、侵害資訊之相關IP位址、由相關行動電話末端裝置或PHS端末裝置連接網路服務發布侵害資訊之使用者識別符號、相關SIM卡識別碼中由該服務傳送者、經特定電信設備傳送侵害資訊之年、月、日及時間等。因為日本規範上述發信者資訊係由「特定電信服務提供者」揭露之，因此，提供的資料即為特定電信（如：BBS、留言版）使用者資料項目。考量現行在偵查網路犯罪工作上，除網路申裝時所填寫之用戶資料外，於線上申請註冊各項網路平台業務、電子郵件或網路帳號時，亦會留下使用者資料，因此，建議於現行規範中針對缺漏之資料項目參考日本法進行補充修訂，以期規範能更臻完備。
第3條（申請許可及登記） 申請經營網路平台事業，應檢具申請	常見之網路平臺提供者類型如：FTP站、網路論壇...等，並非均有商業登

書、事業計畫書及其他相關規定文件，向主管機關申請許可，經依法辦妥公司或商業登記，並取得許可執照後，始得營業。	記，此「經營者」之條件限制，恐將無法規範到部分網路平台業者類型；然而，若不加條件限制，舉凡個人或企業、是否以營利為目的者（如：教育用之免費服務平台）皆涵蓋其中，要求其行使網路平台紀錄保存之義務，又有過度擴張公權力行使範圍之虞，必定會產生執行上之困難。因此，建議參考第二類電信事業管理規則第四條第一項，要求「依法辦理公司或商業登記」之網路平台提供者於營利之同時，亦須擔負提供網路平台紀錄之義務。
第 4 條（查詢依據） 有事實足認被告或犯罪嫌疑人之違法行為係透過網路平台為之者，得向平台提供者查詢通訊紀錄。 平台提供者對於通訊紀錄及使用者資料之存取，應建置足夠性能之相關設備，以供司法警察機關依法令偵查調閱。 為確保網路平台系統設備、資料及網路之安全，保障民眾通信權益，平台提供者應辦理下列事項： 一、建立資通安全管理機制。 二、建立資通安全防護及偵測設施。 三、建立資通安全聯防及資通安全事件之通報、處理、回報等資通安全應	通訊保障及監察法第 5 條第 1 項以「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」為聲請通訊監察之構成要件。考量通訊保障及監察法之監察客體為「通訊內容」，而「網路通訊紀錄」並非通訊內容，侵犯個人隱私之程度較輕，且網路相關犯罪不若通訊監察多涉及三年以上有期徒刑之刑事案件，因此，可不必限定如此嚴格之犯罪類型，改以較寬鬆之要件取代之，亦即調閱網路通訊紀錄僅需符合一般發動偵查之要件（刑事訴訟法第 228 條），且係以網路平台為犯罪工

變措施。 四、使用經資通安全審驗之資通設備。 前項系統設備包括核心網路設備、傳輸網路設備、接取網路設備、網路管理系統設備及其他重要電信設備。 平台提供者處理資通安全事件時，得要求用戶及使用人配合辦理資通安全有關措施；其屬重大資通安全事件者，必要時得暫停或終止服務之一部或全部。 前項之規定意旨，平台提供者應以顯著方式載明於營業規章及服務契約。 平台提供者資通安全管理機制之查核項目與程序、適用之驗證標準與範圍、資通安全之防護與偵測、聯防與應變、重大資通安全事件範圍及其他應遵行事項之管理辦法，由主管機關定之。 主管機關為進行網際網路資通安全聯防，應建置及管理資通安全聯防應變系統。必要時，得指定專責機構建置及管理之。 第一項第四款資通設備應施檢驗項目及其資通安全檢測技術規範，由主管機關訂定公告之。主管機關為資通設備安全檢測需要，應建置及管理資通安全測試樣本資料庫。必要時，得指	具或犯罪場所者即可，以供執行機關評估符合網路通訊紀錄調閱之要件與法源依據。 通訊保障及監察法施行細則第 26 條第 6 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」。國家通訊傳播委員會於 2006 年 10 月 14 日公告第二類電信事業須設置通訊監察設備之業務種類如下：一、非 E.164 用戶號碼網路電話服務（不含不透過業者 VoIP Gateway 直接於網際網路間互相傳輸語音者）。二、E.164 用戶號碼網路電話服務。三、語音單純轉售服務。四、由網際網路接取服務經營者附加提供之電子郵件服務。換言之，網路平台業者如未兼營上述服務，則無須設置通訊監察設備，自當亦無第 21 條第 1 項、第 3 項及第 24 條第 3 項之適用，惟針對網路平台業者之服務項目，仍應規範其建置足夠性能之相關設備。 第三項立法理由如下[184]： 1、近年來由於網際網路蓬勃發展及電子商務之普及應用，平台提供者利用其通訊系統，結合網際網路傳送訊

[184]資料來源：國家通訊傳播委員會 101 年 7 月 30 日函報行政院審查電信法修正草案版本。

定專責機構建置及管理之。 前項資通設備之審驗方式與程序、審驗證明之核發、換發、補發與廢止、審驗合格標籤之標貼、印鑄與使用，及審驗業務管理等事項之辦法，由主管機關定之。	息、影像或聲音。然網路之便利性，亦引發頻繁之資安事件及日新月異之攻擊手法。我國政府機關（構）自民國九十年起已推動資訊安全管理制度，並獲致一定之成果。為達資通安全防護全面化，對民眾隱私保護影響重大之平台提供者亦應建立資通安全管理機制，另為強化平台提供者資通安全之防護能力，防禦日益頻繁之資安事件發生，平台提供者應建立適當之資通安全防護及偵測設施，蒐集所屬網段遭受惡意程式或殭屍電腦之攻擊行為，以防堵任何資通安全之漏洞與弱點，降低資安所造成之威脅，並為架構我國整體資通基礎設施之資安防護網，爰訂定第三項。 ２、說明系統設備之範圍，爰訂定第四項。 ３、為即時應變資安事件，降低對整體網路之傷害，爰於第五項明定平台提供者處理資通安全事件，得要求使用電信人配合辦理有關措施，且遇重大資通安全事件發生時，得暫停或終止服務之一部或全部。 ４、為使第五項之要求具有明確性，爰於第六項明定應載明於電信事業之營業規章及服務契約中，並應以顯著方式呈現。

	5、第七項授權主管機關訂定管理辦法規範之。 6、為與政府、教育及學術等網路進行網際網路資通安全聯防，主管機關應建置及管理資通安全聯防應變系統，且本系統需要配置足夠之技術人員以對資通安全事件進行蒐集、分析、分享、匯入、審核、通報、回報等工作，並適時擴充系統功能，亟須由專責機構之專業技術人員協助維運，爰參照水污染防治法、空氣污染防制法、海洋污染防治法等規定，授權主管機關於必要時，得指定專責機構建置與管理本系統，爰於第八項明定之。 7、第九項授權主管機關訂定資通安全檢測技術規範。為提供檢測實驗室資通安全測試樣本，需建置測試樣本資料庫，考量該資料庫具高度敏感，並應隨時做樣本蒐集與更新，亟須由專責機構之專業技術人員協助維運，爰參照水污染防治法、空氣污染防制法、海洋污染防治法等規定，授權主管機關於必要時，得指定專責機構建置與管理本系統。 8、第十項授權主管機關訂定審驗辦法。

第 5 條（保存項目及期間） 平台提供者對於調查或蒐集證據，並依法律程序查詢通訊之有無及其內容者，應提供之，惟不得逾相關通訊紀錄及使用者資料之規範保存期間。 平台提供者對於第一項通訊紀錄應至少保存期間如下： 一、使用者線上申請帳號：使用者線上申請帳號之來源 IP 位址、當時系統時間、認證之行動電話、電子郵件帳號，平台提供者應至少保存至服務終止後六個月。 二、電子訊息平台網站張貼（傳送）文章（訊息）：使用者帳號、來源 IP 位址、當時系統時間，應保存六個月。 三、線上購物交易：網路買賣用戶之帳號、交易代號、數量、來源 IP 位址、當時系統時間，應保存六個月。 四、線上遊戲虛擬寶物轉移：遊戲玩家轉移虛擬寶物或遊戲幣之遊戲歷程(轉出帳號、遊戲幣、數量、來源 IP 位址、當時系統時間、轉入帳號、遊戲幣、數量)，應保存六個月。 五、網路證券交易：委託人帳號、委託日期時間、證券種類、股數或面額、限價、有效期間、營業員代號、委託方式、來源 IP 位址、當時系統時間	一、各網路平台雖分屬不同主管機關（如：網路金融業務屬行政院金融監督管理委員會主管、電子商務屬經濟部商業司主管），但營運態樣不同、業務性質差異，應不影響網路紀錄之保存工作，仍可集中於單一法規訂定紀錄保存規定，建議將使用者在網路上常使用之服務，及應保存之紀錄項目與時間予以規範。 二、參考第二類電信事業管理規則第 27 條第 2 項第 4 款「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」，及歐洲理事會「個人通訊資料保存指令（Directive 2006/24/EC）」要求會員國應確保規範中所須保存之資料其保存期限至少六個月，但不得超過自通訊日期起之兩年。平台提供者應至少保存使用者線上申請帳號至服務終止後六個月；電子訊息平台網站張貼文章（含電子郵件、即時訊息等）及線上購物交易（含線上遊戲虛擬寶物轉移），應保存六個月。 三、依據「證券商帳表憑證保存年限表」、「網際網路等電子式交易型態交易資料保存規範」規定，網路證券交易紀錄應保存五年。

，應保存五年。 六、電子銀行交易：交易日期、使用卡號、交易項目、交易金額、交易設備代號、幣別、來源 IP 位址、當時系統時間，應保存五年。	四、依據「電子票證發行管理條例」規定，電子銀行交易應保存五年。
第 6 條（調閱程序） 有關機關查詢通訊紀錄、使用者資料應先考量其必要性、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通訊紀錄或使用者資料查詢單，載明需查詢之通訊紀錄種類、起迄時間、資料用途、使用者姓名及其身分證統一編號、法律依據、案由說明、查詢案號、查詢機關（構）、機關（構）主管、連絡人、連絡電話或傳真機號碼、機關（構）加蓋印信及其首長署名、職章等，送該平台提供者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通訊紀錄或使用者資料查詢單正本。 前項之查詢，經查詢機關與平台提供者雙方認證同意，得以經加密之電子郵件為之，該電子郵件並視同正式公	查詢網路通訊紀錄或使用者資料，援用「電信事業處理有關機關查詢電信通信紀錄實施辦法」第 3 條及「電信事業處理有關機關（構）查詢電信使用者資料實施辦法」第 5 條之程序，以公文送交查詢為原則，緊急時得以檢察/警察機關首長電話或公文傳真為輔，並於三日內補具正式公文或調閱單正本。

文或通訊紀錄或使用者資料查詢單正本。	
第 7 條（受理回覆） 有關機關查詢之通訊紀錄或使用者資料，於平台提供者之保存期限以內者，應予受理並即時提供；已逾網路平台資料保存期限，致無法提供者，平台提供者應書面回覆說明之。	本條規定平台提供者之配合義務，但網路通訊紀錄或使用者資料，因服務階段之不同而分別儲存於不同平台，若待執法單位確認調閱之確切平台，則可能造成案件偵辦之延宕，是故，限期業者提供保存紀錄，或限期提出異議，否則準用違反協助查詢義務之現行罰則。
第 8 條（罰責） 有協助執行查詢義務之平台提供者，違反第 7 條之規定情節嚴重者，處以新台幣十萬元以上五十萬元以下罰鍰；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。	即限期各平台提供者以提供為原則，若經通知限期遵行而仍未予以理會，或是未提出任何異議表明其非指定之保存紀錄儲存平台，自得準用通訊保障及監察法第 31 條相關罰則(罰鍰額度減至 1/5）。

附錄一　通訊保障及監察法（節錄）

修正日期　民國 96 年 07 月 11 日

第 1 條　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，特制定本法。

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。

第 3 條　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。

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 4 條　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。

第 5 條　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。

一、最輕本刑為三年以上有期徒刑之罪。

二、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、第一百零九條第一項、第三項、第四項、第一百二十一條第一項、第一百二十二條第三項、第一百三十一條第一項、第一百四十二條、第一百四十三條第一項、第一百四十四條、第一百四十五條、第二百零一條之一、第二百五十六條第一項、第三項、第二百五十七條第一項、第四項、第二百九十八條第二項、第三百條、第三百三十九條、第三百三十九條之三或第三百四十

六條之罪。

三、貪污治罪條例第十一條第一項、第二項之罪。

四、懲治走私條例第二條第一項、第三項或第三條之罪。

五、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。

六、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。

七、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。

八、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。

九、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。

十、農會法第四十七條之一或第四十七條之二之罪。

十一、漁會法第五十條之一或第五十條之二之罪。

十二、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。

十三、洗錢防制法第九條第一項、第二項之罪。

十四、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。

十五、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。

前項通訊監察書，偵查中由檢察官依司法警察機關聲請或依職權以書面記載第十一條之事項，並敘明理由、檢附相關文件，聲請該管法院核發；檢察官受理申請案件，應於二小時內核復。如案情複雜，得經檢察長同意延長二小時。法院於接獲檢察官核轉受理申請案件，應於二十四小時內核復。審判中由法官依職權核發。法官並得於通訊監察書上對執行人員為適當指示。

前項之聲請經法院駁回者，不得聲明不服。

執行機關應於執行監聽期間，至少作成一次以上之報告書，說明監聽行為之進行情形，以及有無繼續執行監聽之需要。法官依據經驗法則、論理法則自由心證判斷後，發現有不應繼續執行監聽之情狀時，應撤銷原核發之通訊監察書。

違反本條規定進行監聽行為情節重大者，所取得之內容或所衍生之證據，於司法偵查、審判或其他程序中，均不得採為證據。

第 6 條　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。

違反本條規定進行監聽行為情節重大者，所取得之內容或所衍生之證據，於司法偵查、審判或其他程序中，均不得採為證據。

第 7 條　為避免國家安全遭受危害，而有監察下列通訊，以蒐集外國勢力或境外敵對勢力情報之必要者，綜理國家情報工作機關首長得核發通訊監察書。

一、外國勢力、境外敵對勢力或其工作人員在境內之通訊。

二、外國勢力、境外敵對勢力或其工作人員跨境之通訊。

三、外國勢力、境外敵對勢力或其工作人員在境外之通訊。

前項各款通訊之受監察人在境內設有戶籍者，其通訊監察書之核發，應先經綜理國家情報工作機關所在地之高等法院專責法官同意。但情況急迫者不在此限。

前項但書情形，綜理國家情報工作機關應即將通訊監察書核發情形，通知綜理國家情報工作機關所在地之高等法院之專責法官補行同意；其未在四十八小時內獲得同意者，應即停止監察。

違反前二項規定進行監聽行為所取得之內容或所衍生之證據，於司法偵查、審判或其他程序中，均不得採為證據。

第 11 條　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。

前項第八款之執行機關，指蒐集通訊內容之機關。第九款之建置機關，指單純提供通訊監察軟硬體設備而未接觸通訊內容之機關。

核發通訊監察書之程序，不公開之。

第 12 條　第五條、第六條之通訊監察期間，每次不得逾三十日，第七條之通訊監察期間，每次不得逾一年；其有繼續監察之必要者，應附具體理由，至遲於期間屆滿之二日前，提出聲請。

第五條、第六條之通訊監察期間屆滿前，偵查中檢察官、審判中法官認已無監察之必要者，應即停止監察。

第七條之通訊監察期間屆滿前，綜理國家情報工作機關首長認已無監察之必要者，應即停止監察。

第 13 條　通訊監察以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印

或其他類似之必要方法為之。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。

第 14 條　通訊監察之執行機關及處所，得依聲請機關之聲請定之。法官依職權核發通訊監察書時，由核發人指定之；依第七條規定核發時，亦同。

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。

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；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。

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。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。

第 17 條　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。

通訊監察所得資料全部與監察目的無關者，執行機關應即報請檢察官、依職權核發通訊監察書之法官或綜理國家情報工作機關首長許可後銷燬之。

前二項之資料銷燬時，執行機關應紀錄該通訊監察事實，並報請檢察官、依職權核發通訊監察書之法官或綜理國家情報工作機關首長派員在場。

第 29 條　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。

第 30 條　第二十四條第一項、第二十五條第一項及第二十八條之罪，須告訴乃論。

第 31 條　有協助執行通訊監察義務之電信事業及郵政機關（構），違反第十四條第二項之規定者，由交通部處以新台幣五十萬元以上二百五十萬元以下罰鍰；經通知限期遵行而仍不遵行者，按日連續處罰，並得撤銷其特許或許可。

第 33 條　本法施行細則，由行政院會同司法院定之。

第 34 條　本法自公布日施行。

本法修正條文自公布後五個月施行。

附錄二　通訊保障及監察法施行細則（節錄）

修正日期　民國 96 年 12 月 11 日

第 1 條　本細則依通訊保障及監察法（以下簡稱本法）第三十三條規定訂定之。

第 2 條　本法第三條第一項第一款所稱有線及無線電信，包括電信事業所設公共通訊系統及專用電信。

本法第三條第一項第二款所稱郵件及書信，指信函、明信片、特製郵簡、新聞紙、雜誌、印刷物、盲人文件、小包、包裹或以電子處理或其他具有通信性質之文件或物品。

本法第三條第一項第三款所稱言論及談話，指人民非利用通訊設備所發表之言論或面對面之對話；其以手語或其他方式表達意思者，亦包括在內。

本法第三條第二項所稱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，應就客觀事實加以認定。

第 3 條　本法所稱司法警察機關，指內政部警政署與各直轄市、縣（市）警察局所屬分局或刑事警察大隊以上單位、法務部調查局與所屬各外勤調查處（站）、工作組以上單位、憲兵司令部與所屬各地區憲兵隊以上單位、行政院海岸巡防署與所屬偵防查緝隊、各海巡隊、各機動查緝隊以上單位及其他同級以上之司法警察機關。

第 20 條　台灣高等法院得建置通訊監察管理系統，供監督通訊監察之用。建置機關應設置能立即自動傳輸全部上線及下線資訊之設備，即時將全部上線及下線之資訊，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。但軍事審判官核發之通訊監察書及依本法第七條規定無須經法院同意之通訊監察案件不在此限。

第 21 條　電信事業為協助執行通訊監察，應將電信線路以專線接至建置機關監察機房。但專線不敷使用或無法在監察機房內實施時，執行機關得請求建置機關與電信事業協商後，派員進入電信機房附設之監錄場所執行。

執行機關依前項但書指派之人員，不得進入電信機房。

第一項發生專線不敷使用情形時，電信事業應依執行機關或建置機關之需求，儘速擴增軟、硬體設施。

第 26 條　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。

國家通訊傳播委員會應將本細則施行前經特許或許可設置完成之第一類電信事業之通訊系統及通訊網路等相關資料，提供予法務部調查局或內政部警政署評估其所需之通訊監察功能後，由法務部調查局或內政部警政署依第一類電信事業之業務及設備設置情形，向第一類電信事業提出需求；第一類電信事業應即依該需求，擬定所需軟硬體設備、建置時程及費用之建置計畫，與法務部調查局或內政部警政署協商確定後辦理建置。必要時，由國家通訊傳播委員會協助之。

第一類電信事業於本細則施行前已經同意籌設或許可之新設、新增或擴充通訊系統，於本細則施行時尚未完成籌設或建置者，於其通訊系統開始運作前，應依前項之規定擬定配合執行通訊監察所需軟硬體設備、建置時程及費用之建置計畫及辦理建置，並於其通訊系統開始運作時同時協助執行通訊監察。本細則施行前交通部已公告受理特許經營之第一類電信業務，其經核可籌設者，亦同。

第一類電信事業新設、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，該電信事業儘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。

前三項建置計畫是否具有配合通訊監察所需之功能發生爭執時，由國

家通訊傳播委員會認定並裁決之。第一類電信事業應即依裁決結果辦理。

第二類電信事業須設置通訊監察設備之業務種類，由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。

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。

附錄三　電信法（節錄）

修正日期　民國 96 年 07 月 11 日

第一章　總則

第一條　為健全電信發展，增進公共福利，保障通信安全及維護使用者權益，特制定本法；本法未規定者，依其他法律之規定。

第二條　本法用詞定義如下：

一、電信：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。

二、電信設備：指電信所用之機械、器具、線路及其他相關設備。

三、管線基礎設施：指為建設電信網路所需之架空、地下或水底線路、電信引進線、電信用戶設備線路、及各項電信傳輸線路所需之管道、人孔、手孔、塔臺、電桿、配線架、機房及其他附屬或相關設施。

四、電信服務：指利用電信設備所提供之通信服務。

五、電信事業：指經營電信服務供公眾使用之事業。

六、專用電信：指公私機構、團體或國民所設置，專供其本身業務使用之電信。

七、公設專用電信：指政府機關所設置之專用電信。

八、通信紀錄：指電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼、通信日期、通信起訖時間等紀錄，並以電信系統設備性能可予提供者為原則。電信號碼係指電話號碼或用戶識別碼。

第三條　電信事業之主管機關為交通部。

交通部為監督、輔導電信事業並辦理電信監理，設電信總局；其組織另以法律定之。

前項電信總局應訂定整體電信發展計畫，督導電信事業，促進資訊社會發展，以增進公共福利。

第八條　電信之內容及其發生之效果或影響，均由使用電信人負其責任。

以提供妨害公共秩序及善良風俗之電信內容為營業者，電信事業得停

止其使用。

擅自設置、張貼或噴漆有礙景觀之廣告物，並於廣告物上登載自己或他人之電話號碼或其他電信服務識別符號、號碼，作為廣告宣傳者，廣告物主管機關得通知電信事業者，停止提供該廣告物登載之電信服務。

第二章　電信事業之經營

第十一條　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。

前項電信機線設備指連接發信端與受信端之網路傳輸設備、與網路傳輸設備形成一體而設置之交換設備、以及二者之附屬設備。

第二類電信事業指第一類電信事業以外之電信事業。

第十七條　經營第二類電信事業，應向電信總局申請許可，經依法辦理公司或商業登記後，發給許可執照，始得營業。

第二類電信事業營業項目、技術規範與審驗項目、許可之方式、條件與程序、許可執照有效期間、營運之監督與管理及其他應遵行事項之管理規則，由交通部訂定之。

附錄四　第二類電信事業管理規則（節錄）

修正日期　民國 99 年 11 月 05 日

第 一 章　總則

第 1 條　本規則依電信法（以下簡稱本法）第十七條第二項規定訂定之。

第 2 條　本規則用詞定義如下：

一、經營者：指經主管機關許可並發給執照經營第二類電信事業者。

二、用戶：指與經營者訂定契約，使用該經營者提供之通信服務者。

三、使用者：指用戶及其他使用經營者提供之通信服務者。

四、第二類電信事業特殊業務：指經營語音單純轉售服務、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。

五、語音單純轉售服務：指經營者以租用電信事業之電路或頻寬連接公眾交換電信網路，提供國際或長途語音服務，或話務轉接服務。

六、網路電話服務：指經營者透過網際網路傳送與接收所提供之語音服務。

七、E.164 用戶號碼網路電話服務：指依國際電信聯合會對電信號碼編定規格書之編號，經營者可利用 E.164 用戶號碼提供之網路電話服務。

八、非 E.164 用戶號碼網路電話服務：指經營者未利用 E.164 用戶號碼所提供之網路電話服務。

九、第二類電信事業一般業務：指第四款以外之第二類電信事業業務。

十、公司內部網路通信服務：指經營者以租用第一類電信事業之電路，並設置節點構成網路，以提供用戶作公司之內部單位、分公司、分支機構及其關係企業間通信之服務。

十一、批發轉售服務：指經營者未租用電信事業之電路或頻寬，以批發方式承購或承租電信事業之電信服務後，並以自己名義向用戶或使用者提供電信服務。

十二、公用電話轉售服務：指經營者以承購或承租電信事業之電信服務，並設置以投幣、簽帳卡、信用卡或預付卡付費，供公眾使用電話之批發轉售服務。

十三、預付式電話卡轉售服務：指經營者以承購或承租電信事業之電信服務，提供使用者以經由國內撥接電信號碼或密碼構成通話之預付式批發轉售服務。

十四、行動網路業務經營者：指經主管機關特許並發給執照之行動電話業務經營者、第三代行動通信業務經營者、一九○○兆赫數位式低功率無線電話經營者及無線寬頻接取業務經營者。

十五、虛擬行動網路服務：指經營者經營行動轉售服務或行動轉售及加值服務。

十六、行動轉售服務：指經營者以批發方式承購或承租行動網路業務經營者之通信服務後，並以自己名義向用戶或使用者提供電信服務。

十七、行動轉售及加值服務：指經營者除經營行動轉售服務外，並設置加值服務之網路元件提供行動通信之加值服務。

經營前項第十七款服務者，如其提供之加值服務包含前項第四款所定之服務者，應另依本規則有關第二類電信事業特殊業務之規定辦理。

第 3 條　本規則之主管機關為國家通訊傳播委員會。

第 二 章　經營許可

第 4 條　申請經營第二類電信事業，應檢具申請書、事業計畫書及其他相關規定文件，向主管機關申請許可，經依法辦妥公司或商業登記，並取得許可執照後，始得營業。

前項申請書，應載明下列各款事項：

一、申請人之名稱及住所：其為法人者，並記載代表人之姓名及主事務所；其為獨資經營者，並記載出資人或負責人及所在地；其為合夥經營者，並記載執行業務之合夥人及所在地。

二、營業項目。

三、營業區域。

四、通訊型態。

五、電信設備概況。

第一項事業計畫書，應載明下列各款事項：

一、網路或系統架構圖、電信設備機房建設地點、各地點建設計畫之電信設備概況。

二、預定開始經營日期。

三、與國內電信事業合作者，以提供預付式電話卡轉售服務或公用電話轉售服務經營者，應檢具與該電信事業合作協議之相關文件。

四、申請經營虛擬行動網路服務者，應檢具與行動網路業務經營者合作協議之相關文件，協議文件內並應具體載明雙方配合通訊保障及監察法相關規定及確保提供第十六條之一第三項所定服務之合作內容。

