RP02/04-05

選定司法管轄區對截取通訊的規管

2005年2月2日

黃少健

立法會秘書處
資料研究及圖書館服務部

香港中區花園道3號花旗銀行大廈5樓
電　　話： (852) 2869 9621
圖文傳真： (852) 2509 9268
網　　址： http://www.legco.gov.hk
電子郵箱： library@legco.gov.hk

目錄

頁

鳴謝

資料研究及圖書館服務部在撰寫本研究報告期間，承蒙多位人士誠意協助，謹此致謝。本部特別向下列曾向本部提供寶貴資料的人士／組織表示謝意：

美國司法部聯邦調查局助理法律事務聯絡主任Chan, Becky女士；

英國內政部滅罪及社區安全小組Cooper, Tony先生；

英國下議院首席法案秘書Cranmer, Frank先生；

澳洲國會眾議院人民策略事務長Fitzgerald, David先生；

美國電子私隱資訊中心政策顧問Laurant, Cedric女士；

香港特別行政區政府保安局；

美國司法部聯邦調查局行政秘書處辦公室Trigeiro-Pabst, Linda M.女士；及

英國保安處網絡事務小組。

研究摘要

1. 本報告探討英國、美國及澳洲截取通訊的法定規管機制，並按以下10方面研究該些機制：法律架構；發出手令的機構；申請程序；發出手令的理據；手令的有效期、終止有效期及續發安排；沒有手令下合法截取通訊；內部保障措施；由行政機關、司法機構、立法機關及公眾監察的外在保障機制；實施法例的行政酌情權權限；以及與"911"事件及通訊科技發展有關的法例修訂。

2. 在英國，截取通訊主要由一項名為《2000年調查權力規管法令》的單一法例規管。只有執法或保安機關的首長或其代表，才有資格申請截取手令。這些手令由事務大臣簽發。手令申請必須符合是否必要和目的與效果是否相稱的驗證標準。所有新簽發手令的有效期一律相同，但獲續期後，手令的有效期可視乎其目的而各有不同。除有限情況外，被截取材料在法律程序中不獲接納為證據。截取權力的行使由截取通訊專員監察，而截取通訊專員每年向首相提交的報告亦會提交議會省覽，然後公開讓公眾查閱。為國家安全而進行截取通訊的開支、管理及政策事宜，由一個法定的議會委員會監察。公眾人士可向調查權力審裁處投訴，該審裁處有權取消手令及判處賠償。近年，當局曾引入多項法例修訂，以加強執行截取法例及打擊恐怖主義活動。

3. 在美國，截取通訊主要由3項聯邦法規規管。《1968年安全街道及罪行管制綜合法令標題III》("《標題III》")規管為執法而截取通訊內容的活動。《1978年外國情報監視法令》("《情報監視法令》")規管就美國境內的外國勢力及其代理人的通訊內容的截取活動。《標題18》有關通訊紀錄器及監測追蹤裝置的一章("《通訊紀錄／監測法規》")規管就通訊中與內容無關的資料的截取活動。上述3項法規的截取令均由法官簽發。根據《標題III》及《情報監視法令》，發出法院命令的申請必須獲高層司法官員授權或批准，而發出法院命令必須符合"很可能成立的因由"的驗證標準。《通訊紀錄／監測法規》的規管制度較寬鬆，只要將被截取的資料與刑事調查有關，便可發出法院命令。《情報監視法令》的命令有效期最長，《標題III》的命令有效期則最短。合法蒐集所得的證據可在法律程序中使用。該3項截取法規均規定司法部首長須每年向國會提交報告，但報告所披露的資料則各有不同。截取機關須向國會委員會交代其工作。在"911"事件後，當局制定了《提供必要的阻截恐怖主義的合適工具以團結和增強美國法令》，就該3項截取法規作出了重要修訂，以增加政府的截取權力。