五、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同意之通訊監察系統功能之建置計畫。

六、其他經主管機關指定之文件。

E.164 用戶號碼網路電話服務經營者得經營非 E.164 用戶號碼網路電話服務，且有關許可費、網路互連、號碼可攜、緊急電話服務之提供及其他相關義務均依經營 E.164 用戶號碼網路電話服務之規定辦理。

提供利用外國 E.164 用戶號碼之網路電話服務者，以 E.164 用戶號碼網路電話服務經營者為限。

E.164 用戶號碼網路電話服務經營者提供前項服務前，應檢具有關提供臺灣地區免費一一○及一一九緊急電話服務、使用外國 E.164 門號之用戶資料查核方式及配合臺灣地區通訊監察作業之文件，向主管機關申請核准後，始得提供服務。

第 5 條　申請經營第二類電信事業，應具備之文件不全或其記載內容不完備者，應於接獲主管機關通知補正之期限內補正，逾期不補正或補正而仍記載不完備者，不予受理。

第 23 條　經營公司內部網路通信服務者，應至少保存其用戶基本資料至契約終止後一年。

前項用戶基本資料，包括公司之內部單位、分公司、分支機構及其關

係企業之名稱與地址、公司內部關係證明文件、公司內部撥號計畫及用戶與業者網路連接之專線電路編號等。

如用戶之公司內部關係為其關係企業時，經營公司內部網路通信服務者，應檢具用戶名稱、地址及公司內部關係證明文件報請主管機關備查。

第 24 條　經營公司內部網路通信服務者，應登錄及保存連接網路內部節點之專線電路編號、相關路由表及通信紀錄資料。

前項連接網路內部節點之專線電路編號、相關路由表於經營期間內須持續保存，通話紀錄資料應至少保存六個月。

第 四 章　通信設備維運之管理

第 25 條　第二類電信事業特殊業務之經營者，應遴用符合規定資格之高級電信工程人員，負責及監督各項電信設備之施工、維護及運用。

第 26 條　經營者設置之電信設備，應符合主管機關所定之技術規範。

違反前項規定者，主管機關得限期命其改善或限制其使用。

第 27 條 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、國民身分證統一編號、第二證件號碼及住址等資料，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。用戶如為政府機關、公立學校及公營事業機構，得以該機關（構）公文書作為識別用戶身分之證明文件。

前項證件號碼，於外國人申請時，指護照號碼及護照外之其他足資辨認身分之證明文件證號；於法人申請時，指公司登記統一編號及代表人國民身分證統一編號；於自然人申請時，指身分證號及足資辨識身分之證明文件證號。

主管機關得限制經營者受理民眾以同一身分證統一編號申請電信服務之用戶號碼數。經營者應依主管機關公告之限制條件及執行方式辦理。

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。

第 27-1 條　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以預付卡或其他預付資費方式提供服務者，應每週複查其用戶資料，如有使用者已經啟用服務而無使用者資料之情事，經營者應暫停其通信。

前項規定，經營者應於其營業規章及服務契約內定之。

附錄五　電腦網路內容分級處理辦法
（101 年 6 月 13 日廢止）

第一條　本辦法依兒童及少年福利法第二十七條第三項規定訂定之。

第二條　本辦法用詞，定義如下：

一、電腦網路：指以連線方式擷取網站資訊之開放式應用網際網路。

二、電腦網路服務提供者：指網際網路接取提供者、網際網路平臺提供者及網際網路內容提供者。

三、網際網路接取提供者：指以專線、撥接等方式提供網際網路連線服務之業者。

四、網際網路平臺提供者（以下簡稱平臺提供者）：指在網際網路上提供硬體之儲存空間、或利用網際網路建置網站提供資訊發佈及網頁連結服務功能者。

五、網際網路內容提供者（以下簡稱內容提供者）：指實際提供網際網路網頁資訊內容者。

六、電腦網路分級服務機構：指受政府委託統籌網際網路內容分級運作之非營利性法人組織。

附錄六　兒童及少年福利與權益保障法（節錄）

修正日期　民國 100 年 11 月 30 日

本法 100.11.30　修正之第 25、26、90 條條文自公布三年後施行。

第 一 章　總則

第 1 條　為促進兒童及少年身心健全發展，保障其權益，增進其福利，特制定本法。

第 2 條　本法所稱兒童及少年，指未滿十八歲之人；所稱兒童，指未滿十二歲之人；所稱少年，指十二歲以上未滿十八歲之人。

第 3 條　父母或監護人對兒童及少年應負保護、教養之責任。對於主管機關、目的事業主管機關或兒童及少年福利機構、團體依本法所為之各項措施，應配合及協助之。

第 4 條　政府及公私立機構、團體應協助兒童及少年之父母、監護人或其他實際照顧兒童及少年之人，維護兒童及少年健康，促進其身心健全發展，對於需要保護、救助、輔導、治療、早期療育、身心障礙重建及其他特殊協助之兒童及少年，應提供所需服務及措施。

第 5 條　政府及公私立機構、團體處理兒童及少年相關事務時，應以兒童及少年之最佳利益為優先考量，並依其心智成熟程度權衡其意見；有關其保護及救助，並應優先處理。

兒童及少年之權益受到不法侵害時，政府應予適當之協助及保護。

第 6 條　本法所稱主管機關：在中央為內政部；在直轄市為直轄市政府；在縣（市）為縣（市）政府。

第 7 條　本法所定事項，主管機關及目的事業主管機關應就其權責範圍，針對兒童及少年之需要，尊重多元文化差異，主動規劃所需福利，對涉及相關機關之兒童及少年福利業務，應全力配合之。

主管機關及目的事業主管機關均應辦理兒童及少年安全維護及事故傷害防制措施；其權責劃分如下：

一、主管機關：主管兒童及少年福利政策之規劃、推動及監督等相關事宜。

二、衛生主管機關：主管婦幼衛生、生育保健、發展遲緩兒童早期醫療、兒童及少年身心健康、醫療、復健及健康保險等相關事宜。

三、教育主管機關：主管兒童及少年教育及其經費之補助、特殊教育、幼稚教育、安全教育、家庭教育、中介教育、職涯教育、休閒教育、性別平等教育、社會教育、兒童及少年就學權益之維護及兒童課後照顧服務等相關事宜。

四、勞工主管機關：主管年滿十五歲或國民中學畢業少年之職業訓練、就業準備、就業服務及勞動條件維護等相關事宜。

五、建設、工務、消防主管機關：主管兒童及少年福利機構建築物管理、公共設施、公共安全、建築物環境、消防安全管理、遊樂設施等相關事宜。

六、警政主管機關：主管兒童及少年人身安全之維護及觸法預防、失蹤兒童及少年、無依兒童及少年之父母或監護人之協尋等相關事宜。

七、法務主管機關：主管兒童及少年觸法預防、矯正與犯罪被害人保護等相關事宜。

八、交通主管機關：主管兒童及少年交通安全、幼童專用車檢驗等相關事宜。

九、新聞主管機關：主管兒童及少年閱聽權益之維護、出版品及錄影節目帶分級等相關事宜。

十、通訊傳播主管機關：主管兒童及少年通訊傳播視聽權益之維護、內容分級之規劃及推動等相關事宜。

十一、戶政主管機關：主管兒童及少年身分資料及戶籍等相關事宜。

十二、財政主管機關：主管兒童及少年福利機構稅捐之減免等相關事宜。

十三、金融主管機關：主管金融機構對兒童及少年提供財產信託服務之規劃、推動及監督等相關事宜。

十四、經濟主管機關：主管兒童及少年相關商品與非機械遊樂設施標準之建立及遊戲軟體分級等相關事宜。

十五、體育主管機關：主管兒童及少年體育活動等相關事宜。

十六、文化主管機關：主管兒童及少年藝文活動等相關事宜。

十七、其他兒童及少年福利措施，由相關目的事業主管機關依職權辦理。

第 46 條　為防止兒童及少年接觸有害其身心發展之網際網路內容，由通訊傳播主管機關召集各目的事業主管機關委託民間團體成立內容防護機構，並辦理下列事項：

一、兒童及少年使用網際網路行為觀察。

二、申訴機制之建立及執行。

三、內容分級制度之推動及檢討。

四、過濾軟體之建立及推動。

五、兒童及少年上網安全教育宣導。

六、推動網際網路平臺提供者建立自律機制。

七、其他防護機制之建立及推動。

網際網路平臺提供者應依前項防護機制，訂定自律規範採取明確可行防護措施；未訂定自律規範者，應依相關公（協）會所定自律規範採取必要措施。

網際網路平臺提供者經目的事業主管機關告知網際網路內容有害兒童及少年身心健康或違反前項規定未採取明確可行防護措施者，應為限制兒童及少年接取、瀏覽之措施，或先行移除。

前三項所稱網際網路平臺提供者，指提供連線上網後各項網際網路平臺服務，包含在網際網路上提供儲存空間，或利用網際網路建置網站提供資訊、加值服務及網頁連結服務等功能者。

附錄七　個人資料保護法（節錄）

修正日期　民國 99 年 05 月 26 日

第 一 章　總則

第 1 條　為規範個人資料之蒐集、處理及利用，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。

第 2 條　本法用詞，定義如下：

一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

二、個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

三、蒐集：指以任何方式取得個人資料。

四、處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

五、利用：指將蒐集之個人資料為處理以外之使用。

六、國際傳輸：指將個人資料作跨國（境）之處理或利用。

七、公務機關：指依法行使公權力之中央或地方機關或行政法人。

八、非公務機關：指前款以外之自然人、法人或其他團體。

九、當事人：指個人資料之本人。

第 3 條　當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：

一、查詢或請求閱覽。

二、請求製給複製本。

三、請求補充或更正。

四、請求停止蒐集、處理或利用。

五、請求刪除。

第 4 條　受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於

本法適用範圍內，視同委託機關。

第 5 條　個人資料之蒐集、處理或利用，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，並應與蒐集之目的具有正當合理之關聯。

第 6 條　有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：

一、法律明文規定。

二、公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施。

三、當事人自行公開或其他已合法公開之個人資料。

四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序所為蒐集、處理或利用之個人資料。

前項第四款個人資料蒐集、處理或利用之範圍、程序及其他應遵行事項之辦法，由中央目的事業主管機關會同法務部定之。

第 7 條　第十五條第二款及第十九條第五款所稱書面同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之書面意思表示。

第十六條第七款、第二十條第一項第六款所稱書面同意，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之書面意思表示。

第 8 條　公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：

一、公務機關或非公務機關名稱。

二、蒐集之目的。

三、個人資料之類別。

四、個人資料利用之期間、地區、對象及方式。

五、當事人依第三條規定得行使之權利及方式。

六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

有下列情形之一者，得免為前項之告知：

一、依法律規定得免告知。

二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。

三、告知將妨害公務機關執行法定職務。

四、告知將妨害第三人之重大利益。

五、當事人明知應告知之內容。

第 9 條　公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項。

有下列情形之一者，得免為前項之告知：

一、有前條第二項所列各款情形之一。

二、當事人自行公開或其他已合法公開之個人資料。

三、不能向當事人或其法定代理人為告知。

四、基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。

五、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。

第一項之告知，得於首次對當事人為利用時併同為之。

第 10 條　公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限：

一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。

二、妨害公務機關執行法定職務。

三、妨害該蒐集機關或第三人之重大利益。

第 11 條　公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。

個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但因執行職務或業務所必須並註明其爭議或經當事人書面同意者，不在此限。

個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。

違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。

因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。

第 二 章　公務機關對個人資料之蒐集、處理及利用

第 17 條　公務機關應將下列事項公開於電腦網站，或以其他適當方式供公眾查閱；其有變更者，亦同：

一、個人資料檔案名稱。

二、保有機關名稱及聯絡方式。

三、個人資料檔案保有之依據及特定目的。

四、個人資料之類別。

附錄八　電信事業處理有關機關查詢電信通信紀錄實施辦法

修正日期　民國 99 年 07 月 07 日

第 1 條　本辦法依電信法第七條第二項規定訂定之。

第 2 條本辦法所稱通信紀錄，指電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼、通信日期、通信起迄時間等紀錄，並以電信系統設備性能可予提供者為原則。

前項所稱電信號碼，係指電話號碼或用戶識別碼。

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。

第 4 條　有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，電信事業應書面回覆說明之。

第 5 條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、行動通信通信紀錄：最近六個月以內。

前項期限，自受理查詢日回溯起算。

第二類電信事業通信紀錄之保存期限，依第二類電信事業管理規則之規定。

第 6 條　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 7 條　查詢費用依下列方式計收：

一、單向發信通信紀錄：以每頁新臺幣十元計收。

二、雙向通信紀錄：以每號每日新臺幣一百元計收，查詢期間不滿一日以一日計收。

前項查詢結果無資料者，仍需計費。

查詢費用，查詢機關應於帳單繳費期限內付清。

第 8 條　法官、軍事審判官、檢察官、軍事檢察官或監察院、審計部及所屬審計機關依法查詢電信通信紀錄者，查詢費用得予減收或免收。

第 9 條　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　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。

第 11 條　本辦法自發布日施行。

附錄九　電信事業處理有關機關（構）查詢電信使用者資料實施辦法

修正日期　民國 96 年 07 月 20 日

第一條　本辦法依電信法第七條第二項規定訂定之。

第二條　本辦法所稱電信事業，係指以經營電信服務供公眾使用，並經國家通訊傳播委員會發給特許執照或許可執照之事業。

第三條　下列情形得依法向電信事業查詢使用者資料：

一、司法機關、監察機關或治安機關因偵查犯罪或調查證據所需者。

二、其他政府機關因執行公權力所需者。

三、與公眾生命安全有關之機關（構）為緊急救助所需者。

依前項第一款、第二款規定查詢者，應敘明其法律依據。

第四條　本辦法所稱使用者資料，指電信使用者姓名或名稱、身分證統一編號、地址、電信號碼等資料，並以用戶申請各項電信業務所填列之資料為限。

前項所稱電信號碼，係指電話號碼或用戶識別碼。

第五條　有關機關（構）查詢使用者資料應備正式公文或電信使用者資料查詢單（格式如附件），載明需查詢之電信號碼或姓名及其身分證統一編號、電信服務種類、法律依據、案由說明、查詢案號、資料用途、查詢機關、機關（構）主管、連絡人、連絡電話或傳真機號碼、機關（構）加蓋印信及其首長署名、職章等，送該電信使用者所屬電信事業指定之受理單位辦理。

對於案由特殊、情況緊急之查詢，得由法官、檢察官或查詢機關（構）之首長或經其授權之主管署名並加蓋職章及連絡人之資料，視同機關（構）正式公文書先傳真之，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使用者資料查詢單正本。

前二項之查詢，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使用者資料查詢單正本。

第六條　為處理前條之查詢，各電信事業應指定受理單位，並設置專用之電話傳真機或電子媒體，供為受理與答覆查詢使用者資料之用。電信事業於查得使用者資料後，得以傳真機或電子媒體傳送至有關機關（構）。

各查詢機關（構）應事先以正式公文函告傳真機號碼或電子媒體帳號，查詢機關（構）不得以任何理由，要求將答覆資料傳送至另一地點，或要求臨時更換傳真機號碼或電子媒體帳號等。

第七條　查詢單中之某一電信使用者不屬受理查詢之電信事業或已逾電信事業資料保存期限，致無法提供者，該電信事業應於查詢單加註明「無資料」答覆之。

第八條　電信事業處理查詢使用者資料，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，得優先處理。

第九條　電信事業處理有關機關（構）查詢使用者資料時，得以每號新臺幣五元計收，按月結算之。法官、檢察官或監察院依法查詢電信使用者資料者，查詢費用得予減收或免收。

有關機關如已付費調閱通信紀錄，所併查詢使用者資料應予免收查詢費用。

第十條　有關機關（構）申請查詢之公文或查詢單，各電信事業受理單位應以專冊登記列管，並保存一年。

第十一條　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。

附錄十　第一類電信事業經營者名單暨其業務項目一覽表

第一類電信事業經營者名單暨其業務項目一覽表 製表日:99.10.19												
序號	經營者名單 （略）	業務項目										
		固定通信網路業務				行動通信網路業務					衛星固定通信業務	
		綜合網路業務	業務國際海纜電路出租	市內、國內長途陸纜電路出租	市內網路業務	無線寬頻接取業務	第三代行動通信業務	行動電話業務	無線電叫人業務	數位式低功率無線電話業務		

附錄十一　第二類電信事業經營者名單暨其許可服務範圍一覽表

第二類電信事業經營者名單暨其許可服務範圍一覽表																	
統計期間：至 2010/8/31 止																	
申請編號	執照號數	經營者名單（略）	服務項目														
			語音單純轉售服務	非E．164網路電話服務	E．164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務

附錄十二　美國電子通訊隱私法（Electronic Communications Privacy Act, ECPA）（節錄）

TITLE 18--CRIMES AND CRIMINAL PROCEDURE PART I--CRIMES

CHAPTER　119--WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

Sec. 2510. Definitions

As used in this chapter—

（1） ``wire communication'' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception （including the use of such connection in a switching station） furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

（4） ``intercept'' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.

（12）``electronic communication'' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--

（A） any wire or oral communication;

（B） any communication made through a tone-only paging device;

（C）any communication from a tracking device（as defined in section 3117 of this title）; or

（D） electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

（15） ``electronic communication service'' means any service which provides to users thereof the ability to send or receive wire or electronic communications;

（17） ``electronic storage'' means--

（A）any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

（B） any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

附錄十三　美國愛國者法(USA Patriot Act, USAPA)(節錄)

UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM （USA PATRIOT ACT） ACT OF 2001

TITLE I—ENHANCING DOMESTIC SECURITY AGAINST TERRORISM

Sec. 101. Counterterrorism fund.

Sec. 102. Sense of Congress condemning discrimination against Arab and Muslim Americans.

Sec. 103. Increased funding for the technical support center at the Federal Bureau of Investigation.

Sec. 104. Requests for military assistance to enforce prohibition in certain emergencies.

Sec. 105. Expansion of National Electronic Crime Task Force Initiative.

Sec. 106. Presidential authority.

TITLE II—ENHANCED SURVEILLANCE PROCEDURES

Sec. 201. Authority to intercept wire, oral, and electronic communications relating to terrorism.

Sec. 202. Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses.

Sec. 203. Authority to share criminal investigative information.

Sec. 204. Clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications.

Sec. 205. Employment of translators by the Federal Bureau of Investigation.

Sec. 206. Roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978.

Sec. 207. Duration of FISA surveillance of non-United States persons who are agents of a foreign power.

Sec. 208. Designation of judges.

Sec. 209. Seizure of voice-mail messages pursuant to warrants.

Sec. 210. Scope of subpoenas for records of electronic communications.

Sec. 211. Clarification of scope.

Sec. 212. Emergency disclosure of electronic communications to protect life and limb.

Sec. 213. Authority for delaying notice of the execution of a warrant.

Sec. 214. Pen register and trap and trace authority under FISA.

Sec. 215. Access to records and other items under the Foreign Intelligence Surveillance Act.

Sec. 216. Modification of authorities relating to use of pen registers and trap and trace devices.

Sec. 217. Interception of computer trespasser communications.

Sec. 218. Foreign intelligence information.

Sec. 219. Single-jurisdiction search warrants for terrorism.

Sec. 220. Nationwide service of search warrants for electronic evidence.

Sec. 221. Trade sanctions.

Sec. 222. Assistance to law enforcement agencies.

Sec. 223. Civil liability for certain unauthorized disclosures.

Sec. 224. Sunset.

Sec. 225. Immunity for compliance with FISA wiretap

附錄十四　美國愛國者改進與再授權法案（USA Patriot Improvement and Reauthorization Act, 2005）（節錄）

H.R. 3199 （109th）: USA PATRIOT Improvement and Reauthorization Act of 2005

Title I - USA PATRIOT Improvement and Reauthorization Act

Section 102 -

Repeals the sunset date for （thus making permanent） the surveillance provisions of the USA PATRIOT Act, with the following exceptions. Provides for a four-year extension （through December 31, 2009） of provisions: （1） granting roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978 （FISA） where the Court finds that the actions of the target may thwart the identification of a specified person; and （2） authorizing the Director of the Federal Bureau of Investigation （FBI） to apply for a court order requiring production of tangible things （including books, records, papers, and documents） for foreign intelligence and international terrorism investigations.

Section 105 -

Amends FISA to apply provisions governing the duration of an order for electronic surveillance or a physical search to surveillance targeted against a foreign power who is not a U.S. person. Limits to one year an order （or extension） for the use of pen registers and trap and trace devices where the applicant has certified that the information likely to be obtained is foreign intelligence information not concerning a U.S. person.

Section 106 -

Amends the FISA provisions governing orders for the production of tangible things to authorize the Director of the FBI to delegate to the Deputy Director or the Executive Assistant Director for National Security the authority to make an application for such an order involving library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person. Requires an application for such an order to:（1） include a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation; （2） include an enumeration of minimization procedures adopted by the Attorney General that are applicable to the retention and dissemination by the FBI of any tangible things produced; and（3）describe the tangible things to be produced with sufficient particularity to permit them to be fairly identified. Sets forth provisions concerning review by a panel of three judges of petitions filed by recipients challenging an order's legality. Requires the Attorney General to report to specified congressional committees annually on requests and order applications for the production of

tangible things and semiannually on orders for the production of library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, and medical records that would identify a person. （Sec. 106A） Directs the Inspector General of the Department of Justice （DOJ） to perform and report to Congress on a comprehensive audit of the effectiveness and use of the investigative authority provided to the FBI under FISA.

附錄十五　美國犯罪偵查通訊協助法（Communications Assistance for Law Enforcement Act, CALEA）（節錄）

Communications Assistance for Law Enforcement Act of 1994
Pub. L. No. 103-414, 108 Stat. 4279
One Hundred Third Congress of the United States of America
AT THE SECOND SESSION

An Act

To amend title 18, United States Code, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

TITLE 47-TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS
CHAPTER 9-INTERCEPTION OF DIGITAL AND OTHER COMMUNICATIONS
SUBCHAPTER I-INTERCEPTION OF DIGITAL AND OTHER COMMUNICATIONS

Sec. 102. ASSISTANCE CAPABILITY REQUIREMENTS.

（a）CAPABILITY REQUIREMENTS- Except as provided in subsections（b）,（c）, and（d）of this section and sections 108（a） and 109（b） and （d）, a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of—

（1） expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government;

（2） expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier—

（A）before, during, or immediately after the transmission of a wire or electronic communication（or at such later time as may be acceptable to the government）; and

（B） in a manner that allows it to be associated with the communication to which it pertains, except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices （as defined in section 3127 of title 18, United States Code）, such call-identifying information shall not include any information that may disclose the physical

location of the subscriber （except to the extent that the location may be determined from the telephone number）;

（3） delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier; and

（4） facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects—

（A）the privacy and security of communications and call-identifying information not authorized to be intercepted; and
（B） information regarding the government's interception of communications and access to call-identifying information.

（b） LIMITATIONS-

（1） DESIGN OF FEATURES AND SYSTEMS CONFIGURATIONS- This title does not authorize any law enforcement agency or officer--

（A） to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services; or
（B） to prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services.

（2） INFORMATION SERVICES; PRIVATE NETWORKS AND INTERCONNECTION SERVICES AND FACILITIES- The requirements of subsection （a） do not apply to—

（A） information services; or
（B） equipment, facilities, or services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers.

（3） ENCRYPTION- A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.

（c） EMERGENCY OR EXIGENT CIRCUMSTANCES- In emergency or exigent circumstances （including those described in sections 2518 （7） or （11）（b） and 3125 of

title 18, United States Code, and section 1805（e） of title 50 of such Code）, a carrier at its discretion may comply with subsection （a）（3） by allowing monitoring at its premises if that is the only means of accomplishing the interception or access.

（d） MOBILE SERVICE ASSISTANCE REQUIREMENTS- A telecommunications carrier that is a provider of commercial mobile service（as defined in section 332(d）of the Communications Act of 1934） offering a feature or service that allows subscribers to redirect, hand off, or assign their wire or electronic communications to another service area or another service provider or to utilize facilities in another service area or of another service provider shall ensure that, when the carrier that had been providing assistance for the interception of wire or electronic communications or access to call-identifying information pursuant to a court order or lawful authorization no longer has access to the content of such communications or call-identifying information within the service area in which interception has been occurring as a result of the subscriber's use of such a feature or service, information is made available to the government （before, during, or immediately after the transfer of such communications） identifying the provider of a wire or electronic communication service that has acquired access to the communications.

Sec . 103. NOTICES OF CAPACITY REQUIREMENTS.

（a） NOTICES OF MAXIMUM AND ACTUAL CAPACITY REQUIREMENTS-

（1） IN GENERAL- Not later than 1 year after the date of enactment of this title, after consulting with State and local law enforcement agencies, telecommunications carriers, providers of telecommunications support services, and manufacturers of telecommunications equipment, and after notice and comment, the Attorney General shall publish in the Federal Register and provide to appropriate telecommunications industry associations and standard-setting organizations--

（A） notice of the actual number of communication interceptions, pen registers, and trap and trace devices, representing a portion of the maximum capacity set forth under subparagraph （B）, that the Attorney General estimates that government agencies authorized to conduct electronic surveillance may conduct and use simultaneously by the date that is 4 years after the date of enactment of this title; and

（B） notice of the maximum capacity required to accommodate all of the communication interceptions, pen registers, and trap and trace devices that the Attorney General estimates that government agencies authorized to conduct electronic surveillance may conduct and use simultaneously after the date that is 4 years after the date of enactment of this title.

（2） BASIS OF NOTICES- The notices issued under paragraph （1）—

（A） may be based upon the type of equipment, type of service, number of subscribers, type or size or carrier, nature of service area, or any other measure; and

（B） shall identify, to the maximum extent practicable, the capacity required at specific geographic locations.

（b） COMPLIANCE WITH CAPACITY NOTICES-

（1） INITIAL CAPACITY- Within 3 years after the publication by the Attorney General of a notice of capacity requirements or within 4 years after the date of enactment of this title, whichever is longer, a telecommunications carrier shall, subject to subsection （e）, ensure that its systems are capable of--

（A） accommodating simultaneously the number of interceptions, pen registers, and trap and trace devices set forth in the notice under subsection （a）（1）（A）; and
（B） expanding to the maximum capacity set forth in the notice under subsection（a)(1)(B).

（2） EXPANSION TO MAXIMUM CAPACITY- After the date described in paragraph （1）, a telecommunications carrier shall, subject to subsection （e）, ensure that it can accommodate expeditiously any increase in the actual number of communication interceptions, pen registers, and trap and trace devices that authorized agencies may seek to conduct and use, up to the maximum capacity requirement set forth in the notice under subsection （a）（1）（B）.

（c） NOTICES OF INCREASED MAXIMUM CAPACITY REQUIREMENTS-

（1） NOTICE- The Attorney General shall periodically publish in the Federal Register, after notice and comment, notice of any necessary increases in the maximum capacity requirement set forth in the notice under subsection （a）（1）（B）.

（2） COMPLIANCE- Within 3 years after notice of increased maximum capacity requirements is published under paragraph（1）, or within such longer time period as the Attorney General may specify, a telecommunications carrier shall, subject to subsection （e）, ensure that its systems are capable of expanding to the increased maximum capacity set forth in the notice.

（d） CARRIER STATEMENT- Within 180 days after the publication by the Attorney General of a notice of capacity requirements pursuant to subsection （a） or （c）, a telecommunications carrier shall submit to the Attorney General a statement identifying any of its systems or services that do not have the capacity to accommodate simultaneously the number of interceptions, pen registers, and trap and trace devices set forth in the notice under such subsection.

（e） REIMBURSEMENT REQUIRED FOR COMPLIANCE- The Attorney General shall review the statements submitted under subsection （d） and may, subject to the availability of appropriations, agree to reimburse a telecommunications carrier for costs directly associated with modifications to attain such capacity requirement that are determined to be reasonable in accordance with section 109（e）. Until the Attorney General agrees to reimburse such carrier for such modification, such carrier shall be considered to be in compliance with the capacity notices under subsection （a） or （c）.

Sec . 108. PAYMENT OF COSTS OF TELECOMMUNICATIONS CARRIERS TO COMPLY WITH CAPABILITY REQUIREMENTS.

（a） EQUIPMENT, FACILITIES, AND SERVICES DEPLOYED ON OR BEFORE JANUARY 1, 1995- The Attorney General may, subject to the availability of appropriations, agree to pay telecommunications carriers for all reasonable costs directly associated with the modifications performed by carriers in connection with equipment, facilities, and services installed or deployed on or before January 1, 1995, to establish the capabilities necessary to comply with section 103.

（b） EQUIPMENT, FACILITIES, AND SERVICES DEPLOYED AFTER JANUARY 1, 1995-

（1） DETERMINATIONS OF REASONABLY ACHIEVABLE- The Commission, on petition from a telecommunications carrier or any other interested person, and after notice to the Attorney General, shall determine whether compliance with the assistance capability requirements of section 103 is reasonably achievable with respect to any equipment, facility, or service installed or deployed after January 1, 1995. The Commission shall make such determination within 1 year after the date such petition is filed. In making such determination, the Commission shall determine whether compliance would impose significant difficulty or expense on the carrier or on the users of the carrier's systems and shall consider the following factors:

（A） The effect on public safety and national security.

（B） The effect on rates for basic residential telephone service.

（C） The need to protect the privacy and security of communications not authorized to be intercepted.

（D） The need to achieve the capability assistance requirements of section 103 by cost-effective methods.

（E） The effect on the nature and cost of the equipment, facility, or service at issue.

（F） The effect on the operation of the equipment, facility, or service at issue.

（G） The policy of the United States to encourage the provision of new technologies and services to the public.

（H） The financial resources of the telecommunications carrier.

（I） The effect on competition in the provision of telecommunications services.

（J） The extent to which the design and development of the equipment, facility, or service was initiated before January 1, 1995.

（K） Such other factors as the Commission determines are appropriate.

（2） COMPENSATION- If compliance with the assistance capability requirements of section 103 is not reasonably achievable with respect to equipment, facilities, or services deployed after January 1, 1995—

（A） the Attorney General, on application of a telecommunications carrier, may agree, subject to the availability of appropriations, to pay the telecommunications carrier for the additional reasonable costs of making compliance with such assistance capability requirements reasonably achievable; and
（B） if the Attorney General does not agree to pay such costs, the telecommunications carrier shall be deemed to be in compliance with such capability requirements.

（c） ALLOCATION OF FUNDS FOR PAYMENT- The Attorney General shall allocate funds appropriated to carry out this title in accordance with law enforcement priorities determined by the Attorney General.

（d） FAILURE TO MAKE PAYMENT WITH RESPECT TO EQUIPMENT, FACILITIES, AND SERVICES DEPLOYED ON OR BEFORE JANUARY 1, 1995- If a carrier has requested payment in accordance with procedures promulgated pursuant to subsection （e）, and the Attorney General has not agreed to pay the telecommunications carrier for all reasonable costs directly associated with modifications necessary to bring any equipment, facility, or service deployed on or before January 1, 1995, into compliance with the assistance capability requirements of section 103, such equipment, facility, or service shall be considered to be in compliance with the assistance capability requirements of section 103 until the equipment, facility, or service is replaced or significantly upgraded or otherwise undergoes major modification.

（e） COST CONTROL REGULATIONS-

（1） IN GENERAL- The Attorney General shall, after notice and comment, establish regulations necessary to effectuate timely and cost-efficient payment to telecommunications carriers under this title, under chapters 119 and 121 of title 18, United States Code, and under the Foreign Intelligence Surveillance Act of 1978 （50 U.S.C. 1801 et seq.）.

（2） CONTENTS OF REGULATIONS- The Attorney General, after consultation with the Commission, shall prescribe regulations for purposes of determining reasonable costs under this title. Such regulations shall seek to minimize the cost to the Federal Government and shall--

（A） permit recovery from the Federal Government of--

（i） the direct costs of developing the modifications described in subsection （a）, of providing the capabilities requested under subsection（b）(2), or of providing the capacities requested under section 104（e）, but only to the extent that such costs have not been recovered from any other governmental or non-governmental entity;

（ii） the costs of training personnel in the use of such capabilities or capacities; and
（iii） the direct costs of deploying or installing such capabilities or capacities;

（B） in the case of any modification that may be used for any purpose other than lawfully-authorized electronic surveillance by a law enforcement agency of a government, permit recovery of only the incremental cost of making the modification suitable for such law enforcement purposes; and

（C） maintain the confidentiality of trade secrets.

（3） SUBMISSION OF CLAIMS- Such regulations shall require any telecommunications carrier that the Attorney General has agreed to pay for modifications pursuant to this section and that has installed or deployed such modification to submit to the Attorney General a claim for payment that contains or is accompanied by such information as the Attorney General may require.

附錄十六　美國外國情報監察法修正案（Foreign Intelligence Surveillance Act Amendments Act, 2008）(節錄)

Title I - Foreign Intelligence Surveillance

Section 101 -

Amends the Foreign Intelligence Surveillance Act of 1978 （FISA） to add a new title concerning additional procedures for acquiring the communications of certain persons outside the United States. Authorizes the Attorney General （AG） and Director of National Intelligence （DNI） to jointly authorize, for periods up to one year, the targeting（electronic surveillance）of persons located outside the United States in order to acquire foreign intelligence information, under specified limitations, including: （1） prohibiting an acquisition intentionally targeting a person reasonably believed to be outside the United States in order to acquire the communications of a specific person reasonably believed to be inside the United States; and（2）requiring the targeting to be conducted in a manner consistent with the fourth amendment to the Constitution. Requires:（1） certain targeting and minimization procedures to be followed;（2） the AG to adopt guidelines to ensure that such limitations and procedures are followed;（3） the AG to submit such guidelines to the congressional intelligence and judiciary committees and the Foreign Intelligence Surveillance Court （Court） for review; and （4） prior to such targeting, a certification by the AG and DNI as to the necessity of such targeting and that appropriate procedures and limitations will be followed. Allows the AG and DNI, if immediate targeting is determined to be required due to an emergency situation, to commence such targeting, but to submit the certification within seven days of such determination. Requires all certifications to be submitted to the Court for review. Authorizes the AG and DNI to direct an electronic communication service provider to: （1） immediately provide the government with all information, facilities, and assistance necessary to accomplish an acquisition; and（2）maintain under security procedures any records concerning such acquisition. Outlines legal procedures with respect to directive challenges, standards for review, enforcement, and appeals. Provides for: （1） judicial review of certifications and targeting and minimization procedures; and （2） review of Court rulings by the Foreign Intelligence Surveillance Court of Review （with certiorari to the Supreme Court）. Outlines conditions under which the AG and DNI may, through the Court: （1） replace a targeting acquisition already in effect before the enactment of this Act with an acquisition authorized under this Act; or （2） reauthorize a current acquisition under the procedures and guidelines of this Act. Requires Court maintenance and security of records and proceedings with respect to acquisition applications, orders, appeals, and determinations. Requires the AG and DNI,

at least every six months, to: （1） assess compliance with required targeting and minimization procedures and related guidelines; and （2） submit assessment results to the Court and the intelligence and judiciary committees. Authorizes inspectors general of the Department of Justice （DOJ） and elements of the intelligence community （IC） authorized to acquire foreign intelligence information to review their agency or element's compliance with such procedures and guidelines and provide review results to the AG, the DNI, and the intelligence and judiciary committees. Requires the head of any IC element conducting an acquisition of foreign intelligence information to annually review such acquisitions and report review results to the Court, the AG, the DNI, and the intelligence and judiciary committees. Provides Court jurisdiction for approving the targeting of a U.S. person located outside the United States when the acquisition of information is conducted inside the United States. Requires an application for such acquisition to be made by a federal officer （and approved by the AG）, and to contain certain requirements, including that the target is believed to be a foreign power or agent, officer, or employee of a foreign power. Provides for judicial review of a Court order approving such an acquisition. Makes approval orders effective for 90 days, with authorized 90-day renewals. Allows the AG to authorize an emergency acquisition of such a target under certain circumstances, including: （1） determining that an emergency exists; （2） informing a Court judge of such determination; and （3） applying within seven days for a Court order authorizing such surveillance. Provides similar Court jurisdiction and outlines similar procedures for the acquisition （and emergency acquisition） by an IC element of a physical search. Authorizes the: （1） joint applications and concurrent approvals of requests for acquisitions proposed to be conducted both inside and outside the United States; and （2） concurrent authorizations of electronic surveillance and physical searches. Directs the AG to report semiannually to the intelligence and judiciary committees concerning the implementation of acquisition requirements.

Section 102 -

States that, other than by express statutory authorization, FISA and the procedures of chapters 119 （Wire and Electronic Communications Interception and Interception of Oral Communications）, 121 （Stored Wire and Electronic Communications and Transactional Records Access）, and 206 （Pen Registers and Trap and Trace Devices） of the federal criminal code shall be the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted.

Section 103 -

Requires the AG to submit semiannually to the intelligence committees copies of any orders of the Court or the Foreign Intelligence Surveillance Court of Review that include

significant construction or interpretation of FISA, including any such orders issued during the five-year period before the enactment of this Act. Allows for the redaction of submitted materials for the protection of national security.

Section 104 -

Revises provisions concerning the application for, and issuance of, Court orders, including provisions concerning paperwork requirements and government officials who may authorize FISA actions.

Section 105 -

Allows the AG to authorize the emergency employment of electronic surveillance if the AG, among other things: （1） determines that an emergency exists; （2） informs a Court judge of such determination; and （3） applies for a Court order authorizing such surveillance.

Section 107 -

Provides similar revisions and outlines similar procedures as in sections 104 and 105 above for the emergency employment of physical searches.

Section 108 -

Requires the AG, after authorizing the installation and use of a pen register or trap and trace device on an emergency basis, to apply to the Court for an authorization order within seven days （current law requires 48 hours） after the emergency installation and use.

Section 109 -

Authorizes the Court to sit en banc when: （1） necessary to secure or maintain uniformity of Court decisions; or（2）the proceeding involves a question of exceptional importance.

Section 110 -

Authorizes the acquisition of foreign intelligence information from an entity not substantially composed of U.S. persons that is engaged in the international proliferation of weapons of mass destruction, or in activities in preparation therefor on behalf of a foreign power.

附錄十七　歐盟 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data（節錄）

CHAPTER III JUDICIAL REMEDIES, LIABILITY AND SANCTIONS

Article 22

Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23

Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.
2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24

Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.
2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the

data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.
4. Where the Commission finds, under the procedure provided for in Article 31 （2）, that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.
5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.
6. The Commission may find, in accordance with the procedure referred to in Article 31 （2）, that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

附錄十八　歐盟 Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector（節錄）

(1) Whereas Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data（4） requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community;

(4) Whereas this is the case, in particular, with the introduction of the Integrated Services Digital Network （ISDN） and digital mobile networks;

(5) Whereas the Council, in its Resolution of 30 June 1988 on the development of the common market for telecommunications services and equipment up to 1992 （5）, called for steps to be taken to protect personal data, in order to create an appropriate environment for the future development of telecommunications in the Community; whereas the Council re-emphasised the importance of the protection of personal data and privacy in its Resolution of 18 July 1989 on the strengthening of the coordination for the introduction of the Integrated Services Digital Network （ISDN） in the European Community up to 1992 （6）;

(6) Whereas the European Parliament has underlined the importance of the protection of personal data and privacy in the telecommunications networks, in particular with regard to the introduction of the Integrated Services Digital Network （ISDN）;

(7) Whereas, in the case of public telecommunications networks, specific legal, regulatory, and technical provisions must be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing risk connected with automated storage and processing of data relating to subscribers and users;

HAVE ADOPTED THIS DIRECTIVE:

Article 1 Object and scope

1. This Directive provides for the harmonisation of the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector and to ensure the free movement of such data and of telecommunications equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to the activities which fall outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security（including the economic well-being of the State when the activities relate to State security matters） and the activities of the State in areas of criminal law.

Article 3 Services concerned

1. This Directive shall apply to the processing of personal data in connection with the provision of publicly available telecommunications services in public telecommunications networks in the Community, in particular via the Integrated Services Digital Network （ISDN） and public digital mobile networks.

2. Articles 8, 9 and 10 shall apply to subscriber lines connected to digital exchanges and, where technically possible and if it does not require a disproportionate economic effort, to subscriber lines connected to analogue exchanges.

3. Cases where it would be technically impossible or require a disproportionate investment to fulfil the requirements of Articles 8, 9 and 10 shall be notified to the Commission by the Member States.

Article 6 Traffic and billing data

1. Traffic data relating to subscribers and users processed to establish calls and stored by the provider of a public telecommunications network and/or publicly available telecommunications service must be erased or made anonymous upon termination of the call without prejudice to the provisions of paragraphs 2, 3 and 4.

2. For the purpose of subscriber billing and interconnection payments, data indicated in the Annex may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment may be pursued.

3. For the purpose of marketing its own telecommunications services, the provider of a publicly available telecommunications service may process the data referred to in paragraph 2, if the subscriber has given his consent.

4. Processing of traffic and billing data must be restricted to persons acting under the authority of providers of the public telecommunications networks and/or publicly available telecommunications services handling billing or traffic management, customer enquiries, fraud detection and marketing the provider's own telecommunications services and it must be restricted to what is necessary for the purposes of such activities.

Paragraphs 1, 2, 3 and 4 shall apply without prejudice to the possibility for competent authorities to be informed of billing or traffic data in conformity with applicable legislation in view of settling disputes, in particular interconnection or billing disputes.

附錄十九　歐盟 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector （Directive on privacy and electronic communications）（節錄）

(14) Location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.

(15) A communication may include any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication. Traffic data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission. Traffic data may, inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network.

HAVE ADOPTED THIS DIRECTIVE:

Article 6

Traffic data

1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15（1）.
2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.
3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.
4. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.

5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.
6. Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

Article 9

Location data other than traffic data

1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.
2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.
3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

附錄二十　歐盟 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC（節錄）

Article 1

Subject matter and scope

1. This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.

Article 5

Categories of data to be retained

1. Member States shall ensure that the following categories of data are retained under this Directive:

（a） data necessary to trace and identify the source of a communication:

（1） concerning fixed network telephony and mobile telephony:

（i） the calling telephone number;

（ii） the name and address of the subscriber or registered user;

（2） concerning Internet access, Internet e-mail and Internet telephony:

（i） the user ID（s） allocated;

（ii） the user ID and telephone number allocated to any communication entering the public telephone network;

（iii） the name and address of the subscriber or registered user to whom an Internet Protocol （IP） address, user ID or telephone number was allocated at the time of the communication;

（b） data necessary to identify the destination of a communication:

（1） concerning fixed network telephony and mobile telephony:

（i） the number（s） dialled （the telephone number（s） called）, and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

（ii） the name（s） and address（es） of the subscriber（s） or registered user（s）;

（2） concerning Internet e-mail and Internet telephony:

（i） the user ID or telephone number of the intended recipient（s） of an Internet telephony call;

（ii） the name（s） and address（es） of the subscriber（s） or registered user（s） and user ID of the intended recipient of the communication;

（c） data necessary to identify the date, time and duration of a communication:

（1） concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

（2） concerning Internet access, Internet e-mail and Internet telephony:

（i） the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

（ii） the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

（d） data necessary to identify the type of communication:

（1） concerning fixed network telephony and mobile telephony: the telephone service used;

（2） concerning Internet e-mail and Internet telephony: the Internet service used;

（e） data necessary to identify users' communication equipment or what purports to be their equipment:

（1） concerning fixed network telephony, the calling and called telephone numbers;

（2） concerning mobile telephony:

（i） the calling and called telephone numbers;

（ii） the International Mobile Subscriber Identity （IMSI） of the calling party;

（iii） the International Mobile Equipment Identity （IMEI） of the calling party;

（iv） the IMSI of the called party;

（v） the IMEI of the called party;

（vi） in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label （Cell ID） from which the service was activated;

（3） concerning Internet access, Internet e-mail and Internet telephony:

（i） the calling telephone number for dial-up access;

（ii） the digital subscriber line （DSL） or other end point of the originator of the communication;

（f） data necessary to identify the location of mobile communication equipment:

（1） the location label （Cell ID） at the start of the communication;

（2） data identifying the geographic location of cells by reference to their location labels （Cell ID） during the period for which communications data are retained.

2. No data revealing the content of the communication may be retained pursuant to this Directive.

Article 6

Periods of retention

Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

Article 7

Data protection and data security

Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with this Directive:

(a) the retained data shall be of the same quality and subject to the same security and protection as those data on the network;

(b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;

(c) the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only; and

(d) the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.

Article 8

Storage requirements for retained data

Member States shall ensure that the data specified in Article 5 are retained in accordance with this Directive in such a way that the data retained and any other necessary information relating to such data can be transmitted upon request to the competent authorities without undue delay.

Article 9

Supervisory authority

1. Each Member State shall designate one or more public authorities to be responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to Article 7 regarding the security of the stored data. Those authorities may be the same authorities as those referred to in Article 28 of Directive 95/46/EC.

2. The authorities referred to in paragraph 1 shall act with complete independence in carrying out the monitoring referred to in that paragraph.

Article 13

Remedies, liability and penalties

1. Each Member State shall take the necessary measures to ensure that the national measures implementing Chapter III of Directive 95/46/EC providing for judicial remedies, liability and sanctions are fully implemented with respect to the processing of data under this Directive.
2. Each Member State shall, in particular, take the necessary measures to ensure that any intentional access to, or transfer of, data retained in accordance with this Directive that is not permitted under national law adopted pursuant to this Directive is punishable by penalties, including administrative or criminal penalties, that are effective, proportionate and dissuasive.

Article 15

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by no later than 15 September 2007. They shall forthwith inform the Commission thereof. When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.
2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Until 15 March 2009, each Member State may postpone application of this Directive to the retention of communications data relating to Internet Access, Internet telephony and Internet e-mail. Any Member State that intends to make use of this paragraph shall, upon adoption of this Directive, notify the Council and the Commission to that effect by way of a declaration. The declaration shall be published in the Official Journal of the European Union.

附錄二十一　歐盟網路犯罪公約（Cyber-crime Convention）（節錄）

Convention on Cybercrime

Budapest, 23.XI.2001

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15

附錄二十二　日本刑事訴訟法（節錄）[185]

第百九十七条の次に次の三項を加える

３　検察官、検察事務官又は司法警察員は、差押え又は記録命令付差押えをするため必要があるときは、電気通信を行うための設備を他人の通信の用に供する事業を営む者又は自己の業務のために不特定若しくは多数の者の通信を媒介することのできる電気通信を行うための設備を設置している者に対し、その業務上記録している電気通信の送信元、送信先、通信日時その他の通信履歴の電磁的記録のうち必要なものを特定し、三十日を超えない期間を定めて、これを消去しないよう、書面で求めることができる。この場合において、当該電磁的記録について差押え又は記録命令付差押えをする必要がないと認めるに至つたときは、当該求めを取り消さなければならない。

４　前項の規定により消去しないよう求める期間については、特に必要があるときは、三十日を超えない範囲内で延長することができる。ただし、消去しないよう求める期間は、通じて六十日を超えることができない。

５　第二項又は第三項の規定による求めを行う場合において、必要があるときは、みだりにこれらに関する事項を漏らさないよう求めることができる。

第 197 條增修條文[186]

第 3 項　檢察官、檢察事務官或司法警察官，於認為有扣押或紀錄指令附帶扣押之必要時，對於提供電信設備以為他人通信之用之業者或為了自己的業務媒介不特定或多數人通信而架設電信設備者，特別指定該業務上紀錄之通信來源、目的、日期時間、其他通信歷史紀錄之必要者，得以書面要求於 30 日期間內不得刪除。在此情形下，如認為相關電磁紀錄扣押或紀錄指令附帶扣押不必要時，應取消相關要求。

第 4 項　依前項規定，有關要求不可刪除之期間，有特殊必要時，在不超過 30 日範圍內得延長之。但要求不可刪除期間，最長不得超過 60 日。

第 5 項　依第二項或第三項之要求情形，必要時，得要求不得擅自洩漏相關事項。

第九十九条の二　裁判所は、必要があるときは、記録命令付差押え（電磁的

[185] 最終改正：平成 23 年 6 月 24 日法律第 74 号，目前尚未施行。
[186] 本研究將與研究主題相關之條文翻成中文。

記録を保管する者その他電磁的記録を利用する権限を有する者に命じて必要な電磁的記録を記録媒体に記録させ、又は印刷させた上、当該記録媒体を差し押さえることをいう。以下同じ。）をすることができる。

第 99 條之 2　法院於必要時得行使附紀錄命令之扣押（指命令電磁紀錄之保管者及其他具備利用權限者，將必要之電磁紀錄儲存或印刷於紀錄媒體後，扣押之）。

第二百十八条　　検察官、検察事務官又は司法警察職員は、犯罪の捜査をするについて必要があるときは、裁判官の発する令状により、記録命令付差押えをすることができるものとすること。

第 218 條第 1 項

檢察官、檢察事務官或司法警察，於實施犯罪偵查之必要時，得依法官核發之令狀，行使附紀錄命令之扣押。

附錄二十三　日本法務省／通信履歷の電磁的記録の保全要請に関するＱ＆Ａ[187]

これは，犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案により新設されることとなる通信履歴の電磁的記録の保全要請の制度に関するものです。

Ｑ１　通信履歴の保全要請の制度は，なぜ必要なのですか。

Ａ１　コンピュータ・ネットワークを利用した犯罪においては，その匿名性ゆえに，犯人の特定等のため，通信履歴の電磁的記録を確保することが極めて重要です。しかし，通信履歴の電磁的記録は一般的に短期間で消去される場合が多いことから，令状を得てこれを差し押さえるまでの間に消去されてしまう場合も少なくありません。そのため，捜査に必要な通信履歴の電磁的記録については，通信プロバイダ等の保管者に対し，令状による差押えの前の段階で，これを消去しないよう求める必要性が大きいと考えられます。そのため，今般，そのような保全要請の規定を設けることとしたものです。

Ｑ２　通信履歴とは何ですか。電子メールの本文もこれに当たるのですか。

Ａ２　「通信履歴」とは，通信に関わる事項の記録のうち，通信内容を除くものをいいます。具体的には，電気通信の送信先，送信元，通信日時等の通常ログと呼ばれているものがこれに当たることとなります。したがって，電子メールの本文等，通信の内容に関するものは，これに当たりません。

Ｑ３　保全要請の対象となる通信履歴の範囲を教えてください。

Ａ３　通信履歴の電磁的記録のうち，保全要請の対象となるのは，要請があった時点において通信プロバイダ等が業務上記録しているものに限られます。通信プロバイダ等がそもそも記録していないものや，要請があった時点で未だ記録されていない将来の通信履歴は対象になりません。