4. 在澳洲，截取通訊主要由一項名為《1979年電訊(截取)法令》的法例規管。國家安全手令由總檢察長簽發，其申請必須由保安事務長提出。發出此類手令的理由不一定涉及某些特定的罪行。執法手令的申請須由合資格的機構提出，此類調查指明罪行的手令由法官或一個審裁處的獲提名成員簽發。國家安全手令的有效期最長可達執法手令有效期的兩倍。在獲豁免的法律程序中、若干已被界定的情況下或為了獲認許之目的，經合法截取所得的資料可獲接納為證據。申訴專員獲賦權查核執法手令紀錄。總檢察長須提交周年報告供澳洲國會省覽，並在報告中列述為執法而進行截取電訊行動的詳細資料。執法及安全機關須向兩個法定的議會委員會交代其工作。澳洲國會曾訂立數項重要的法例修訂，它們大都是澳洲政府對付恐怖主義活動措施的一部分。

5. 本報告分析的重點是，比較3個選定司法管轄區截取手令制度的各項特點，並參考現時規管香港特別行政區截取通訊事宜的《電訊條例》、在1997年6月制定但政府至今尚未實施的《截取通訊條例》，以及政府於1997年2月發表作公眾諮詢，但一直沒有向前立法局／立法會提交的有關截取通訊的白紙條例草案。

選定司法管轄區
對截取通訊的規管

第1章 —— 引言

1.1 背景

1.1.1 保安事務委員會在2004年4月2日會議上，要求資料研究及圖書館服務部研究海外司法管轄區對截取通訊的規管。是項研究之目的，是協助事務委員會就政府當局檢討《截取通訊條例》的有關事宜進行商議。該條例於1997年6月28日制定，但至今尚未實施。事務委員會在2004年5月13日會議上通過建議的研究大綱。委員要求資料研究及圖書館服務部在研究中加入其他司法管轄區因應"911"事件及通訊科技發展而作出的法例修訂的研究，以及關於其他司法管轄區有否規定須獲得法院手令或行政命令方可截取通訊的分析。

1.2 研究範圍

1.2.1 是項研究涵蓋下列地方對截取通訊的法定規管：

(a) 英國；

(b) 美國；及

(c) 澳洲。

1.2.2 選取上述3個普通法司法管轄區作為研究對象，不僅在於它們各自具有若干獨特的規管元素，亦由於它們近年均進行了多項重要的法律修改，影響個人私隱和執法機關的截取權力。特別是，英國已制定了一項法令，就截取通訊訂立新的架構。美國亦訂定了一項法令，加強有關恐怖主義活動的監視程序。澳洲則修訂了截取電訊法例，可用截取手令調查恐怖主義行為。

1.2.3 建議選取這些司法管轄區，與法律改革委員會於1996年發表，名為"*私隱權：規管截取通訊的活動研究*"報告書的涵蓋範圍一致。該報告書亦曾探討該3個司法管轄區的相關經驗。

1.2.4 對規管截取通訊的研究包括下列事宜：

(a) 法律架構；

(b) 發出手令的機構；

(c) 申請程序；

(d) 發出手令的理據；

(e) 手令的有效期、終止有效期及續發安排；

(f) 沒有手令下合法截取通訊；

(g) 內部保障措施；

(h) 由行政機關、司法機構、立法機關及公眾監察的機制；

(i) 實施法例的行政酌情權權限；及

(j) 近年與"911"事件及通訊科技發展有關的法例修訂。

1.3 研究方法

1.3.1 是項研究以資料閱覽的方式進行，包括在互聯網查閱資料、參考及分析文獻資料，以及與有關當局通訊。

第2章 —— 英國

2.1 背景

2.1.1 在英國，政府截取通訊是存在已久且眾所周知的行為。[1] 在1985年之前，英國並無任何整體的法定架構規管該種行為，而僅是藉著不同條例的條文管制部分的截取通訊行為。因此，截取通訊的法律依據並不清晰。而事務大臣獲賦予權力，可發出手令授權截取郵遞及電報通訊。這意味著截取通訊的過程是受行政當局而非法定架構管制[2]。