Ｑ４　令状なくして保全要請をするのは，通信の秘密との関係で問題になりませんか。

---

[187] 參閱日本法務省網頁 http://www.moj.go.jp/ ，有關法務省の概要／各組織の説明／内部部局／刑事局／過去の国会提出法律案（平成 10 年 3 月から平成 18 年 2 月までに提出されたもの）項下之刊載，標題「通信履歴の電磁的記録の保全要請に関するＱ＆Ａ」。

Ａ４ 保全要請の対象となる通信履歴には，通信の秘密の保護が及びますが，保全要請は，通信プロバイダ等がその業務上記録している通信履歴を消去しないように求めるにすぎず，その内容を捜査機関に開示させるものではないことから，令状を要することとする必要はなく，通信の秘密を不当に制約するものではないと考えられます。

Ｑ５ 保全要請の制度を設けると，通信業者などに過度な負担を負わせることになりませんか。

Ａ５ 保全要請の制度は，通信プロバイダ等に対し，新たに通信履歴の記録を義務づけるものでも，一律に全ての通信履歴を保存することを義務づけるものでもありません。通信プロバイダ等が既に業務上記録している通信履歴のうち，捜査に必要なものを特定した上，一定の期間これを消さないようにすることを要請するという制度です。また，保全の必要がなくなったときには，捜査機関は，保全要請を取り消すことが義務づけられているなど，通信プロバイダ等に過度な負担を負わせないような制度となっています。

Ｑ６ 保全要請の期間として，９０日も必要なのですか。

Ａ６ 保全の期間の上限を９０日間としたのは，サイバー犯罪に関する条約の規定に従ったものですが，実務的にもその程度の期間とする必要があります。現在においても，捜査機関は，通信履歴の電磁的記録に係る差押えを行うに際し，事前に通信プロバイダ等に連絡し，必要な通信履歴の電磁的記録について，差押え実施のための日程調整等を行うことがありますが，中には差押えの実施まで２か月程度かかることもあると承知しています。したがって，保全要請の期間の上限は９０日間程度とする必要があるのです。

もっとも，この９０日間というのは，あくまでも保全期間の上限であり，個々の保全要請の実施に当たっては，具体的事案に応じて，犯罪捜査に必要な適切な期間が定められるものと考えています。また，捜査機関は，保全期間内であっても，保全対象の電磁的記録に係る差押えが可能となれば，速やかに差押えを実施することになります。

附錄二十四 日本サイバー犯罪条約（節錄）

第十六条　蔵置されたコンピュータ・データの迅速な保全

１　締約国は、特に、自国の権限のある当局がコンピュータ・システムによって蔵置された特定のコンピュータ・データ（通信記録を含む。）が特に滅失しやすく又は改変されやすいと信ずるに足りる理由がある場合には、当該権限のある当局が当該コンピュータ・データについて迅速な保全を命令すること又はこれに類する方法によって迅速な保全を確保することを可能にするため、必要な立法その他の措置をとる。

２　締約国は、ある者が保有し又は管理している特定の蔵置されたコンピュータ・データを保全するよう当該者に命令することによって１の規定を実施する場合には、自国の権限のある当局が当該コンピュータ・データの開示を求めることを可能にするために必要な期間（九十日を限度とする。）、当該コンピュータ・データの完全性を保全し及び維持することを当該者に義務付けるため、必要な立法その他の措置をとる。締約国は、そのような命令を引き続き更新することができる旨定めることができる。

３　締約国は、コンピュータ・データを保全すべき管理者その他の者に対し、１又は２に定める手続がとられていることについて、自国の国内法に定める期間秘密のものとして取り扱うことを義務付けるため、必要な立法その他の措置をとる。

４　この条に定める権限及び手続は、前二条の規定に従うものとする。

第十六條-已儲存電腦資料的迅速保存

1. 各簽約國應立法或採取其他必要措施，在有合理根據相信電腦資料特別容易滅失或遭竄改時，使主管機關得以命令或他法迅速保存該特定電腦資料（包括通訊資料）。
2. 當簽約國主管機關欲根據第一項頒發命令，要求特定人保存其所有或控制之特定電腦資訊時，締約國應立法或採取其他必要措施，要求特定人在必要時間（最多九十天）內，保存及維持該電腦資料之完整性，以使主管機關得尋求該資料之開示。簽約國應規定該命令得隨後被更新。
3. 各簽約國應立法或採取必要措施，對於命其保存電腦資料之人，在其內國法所

規定一定時間內，課予其保持秘密之義務。

4. 本條所規定之權限以及程序必須遵照前二條之規定。

第十七条　通信記録の迅速な保全及び部分開示

1　締約国は、前条の規定に基づいて保全される通信記録について、次のことを行うため、必要な立法その他の措置をとる。

ａ　通信の伝達に関与したサービス・プロバイダが一であるか二以上であるかにかかわらず、通信記録の迅速な保全が可能となることを確保すること。

ｂ　当該サービス・プロバイダ及び通信が伝達された経路を自国が特定することができるようにするために十分な量の通信記録が、自国の権限のある当局又は当該権限のある当局によって指名された者に対して迅速に開示されることを確保すること。

2　この条に定める権限及び手続は、第十四条及び第十五条の規定に従うものとする。

第十七條-通訊資料的迅速保存以及部分揭露

1. 簽約國在依照第十六條規定保存通訊資料時，應採取必要之立法或其他措施，以達成下列目的：

a. 不論該訊息傳輸牽涉到一個或多個服務提供者，皆應確保該迅速保存之通訊資料具有可利用性。

b. 確保對簽約國之主管機關或主管機關指定之人迅速揭露足夠數量之通訊資料，使簽約國得以識別服務提供者及其訊息傳輸之路徑。

2. 本條所規定之權限以及程序必須遵照第十四條及第十五條之規定。

第十八条　提出命令

1　締約国は、自国の権限のある当局に対し次のことを行う権限を与えるため、必要な立法その他の措置をとる。

ａ　自国の領域内に所在する者に対し、当該者が保有し又は管理している特定のコンピュータ・データであって、コンピュータ・システム又はコンピュータ・データ記憶媒体の内部に蔵置されたものを提出するよう命令すること。

ｂ　自国の領域内でサービスを提供するサービス・プロバイダに対し、当

該サービス・プロバイダが保有し又は管理している当該サービスに関連する加入者情報を提出するよう命令すること。

2　この条に定める権限及び手続は、第十四条及び第十五条の規定に従うものとする。

3　この条の規定の適用上、「加入者情報」とは、コンピュータ・データという形式又はその他の形式による情報のうち、サービス・プロバイダが保有するサービス加入者に関連する情報（通信記録及び通信内容に関連するものを除く。）であって、それにより次のことが立証されるものをいう。

ａ　利用された通信サービスの種類、当該サービスのためにとられた技術上の措置及びサービスの期間

ｂ　加入者の身元、郵便用あて名又は住所及び電話番号その他のアクセスのための番号並びに料金の請求及び支払に関する情報であって、サービスに関する契約又は取決めに基づいて利用可能なもの

ｃ　通信設備の設置場所に関するその他の情報であってサービスに関する契約又は取決めに基づいて利用可能なもの

第十八條－提出命令

1.簽約國應採取必要之立法或其他措施，以授權主管機關得為下列命令：

a. 對其領域範圍內之人，命其提出其所有或在其控制下儲存於電腦系統或電腦資訊儲存媒介中之特定電腦資料。

b. 對在締約國領域範圍內提供服務之服務提供者，命其提供其所有或在其控制下與該服務相關之使用者資訊。

2. 本條所規定之權限以及程序必須遵照第十四條及第十五條之規定。

3. 本條規定之適用上，「使用者資訊」係指電磁紀錄或其他形式之資訊，由服務提供者保有之相關使用者資訊（通信紀錄與通信內容除外），包含：

a. 所使用的通訊服務類型、技術條款與使用期限。

b. 基於服務協議或約定可得，而載明於服務契約中之使用人身份及住址。

c. 基於服務協議或約定可得，而存於服務契約中之其他有關裝機處所之資訊。

第二十条　通信記録のリアルタイム収集

1　締約国は、自国の権限のある当局に対し、コンピュータ・システムによって伝達される自国の領域内における特定の通信に係る通信記録について

リアルタイムで次のことを行う権限を与えるため、必要な立法その他の措置をとる。

ａ　自国の領域内にある技術的手段を用いることにより、当該通信記録を収集し又は記録すること。

ｂ　サービス・プロバイダに対し、その既存の技術的能力の範囲内で次のいずれかのことを行うよう強制すること。

ｉ　自国の領域内にある技術的手段を用いることにより、当該通信記録を収集し又は記録すること。

ii　当該権限のある当局が当該通信記録を収集し又は記録するに当たり、これに協力し及びこれを支援すること。

２　締約国は、自国の国内法制の確立された原則により１ａに定める措置をとることができない場合には、当該措置に代えて、自国の領域内にある技術的手段を用いることにより、自国の領域内において伝達される特定の通信に係る通信記録をリアルタイムで収集し又は記録することを確保するため、必要な立法その他の措置をとることができる。

３　締約国は、サービス・プロバイダに対し、この条に定める権限の行使の事実及び当該権限の行使に関する情報について秘密のものとして取り扱うことを義務付けるため、必要な立法その他の措置をとる。

４　この条に定める権限及び手続は、第十四条及び第十五条の規定に従うものとする。

第二十條-通訊紀錄之即時收集

1. 簽約國應立法及採取其他必要措施，授權其主管機關得

a. 在其領域內經由科技性手段即時蒐集或記錄。

b. 要求服務提供者在其技術範圍內，在簽約國領域內經由技術設備即時蒐集或記錄，或　與執法機關合作或協助，即時蒐集或記錄有關在其領土內以電腦系統傳送之特定通信之通訊資料。

2. 當簽約國因遵守其內國法法體系中所確立之原則，而無法採取第一項之措施時，其可立法或採取其他必要措施，以確保在該簽約國領域內，可透過技術性措施之適用，以確保與其領土內特定通信有關連之通訊資料的即時收集及記錄，作為替代。

3. 簽約國應立法及採取其他必要措施，使服務提供者負有與本條規定之權限行使相關之事實與情報之保密義務。

4. 本條所規定之權限以及程序必須遵照第十四條及第十五條之規定。

第二十一条　通信内容の傍受

１　締約国は、自国の権限のある当局に対し、自国の国内法に定める範囲の重大な犯罪に関して、コンピュータ・システムによって伝達される自国の領域内における特定の通信の通信内容についてリアルタイムで次のことを行う権限を与えるため、必要な立法その他の措置をとる。

ａ　自国の領域内にある技術的手段を用いることにより、当該通信内容を収集し又は記録すること。

ｂ　サービス・プロバイダに対し、その既存の技術的能力の範囲内で次のいずれかのことを行うよう強制すること。

i　自国の領域内にある技術的手段を用いることにより、当該通信内容を収集し又は記録すること。

ii　当該権限のある当局が当該通信内容を収集し又は記録するに当たり、これに協力し及びこれを支援すること。

２　締約国は、自国の国内法制の確立された原則により１ａに定める措置をとることができない場合には、当該措置に代えて、自国の領域内にある技術的手段を用いることにより、自国の領域内における特定の通信の通信内容をリアルタイムで収集し又は記録することを確保するため、必要な立法その他の措置をとることができる。

３　締約国は、サービス・プロバイダに対し、この条に定める権限の行使の事実及び当該権限の行使に関する情報について秘密のものとして取り扱うことを義務付けるため、必要な立法その他の措置をとる。

４　この条に定める権限及び手続は、第十四条及び第十五条の規定に従うものとする。

第二十一條　通信內容之監聽

1. 簽約國應立法及採取其他必要措施，在內國法所認定一定嚴重犯罪範圍內，授權其主管機關得

a. 在其領域內經由科技性手段即時蒐集或記錄。

b. 要求服務提供者在其技術範圍內，在簽約國領域內經由技術設備即時蒐集或記錄，或與執法機關合作或協助，即時蒐集或記錄有關在其領土內以電腦系統傳送之特定通信之內容資料。

2. 當簽約國因遵守其內國法法體系中所確立之原則，而無法採取第一項之措施時，其可立法或採取其他必要措施，以確保在該簽約國領域內，可透過技術性措施之適用，以確保與其領土內特定通信有關連之通訊資料的即時收集及記錄，作為替代。

3. 簽約國應立法及採取其他必要措施，使服務提供者負有與本條規定之權限行使相關之事實與情報之保密義務。

4. 本條所規定之權限以及程序必須遵照第十四條及第十五條之規定。

附錄二十五　日本ハイテク犯罪に対処するための刑事法の整備に関する要綱

第一　不正指令電磁的記録等作成等の罪の新設等

一　人の電子計算機における実行の用に供する目的で、人の使用する電子計算機についてその意図に沿うべき動作をさせず、又はその意図に反する動作をさせる不正な指令に係る電磁的記録その他の記録を作成し、又は提供した者は、三年以下の懲役又は五十万円以下の罰金に処するものとすること。

二　一の不正な指令を与える電磁的記録を人の電子計算機において実行の用に供した者も、一と同様とすること。

三　二の未遂は、罰するものとすること。

四　一の目的で、一の不正な指令に係る電磁的記録その他の記録を取得し、又は保管した者は、二年以下の懲役又は三十万円以下の罰金に処するものとすること。

五　電子計算機損壊等業務妨害の罪（刑法第二百三十四条の二）の未遂は、罰するものとすること。

第二　わいせつ物頒布等の罪（刑法第百七十五条）の改正

一　わいせつな文書、図画、電磁的記録に係る記録媒体その他の物を頒布し、又は公然と陳列した者は、二年以下の懲役若しくは二百五十万円以下の罰金若しくは科料に処し、又は懲役及び罰金を併科するものとすること。電気通信の送信によりわいせつな電磁的記録その他の記録を頒布した者も同様とすること。

二　有償で頒布する目的で、一の物又は電磁的記録を所持し、又は保管した者も、一と同様とすること。

第三　電磁的記録に係る記録媒体の差押えの執行方法

一　差し押さえるべき物が電磁的記録に係る記録媒体であるときは、差押状の執行をする者又は差押許可状により差押えをする捜査機関は、その差押えに代えて次の処分をすることができるものとすること。公判廷で差押えをする場合も、同様とすること。

1　差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写し、印刷し、又は移転した上、当該他の記録媒体を差し押さえること。

2　差押状の執行を受ける者又は差押許可状による差押えを受ける者に当該記録媒体に記録された電磁的記録を他の記録媒体に複写させ、印刷させ、又は移転させた上、当該他の記録媒体を差し押さえること。

二　押収物が一の規定により電磁的記録を移転し、又は移転させた上差し押さえた他の記録媒体で留置の必要がないものである場合において、差押状の執行を受けた者又は差押許可状による差押えを受けた者と当該他の記録媒体の所有者、所持者又は保管者が異なるときは、還付に代えて差押状の執行を受けた者等に当該他の記録媒体を交付し、又は差押状の執行を受けた者等に当該電磁的記録を複写させた上、当該他の記録媒体の所有者等に当該他の記録媒体を還付しなければならないものとすること。

第三　與電磁紀錄相關記錄媒體之扣押執行方法

一、應扣押物是與電磁紀錄相關記錄媒體時，執行扣押令狀者或依據扣押許可狀執行扣押之偵查機關，為了取代該扣押行為，可以為如下之處分。在審判庭上執行扣押者，亦同。

1. 將應扣押之記錄媒體中所記錄之電磁紀錄予以複製、列印、或移轉至其他記錄媒體後，扣押該當其他記錄媒體。

2. 命受扣押令狀執行者或受扣押許可狀之扣押者，將該當電磁記錄媒體中記錄之電磁紀錄，複製、列印、或移轉至其他記錄媒體後，扣押該當其他記錄媒體。

二、扣押物依據第一項規定移轉電磁紀錄或移轉後所扣押之其他記錄媒體已無留置之必要者，如受扣押狀之執行者或受扣押執行狀之允許扣押執行者，與該記錄媒體之所有者、持有者或保管者不同時，代替返還而交付該當其他記錄媒體予受扣押令狀之執行者，或使受扣押狀之執行者複製該當電磁紀錄後，應將該當他電磁記錄媒體返回予其所有者等。

第四　記録命令差押え

一　裁判所は、記録命令差押え（電磁的記録を保管する者その他電磁的記録を利用する権限を有する者に命じて必要な電磁的記録を記録媒体に記録

させ、又は印刷させた上、当該記録媒体を差し押さえることをいう。）をすることができるものとすること。公判廷外において記録命令差押えを行う場合は、令状を発してこれをしなければならないものとすること。

二　捜査機関は、犯罪の捜査をするについて必要があるときは、裁判官の発する令状により、記録命令差押えをすることができるものとすること。

三　一及び二の令状には、電磁的記録を記録させ、又は印刷させるべき者及び記録させ、又は印刷させるべき電磁的記録を記載しなければならないものとすること。

四　その他、記録命令差押えに関する所要の法整備を行うこと。

第四　附紀錄命令之扣押

一、法院得行使附紀錄命令之扣押（亦即命令電磁紀錄之保管者或其他具備利用權限者，將必要之電磁紀錄儲存或印刷於電磁媒體後，扣押該當記錄媒體）。在審判庭外實行附紀錄命令之扣押時，應簽發令狀並據以實行之。

二、偵查機關如有實行犯罪偵查之必要情形，得依據法院所簽發之令狀，實行附紀錄命令之扣押。

三、第一項及第二項之令狀，應記載命其儲存或印刷電磁紀錄之人，以及應儲存或印刷之電磁紀錄。

四、應檢討其他關於附紀錄命令之扣押之相關法律規定。

第五　電子計算機に電気通信回線で接続している記録媒体からの複写

一　裁判所は、差し押さえるべき物が電子計算機であるときは、当該電子計算機に電気通信回線で接続している記録媒体であって、当該電子計算機で処理すべき電磁的記録を保管するために使用されていると認めるに足りる状況にあるものから、その電磁的記録を当該電子計算機又は他の記録媒体に複写した上、当該電子計算機又は他の記録媒体を差し押さえることができるものとすること。

二　一の規定は、捜査機関が刑事訴訟法第二百十八条の規定によってする差押えについてこれを準用するものとすること。

三　一の差押状及び二の差押許可状には、差し押さえるべき電子計算機に電気通信回線で接続している記録媒体であって、その電磁的記録を複写すべきものの範囲を記載しなければならないものとすること。

第五　以電氣通訊線路連接電子計算機之記錄媒體的複製

一、法院於應扣押之物為電子計算機時，對於以電氣通訊線路連接該當電子計算機之記錄媒體，在足以認定該記錄媒體之使用，是為了保管該當電子計算機所應處理之電磁紀錄時，在將該當電磁紀錄複製至該當電子計算機或其他記錄媒體後，可以扣押該當電子計算機或其他記錄媒體。

二、第一項之規定，偵查機關依據刑事訴訟法第二百十八條之規定進行扣押時，得準用之。

三、第一項之扣押令狀，或第二項之扣押許可狀中，應記載以電氣通訊線路連接該當電子計算機之記錄媒體，其應複製的電磁紀錄之範圍。

第六　電磁的記録に係る記録媒体の差押状の執行を受ける者等への協力要請

一　差し押さえるべき物が電磁的記録に係る記録媒体であるときは、差押状若しくは捜索状の執行をする者又は差押許可状若しくは捜索許可状により差押え若しくは捜索をする捜査機関は、差押状若しくは捜索状の執行を受ける者又は差押許可状若しくは捜索許可状による差押え若しくは捜索を受ける者に対して、電子計算機の操作その他の必要な協力を求めることができるものとすること。公判廷で差押えをする場合も同様とすること。

二　検証すべき物が電磁的記録に係る記録媒体であるときは、裁判所又は裁判官の発する令状により検証をする捜査機関は、一と同様の協力を求めることができるものとすること。

第七　保全要請等

一　捜査については、電気通信を行うための設備を他人の通信の用に供する事業を営む者又は自己の業務のために不特定若しくは多数の者の通信を媒介することのできる電気通信を行うための設備を設置している者に対して、その業務上記録し、又は記録すべき電気通信の送信元、送信先、通信日時その他の通信履歴の電磁的記録のうち必要なものを特定し、九十日を超えない期間を定めて、これを消去しないよう求めることができるものとすること。

二　捜査関係事項照会及び一の保全要請を行う場合において、必要があるときは、みだりにこれらの要請に関する事項を漏らさないよう求めること

ができるものとすること。

第七　保全處分等

一、關於偵查，得以經營事業者，或設備設置者為對象，對於其業務上所記錄之電氣通訊之送信者、送信來源、通訊日期或其他通訊履歷之電磁記錄中，特定出必要者，訂出不超過90天之期間，請求於期間內不刪除之。但認為沒有必要執行扣押或附記錄命令之扣押時，應取消該當保全要求。(上述經營事業者所經營之事業，係指將執行電氣通信之設備，提供他人之用；上述設備設置者所設置之設備，係指為自己之業務，而使不特定或多數人之電氣通訊得以實行之媒介)。

二、詢問偵查相關事項以及執行第一項之保全要求時，必要時，應要求不得任意洩漏與上述要求相關之事項。

第八　不正に作られた電磁的記録等の没収

一　不正に作られた電磁的記録又は没収された電磁的記録に係る記録媒体を返還し、又は交付する場合には、当該電磁的記録を消去し、又は当該電磁的記録が不正に利用されないようにする処分をしなければならないものとすること。

二　不正に作られた電磁的記録に係る記録媒体が公務所に属する場合において、当該電磁的記録に係る記録媒体が押収されていないときは、不正に作られた部分を公務所に通知して相当な処分をさせなければならないものとすること。

三　刑事事件における第三者所有物の没収手続に関する応急措置法の適用については、被告人以外の者に帰属する電磁的記録は、その者の所有に属するものとみなすものとすること。

附錄二十六　日本プロバイダ責任制限法[188]（特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律）（節錄）

第一条 この法律は、特定電気通信による情報の流通によって権利の侵害があった場合について、特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示を請求する権利につき定めるものとする。

第一條　本法規定，因特定電信流通資訊造成權利侵害時，特定電信服務提供者之損害賠償責任限制及請求揭露發信者資訊之權利。

第二条 この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

一　特定電気通信 不特定の者によって受信されることを目的とする電気通信（電気通信事業法（昭和五十九年法律第八十六号）第二条第一号に規定する電気通信をいう。以下この号において同じ。）の送信（公衆によって直接受信されることを目的とする電気通信の送信を除く。）をいう。

二　特定電気通信設備 特定電気通信の用に供される電気通信設備（電気通信事業法第二条第二号に規定する電気通信設備をいう。）をいう。

三　特定電気通信役務提供者 特定電気通信設備を用いて他人の通信を媒介し、その他特定電気通信設備を他人の通信の用に供する者をいう。

四　発信者 特定電気通信役務提供者の用いる特定電気通信設備の記録媒体（当該記録媒体に記録された情報が不特定の者に送信されるものに限る。）に情報を記録し、又は当該特定電気通信設備の送信装置（当該送信装置に入力された情報が不特定の者に送信されるものに限る。）に情報を入力した者をいう。

第二條　本法中各種名詞之定義如下：

一、特定電信：以發送給不特定接收者為目的之電信（電信事業法第二條第一項所稱之電信）（以公眾為直接接收目的之電信發送除外）。

二、特定電信設備：供特定電信用之電信設備（電信事業法第二條第二項所稱之電信設備）。

三、特定電信服務提供者：以特定電信設備媒介他人通信，及其他提供特定電信

[188] 同註 6。

設備以為他人通信之用者。

四、發信者：在特定電信服務提供者所用之特定電信設備的紀錄媒體（以發送該紀錄媒體紀錄之資訊予不特定人為限）上紀錄資訊、或在該特定電信設備的發送裝置（以發送該發送裝置輸入之資訊予不特定人為限）輸入資訊者。

第四条　特定電気通信による情報の流通によって自己の権利を侵害されたとする者は、次の各号のいずれにも該当するときに限り、当該特定電気通信の用に供される特定電気通信設備を用いる特定電気通信役務提供者(以下「開示関係役務提供者」という。)に対し、当該開示関係役務提供者が保有する当該権利の侵害に係る発信者情報(氏名、住所その他の侵害情報の発信者の特定に資する情報であって総務省令で定めるものをいう。以下同じ。)の開示を請求することができる。

一　侵害情報の流通によって当該開示の請求をする者の権利が侵害されたことが明らかであるとき。

二　当該発信者情報が当該開示の請求をする者の損害賠償請求権の行使のために必要である場合その他発信者情報の開示を受けるべき正当な理由があるとき。

2　開示関係役務提供者は、前項の規定による開示の請求を受けたときは、当該開示の請求に係る侵害情報の発信者と連絡することができない場合その他特別の事情がある場合を除き、開示するかどうかについて当該発信者の意見を聴かなければならない。

3　第一項の規定により発信者情報の開示を受けた者は、当該発信者情報をみだりに用いて、不当に当該発信者の名誉又は生活の平穏を害する行為をしてはならない。

4　開示関係役務提供者は、第一項の規定による開示の請求に応じないことにより当該開示の請求をした者に生じた損害については、故意又は重大な過失がある場合でなければ、賠償の責めに任じない。ただし、当該開示関係役務提供者が当該開示の請求に係る侵害情報の発信者である場合は、この限りでない。

第四條　因特定電信資訊之流通而使自身權利遭受侵害者，以符合下列二款者為限，對於使用特定電信設備提供該特定電信用途之特定電信服務提供者，得請求揭露其保有之關於侵害權利之發信者資料（係指總務省令規定之姓名、住址及其他侵害資訊之發信者之特定資料）。

一、因侵害資訊之流通，顯有侵害該請求揭露者之權利者。

二、請求揭露者為行使損害賠償請求權之必要，及有其他正當理由揭露發信者資料者。

附錄二十七　日本電気通信事業における個人情報に関するガイドライン（節錄）[189]

（保存期間等）

第１０条　電気通信事業者は、個人情報を取り扱うに当たっては、原則として利用目的に必要な範囲内で保存期間を定めるものとし、当該保存期間経過後又は当該利用目的を達成した後は、当該個人情報を遅滞なく消去するものとする。

２　前項の規定にかかわらず、電気通信事業者は、次の各号のいずれかに該当すると認めるときは、保存期間経過後又は利用目的達成後においても当該個人情報を消去しないことができる。

一　法令の規定に基づき、保存しなければならないとき。

二　本人の同意があるとき。

三　電気通信事業者が自己の業務の遂行に必要な限度で個人情報を保存する場合であって、当該個人情報を消去しないことについて相当な理由があるとき。

四　前３号に掲げる場合のほか、当該個人情報を消去しないことについて特別の理由があるとき。

第 10 條 電信事業者處理個人資料時，以於使用目的必要範圍內定訂保存期間為原則，該保存期間經過後或該使用目的達成後，應立即刪除該個人資料。

2　電信事業者認為有下列各款情形之一者，雖有前項規定，於保存期間經過後或使用目的達成後，得不刪除該個人資料。

一、基於法令規定應予保存者。

二、經本人同意者。

三、電信事業者為遂行業務，於必要限度內認有保存個人資料之需要，有相當理由不予刪除者。

四、除前 3 款所列情形外，有特別理由不予刪除者。

（第三者提供の制限）

第１５条 電気通信事業者は、次の各号のいずれかに該当する場合を除くほか、あらかじめ本人の同意を得ないで、個人情報を第三者に提供しないものとする。

---

[189] 參閱日本總務省網站 http://www.soumu.go.jp/，会議資料・開催案内等項下，標題「電気通信事業における個人情報保護に関するガイドライン」，最終改正：平成 23 年 11 月 2 日総務省告示第 465 号，上網日期：2012 年 4 月 28 日。

一　法令に基づく場合

二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

２　電気通信事業者は、第三者に提供される個人情報について、本人の求めに応じて当該本人が識別される個人情報の第三者への提供を停止することとしている場合であって、次に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にかかわらず、当該個人情報を第三者に提供することができる。

一　第三者への提供を利用目的とすること。

二　第三者に提供される個人情報の項目

三　第三者への提供の手段又は方法

四　本人の求めに応じて当該本人が識別される個人情報の第三者への提供を停止すること。

３　電気通信事業者は、前項第２号又は第３号に掲げる事項を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くものとする。

４　次に掲げる場合において、当該個人情報の提供を受ける者は、前３項の規定の適用については、第三者に該当しないものとする。

一　電気通信事業者が利用目的の達成に必要な範囲内において個人情報の取扱いの全部又は一部を委託する場合

二　合併その他の事由による事業の承継に伴って個人情報が提供される場合

三　個人情報を特定の者との間で共同して利用する場合であって、その旨並びに共同して利用される個人情報の項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人情報の管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いて

いるとき。

5　電気通信事業者は、前項第３号に規定する利用する者の利用目的又は個人情報の管理について責任を有する者の氏名若しくは名称を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くものとする。

6　電気通信事業者は、個人情報を第三者に提供するに当たっては、通信の秘密の保護に係る電気通信事業法第４条その他の関連規定を遵守するものとする。

第 15 條　電信事業者，除下列各款情形之一者外，非事先經本人同意，不得提供個人資料予第三人。

一、基於法令者。

二、為保護個人生命、身體或財產之必要，取得本人同意有困難者。

三、為提升公共衛生或促進兒童健全發展，有特殊必要，取得本人同意有困難者。

四、國家機關或地方公共團體或其他受委託者，對於遂行法令規定事務有協助必要，取得本人同意有妨礙該事務遂行之虞者。

2　電信事業者，因應本人請求停止提供可識別之個人資料予第三人之情形，於下列事項預先通知本人或本人處於容易知悉狀態時，雖有前項規定，得提供該個人資料予第三人。

一、提供予第三人之使用目的。

二、提供予第三人之個人資料項目。

三、提供予第三人之手段或方法。

四、因應本人請求停止提供可識別之個人資料予第三人。

3　電信事業者變更前項第 2 款或第 3 款所列事項，變更內容應預先通知本人或使本人處於容易知悉狀態者。

4　下列情形中，該個人資料之接受者，有前 3 項規定之情形時，不該當為第三人。

一、電信事業者於達成使用目的之必要範圍內，委託處理個人資料之全部或部分者。

二、因合併及其他事由，事業繼承伴隨提供個人資料者。

三、特定人之間共同使用個人資料者，意謂共同使用之個人資料項目、共同使用者之範圍、使用目的及該個人資料管理之相關負責人姓名或名稱，預先通知本人或使本人處於容易知悉狀態者。

5　電信事業者，前項第 3 款規定之使用目的或個人資料管理之相關負責人姓名或名稱變更時，變更內容應預先通知本人或使本人處於容易知悉狀態者。

6　電信事業者，提供個人資料予第三人時，有關通信秘密之保護，應遵守電氣通信事業法第 4 條及其他相關規定。

（通信履歴）

第２３条 電気通信事業者は、通信履歴（利用者が電気通信を利用した日時、当該通信の相手方その他の利用者の通信に係る情報であって通信内容以外のものをいう。以下同じ。）については、課金、料金請求、苦情対応、不正利用の防止その他の業務の遂行上必要な場合に限り、記録することができる。

２　電気通信事業者は、利用者の同意がある場合、裁判官の発付した令状に従う場合、正当防衛又は緊急避難に該当する場合その他の違法性阻却事由がある場合を除いては、通信履歴を他人に提供しないものとする。

第 23 條　電信事業者，得紀錄之通信歷程（指使用者使用電信的日期、時間，該通信對方使用者之通信內容以外之相關通信資料），以罰款、通信費用請求、申訴處理、防止不當利用及其他業務遂行必要情形者為限。

2　電信事業者，除經使用者同意、依據法官核發之令狀、該當正當防衛或緊急避難及其他阻卻違法事由之情形外，不得將通信歷程提供他人。

附錄二十八　日本電気通信事業法（節錄）

第二条　この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

一　電気通信　有線、無線その他の電磁的方式により、符号、音響又は影像を送り、伝え、又は受けることをいう。

二　電気通信設備　電気通信を行うための機械、器具、線路その他の電気的設備をいう。

三　電気通信役務　電気通信設備を用いて他人の通信を媒介し、その他電気通信設備を他人の通信の用に供することをいう。

四　電気通信事業　電気通信役務を他人の需要に応ずるために提供する事業（放送法（昭和二十五年法律第百三十二号）第百十八条第一項に規定する放送局設備供給役務に係る事業を除く。）をいう。

五　電気通信事業者　電気通信事業を営むことについて、第九条の登録を受けた者及び第十六条第一項の規定による届出をした者をいう。

六　電気通信業務　電気通信事業者の行う電気通信役務の提供の業務をいう。

第二條　以下所列為本法各用語之定義：

一、電信：指以有線、無線及其他電磁方式發送、傳輸或接收符號、聲音或影像。

二、電信設備：指電信所用之機械、器具、線路及其他電氣設備。

三、電信服務：指使用電信設備媒介他人通信、及其他提供電信設備供他人通信之服務。

四、電信事業：指應他人需要而提供電信服務之事業。

五、電信業者：經營電信事業，受理第9條之登錄及依第16條第1項規定提出報告者。

六、電信業務：電信事業者提供電信服務之業務。

第四条　電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。

２　電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。

第四條　任何人對於有關電信業者處理中之通信秘密，不得侵害之。

2　從事電信事業之工作人員，於任職期間，因處理電信業者之相關通信，而得知

他人秘密者，應保密之。於退職後亦同。

附錄二十九　日本個人情報の保護に関する法律（節錄）[190]

（利用目的による制限）

第十六条　個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。

2　個人情報取扱事業者は、合併その他の事由により他の個人情報取扱事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。

3　前二項の規定は、次に掲げる場合については、適用しない。

一　法令に基づく場合

二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

第十六條　個人資訊處理業者，未事先取得本人之同意，不得作超過前條規定為達特定使用目的所需範圍之個人資訊之處理。

2 個人資訊處理事業者，因合併及其他事由，自其他個人資訊處理業者繼承事業伴隨而得個人資訊時，不須事先經本人同意，但在繼承前超過達成該個人資訊使用目的之必要範圍時，不得處理之。

3 前二項之規定，下列情形不適用之。

一、基於法令者。

二、為保護個人生命、身體或財產之必要，取得本人同意有困難者。

三、為提升公共衛生或促進兒童健全發展，有特殊必要，取得本人同意有困難

[190] 最終改正：平成 21 年 6 月 5 日法律第 49 号。

者。

四、國家機關或地方公共團體或其他受委託者，對於遂行法令規定事務有協助必要，取得本人同意有妨礙該事務遂行之虞者。

附錄三十　日本犯罪捜査のための通信傍受に関する法律（節錄）

第二条　この法律において「通信」とは、電話その他の電気通信であって、その伝送路の全部若しくは一部が有線（有線以外の方式で電波その他の電磁波を送り、又は受けるための電気的設備に附属する有線を除く。）であるもの又はその伝送路に交換設備があるものをいう。

２　この法律において「傍受」とは、現に行われている他人間の通信について、その内容を知るため、当該通信の当事者のいずれの同意も得ないで、これを受けることをいう。

３　この法律において「通信事業者等」とは、電気通信を行うための設備（以下「電気通信設備」という。）を用いて他人の通信を媒介し、その他電気通信設備を他人の通信の用に供する事業を営む者及びそれ以外の者であって自己の業務のために不特定又は多数の者の通信を媒介することのできる電気通信設備を設置している者をいう。

第三条　検察官又は司法警察員は、次の各号のいずれかに該当する場合において、当該各号に規定する犯罪（第二号及び第三号にあっては、その一連の犯罪をいう。）の実行、準備又は証拠隠滅等の事後措置に関する謀議、指示その他の相互連絡その他当該犯罪の実行に関連する事項を内容とする通信（以下この項において「犯罪関連通信」という。）が行われると疑うに足りる状況があり、かつ、他の方法によっては、犯人を特定し、又は犯行の状況若しくは内容を明らかにすることが著しく困難であるときは、裁判官の発する傍受令状により、電話番号その他発信元又は発信先を識別するための番号又は符号(以下「電話番号等」という。)によって特定された通信の手段（以下「通信手段」という。）であって、被疑者が通信事業者等との間の契約に基づいて使用しているもの（犯人による犯罪関連通信に用いられる疑いがないと認められるものを除く。）又は犯人による犯罪関連通信に用いられると疑うに足りるものについて、これを用いて行われた犯罪関連通信の傍受をすることができる。

一　別表に掲げる罪が犯されたと疑うに足りる十分な理由がある場合において、当該犯罪が数人の共謀によるものであると疑うに足りる状況があ

るとき。

二　別表に掲げる罪が犯され、かつ、引き続き次に掲げる罪が犯されると疑うに足りる十分な理由がある場合において、これらの犯罪が数人の共謀によるものであると疑うに足りる状況があるとき。

イ　当該犯罪と同様の態様で犯されるこれと同一又は同種の別表に掲げる罪

ロ　当該犯罪の実行を含む一連の犯行の計画に基づいて犯される別表に掲げる罪

三　死刑又は無期若しくは長期二年以上の懲役若しくは禁錮に当たる罪が別表に掲げる罪と一体のものとしてその実行に必要な準備のために犯され、かつ、引き続き当該別表に掲げる罪が犯されると疑うに足りる十分な理由がある場合において、当該犯罪が数人の共謀によるものであると疑うに足りる状況があるとき。

2　別表に掲げる罪であって、譲渡し、譲受け、貸付け、借受け又は交付の行為を罰するものについては、前項の規定にかかわらず、数人の共謀によるものであると疑うに足りる状況があることを要しない。

3　前二項の規定による傍受は、通信事業者等の看守する場所で行う場合を除き、人の住居又は人の看守する邸宅、建造物若しくは船舶内においては、これをすることができない。ただし、住居主若しくは看守者又はこれらの者に代わるべき者の承諾がある場合は、この限りでない。

第三條　檢察官及司法警察，於該當下列各款之一情形時，足以懷疑其通信內容與該犯罪之實行、準備或湮滅證據等事後措施相關之策劃、指示及其他相互聯絡或與該犯罪之實行相關（以下稱「犯罪關聯通信」），且以其他方法查明犯罪嫌疑人或犯罪事實顯有困難時，得依法官核發之通信監察令狀，以電話號碼及其他可識別發信來源或目的之號碼或符號（以下稱「電話號碼等」）特定通信之方式（以下稱「通信方式」），犯罪嫌疑人基於與通信事業者之契約而使用之通信方式（認為沒有使用於犯罪關聯通信者除外），或足以懷疑用於犯罪關聯通信者，得實施通信監察。

一、有充分理由足以懷疑犯有附表所列之罪，且足以懷疑該犯罪係由數人共謀時。

二、犯有附表所列之罪，且有充分理由足以懷疑其接續犯有下列之罪，足以懷

疑該等犯罪係由數人共謀時。

1、以與該犯罪相同之樣態，所犯附表中與該罪相同或同種之罪。

2、依據包含該犯罪在內之一系列犯罪計畫，而犯有附表所列之罪。

三、死刑、無期徒刑、2 年以上有期徒刑或監禁之罪，視為與附表所列一體之必要準備行為之罪，且足以懷疑接續犯有附表所列之罪，足以懷疑該犯罪係由數人共謀時。

2　有關附表所列犯罪之讓渡、繼承、借貸或交付行為之處罰，不受前項規定限制，非必要足以懷疑係由數人共謀。

3　前二項規定之監聽，除有通信事業者等看守之場所外，不得在有人居住或有人看守之宅邸、建築物或船舶內為之。但經住居所主人、看守人或應代理人承諾者，不在此限。

第四条　傍受令状の請求は、検察官（検事総長が指定する検事に限る、第七条において同じ。）又は司法警察員（国家公安委員会又は都道府県公安委員会が指定する警視以上の警察官、厚生労働大臣が指定する麻薬取締官及び海上保安庁長官が指定する海上保安官に限る。同条において同じ。）から地方裁判所の裁判官にこれをしなければならない。

2　検察官又は司法警察員は、前項の請求をする場合において、当該請求に係る被疑事実の全部又は一部と同一の被疑事実について、前に同一の通信手段を対象とする傍受令状の請求又はその発付があったときは、その旨を裁判官に通知しなければならない。

第四條　監察令狀之聲請，應由檢察官（以檢察總長指定之檢察官為限）或司法警察（以國家公安委員會、都道府縣公安委員會指定之警視以上警察官、厚生勞動大臣指定之麻藥取締官及海上保安廳長官指定之海上保安官為限）向地方法院之法官為之。

2　檢察官或司法警察，於前項聲請時，該聲請之相關懷疑事實之全部或部分與同一懷疑事實，所使用之通信方式之監聽令狀之聲請或核發時，應將要旨通知法官。

第五条　前条第一項の請求を受けた裁判官は、同項の請求を理由があると認めるときは、傍受ができる期間として十日以内の期間を定めて、傍受令状を発する。

2　裁判官は、傍受令状を発する場合において、傍受の実施（通信の傍受をすること及び通信手段について直ちに傍受をすることができる状態で通信の状況を

監視することをいう。以下同じ。）に関し、適当と認める条件を付することができる。

第五條　法官受理前條第一項之聲請，認為有理由時，得核發監聽令狀，並訂定 10 日內之監聽期間。

２　法官核發監聽令狀時，得附加實施監聽（指通信的監聽及通信方式在可直接監聽之狀態下監視通信的狀況）之適當條件。

第七条　地方裁判所の裁判官は、必要があると認めるときは、検察官又は司法警察員の請求により、十日以内の期間を定めて、傍受ができる期間を延長することができる。ただし、傍受ができる期間は、通じて三十日を超えることができない。

２　前項の延長は、傍受令状に延長する期間及び理由を記載し記名押印してこれをしなければならない。

第七條　地方法院之法官於認有必要時，得依檢察官或司法警察之聲請，訂定 10 日內之延長監聽期間。但監聽期間總計不得超過 30 日。

２　前項之延長，應於令狀內記載延長之期間及理由，並簽名奈印。

第十一条　検察官又は司法警察員は、通信事業者等に対して、傍受の実施に関し、傍受のための機器の接続その他の必要な協力を求めることができる。この場合においては、通信事業者等は、正当な理由がないのに、これを拒んではならない。

第十一條　檢察官或司法警察於實施監聽時，得要求通信事業者架設監聽設備及其他必要之協助。通信事業者無正當理由，不得拒絕之。

第十三条　検察官又は司法警察員は、傍受の実施をしている間に行われた通信であって、傍受令状に記載された傍受すべき通信（以下単に「傍受すべき通信」という。）に該当するかどうか明らかでないものについては、傍受すべき通信に該当するかどうかを判断するため、これに必要な最小限度の範囲に限り、当該通信の傍受をすることができる。

２　外国語による通信又は暗号その他その内容を即時に復元することができない方法を用いた通信であって、傍受の時にその内容を知ることが困難なため、傍受すべき通信に該当するかどうかを判断することができないものについては、その全部の傍受をすることができる。この場合においては、速やかに、傍受すべき通信に該当するかどうかの判断を行わなければならない。

第十三條 檢察官或司法警察，對於監察之通信，是否該當記載於監聽令狀之應監

察通信（以下稱「應監察通信」）不明顯時，為判斷是否該當應監察通信，得於必要之最小限度範圍內實施監聽。

2　使用外語通信或暗號及其他內容無法即時復原之方法所為之通信，監察時為順利知悉其內容，得實施全部監聽以判斷是否該當應監察通信。在此情形下，應儘速判斷是否該當應監察通信。

第二十九条　政府は、毎年、傍受令状の請求及び発付の件数、その請求及び発付に係る罪名、傍受の対象とした通信手段の種類、傍受の実施をした期間、傍受の実施をしている 間におげる通話の回数、このうち第二十二条第二項第一号又は第三号に掲げる通信が行われたものの数並びに傍受が行われた事件に関して逮捕した人員数を国会に報告するとともに、公表するものとする。ただし、罪名については、捜査に支障を生じるおそれがあるときは、その支障がなくなった後においてこれらの措置を執るものとする。

第二十九條　政府應每年向國會報告監聽令狀之聲請及核發件數、罪名、監聽對象通信方式之種類、監聽期間、監聽通話次數、第二十二條第二項第一款或第三款所列通信次數與相關案件逮捕人數，並公布之。但罪名公開有礙偵查之進行時，俟障礙原因消滅後，始公布之。

別表（第三条関係 第十四条関係）

一　大麻取締法（昭和二十三年法律第百二十四号）第二十四条（栽培、輸入等）又は第二十四条の二（所持、譲渡し等）の罪。

二　覚せい剤取締法（昭和二十六年法律第二百五十二号）第四十一条（輸入等）若しくは第四十一条の二（所持、譲渡し等）の罪、同法第四十一条の三第一項第三号（覚せい剤原料の輸入等）若しくは第四号（覚せい剤原料の製造）の罪若しくはこれらの罪に係る同条第二項（営利目的の覚せい剤原料の輸入等）の罪若しくはこれらの罪の未遂罪又は同法第四十一条の四第一項第三号（覚せい剤原料の所持）若しくは第四号（覚せい剤原料の譲渡し等）の罪若しくはこれらの罪に係る同条第二項（営利目的の覚せい剤原料の所持、譲渡し等）の罪若しくはこれらの罪の未遂罪。

三　出入国管理及び難民認定法（昭和二十六年政令第三百十九号）第七十四条（集団密航者を不法入国させる行為等）、第七十四条の二（集団密航者の輸送）又は第七十四条の四（集団密航者の収受等）の罪。

四　麻薬及び向精神薬取締法（昭和二十八年法律第十四号）第六十四条（ジアセチルモルヒネ等の輸入等）、第六十四条の二（ジアセチルモルヒネ等の譲渡し、所持等）、第六十五条（ジアセチルモルヒネ等以外の麻薬の輸入等）、第六十六条（ジアセチルモルヒネ等以外の麻薬の譲渡し、所持等）、第六十六条の三（向精神薬の輸入等）又は第六十六条の四（向精神薬の譲渡し等）の罪。

五　武器等製造法（昭和二十八年法律第百四十五号）第三十一条（銃砲の無許可製造）、第三十一条の二（銃砲弾の無許可製造）又は第三十一条の三第一号（銃砲及び銃砲弾以外の武器の無許可製造）の罪。

六　あへん法（昭和二十九年法律第七十一号）第五十一条（けしの栽培、あへんの輸入等）又は第五十二条（あへん等の譲渡し、所持等）の罪。

七　銃砲刀剣類所持等取締法（昭和三十三年法律第六号）第三十一条から第三十一条の四まで（けん銃等の発射、輸入、所持、譲渡し等）、第三　十一条の七から第三十一条の九まで（けん銃実包の輸入、所持、譲渡し等）、第三十一条の十一第一項第二号（けん銃部品の輸入）若しくは第二項（未遂罪）又は第三十一条の十六第一項第二号（けん銃部品の所持）若しくは第三号（けん銃部品の譲渡し等）若しくは第二項（未遂罪）の罪。

八　国際的な協力の下に規制薬物に係る不正行為を助長する行為等の防止を図るための麻薬及び向精神薬取締法等の特例等に関する法律（平成三年法律第九十四号）第五条（業として行う不法輸入等）の罪。

九　組織的な犯罪の処罰及び犯罪収益の規制等に関する法律（平成十一年法律第百三十六号）第三条第一項第七号に掲げる罪に係る同条（組織的な殺人等）の罪又はその未遂罪。

附表

一、大麻管理法（昭和23年第124號法律）第24條（栽培、輸入等）或第24條之2（持有、轉讓等）之罪。

二、興奮劑管理法（昭和26年第252號法律）第41條（輸入等）或第41條之2（持有、轉讓等）之罪，同法第41條之3第1項第3款（輸入興奮劑原料等）或第4款（製造興奮劑原料）之罪或與該等犯罪相關之同條第2項（以營利為目的輸入興奮劑原料等）之罪或未遂之罪，或同法第41條之4第1項第3款（持有

興奮劑原料）或第4款（轉讓興奮劑原料等）之罪或與該等犯罪相關之同條第2項（以營利為目的持有、轉讓興奮劑原料等）之罪或未遂之罪。

三、出入境管理及難民認定法（昭和26年第319號政令）第74條（使集體偷渡者非法入境之行為等）、第74條之2（運送集體偷渡者）或第74條之4（收容集體偷渡者等）之罪。

四、麻醉藥品及精神藥品管理法（昭和28年第14號法律）第64條（輸入海洛因等）、第64條之2（轉讓、持有海洛因等）、第65條（輸入海洛因等以外之麻醉藥品等）、第66條（轉讓、持有海洛因等以外之麻醉藥品等）、第66條之3（輸入精神藥品等）或第66條之4（轉讓精神藥品等）之罪。

五、武器等製造法（昭和28年第145號法律）第31條（未經許可製造槍砲）、第31條之2（未經許可製造彈藥）或第31條之3第1款（未經許可製造槍砲及彈藥以外之武器）之罪。

六、鴉片法（昭和29年第71號法律）第51條（種植罌粟、輸入鴉片等）或第52條（轉讓、持有鴉片等）之罪。

七、持有槍砲、刀械管理法（昭和33 年第6號法律）第31條至第31條之4（發射、輸入、持有、轉讓手槍等）、第31條之7至第31條之9（輸入、持有、轉讓手槍子彈等）、第31條之11第1項第2款（輸入手槍零件）或第2項（未遂罪）或第31條之16第1項第2款（持有手槍零件）或第3款（轉讓手槍零件等）或第2 項（未遂罪）之罪。

八、關於國際合作下防止助長限制藥物之不當行為之麻醉藥品及精神藥品管理法等特例法律（平成3年第94號法律）第5條（以非法輸入為職業等）之罪。

九、處罰組織犯罪及規定犯罪收益法律（平成11年第136號法律）第3條第1項第7款所列之罪相關之同條（組織殺人等）之罪或其未遂之罪。

附錄三十一　中國大陸互聯網電子公告服務管理規定（節錄）

第一條　為了加強對互聯網電子公告服務（以下簡稱電子公告服務）的管理，規範電子公告信息發佈行為，維護國家安全和社會穩定，保障公民、法人和其他組織的合法權益，根據《互聯網信息服務管理辦法》的規定，制定本規定。

第二條　在中華人民共和國境內開展電子公告服務和利用電子公告發佈信息，適用本規定。

本規定所稱電子公告服務，是指在互聯網上以電子佈告牌、電子白板、電子論壇、網絡聊天室、留言板等交互形式為上網用戶提供信息發佈條件的行為。

第九條　任何人不得在電子公告服務系統中發佈含有下列內容之一的信息：

（一）反對憲法所確定的基本原則的；

（二）危害國家安全，洩露國家秘密，顛覆國家政權，破壞國家統一的；

（三）損害國家榮譽和利益的；

（四）煽動民族仇恨、民族歧視，破壞民族團結的；

（五）破壞國家宗教政策，宣揚邪教和封建迷信的；

（六）散佈謠言，擾亂社會秩序，破壞社會穩定的；

（七）散佈淫穢、色情、賭博、暴力、兇殺、恐怖或者教唆犯罪的；

（八）侮辱或者誹謗他人，侵害他人合法權益的；

（九）含有法律、行政法規禁止的其他內容的；

第十二條　電子公告服務提供者應當對上網用戶的個人信息保密，未經上網用戶同意不得向他人洩露，但法律另有規定的除外。

第十三條　電子公告服務提供者發現其電子公告服務系統中出現明顯屬於本辦法第九條所列的信息內容之一的，應當立即刪除，保存有關記錄，並向國家有關機關報告。

第十四條　電子公告服務提供者應當記錄在電子公告服務系統中發佈的信息內容及其發佈時間、互聯網地址或者域名。記錄備份應當保存 60 日，並在國家有關機關依法查詢時，予以提供。

第十五條　互聯網接入服務提供者應當記錄上網用戶的上網時間、用戶帳號、互聯網地址或者域名、主叫電話號碼等信息，記錄備份應保存 60 日，並在國家有關機關依法查詢時，予以提供。

第十七條　在電子公告服務系統中發佈本規定第九條規定的信息內容之一的，依據《互聯網信息服務管理辦法》第二十條的規定處罰。

第十九條　違反本規定第十二條的規定，未經上網用戶同意，向他人非法洩露上網用戶個人信息的，由省、自治區、直轄市電信管理機構責令改正；給上網用戶造成損害或者損失的，依法承擔法律責任。

第二十條　未履行本規定第十三條、第十四條、第十五條規定的義務的，依據《互聯網信息服務管理辦法》第二十一條、第二十三條的規定處罰。

附錄三十二　中國大陸互聯網信息服務管理辦法（節錄）

第一條　為了規範互聯網信息服務活動，促進互聯網信息服務健康有序發展，制定本辦法。

第二條　在中華人民共和國境內從事互聯網信息服務活動，必須遵守本辦法。

本辦法所稱互聯網信息服務，是指通過互聯網向上網用戶提供信息的服務活動。

第三條　互聯網信息服務分為經營性和非經營性兩類。

經營性互聯網信息服務，是指通過互聯網向上網用戶有償提供信息或者網頁制作等服務活動。

非經營性互聯網信息服務，是指通過互聯網向上網用戶無償提供具有公開性、共享性信息的服務活動。

第四條　國家對經營性互聯網信息服務實行許可制度；對非經營性互聯網信息服務實行備案制度。

未取得許可或者未履行備案手續的，不得從事互聯網信息服務。

第十三條　互聯網信息服務提供者應當向上網用戶提供良好的服務，並保證所提供的信息內容合法。

第十四條　從事新聞、出版以及電子公告等服務項目的互聯網信息服務提供者，應當記錄提供的信息內容及其發布時間、互聯網地址或者域名；互聯網接入服務提供者應當記錄上網用戶的上網時間、用戶賬號、互聯網地址或者域名、主叫電話號碼等信息。

互聯網信息服務提供者和互聯網接入服務提供者的記錄備份應當保存 60 日，並在國家有關機關依法查詢時，予以提供。

第十五條　互聯網信息服務提供者不得制作、復制、發布、傳播含有下列內容的信息：

（一）反對憲法所確定的基本原則的；

（二）危害國家安全，泄露國家秘密，顛覆國家政權，破壞國家統一的；

（三）損害國家榮譽和利益的；

（四）煽動民族仇恨、民族歧視，破壞民族團結的；

（五）破壞國家宗教政策，宣揚邪教和封建迷信的；

（六）散布謠言，擾亂社會秩序，破壞社會穩定的；

（七）散布淫穢、色情、賭博、暴力、兇殺、恐怖或者教唆犯罪的；

（八）侮辱或者誹謗他人，侵害他人合法權益的；

（九）含有法律、行政法規禁止的其他內容的。

第十六條 互聯網信息服務提供者發現其網站傳輸的信息明顯屬于本辦法第十五條所列內容之一的，應當立即停止傳輸，保存有關記錄，並向國家有關機關報告。

第二十一條 未履行本辦法第十四條規定的義務的，由省、自治區、直轄市電信管理機構責令改正；情節嚴重的，責令停業整頓或者暫時關閉網站。

第二十三條 違反本辦法第十六條規定的義務的，由省、自治區、直轄市電信管理機構責令改正；情節嚴重的，對經營性互聯網信息服務提供者，並由發證機關吊銷經營許可證，對非經營性互聯網信息服務提供者，並由備案機關責令關閉網站。

附錄三十三　中國大陸計算機信息網絡國際聯網安全保護管理辦法（節錄）

第二條　中華人民共和國境內的計算機信息網絡國際聯網安全保護管理，適用本辦法。

第三條　公安部計算機管理監察機構負責計算機信息網絡國際聯網的安全保護管理工作。公安機關計算機管理監察機構應當保護計算機信息網絡國際聯網的公共安全，維護從事國際聯網業務的單位和個人的合法權益和公眾利益。

第四條　任何單位和個人不得利用國際聯網危害國家安全、泄露國家秘密，不得侵犯國家的、社會的、集體的利益和公民的合法權益，不得從事違法犯罪活動。

第五條　任何單位和個人不得利用國際聯網製作、複製、查閱和傳播下列信息：

（一）煽動抗拒、破壞憲法和法律、行政法規實施的；

（二）煽動顛覆國家政權，推翻社會主義制度的；

（三）煽動分裂國家、破壞國家統一的；

（四）煽動民族仇恨、民族歧視，破壞民族團結的；

（五）捏造或者歪曲事實，散布謠言，擾亂社會秩序的；

（六）宣揚封建迷信、淫穢、色情、賭博、暴力、兇殺、恐怖，教唆犯罪的；

（七）公然侮辱他人或者捏造事實誹謗他人的；

（八）損害國家機關信譽的；

（九）其他違反憲法和法律、行政法規的。

第八條　從事國際聯網業務的單位和個人應當接受公安機關的安全監督、檢查和指導，如實向公安機關提供有關安全保護的信息、資料及數據文件，協助公安機關查處通過國際聯網的計算機信息網絡的違法犯罪行為。

第十條　互聯單位、接入單位及使用計算機信息網絡國際聯網的法人和其他組織應當履行下列安全保護職責：

（一）負責本網絡的安全保護管理工作，建立健全安全保護管理制度；

（二）落實安全保護技術措施，保障本網絡的運行安全和信息安全；

（三）負責對本網絡用戶的安全教育和培訓；

（四）對委託發布信息的單位和個人進行登記，並對所提供的信息內容按照本辦法第五條進行審核

（五）建立計算機信息網絡電子公告系統的用戶登記和信息管理制度；

（六）發現有本辦法第四條、第五條、第六條、第七條所列情形之一的，應當保留有關原始記錄，並在二十四小時內向當地公安機關報告；

（七）按照國家有關規定，刪除本網絡中含有本辦法第五條內容的地址、目錄或者關閉服務器。

第十五條　省、自治區、直轄市公安廳（局），地（市）、縣（市）公安局，應當有相應機構負責國際聯網的安全保護管理工作。

第十七條　公安機關計算機管理監察機構應當督促互聯單位、接入單位及有關用戶建立健全安全保護管理制度。監督、檢查網絡安全保護管理以及技術措施的落實情況。公安機關計算機管理監察機構在組織安全檢查時，有關單位應當派人參加。公安機關計算機管理監察機構對安全檢查發現的問題，應當提出改進意見，作出詳細記錄，存檔備查。

第十八條　公安機關計算機管理監察機構發現含有本辦法第五條所列內容的地址、目錄或者服務器時，應當通知有關單位關閉或者刪除。

附錄三十四　中華人民共和國計算機信息網絡國際聯網管理暫行規定實施辦法（節錄）

第二條　中華人 民共和國境內的計算機信息網絡進行國際聯網，依照本辦法辦理。

第三條　本辦法下列用語的含義是：

（一）國際聯網，是指中華人 民共和國境內的計算機互聯網絡、專業計算機　信息網絡、企業計算機信息網絡，以及其他通過專線進行國際聯網的計算機信息網絡同外國的計算機信息網絡相聯接。

（二）接入網絡，是指通過接入互聯網絡進行國際聯網的計算機信息網絡；接入網絡可以是多級聯接的網絡。

（三）國際出入口信道，是指國際聯網所使用的物理信道。

（四）用戶，是指通過接入網絡進行國際聯網的個人、法人和其他組織；個人用戶是指具有聯網帳號的個人。

（五）專業計算機信息網絡，是指為行業服務的專用計算機信息網絡。

（六）企業計算機信息網絡，是指企業內部自用的計算機信息網絡。

第十九條　國際出入口信道提供單位、互聯單位和接入單位應當保存與其服務相關的所有信息資料；在國務院信息化工作領導小組辦公室和有關主管部門進行檢查時，應當及時提供有關信息資料。

國際出入口信道提供單位、互聯單位每年二月份向國務院信息化工作領導小組辦公室提交上一年度有關網絡運行、業務發展、組織管理的報告。

第二十條　互聯單位、接入單位和用戶應當遵守國家有關法律、行政法規，嚴格執行國家安全保密製度；不得利用國際聯網從事危害國家安全、洩露國家秘密等違法犯罪活動，不得製作、查閱、複製和傳播妨礙社會治安和淫穢色情等有害信息；發現有害信息應當及時向有關主管部門報告，並採取有效措施，不得使其擴散。

附錄三十五　中國大陸互聯網新聞信息服務管理規定（節錄）

第一條　為了規範互聯網新聞信息服務，滿足公眾對互聯網新聞信息的需求，維護國家安全和公共利益，保護互聯網新聞信息服務單位的合法權益，促進互聯網新聞信息服務健康、有序發展，制定本規定。

第二條　在中華人 民共和國境內從事互聯網新聞信息服務，應當遵守本規定。

本規定所稱新聞信息，是指時政類新聞信息，包括有關政治、經濟、軍事、外交等社會公共事務的報導、評論，以及有關社會突發事件的報導、評論。

本規定所稱互聯網新聞信息服務，包括通過互聯網登載新聞信息、提供時政類電子公告服務和向公眾發送時政類通訊信息。

第五條　互聯網新聞信息服務單位分為以下三類：

（一）新聞單位設立的登載超出本單位已刊登播發的新聞信息、提供時政類電子公告服務、向公眾發送時政類通訊信息的互聯網新聞信息服務單位；

（二）非新聞單位設立的轉載新聞信息、提供時政類電子公告服務、向公眾發送時政類通訊信息的互聯網新聞信息服務單位；

（三）新聞單位設立的登載本單位已刊登播發的新聞信息的互聯網新聞信息服務單位。

第十九條　互聯網新聞信息服務單位登載、發送的新聞信息或者提供的時政類電子公告服務，不得含有下列內容：

（一）違反憲法確定的基本原則的；

（二）危害國家安全，洩露國家秘密，顛覆國家政權，破壞國家統一的；

（三）損害國家榮譽和利益的；

（四）煽動民族仇恨、民族歧視，破壞民族團結的；

（五）破壞國家宗教政策，宣揚邪教和封建迷信的；

（六）散佈謠言，擾亂社會秩序，破壞社會穩定的；

（七）散佈淫穢、色情、賭博、暴力、恐怖或者教唆犯罪的；

（八）侮辱或者誹謗他人，侵害他人合法權益的；

（九）煽動非法集會、結社、遊行、示威、聚眾擾亂社會秩序的；

（十）以非法民間組織名義活動的；

（十一）含有法律、行政法規禁止的其他內容的。

第二十條　互聯網新聞信息服務單位應當建立新聞信息內容管理責任制度。不得登載、發送含有違反本規定第三條第一款、第十九條規定內容的新聞信息；發現提供的時政類電子公告服務中含有違反本規定第三條第一款、第十九條規定內容的，應當立即刪除，保存有關記錄，並在有關部門依法查詢時予以提供。

第二十一條　互聯網新聞信息服務單位應當記錄所登載、發送的新聞信息內容及其時間、互聯網地址，記錄備份應當至少保存 60 日，並在有關部門依法查詢時予以提供。

第二十三條　國務院新聞辦公室和省、自治區、直轄市人民政府新聞辦公室，應當對互聯網新聞信息服務進行監督；發現互聯網新聞信息服務單位登載、發送的新聞信息或者提供的時政類電子公告服務中含有違反本規定第三條第一款、第十九條規定內容的，應當通知其刪除。

互聯網新聞信息服務單位應當立即刪除，保存有關記錄，並在有關部門依法查詢時予以提供。

第二十七條　互聯網新聞信息服務單位登載、發送的新聞信息含有本規定第十九條禁止內容，或者拒不履行刪除義務的，由國務院新聞辦公室或者省、自治區、直轄市人民政府新聞辦公室給予警告，可以並處 1 萬元以上 3 萬元以下的罰款；情節嚴重的，由電信主管部門根據有關主管部門的書面認定意見，按照有關互聯網信息服務管理的行政法規的規定停止其互聯網信息服務或者責令互聯網接入服務者停止接入服務。

互聯網新聞信息服務單位登載、發送的新聞信息含有違反本規定第三條第一款規定內容的，由國務院新聞辦公室或者省、自治區、直轄市人民政府新聞辦公室依據各自職權依照前款規定的處罰種類、幅度予以處罰。

附錄三十六　新加坡濫用電腦法（節錄）

COMPUTER MISUSE ACT
（CHAPTER 50A）

（Original Enactment: Act 19 of 1993）

REVISED EDITION 2007
（31st July 2007）

An Act to make provision for securing computer material against unauthorised access or modification and for matters related thereto.

[30th August 1993]

PART I

PRELIMINARY

Short title

1. This Act may be cited as the Computer Misuse Act.

Interpretation

2. —（1） In this Act, unless the context otherwise requires —

"computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include —

（*a*） an automated typewriter or typesetter;

（*b*） a portable hand-held calculator;

（*c*） a similar device which is non-programmable or which does not contain any data storage facility; or

（*d*）such other device as the Minister may, by notification in the *Gazette*, prescribe;

"computer output" or "output" means a statement or representation （whether in written, printed, pictorial, graphical or other form） purporting to be a statement or representation of fact —

（*a*） produced by a computer; or

（*b*） accurately translated from a statement or representation so produced;

"computer service" includes computer time, data processing and the storage or retrieval of data;

"damage" means, except for the purposes of section 13, any impairment to a computer or the integrity or availability of data, a program or system, or information, that —

(*a*) causes loss aggregating at least $10,000 in value, or such other amount as the Minister may, by notification in the *Gazette*, prescribe except that any loss incurred or accrued more than one year after the date of the offence in question shall not be taken into account;

(*b*) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment or care of one or more persons;

(*c*) causes or threatens physical injury or death to any person; or

(*d*) threatens public health or public safety;

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer;

"electro-magnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer;

"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer;

"intercept", in relation to a function of a computer, includes listening to or recording a function of a computer, or acquiring the substance, meaning or purport thereof;

"program or computer program" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function.

[21/98]

(2) For the purposes of this Act, a person secures access to any program or data held in a computer if by causing a computer to perform any function he —

(*a*) alters or erases the program or data;

(*b*) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

（*c*） uses it; or

（*d*） causes it to be output from the computer in which it is held （whether by having it displayed or in any other manner）,

and references to access to a program or data （and to an intent to secure such access） shall be read accordingly.

（3）For the purposes of subsection（2）(*c*), a person uses a program if the function he causes the computer to perform —

（*a*） causes the program to be executed; or

（*b*） is itself a function of the program.

（4） For the purposes of subsection （2）（*d*）, the form in which any program or data is output （and in particular whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable of being processed by a computer） is immaterial.

（5） For the purposes of this Act, access of any kind by any person to any program or data held in a computer is unauthorised or done without authority if —

（*a*） he is not himself entitled to control access of the kind in question to the program or data; and

（*b*） he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.

（6） A reference in this Act to any program or data held in a computer includes a reference to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.

（7） For the purposes of this Act, a modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer —

（*a*） any program or data held in the computer concerned is altered or erased;

（*b*） any program or data is added to its contents; or

（*c*） any act occurs which impairs the normal operation of any computer,

and any act which contributes towards causing such a modification shall be regarded as causing it.

[S 92/97]

（8） Any modification referred to in subsection （7） is unauthorised if —

（*a*） the person whose act causes it is not himself entitled to determine whether the modification should be made; and

（*b*） he does not have consent to the modification from any person who is so entitled.

（9） A reference in this Act to a program includes a reference to part of a program.

[UK CMA 1990, s. 17 （2）-（8） and （10）; Canada CLAA 1985, s. 301.2 （2） （part）; S Aust. EA 1929, s. 59A]

附錄三十七　新加坡電子交易法（節錄）

ELECTRONIC TRANSACTIONS ACT
（CHAPTER 88）

（Original Enactment: Act 16 of 2010）

REVISED EDITION 2011
（31st December 2011）

An Act to provide for the security and use of electronic transactions, to implement the United Nations Convention on the Use of Electronic Communications in International Contracts adopted by the General Assembly of the United Nations on 23rd November 2005 and to provide for matters connected therewith.

[1st July 2010]

PART I

PRELIMINARY

Short title

1. This Act may be cited as the Electronic Transactions Act.

Interpretation

2.

—（1） In this Act, unless the context otherwise requires —

"addressee", in relation to an electronic communication, means a party who is intended by the originator to receive the electronic communication, but does not include a party acting as an intermediary with respect to that electronic communication;

"authorised officer", in relation to the exercise of any power or performance of any duty under this Act, means a person to whom the exercise of that power or performance of that duty has been delegated under section 27;

"automated message system" means a computer program or an electronic or other automated means used to initiate an action or respond to data messages or performances in whole or in part, without review or intervention by a natural person each time an action is initiated or a response is generated by the program or electronic or other means;

"communication" includes any statement, declaration, demand, notice, request, offer or the acceptance of an offer, that the parties are required to make or choose to make in connection with the formation or performance of a contract;

"Controller" means the Controller appointed under section 27（1） and includes a Deputy or an Assistant Controller appointed under section 27（3）;

"electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities;

"electronic communication" means any communication that the parties make by means of electronic records;

"electronic record" means a record generated, communicated, received or stored by electronic means in an information system or for transmission from one information system to another;

"information" includes data, text, images, sound, codes, computer programs, software and databases;

"information system" means a system for generating, sending, receiving, storing or otherwise processing electronic records;

"originator", in relation to an electronic communication, means a party by whom, or on whose behalf, the electronic communication has been sent or generated prior to storage, if any, but does not include a party acting as an intermediary with respect to that electronic communication;

"public agency" means a department or ministry of the Government, an Organ of State or a public authority established by or under a public Act;

"record" means information that is inscribed, stored or otherwise fixed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form;

"rule of law" includes written law;

"secure electronic record" means an electronic record that is treated as a secure electronic record by virtue of section 17（1） or any other provision of this Act;

"secure electronic signature" means an electronic signature that is treated as a secure electronic signature by virtue of section 18 or any other provision of this Act;

"security procedure" means a procedure for the purpose of —

（*a*） verifying that an electronic record is that of a specific person; or

（*b*） detecting error or alteration in the communication, content or storage of an electronic record since a specific point in time,

which may require the use of algorithms or codes, identifying words or numbers, encryption, answerback or acknowledgment procedures, or similar security devices;

"signed" or "signature" and its grammatical variations means a method （electronic or otherwise） used to identify a person and to indicate the intention of that person in respect of the information contained in a record;

"specified security procedure" means a security procedure which is specified in the Second Schedule;

"specified security procedure provider" means a person involved in the provision of a specified security procedure.

（2） In this Act, "place of business", in relation to a party, means —

（*a*） any place where the party maintains a non-transitory establishment to pursue an economic activity other than the temporary provision of goods or services out of a specific location; or

（*b*） if the party is a natural person and he does not have a place of business, the person's habitual residence.

（3） For the purposes of subsection （2） —

（*a*） if a party has indicated his place of business, the location indicated by him is presumed to be his place of business unless another party proves that the party making the indication does not have a place of business at that location;

（*b*） if a party has not indicated a place of business and has more than one place of business, then the place of business is that which has the closest relationship to the relevant contract, having regard to the circumstances known to or contemplated by the parties at any time before or at the conclusion of the contract;

（*c*） a location is not a place of business merely because that location is —

（i） where equipment and technology supporting an information system used by a party in connection with the formation of a contract are located; or

（ii） where the information system may be accessed by other parties; and

（*d*） the sole fact that a party makes use of a domain name or an electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country.

（4） Where an electronic communication does not relate to any contract, references to a contract in subsection （3） shall refer to the relevant transaction.

[ETA, ss. 2 and 18（4）; UN, Art. 4, 6 and 9（3）（a）; US, s. 106（2）]

Purposes and construction

3. This Act shall be construed consistently with what is commercially reasonable under the circumstances and to give effect to the following purposes:

（*a*） to facilitate electronic communications by means of reliable electronic records;

（*b*） to facilitate electronic commerce, to eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements, and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce;

（*c*） to facilitate electronic filing of documents with public agencies, and to promote efficient delivery by public agencies of services by means of reliable electronic records;

（*d*） to minimise the incidence of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce and other electronic transactions;

（*e*） to help to establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records;

（*f*） to promote public confidence in the integrity and reliability of electronic records and electronic commerce, and to foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium; and

（*g*） to implement the United Nations Convention on the Use of Electronic Communications in International Contracts adopted by the General Assembly of the

United Nations on 23rd November 2005 and to make the law of Singapore on electronic transactions, whether or not involving parties whose places of business are in different States, consistent with the provisions of that Convention.

[ETA, s. 3]

Excluded matters

4.

—（1） The provisions of this Act specified in the first column of the First Schedule shall not apply to any rule of law requiring writing or signatures in any of the matters specified in the second column of that Schedule.

（2） The Minister may, by order published in the *Gazette*, amend the First Schedule.

[ETA, s. 4]

Party autonomy

5.

—（1） Nothing in Part II shall affect any rule of law or obligation requiring the agreement or consent of the parties as to the form of a communication or record, and （unless otherwise agreed or provided by a rule of law） such agreement or consent may be inferred from the conduct of the parties.

（2）Nothing in Part II shall prevent the parties to a contract or transaction from —

（*a*） excluding the use of electronic records, electronic communications or electronic signatures in the contract or transaction by agreement; or

（*b*） imposing additional requirements as to the form or authentication of the contract or transaction by agreement.

（3） Subject to any other rights or obligations of the parties to a contract or transaction, the parties may, by agreement —

（*a*） exclude section 6, 11, 12, 13, 14, 15 or 16 from applying to the contract or transaction; or

（*b*） derogate from or vary the effect of all or any of those provisions in respect of the contract or transaction.

[ETA, s. 5; UN, Art. 3 and 8（2）]

附錄三十八　新加坡電信法（節錄）

TELECOMMUNICATIONS ACT
（CHAPTER 323）

（Original Enactment: Act 43 of 1999）

REVISED EDITION 2000
（30th December 2000）

An Act to provide for the operation and provision of telecommunication systems and services in Singapore, and for matters connected therewith.

[1st December 1999]

PART I

PRELIMINARY

Short title

1. This Act may be cited as the Telecommunications Act.

Interpretation

2. In this Act, unless the context otherwise requires —

"Authority" means the Info-communications Development Authority of Singapore established under the Info-communications Development Authority of Singapore Act （Cap. 137A）;

"broadcasting apparatus" and "broadcasting service" have the same meanings as in the Broadcasting Act （Cap. 28）;

[10/2005 wef 16/02/2005]

"Chief Executive" means the Chief Executive of the Authority and includes any temporary Chief Executive of the Authority appointed under section 10 of the Info-communications Development Authority of Singapore Act;

"code of practice" means a code of practice issued or approved under section 19 or 26;

[Act 19 of 2011 wef 01/02/2012]

"earthworks" includes —

（*a*） any act of excavating earth, rock or other material （by whatever means） in connection with —

（i） any works for or relating to the construction, reconstruction, extension, renovation, alteration, demolition or repair of any building, road, railway, bridge, viaduct, flyover, sewer or sewage works;

（ii） any works for or relating to the laying, inspecting, repairing or renewing of any mains, pipes, cables, fittings or other apparatuses;

（iii） any soil investigation works; or

（iv） such other works as are usually undertaken by a person carrying on business as a contractor in the construction industry or as a professional civil or structural engineer;

（*b*） any act of boring, dredging, jacking, levelling, piling or tunnelling on or under any premises or street by any mechanical means; and

（*c*） the driving or sinking of any earth rod, casing or tube into the ground;

"equipment" includes any appliance, apparatus or accessory used or intended to be used for telecommunications, including （for the avoidance of doubt） any such appliance, apparatus or accessory capable of being used for the operation of any broadcasting service;

[Act 19 of 2011 wef 01/02/2012]

"Hertzian or radio waves" means electro-magnetic waves of frequencies not exceeding 1,000 terahertz propagated in space without any artificial guide;

"installation or plant used for telecommunications" includes all buildings, lands, structures, machinery, equipment, cables, poles and lines used or intended for use in connection with telecommunications;

"Media Development Authority of Singapore" means the Media Development Authority of Singapore established under the Media Development Authority of Singapore Act （Cap. 172）;

[Act 19 of 2011 wef 01/02/2012]

"message" means any sign, signal, writing, image, sound, intelligence or information of any nature transmitted by telecommunications;

"public telecommunication licensee" means a person designated by the Authority under section 6;

"public telecommunication licensee's installation or plant" means any installation or plant used for telecommunications belonging to or used by a public telecommunication licensee;

"radio-communication" means any telecommunication by means of Hertzian or radio waves;

"radio-communication service" means any service for radio-communications;

"radio-communication system" means any system used or intended to be used for radio-communications;

"repealed Act" means the Telecommunication Authority of Singapore Act （Cap. 323, 1993 Ed.） repealed by the Info- communications Development Authority of Singapore Act （Cap. 137A）;

"securities", in relation to a company, includes shares, debentures, bonds and other securities of the company, whether or not constituting a charge on the assets of the company;

"shares" includes stock;

"standard of performance" means a standard of performance issued or approved under section 26;

[Act 19 of 2011 wef 01/02/2012]

"street" includes any way, road, lane, path, passage or open space, whether a thoroughfare or not, over which the public have a right of way and also the roadway and footway over any public bridge and includes any road, footway or passage, used or intended to be used as a means of access to 2 or more holdings, whether the public has a right of way thereover or not;

"TAS" means the Telecommunication Authority of Singapore reconstituted by the repealed Act;

"telecommunication cable" means any cable of a telecommunication system belonging to or under the management or control of a telecommunication system licensee;

"telecommunication cable detection work" means any work of detecting or locating any underground telecommunication cable;

"telecommunication cable detection worker" means any person whose trade or occupation requires or includes the personal performance by him of telecommunication cable detection work;

"telecommunication cable detection work licence" means a licence granted under section 30;

"telecommunication licensee" means a person to whom a licence has been granted under section 5 or 5B;

[Act 19 of 2011 wef 01/02/2012]

"telecommunication line" means a wire or cable used for telecommunications with any casing, coating, tube or pipe enclosing the same and any appliance and apparatus connected therewith for the purpose of fixing or insulating the same;

"telecommunication service" means any service for telecommunications but excludes any broadcasting service;

"telecommunication system" means any system used or intended to be used for telecommunications, including（for the avoidance of doubt）any such system capable of being used for the operation of any broadcasting service;

[Act 19 of 2011 wef 01/02/2012]

"telecommunication system licensee" means a person licensed under section 5 to operate a telecommunication system;

"telecommunications" means a transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature by wire, radio, optical or other electro-magnetic systems whether or not such signs, signals, writing, images, sounds or intelligence have been subjected to rearrangement, computation or other processes by any means in the course of their transmission, emission or reception;

"vessel" includes any ship, boat, air-cushioned vehicle or floating rig or platform used in any form of operations at sea or any other description of vessel.

附錄三十九　電信法修正草案條文對照表（節錄）

國家通訊傳播委員會101年7月30日函報行政院審查電信法修正草案版本

修正條文	現行條文	說明
第一章　總則	第一章　總則	章名未修正。
第一條　為健全電信產業發展，增進公共利益與福祉，促進匯流服務與市場競爭，維護通信安全及保障消費者權益，特制定本法；本法未規定者，依其他法律之規定。	第一條　為健全電信發展，增進公共福利，保障通信安全及維護使用者權益，特制定本法；本法未規定者，依其他法律之規定。	鑑於本次修法重點包括修訂數位匯流、促進市場充分競爭及保障消費者權益等相關規範，爰將本條所揭示之立法目的配合酌作文字修正。
第二章　電信事業之經營	第二章　電信事業之經營	章名未修正。
第十二條　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。 前項電信機線設備指連接發信端與受信端之網路傳輸設備、與網路傳輸設備形成一體而設置之交換設備、以及二者之附屬設備。 第二類電信事業指第一類電信事業以外之電信事業。	第十一條　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。 前項電信機線設備指連接發信端與受信端之網路傳輸設備、與網路傳輸設備形成一體而設置之交換設備、以及二者之附屬設備。 第二類電信事業指第一類電信事業以外之電信事業。	條次變更，其餘未修正。
第三章　利用電信網路提供視聽媒體服務		一、本章新增。 二、本章增訂目的在於促進匯流服務，鼓勵電信事業充分有效發揮其網路效益，讓電信事業除依廣電三法外，仍得依電信法建構視聽媒體傳輸平臺，並使內容提供者可有選擇平臺播放之機會，並朝向消除匯流障礙方向調整，以促進新服務之發展。
第四章　電信建設與管理	第三章　電信建設與管理	章次調整，章名未修正。
第一節　土地之取得與使用	第一節　土地之取得與使用	本節節名未修正。
第二節　電信設備之維護與管理	第二節　電信設備之維護與管理	本節節名未修正。

第五十六條　為確保電信事業系統設備、資料及網路之安全，保障民眾通信權益，電信事業應辦理下列事項： 一、建立資通安全管理機制。 二、建立資通安全防護及偵測設施。 三、建立資通安全聯防及資通安全事件之通報、處理、回報等資通安全應變措施。 四、使用經資通安全審驗之資通設備。 前項系統設備包括核心網路設備、傳輸網路設備、接取網路設備、網路管理系統設備及其他重要電信設備。 電信事業處理資通安全事件時，得要求用戶及使用人配合辦理資通安全有關措施；其屬重大資通安全事件者，必要時得暫停或終止服務之一部或全部。 前項之規定意旨，電信事業應以顯著方式載明於營業規章及服務契約。 電信事業資通安全管理機制之查核項目與程序、適用之驗證標準與範圍、資通安全之防護與偵測、聯防與應變、重大資通安全事件範圍及其他應遵行事項之管理辦法，由主管機關定之。 主管機關為進行網際網路資通安全聯防，應		一、本條新增。 二、近年來由於網際網路蓬勃發展及電子商務之普及應用，電信事業利用其通訊系統，結合網際網路傳送訊息、影像或聲音。然網路之便利性，亦引發頻繁之資安事件及日新月異之攻擊手法。我國政府機關（構）自民國九十年起已推動資訊安全管理制度，並獲致一定之成果。為達資通安全防護全面化，對民眾隱私保護影響重大之電信事業亦應建立資通安全管理機制，另為強化電信事業資通安全之防護能力，防禦日益頻繁之資安事件發生，電信事業應建立適當之資通安全防護及偵測設施，蒐集所屬網段遭受惡意程式或殭屍電腦之攻擊行為，以防堵任何資通安全之漏洞與弱點，降低資安所造成之威脅，並為架構我國整體資通基礎設施之資安防護網，爰訂定第一項。 三、說明系統設備之範圍，爰訂定第二項。 四、為即時應變資安事件，降低對整體網路之傷害，爰於第三項明定電信事業處理資通安全事件，得要求使用電信人配合辦理有關措施，且遇重大資通安全

建置及管理資通安全聯防應變系統。必要時，得指定專責機構建置及管理之。 第一項第四款資通設備應施檢驗項目及其資通安全檢測技術規範，由主管機關訂定公告之。主管機關為資通設備安全檢測需要，應建置及管理資通安全測試樣本資料庫。必要時，得指定專責機構建置及管理之。 前項資通設備之審驗方式與程序、審驗證明之核發、換發、補發與廢止、審驗合格標籤之標貼、印鑄與使用，及審驗業務管理等事項之辦法，由主管機關定之。		事件發生時，得暫停或終止服務之一部或全部。 五、為使第三項之要求具有明確性，爰於第四項明定應載明於電信事業之營業規章及服務契約中，並應以顯著方式呈現。 六、第五項授權主管機關訂定管理辦法規範之。 七、為與政府、教育及學術等網路進行網際網路資通安全聯防，主管機關應建置及管理資通安全聯防應變系統，且本系統需要配置足夠之技術人員以對資通安全事件進行蒐集、分析、分享、匯入、審核、通報、回報等工作，並適時擴充系統功能，亟須由專責機構之專業技術人員協助維運，爰參照水污染防治法、空氣污染防制法、海洋污染防治法等規定，授權主管機關於必要時，得指定專責機構建置與管理本系統，爰於第六項明定之。 八、第七項授權主管機關訂定資通安全檢測技術規範。為提供檢測實驗室資通安全測試樣本，需建置測試樣本資料庫，考量該資料庫具高度敏感，並應隨時做樣本蒐集與更新，亟須由專責機構之專業技術人員協助維運，爰參照水污染防治法、空氣污染防制法、海洋污染防治法等規定，授權主

		管機關於必要時，得指定專責機構建置與管理本系統。 九、第八項授權主管機關訂定審驗辦法。

附錄四十　「網路平台業者紀錄保存規範之研究」座談會會議紀錄

會議時間：民國 101 年 10 月 24 日（星期三）14:00~16:00

會議地點：警政署刑事警察局偵查科技大樓 13 樓會議室

出席人員：

中華警政研究學會　廖有祿主任（主席）

國家通訊傳播委員會　林隆全科長

經濟部商業司　徐漢強組長（資策會代表）

經濟部工業局　沈傳玥技士

資策會科法所　尤騰毅研究員

警政署刑事警察局偵九隊　邱承迪副組長

警政署刑事警察局通訊監察中心　林煒翔組長

警政署刑事警察局偵查科　黃家俊偵查員

警政署刑事警察局資訊室　楊凱勝技正兼組長

警政署刑事警察局司法科　李雅惠組長

警政署刑事警察局研發室　王翔正偵查員

臺灣微軟股份有限公司　蔡文宜法務經理

香港商雅虎資訊股份有限公司　許慶玲法務副總

網路家庭國際資訊股份有限公司　佘仲杰法務專員

Marktplaats BV 公司（奇集集）　簡莉琪產品經理

Marktplaats BV 公司（奇集集）　林宗民客服人員

中華警政研究學會　張維平助理教授

中華警政研究學會　蘇莞筑

中華警政研究學會　劉怡汎

會議紀錄：

一、主席致詞：本計畫為刑事警察局委託的「網路平台服務業者紀錄保存規範之研究」，目前進度已完成歐、美、亞主要國家有關網路平台業者電磁紀錄保存的相關法規蒐集，並對照我國現行法規加以分析，比較各種方案的利弊得

失，找出適合我國法制的可能修法或立法方向，但為避免政策建議不切實際，不符合實務機關需求，本座談會邀集偵查網路犯罪的警察單位、協助提供資料的網路平台業者及主管相關法規的目的事業主管機關進行討論，了解偵查單位辦案的實際需求及平台業者的成本考量，找出可行性高且效益彰顯之方案，供主管機關擬訂修法或立法政策參考，首先就計畫內容簡報（略），接著請大家提供寶貴意見。

二、香港商雅虎許副總：

1. 目前的平台業者大多為電信業者，也不屬於第二類電信事業，若是規範在電信法下的電信事業，是否在電信法中有其他通用的規則或規定能讓全體適用，因為韓國和印度都是在電信法中就有規範，只是規範內容過於籠統易有爭議，像是主管機關有極大職權去解釋法條，導致平台業者無法達到，不若電信業者具有完整的設施與系統而能做到規範要求。有鑑於國外經驗，若相關規範制定於電信法中，是否也會有類似的情況發生，當然業者本身也有自行檢視電信法規範，並將結果回報給各單位的義務。
2. 網路犯罪調查大多與電子商務有關，而電子商務中的交易資訊或銷售販賣等資訊，似乎並不屬於通訊保障及監察法之定義與範疇，可能需要再仔細研究。

三、廖主任：

本研究案主要是討論現有的法律，像是電信法或是通訊保障及監察法，當中明確的規範就是針對電信業者，而第二類電信事業管理規則第 27 條，實際上也只有規範到 IAP 的部分，所以平台業者的相關規範並不明確，當然會有些單位認為已經配合且合作很久，但是本研究仍認為應該明確訂定平台業者的相關規範。研究中將電信法與第二類電信事業管理規則中電信業者之定義擴及到平台業者，這可回應到許副總的問題，平台業者在電信法和通訊保障及監察法中亦未有明確規範，故藉由本次研究在定義上加以釐清，將來在執行上便可有所依據。

四、NCC 林科長：

1. 若將電子商務平台納入電信服務裡，有其適當性之考量，首先須先就電

信法的立場來看，按照組織法，電信法是 NCC 的主管事項，而研究重點為修訂第二類電信事業管理規則第 27 條第五項，也就是將網路平台服務納入，包含電子商務、電子訊息交易、線上購物、網路證券及電子銀行交易等，但這些並非通信服務，純然屬於商業行為的服務，按照電信法的定義，電信事業就是提供電信服務來營業的人，研究中也討論到個人是否能納入，在電信事業中並不會有個人型態，因為按照規定，個人提供電信事業服務必須成立公司或商業行號。

2. 以 NCC 立場來看，上述服務絕不會屬於電信服務，今天討論重點是在治安機關辦案時，最為困擾的就是交易買賣對象、來源及內容物，以雅虎為例，網路購物時出現帳號盜用的詐騙行為，但此行為仍舊屬於交易，從電信服務的角度來看，雅虎會知道是由誰賣出物品與誰上網購物等資訊，因為雅虎本身須認定該筆消費行為而保有紀錄。另外，信用卡的部分，金融機關也有規範提供網路交易必須保留紀錄等要求，例如銀行就有其管理的義務，此類管理的責任就如同將銀行證券交易納入電信紀錄中，並稱為電信事業交由 NCC 來管理，從以上例子來看，將上述服務修訂入第二類電信事業管理規則第 27 條與電信法中，目的就是要保存紀錄，但就主管機關來看是相當地不適宜。

3. 日前 NCC 有召開一個相關議題的會議，會議中行政院對於本身的業務在網際網路上的發展，該有的權責與認定都已很清楚，並不會認為網際網路上的事情都該由 NCC 來主管，舉例而言，在網路上的買賣動物行為，農委會絕不會認定是 NCC 的業務，這是農委會的權責。NCC 很肯定這次研究的辛苦，但是就今天的內容來看，覺得跟想像中是落差相當大。

4. 針對雅虎的問題，若是電信服務的話該如何處理，基本上電信法上的所有義務都要達到，營業規章服務契約都要去訂定，但坦白說這不容易去訂定，而 NCC 也很難去做管理，光是就電子商務的營業規章服務契約如何訂定到電信服務中，恐怕就有很大的困難。

五、廖主任：

1. 回應 NCC 林科長的部分，的確有提到一個很重要的問題，就是到底誰

是網路的主管機關，現在因為網路都是藉由電信去運作，自然就會認為是 NCC 的主管業務，可是我們也很清楚，像有些電子商務應該是由經濟部商業司或是工業局等單位來主管，不過就警察機關的立場來說，總是需要一個機關來主管，當然本研究的想法不一定都正確，也認為交由 NCC 來主管有點牽強，例如剛剛討論的第二類電信事業管理規則應該是針對電信業者，而本研究是規劃將電子商務涵蓋進去，只因為其是透過電信來進行資訊的傳遞，也就是因為這一點而利用定義作為串連，當然這個部分還有一些討論的空間，但這個受委託的研究案，目的總是要找出一個規範，看是訂定在什麼地方，研究結果就是第二類電信事業管理規則第 27 條所列內容最清楚，只是內容仍有不足的，所以才增列一些內容，譬如平台的部分。

2. 就剛剛林科長的意見，研究中所增列的內容與法規名稱是有些出入，所以就想透過解釋與定義的方式將其納入，這就是本研究的初步看法，當然也都還有討論的空間。

六、香港商雅虎許副總：

想請問刑事訴訟法有沒有可能納入相關規範內容？

七、NCC 林科長：

1. 就研究內容來看，瞭解重點就是在警方辦案時，若遇到金融業務必須去找金融單位，遇到商務就必須去找經濟部，遇到農產品就必須去找農委會，所以希望能有單一窗口，實務上 NCC 平常跟刑事局例行業務接觸的非常多，也很瞭解警方的邏輯所在，而這個研究內容算是打破行政院的體制，行政院各部會有分工職權，每個機關絕對按照它的組織法辦事，不可能說將相關內容修訂入電信法，就讓交通部去主管，若是真的修法成功，那未來金融局針對電子金融方面的規定恐怕受影響。

2. 信用卡部分的法規，是按照銀行法授權的，譬如一些金融卡的交易必須保留紀錄的規定，若是將其納入電信法中，是否侵犯到他機關的職權？這根本是打破行政機關之間的體制。另外，就辦案的立場，以 NCC 之前與刑事局資訊交流過的經驗而言，警察的社會秩序維護法中部分業務，也找不到主管機關，但這些業務就治安上又是有疑慮的，也必須要

去處理的，事實上在社會秩序維護法中，也給治安機關有一些權責能夠去處理，就如同剛剛雅虎許副總所述，別的國家也是在刑事訴訟法中有類似規定，就從電信事業主管的立場來看，第二類電信事業管理規則第27條都是針對電信事業的部分，例如電信事業提供上網，就會開始記錄上網的起始時間與提供的IP，介入更深的部分是因為早期很多電子郵件是由電信公司的網路來提供服務的，所以電子郵件也有納入主管範圍，但就現況來看，現在很多電子郵件像是GOOGLE MAIL，根本就是在應用產能上，完全不屬於電信網路範圍內，按照通訊保障及監察法的規定，電信事業根本不可能去瞭解與記錄這部分的通訊內容，包括什麼時候透過WEB發出MAIL，若真的要去記錄，那每天瀏覽網頁資料的記錄量是很驚人的，也是無法去儲存及處理的。

3. 還有提到SKYPE在網路上的服務，也是屬於應用層面的服務，事實上，到底是否能納入電信服務中去規管？用戶自己就可以去下載軟體，今天是因為SKYPE名聲太大，所以大家都清楚，但若用戶本身很厲害，自行寫出通訊的程式，然後就藉此與別人進行溝通，並不會有人知道溝通的內容，那難道能夠將之納入電信服務裡去嗎？其實是真的會很難去界定與處理的，所以基本上就現況而言，對於電腦對電腦的這一塊，事實上也尚未納入通訊保障及監察的對象，因為目前是將它認定為資訊服務，而研究中計畫要修訂的平台定義，當初其實就是屬於資訊服務而非電信服務，現在若要將資訊服務納入電信服務中來規範，還是回歸先前所述，按照NCC職權與在電信的認定上，是有其困難的。

八、廖主任：

1. 針對雅虎許副總提到的刑事訴訟法，本研究有檢視日本去年修訂的刑事訴訟法內容，當一旦犯罪發生，警察機關可以要求現在起所有的紀錄都要保存做為證據，可是現在問題在於，警察辦案通常需要去追溯留存的紀錄，而業者可以表示紀錄未留存，即使有存也會說未存，所以認為日本刑事訴訟法的規範，在我們國家實行可能會有問題。
2. 另外NCC林科長所提到的主管機關，本研究於第二類電信事業管理規則第27條中欲增列的項目，並非單純認為屬於電信就直接納入，像是

銀行法對於電子交易已經有所律定，此即認定為目的事業主管機關，也就是在原來的主管機關中，譬如說電信法與第二類電信事業管理規則的主管機關是 NCC，可是下面還有一些目的事業主管機關，例如銀行之於財政部，而本研究也只是將部分相關規定轉移至電信範圍，另外針對主管機關還有一個想法，警察機關最大的問題是位階比較低，研究中就有收集到大陸方面的資料，當中主管機關是公安部也就是警察，所以警察可以自行訂定規範，業者也必須要配合，但反觀我國就無法適用，所以希望能多收集些偵查單位的意見，畢竟本研究是以犯罪偵查角度為出發點，主要還是以偵查上的協助作為考慮。

3. 電信事業分為第一類與第二類電信事業，而 NCC 主管範圍就都有包含，當然其下 IAP 不可能保存所有的資料，而且客戶數量眾多，本研究的看法認為此屬分層服務，每一個 IPP 甚至下面的 ICP 業者，應該相對會留存一些資料，所以不該將責任都集中在 IAP 上，將來在偵查上，就還必須去跟平台業者調閱資料。

九、NCC 林科長：

1. NCC 支持研究概念，認為經營業務者對於其要防止被攻擊或是要保護交易公平性的目的，而去保留紀錄是合理的，因為經營服務事業，當然就必須負起相對責任，就如同廖主任所述，將紀錄保留的義務完全交由電信事業是不公平的，所以在第二類電信事業管理規則第 27 條也沒有這樣的要求，而針對犯罪偵查需要相關紀錄時，辦案時有些業者會有不配合的情事，所以希望能立法有所依據，但若為這樣的目的立法並納入電信法中，真的是比較不適宜，NCC 還是支持經營服務業者，就該有所屬的規範，譬如銀行法中為了要去健全體制，就有自己的管理辦法，在網際網路上進行信用卡交易時，就該保存相關的紀錄，回歸先前提到的原則，應該根據目的事業的內容，去檢視整體所規管的法規，至於要修法或立專法當然都有其難處，但就個人而言，其實各個法規的主管機關，都應該去檢視現有的法規在現今時代中適不適合，該不該將之補齊？而非單為了要有通訊紀錄或交易紀錄，就通通都歸納入電信法中，因為網路層的服務有別於應用層的服務，電信主管機關就是管網路層的

服務，應用層的服務就根本不會去管，也是由於其自由化的特性。

2. 先前有提到，韓國有將應用層的服務納入電信法中，其實需要去檢視這些國家的屬性，跟臺灣是不同的國情，有些國家是因為政治上的考量，就是需要極度的管理方式，或是因為宗教的因素，所以在其法規的設計架構上，絕對跟我國的環境是不一樣的，因此各國立法的技術和方向也會不同。

十、臺灣微軟蔡經理：

1. 首先我們能理解此研究案的用意，因為長期與警察單位的配合下，只要公文來能配合的都盡力配合，可是有幾個問題，第一個是微軟的伺服器在美國根本不在臺灣，是屬於美商微軟所有，而臺灣方面也是給了警察單位許多方便，不然按照法律規定，臺灣人是根本不會有這些資料，就算公文來要也無法提供。可是今天若是訂了這個法規，仍是一樣無法規範到美商微軟公司，換言之今天想要針對一些會有所規避的公司來制定法律，那些可能也都不是臺灣的公司，舉例說幾年前大家都在抱怨的 Facebook，Facebook 其實在臺灣根本沒有代表，當然現在好不容易建立了關係，有問題是找得到人的，可是他們在臺灣還是沒有公司，所以這個法規就算訂出來了，NCC 也還是不會是 Facebook 的主管機關，即使是以調查犯罪為由，他們還是不會提供，因為他們並不是臺灣的公司。
2. 剛剛還有提到有關 P2P 之間的服務，或是現在最新的通訊軟體，譬如說不管是 LINE 還是 WhatsApp，這些公司有些是在臺灣有些則不是，對於這些層出不窮的新科技所產生新的監察問題或通訊紀錄問題，可能都不是現在所修的這些法律能解決的，想要拿到這些資料而造成調查案件上的困擾，如同剛剛 NCC 所述，若是將這些規範納入電信法中是茲事體大，對於像我們這些平台業者，一旦放入電信法中，即使我們適用但可能不是只要做這些事情，需要做的事情會更多，那這是不是一個合適的規範方式？當然可以理解，臺灣如果有一個網路的主管機關那問題就解決了，但是一直都沒有，所以在思考政策面跟實務面上，的確需要教授們集思廣益，再去思考有沒有更好的方式可以來解決。
3. 還有為什麼電信業者本來需要負擔這麼大的負荷，跟電信本身是一個特

殊管制產業，及大部分電信業者是有收費而有關的，但譬如說以微軟提供的 MSN 服務是不收費的，今天針對於提供免費服務的業者，必須要承擔這麼大的成本，其實這也是一個要去考量是否衡平的一個問題。

十一、 網路家庭余專員：

1. 基本上我們覺得這些相關的法令，都有其修訂的必要，因為個人資料保護法已經施行，譬如第二類電信事業管理規則第 27 條第 2 項，目前只要沒有相關的法律規定，擁有個資的當事人想要刪除這些個資紀錄的時候，所有的警察機關是調不到紀錄的，所以現在面臨的第一個問題，就是一定要有一個專法規定特殊的保存期限和保存的項目，否則當事人都可以要求刪除，那到時候就只有留下 IP，所有的個資都沒有，對要查詢的問題會很大，就犯罪偵查方面來講，要有一些專法去規範保存期限跟項目是很重要的。
2. 第二個問題是要保存在哪裡？如果是保存在電信法裡面，就會有先前 NCC 提到的問題，那我們覺得要符合電信法相關的規則，可能相關的業者會有很多不同的想法，以網路家庭來講，像是 SKYPE 是我們經營的，在第二類電信事業管理規則第 27 條的修訂經營裡，譬如說像第 3 項，某種程度上來講根本不是問題，因為像是商業會計法所有的交易紀錄本來就要保留五年，所以這裡要求保存六個月，其實反而還不是問題，只是上面要求我們保留的項目，可能不是原本交易紀錄上所保存的，像我們這樣的公司，比較大的問題反而是說，我們覺得主管機關應該想辦法的，是就第 1 項和第 2 項找一個適當的地方，去增加保存的期限和項目，就會解決現在這樣的問題，若要納入電信法中也會是一個辦法。

十二、 廖主任：

剛剛網路家庭所提到的問題，其實就有一個聚焦點，大家應該認同說需要訂定法律，尤其在個資法實施後，現在問題就是訂在哪裡？我們現在初步的想法是訂在第二類電信事業管理規則，當然我們也可以瞭解業界似乎都不是很喜歡納入電信事業管理，因為似乎納入管理後 NCC 必定會有一些額外要求，所以解套的方式，是不是要找到一個適當的法規，可以讓這些項目和期間能夠修入，可能就會聚焦在這個法規上，而目前搜尋國內的法律，比較適

用且幅度最小的修法方向=就是納入第二類電信事業管理規則中。

十三、 刑事局研發室王偵查員：

1. 委託機關這邊有一些建議，以今天提出來的意見會有一個很大的問題，就是內容規範會導致法規文不對題，其實我還滿贊成 NCC 的意見，所謂凡走過必留下痕跡，一定要先上網再使用網站，所以上網會有個紀錄，網站也會有個紀錄，那我們希望的是說網站的紀錄要完整一點，上網的紀錄部分 NCC 已經有相關規範，就會變成說電信法就只有規範到上網，若是後續使用的內容也要含括進去，就會變成若是要找相關規定，也不會想到要去找電信法。另外通訊保障及監察法也一定會想到跟監聽有關，不會想到網路交易的紀錄會在該法中，這是我看起來覺得有點文不對題，可是也覺得說裡面有些規定滿好用的，就不一定要放在裡頭，可以建議將那些法規拿出來用。
2. 目前國內的狀況是各目的事業主管機關，在主管一些電子商務像是商業司，所以想請問商業司是否有些建議，有沒有相關法規可以納入新增的條文。

十四、 廖主任：

先回應委託單位的看法，同時也是呼應 NCC 的意見，這些都是本研究案初步的想法，也許在最後會加結論，將 NCC 林科長的意見寫進去，新增條文放在電信法與第二類電信事業管理規則是有些不恰當的地方，而應該是各部會就各自主管的部分，要做較明確的定義。也許像銀行的部分已經有訂定，或是其他機構也有所規定，但仍會擔心若將此決議寫進研究案中，可能就比較沒有強制的效果，各機關允諾後仍舊沒有動作，這也是本研究從比較務實的角度去看，因此會提出較具體的建議。

十五、 NCC 林科長：

即便將這些法條寫進電信法請 NCC 修法，NCC 也不會去修，因為這部分跟 NCC 的職權就是不符合，不能為了一份報告就去修法，因為事實上為了一個法規的立法，刑事局委託此研究案而需要找各機關討論其可行性，就是不希望報告寫出後沒有實際意義，而這個報告的內容通常會被接受，我想 NCC 也會去接受這樣一份委託研究，但目前為止，研究重點就是要修訂第二類電

信事業管理規則第 27 條，而修訂的內容來看，顯然都不是電信服務，既然不是電信服務要如何納入電信法中？這根本就是無法成立的東西，NCC 接了這一份研究報告，也不會拿來就去執行，所以應該是建議，例如有些交易紀錄在事實上，像是 B2C 是屬於商業司的，而 C2C 就非其主管範圍，就業務面來看就真的只是一個業務，該業務本來就該有其業務規範機制，而不能夠說電信在這裡頭有規定，這些業務該有的其他紀錄就通通納入電信法中，讓電信法概括處理，這樣的做法也很難去執行。

十六、 經濟部工業局沈技士：

警政署若有需要任何的目的事業主管機關配合，其實我們都會提供相關的協助服務，譬如說有跟防詐騙 165 專線或是資訊室的專案，都有互相的配合，只要需要的時候我們都會視情形找相關業者提供相關的資訊，協助警政署進行調查工作，舉例來說像是工業局也因應在網路遊戲上，我們有訂定應記載及不得記載事項裡，針對電磁紀錄也有要求業者至少要保存 30 天以上，當時也有討論到是否消保官要求業者保存六個月，業者也是反應有困難，因為玩家太多因此紀錄量會很大，所以其實不是每一個業者都有辦法保存到那麼長的期限，他們有時還是在有必要的時候，可以配合警政署去做一些調整。

十七、 經濟部商業司徐組長（資策會代表）：

1. 資策會有受商業司委託電子交易安全的計畫，因此代表商業司來參與會議，所以並不能代表商業司的立場發言，不過就之前有參與商業司的相關會議，可以瞭解商業司的立場，很多雖然說是電子商務平台上面的一些行為，可是還是比較強調是有做公司登記，而且 B2C 的範圍才是由商業司所主管，至於今天討論到的議題，目前就我所瞭解，其實這邊並沒有比較適合的法規來做修訂，所以可能只能暫時先用電信法，這部分就不做其他任何的建議。
2. 另外我們這邊有接觸一些電子商務業者，也是針對個資法實施之後，面臨到一些像是保留證據等對他有利的事情，但剛剛討論的問題我們並無法去做回應或表達立場。但就實質面談到法律的訂定與修法，可能要特別提到一點是電子紀錄的特性，就是比較容易遭到修改和刪除，以往有些證據只要能用就可以認定，可是在所謂證據保存與數位鑑識這領域，

在法庭上有爭議的就是數位證據是否具有同一性，是否有被竄改的疑慮，因為都只有 0 與 1 的符號，必須要能證明它確實是沒有被竄改過的，不然到了法院上也是會被質疑，雖然說是數位的資料，但它到底是否有效，是否被偽冒或竄改的證據？這部分可能是之後看定位在哪裡，希望可以特別注意這個問題。

十八、 刑事局偵九隊邱副組長：

1. 以目前實務單位來講，我們跟在場的業者在配合上都沒有問題，至於說辦不出來的案子，當然有很多關鍵的地方，相信大家都有的共識，第一個就是希望業者要保留一定的紀錄，那業者的困擾就是成本的問題，如果有個法律能夠給業者依循，那他們也好處理，而我們現在配合的方式，剛剛 NCC 林科長也有提到，像我們跟金融機構去調閱，也是依據金管會的命令，像我們要投單，通訊監察中心也有規定的辦法與依據，而我們也是按照這些在運行。業者部分我們目前也是依循刑事訴訟法的規定去調閱，因為這個問題不會發生在檢察官身上，另外就是組織架構的問題，就是警察非偵查主體，就變成同樣的事情，警察在法律上會有疑義，只是目前大家還是這樣配合。其實要保留多久都是可以討論的，因為這關乎每個業者的成本，至於要用什麼法律，要提供什麼內容，每家業者就如 NCC 林科長所述，這是一個自由的市場，何時會出現什麼新的應用技術，並非現在討論就能夠得知，但對警察實務機關來講，當有犯罪發生的時候，我們有職責要去調查，也要麻煩各位業者或是主管機關的配合，我想我們最大的目的當然就是能夠破案，就是必須要有資料才有辦法處理。
2. 研究中提到要在通訊保障及監察法中做修訂，個人見解是該法立法目的可能跟調閱紀錄的意旨上有所差異，再加上通保法在通訊監察中心的執行上需要很大的成本，若每次調閱都必須要經過檢察官跟法官的同意，那我看應該不會有人會贊同這種方式，而法務部是主管機關，可能也會有所爭議，因為平常我們只要發公文給業者，若程序上要依據通保法，有規定要通知當事人，但調查案件中還通知當事人，不會有機關會去通知，因為這都很需要後續的配套措施。而通保法中我們向法院聲請，過

了之後我們執行完畢，都會有定期的報告，若不通知也要有法官同意，每兩個月都會定期檢討，若是以實務機關來講，就會不希望修訂在通保法中，因為現在並不需要那麼麻煩。

十九、 廖主任：

本研究目的就是要針對比較不願意配合的業者,在偵查單位常會遇到這種狀況,所以就是要有這種規範才會配合，另外偵九隊提到的問題，就是修通保法的難度更高,可是因為通保法中的程序是最清楚的,而且它是在法律的位階,還有若修訂在通保法,那實務單位可能會綁手綁腳,但本研究純粹是以法律的位階來看,這部分事實上還是涉及到民眾的隱私,所以才認為需要提高位階,很多國家也都是訂定在法律位階,我國若不這樣訂當然也可以,可是可能會有一些問題,今天提到的方案當然都各有利弊,像剛剛討論的立法或修法,都各有優缺點,不管放在什麼地方也都會有衍生的問題,如同一開始所講,既然要去探討這問題,總要有人去拋出這個議題,初步搜尋國內外的法規後形成這樣的看法,也許跟國內法律制度有些出入,經內部討論後也的確知道有這樣的問題,所以需要請各單位提供意見。

二十、 刑事局司法科李組長：

司法科認為這個議題比較像是行政規則,最多只到法律位階,若是說訂專法當然是最完善,所有的程序項目全部都包含在專法中,這部分當然就以法完善的立場認為是最妥當的處理方式,而就現有的法律去增訂,不管是增訂在哪裡,都會有很多個人見解,至於刑事訴訟法的部分,因為刑事訴訟法是針對強制處分的部分,像日本修訂的那一條其實也是規定強制處分,並不是針對保存哪些紀錄跟保存多久做處分,所以認為放在刑訴可能是不恰當的考慮。

二十一、 刑事局資訊室楊組長：

研究中提到通保法要增訂第 12 條,而第 12 條的立法緣由是在規範執行機關進行通訊監察所需的期間,這會不會跟網路通訊的部分不太一樣,應該是在規範保存期間。

二十二、 通訊監察中心林組長：

1. 比較接近的法規應該比照「電信事業處理有關機關查詢電信通信紀錄實

施辦法」的精神，來做資料調閱、保存與查詢的動作，若將這層級拉高到通保法，其實那性質又不太一樣，我們之前在中心所做的研究，也是參考歐盟資料保存的法令，比照我們目前的作法大概是這樣子做，在偵查的過程中，也會比較像是通聯調閱的程序，如果說要拉到通保法的階段，不管是由檢察官或法官來執行，案件的數量、時效上還有同意的程度上，在偵查上都會造成影響，而達不到預期的效果。

2. 相關技術性的部分，其實在中心也有相關的研究，這樣一個調閱查詢的機制是可以做得出來，這個是沒有問題的，當然目前以紙本調閱的方式都可以做得到，而中心的想法是若做成系統化的方式，大家在時效上會比較一致，偵辦單位在處理與運用上也會比較方便。就這部分，一個是法規，另一個是經濟的層面，因為要業者配合，沒有相關法規或是要業者負擔相當義務，其實這對業者來講會是一個非常大的負荷。

二十三、　廖主任：

我們有思考這個問題，就是放在行政命令位階比較容易，可是若法律沒有授權，訂定在命令又似乎有逾越母法的問題。

二十四、　奇集集簡經理：

一直以來都會有相關單位要我們提供資料，我們也是都會提供，未來也會是這樣的態度，只是我們好奇的是，未來要提供的資訊內容，會不會有什麼變更，譬如說剛剛提到的 IP 或是 EMAIL ADDRESS，是不是還有其他像是身份證字號之類的，我們關心的就是提供的內容項目。

二十五、　刑事局資訊室楊組長：

目前在調閱資料上都是要依規定，像我們跟健保局調閱資料就是依據調閱的管理辦法，中央健保局本身就有訂定的辦法，內容訂的比較廣是因為民眾也可以去調閱，對於公務機關的需求，通則規定都是要收費，再來是要寫說如何保存這些資料，有個但書是主管機關就不用付費，保證書的部分也就免了，變成說中央健保局因應執法機關的需求，就以法規命令的方式去制定這個辦法。

二十六、　廖主任：

以資訊室楊組長的講法，是與 NCC 林科長的想法相同，像健保局就針對這

個來訂定，現在問題就是說，可能相關的單位非常多，那是不是每一個機關都會本於職權、職責來訂定相關的規定，這可能是另一個問題。

二十七、 NCC 林科長：

若這個建議是可行的，那就是有效的，就是各部會自己去訂，那這個研究就有其成效出來，因為要去建議說哪些機關需要訂定，或許可將這部分臚列出來，向這些機關建議說警察機關在辦案時，在其職權範圍內去幫忙檢視，但有一個問題是，要求對方提供什麼資料及給多久，這個是真的需要去與對方討論，並非要求人家訂多久就多久，因為要考量成本的問題。還有研究中有看到的「歷程資料」，就像是透過網際網路從非洲傳來的，看它經過哪些業者然後經過多少人再傳到我這裡，事實上除非 IP 被竄改，不然就必須去找到它原本的 IP 與目的地的 IP，再要求平台去記錄所有的傳遞歷程，基本上未來要請人家保存資料，還要考慮到第一個成本，第二個對方技術上到底可不可行，而不是去訂自認為很好但執行會有困難的。今天這個委託研究，能夠去訂出一個事實上可行的方案，到底是要去修法還是立專法，就是委託單位要去思考的問題，但我們會覺得說研究報告出去總是要可行，即便這份報告交出來給 NCC 做，坦白說不是 NCC 不願做，而是這根本就是跟 NCC 的職權有所違背，基本上是比較困難的。

二十八、 網路家庭余專員：

當初法務部在修個資法時，其實我們透過很多的管道想要跟法務部反應說，個資法這樣修，到時候想要刪除個資時，一定會產生很大的問題，剛剛有提到關於法律位階的問題，到底是要用法律位階來處理還是主管機關用法規命令來處理就好，因為依照個資法的規定，在第 11 條的規定是說，如果個資收集的特定目的在期限屆滿時，當事人可以要求刪除個資，但在這時要求刪除個資時，司法機關或相關機關因為執行職務的目的，譬如說有法令規定要求相關單位繼續保存個資，那問題是設定在特定目的消失或期限屆滿時，才可以因為法令的規定，而去主張包保留當事人要求刪除的個資，可是回到個資法第 3 條的時候，當事人可以在任意的時間要求刪除個資，這就回到法律位階的問題，才能夠去要求業者保留這個個資，否則所有的個資都會被刪除，那司法機關在執法就會發生大問題。所以我們給個建議就是說，在訂這

個規定一定要注意法律位階，否則到時候個資還是會被刪除。

二十九、　廖主任：

我覺得這個問題很關鍵，現在個資法施行以後，個人資料他要求刪除還是要刪，除非法律有相對應的規範，所以研究中要將位階提升是有道理的，如果各機關都沒有法律依據，未來警察在辦案時拿到的資料會越來越少，譬如說我一個人犯罪，犯罪完之後立即根據個資法，要求業者把我的資料刪除，業者為了避免違法就會將之刪除，所以是否需要相對應的規範，不然將來會造成刑事司法的災難。

三十、　刑事局偵查科黃偵查員：

偵查科針對犯罪偵查部分提供意見，例如網路上的詐欺，電磁紀錄的保存是非常重要的，這個報告結束後，不管是定位在法律位階還是行政命令位階，希望可以獲得共識，能給大家有所依循。

三十一、　總結—廖主任：

1. 今天會議的內容都會詳細記錄下來，我們也會根據剛剛各單位的意見來修正最後的結論，總要提出一些比較具體的作法，當然可能跟部分單位的意見不一定完全一致，不過我們會把各單位的意見儘量呈現出來。
2. 做完這個研究也發現，有一些問題這個研究還沒有處理到，譬如剛剛有提到很多資料存在國外，其實這裡面還有很多沒有觸及的部分，也有待未來再繼續做研究，本研究委託是到十一月，但後續會請研究生針對這些議題再擴及剛剛提到的一些問題，以後可能會跟相關單位或同仁聯繫，再拜託各位給予這方面的協助。做這個研究，一方面對警察機關是很重要的，另外，沒有將個人納入規範，是因為主要針對業者，特別是有營利的業者，在這方面應該也有一部份的責任，所以這個研究對整個網路的秩序，希望能做一些比較長遠的規劃，最後謝謝大家參與討論。

參考文獻

一、中文部分

1. 中國互聯網絡信息中心，互聯網新聞信息服務管理規定，網址：http://www1.cnnic.cn/，上網日期：2012 年 10 月 1 日。
2. 中國互聯網絡訊息中心，互聯網信息服務管理辦法（國務院令第 292 號），網址：http://www.cnnic.net.cn/，上網日期：2012 年 10 月 1 日。
3. 中國百科網，中華人民共和國計算機信息網絡國際聯網管理暫行規定實施辦法，網址：http://www.chinabaike.com/，上網日期：2012 年 9 月 5 日。
4. 中華人民共和國工業和信息化部，互聯網電子公告服務管理規定，網址：http://www.miit.gov.cn/n11293472/index.html，上網日期：2012 年 10 月 1 日。
5. 中華人民共和國公安部，計算機信息網絡國際聯網安全保護管理辦法，網址：http://www.mps.gov.cn/n16/index.html，上網日期：2012 年 10 月 1 日。
6. 王郁琦，資訊、電信與法律，台北：筆者自印，2004 年。
7. 王培任，數位匯流對我國電信管制的挑戰－以網路電話政策之比較分析為例，國立中正大學電信傳播所碩士論文，2007 年。
8. 包國祥，電信法令之分析－依電信媒介各別訂定規範管理模式之檢討，律師雜誌，第 285 期，頁 91-107，2003 年 6 月。
9. 吳嘉生、劉尚志、王煌玄、蘇三榮、王思涵，有關 IP 監察技術可行性評估與法制分析之研究（下）-第二類電信監察技術研究，內政部警政署刑事警察局委託研究報告，台北：內政部警政署刑事警察局，2009 年。
10. 呂雅文，探討通訊隱私範圍之變遷-以美國、德國和台灣法規為例，國立中正大學電訊傳播研究所碩士論文，2000 年 6 月。
11. 呂寧莉，日本通信監察之實施要件及實施現況，檢察新論，第 5 期，頁 299-302，2009 年 1 月。
12. 林祝興、張明信，資訊安全導論，旗標出版公司，2009 年。
13. 林富郎，通訊監察法制化之研究，中正大學法律研究所碩士論文，2000 年。
14. 林裕順，電磁紀錄之證據保全－檢討日本代表性判例的啟示，法令月刊，第 58 卷第 10 期，頁 1325-1326，2007 年 10 月。
15. 林慶隆，通訊監察制度之研究—以法制面、證據面、科技面為中心，中央警察

大學公共安全研究所碩士論文，2010 年 12 月。

16. 林豐裕、林瑋翔、邱佩俞，網路電話追蹤與資料保留，2009 年數位鑑識執法學術暨實務研討會，桃園：中央警察大學，2009 年。
17. 邱佩俞，電信詐欺犯罪運作歷程及其查緝因應策略之研究，中央警察大學犯罪防治研究所博士論文，2011 年 12 月。
18. 范錚強、侯永昌、范懿文、李世材，資訊管理導論，旗標出版，2006 年。
19. 徐智明，通訊監察之保障與規範，國立中正大學法律學研究所碩士論文，2004 年。
20. 國家通訊傳播委員會網站，公告第二類電信事業須設置通訊監察設備之業務種類，網址：
    http://webcache.googleusercontent.com/search?q=cache:C_tIbaW6TCEJ:www.ncc.gov.tw/Chinese/news_detail.aspx%3Fsite_content_sn%3D566%26is_history%3D0%26pages%3D7%26sn_f%3D9795+&cd=2&hl=zh-TW&ct=clnk，上網日期：2012 年 09 月 19 日。
21. 寇健文，中共對網路資訊傳播的政治控制，問題與研究，第 40 卷第 2 期，頁 33-53，2001 年 3、4 月。
22. 張乃文，科技法務透析，談美國對於網站平台提供者揭露用戶資料規範及程序，頁 19-23，2008 年 11 月。
23. 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，國立臺北大學資訊管理研究所碩士論文，2006 年。
24. 張靜婕，凡走過必留下 IP，淺談 IP 位址是否係屬個資法之個人資料，達文西個資暨高科技法律事務所網站 http://www.davinci.idv.tw/，2011 年 12 月 19 日。
25. 梁隆星，網路業者對網際網路著作權侵權之法律責任—以法律經濟分析為基礎，中原大學財經法律學系碩士論文，2008 年 7 月。
26. 章光明、張維平，2005 台灣年鑑—第十一章司法與人權-莫讓網路成為犯罪天堂路，中央通訊社，2005 年。
27. 章忠信，網路服務提供者著作權侵害責任限制之立法思考與方向，第 347 期，頁 40-41，2008 年 8 月。
28. 許慈健，網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究，國立交通大學管理學院在職專班碩士論文，2005 年 10 月。

29. 陳信郎，資訊隱私權保障與網路犯罪通訊監察法制，國立政治大學法律學研究所碩士論文，2004 年 8 月。

30. 陳欽錫，網路犯罪與偵防對策之研究，逢甲大學公共政策研究所碩士論文，2007 年 8 月。

31. 陳誌泓，電腦、網路與刑事偵查－以網路犯罪公約於日本法的落實為中心，國立臺灣大學法律學研究所碩士論文，2005 年 7 月。

32. 陳銘祥，網際網路之規範上定位－從通信之法規體系談起，經社法制論叢，第 24 期，頁 73-92，1999 年 7 月。

33. 陳慧真，網路交通安全，中時電子報，第 2009.10 期，2009 年。

34. 彭賢恩、劉怡靖、彭曉珍，刑法應用於網路誹謗案例之分析，資訊社會研究（11），頁 245-273，2006 年 7 月。

35. 馮衛國、張立宇，網路空間的犯罪與刑法面臨的挑戰，網路法律評論，7 月號，頁 2-23，2002 年。

36. 黃燦堂，網路犯罪偵查方式與網路服務業者法律責任，國立高雄第一科技大學科技法律研究所碩士論文，2008 年 6 月。

37. 楊崇森，美國聯邦司法部之組織與功能，法學講座，軍法專刊，第 56 卷第 4 期，頁 240，2010 年 8 月。

38. 資策會科技法律中心，日本擬立法明訂 ISP 侵權責任範圍暨公開發信人身份資訊之程序，科技法律透析，頁 6-8，2001 年 12 月。

39. 資策會科技法律中心，網際網路服務提供者法律責任與相關法制之研究，行政院經濟建設委員會委託研究，2003 年 12 月。

40. 蔡美智，通訊保障及監察法關於網路監聽的相關爭議，資訊法務透析，12 月號，頁 32-45，1999 年。

41. 鄧湘全，通訊監察之合憲性探討，月旦法學，40 期，9 月號，頁 102-113，1998 年。

42. 錢世傑，網路通訊監察法制與相關問題研究，中原大學財經法學系碩士論文，2002 年。

43. 謝昆峰，網際網路與刑事偵查，國立臺灣大學法律學研究所碩士論文，2002 年。

44. 鍾雅蘭，網路犯罪中通訊監察與基本權保障之研究--以美國法制為主，東吳大

網路平台業者紀錄保存規範之研究
學法律學系碩士論文，2007 年。
45. 蘇三榮，網路時代通訊監察與個人資料保護之法制研究，國立交通大學科技法律研究所碩士論文，2009 年 6 月。
46. 鐘嘉德，高天助，楊嘉栩，雲端運算與產業發展，研考雙月刊第 34 卷第 4 期，頁 20-31，2010 年 8 月。

二、英文部分

1. CNET News.com, Europe passes tough new data retention laws, December 14, 2005, http://news.cnet.com/Europe-passes-tough-new-data-retention-laws/2100-7350_3-5995089.html
2. CNET, Police: Internet providers must keep user logs, CNET, July 11, 2011,http://news.cnet.com.
3. Communications Assistance for Law Enforcement Act （CALEA）.
4. Cyber-crime Convention, website: http://conventions.coe.int/Treaty/en/Treaties/html/185.htm, last viewed: 2012/06/05.
5. Directive 2002/58/EC of the European Parliament and of the Council, Concerning the processing of personal data and the protection of privacy in the electronic communications sector, Directive 2002/58/EC.
6. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC of 2006, Directive 2006/24/EC.
7. Directive 95/46/EC of the Europe Parliament and the Council on the Protection of Individuals with regard to Processing of Personal Data and on the Free Movement of such Data of 1995 （Directive 95/46/EC）.
8. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in

the Telecommunications Sector of 1997 （Directive 97/66/EC）.

9. Electronic Communication Privacy Act of 1986 （ECPA）, 18 U.S.C §2510-2522.
10. Electronic Communication Privacy Act of 1986 （ECPA）, 18 U.S.C §2701-2712.
11. Electronic Communication Privacy Act of 1986 （ECPA）, 18 U.S.C §3121-3127.
12. Eleni K. & Peggy V., Telecommunications - the EU data retention directive - Retaining the data retention directive, Computer law & security report, Vol. 22, pp.370-380, 2006.
13. H. R. 1981, To amend title 18, United States Code, with respect to child pornography and child exploitation offenses, IN THE HOUSE OF REPRESENTATIVESMAY 25, 2011.
14. IT & Communications Community, A review by InTechnology of legislation and regulation concerning data storage in the UK and Europe, http://www.intechnology.co.uk/.
15. Mark T., Electronic communications - EU - The EU Data Retention Directive, Computer law & security report, Vol. 22, pp.309-312, 2006.
16. Regulation of Investigatory Powers Act 2000 （RIPA）.
17. Stephen S., European parliament says ‘No!’ to member states’ data retention proposals, Computer law & security report, Vol. 21, pp.279-280, 2005.
18. Uniting and Strengthening America by Providing Appropriate Tool Required to Intercept and Obstruct Terrorism Act of 2001 （USAPA）.
19. Watson Hall Ltd, UK data retention requirements, Watson Hall Ltd, 2009.

三、日文部分

1. 日本外務省，サイバー犯罪に関する条約説明書，網址：http://www.mofa.go.jp/mofaj/index.html，上網日期：2012 年 5 月 13 日。
2. 日本法務省，通信履歴の電磁的記録の保全要請に関するＱ＆Ａ，網址：http://www.moj.go.jp/houan1/houan_houan24.html，上網日期：2012 年 4 月 20 日。
3. 日本法務省，ハイテク犯罪に対処するための刑事法の整備に関する諮問，網

址：http://www.moj.go.jp/shingi1/shingi_030324-2.html，上網日期：2012 年 5 月 16 日。

4. 日本法務省，情報処理の高度化等に対処するための刑法等の一部を改正する法律案，網址：http://www.moj.go.jp/keiji1/keiji12_00025.html，上網日期：2012 年 5 月 30 日。
5. 日本「プロバイダ責任制限法 関連情報 Web サイト」網站，網址：http://www.isplaw.jp/，上網日期：2012 年 4 月 20 日。
6. 日本總務省，特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律第四条第一項の発信者情報を定める省令，網址：http://www.soumu.go.jp/menu_hourei/d_shinjigyou.html，上網日期：2012 年 4 月 20 日。
7. 日本總務省網站，電気通信事業における個人情報保護に関するガイドライン，網址：http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/telecom_perinfo_guideline_intro.html，上網日期：2012 年 4 月 28 日。
8. 日本ベルマン法務事務所網站，発信者情報開示の現行法の問題点 日本弁護士連合会 壇俊光先生 ,網址:http://www.cyber-eraser.jp/category/1462413.html，上網日期：2012 年 5 月 24 日。