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

---

1 內政部(1999年)第3頁及歐洲人權法院(1984年)第7頁。1663年5月25日發出的公告，首次提述事務大臣可發出手令授權拆閱信件。1937年，當局決定在政策上須由事務大臣簽發手令，授權截取電話交談的內容。

2 歐洲人權法院(1984年)第5至10頁。

3 《Birkett報告書》由Birkett勳爵擔任主席的樞密院顧問委員會擬備。該報告書主要載述向保安處發出手令的原則。《1980年白皮書》旨在更新《Birkett報告書》有關截取事宜的最新資料，並確認行政當局有權發出截取通訊的手令。《Diplock報告書》由上議院執掌最高司法職務的Diplock勳爵擬備，其目的是持續地獨立審查當局有否按照既定目的及程序截取通訊。請參閱歐洲人權法院(1984年)第6頁及內政部(1999年)第3至4頁。

2.1.3 直至1985年，政府才在一份白皮書中表明有意就截取通訊訂立法例。是次立法需要，乃歐洲人權法院於1984年就Malone v. UK一案的判決引致。[4] 在該個案中，法院裁定英國的本土法例雖訂有規管截取通訊的詳細程序，卻沒有清楚表明有哪些截取權力的元素已納入法律規則，有哪些元素則仍然屬行政當局的酌情範圍。[5] 法院進一步裁定，警方截取個人通訊的做法，違反了《歐洲人權公約》第八條。[6]

2.1.4 在發出《1985年白皮書》後，當局制定了《1985年截取通訊法令》。該法例首次就截取郵遞或公眾電訊系統的通訊訂立法定基礎[7]，把非法截取通訊的行為列為罪行，並在法例中訂定手令制度的運作架構，以及訂立保障、監察及投訴機制。[8]

2.1.5 自《1985年截取通訊法令》制定以來，電訊科技及通訊服務出現了巨大變化，例如流動電話及互聯網通訊日趨普及、私營電訊網絡擴展，以及提供包裹和文件送遞服務的私營公司數目大增。上述種種變化引發了新的人權問題，而這些問題已超出了《1985年截取通訊法令》的規管範圍。因此，英國政府了解到有需要訂立1999年發表的諮詢文件所述的新法例。[9] 一年後，當局廢除了《1985年截取通訊法令》，並以《2000年調查權力規管法令》取代，後者便成爲英國規管截取通訊的主要法例。

---

4 內政部(1999年)第5頁。

5 歐洲人權法院(1984年)第28至29頁。

6 根據《歐洲人權公約》第八條，"*人人有權使他的私人和家庭生活，他的家庭和通信受到尊重*"，以及"*公共機關不得干預上述權利的行使，但是依照法律的干預以及在民主社會中為了國家安全、公共安全或國家經濟福祉的利益，為了防止混亂或犯罪，為了保護健康或道德，或為了保護他人的權利與自由，而有必要干預者，不在此限。*"公約文本載於以下網址：http://www.hrcr.org/docs/Eur_Convention/euroconv3.html。

7 內政部(1999年)第5頁。

8 同上。

9 內政部(1999年)。

2.2 法律架構

2.2.1 《2000年調查權力規管法令》分為5部分，其中第I及IV部建立了截取通訊的法律架構。[10] 第I部的主要目的是界定非法截取的罪行、列明在何種情況下截取屬合法行為、訂立授權及簽發手令的制度、就截取能力設下規定，以及限制被截取材料的使用。第IV部主要涉及調查權力的審查，包括成立獨立的司法監察組織及審裁處，讓不滿有關權力運用的人士有一申訴途徑。

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

2.2.3 根據《2000年調查權力規管法令》，[11] 任何人在通訊傳送過程中，透過改變或干擾傳送系統或監察傳送情況，讓"*該通訊的發送者或預定接收者以外的其他人士，取得傳送中通訊的部分或全部內容*"，即屬截取通訊。《2000年調查權力規管法令》把通訊界定為"*在傳送過程中*"及／或"儲存於傳送系統中"的通訊。[12] 因此，"*已儲存的通訊*"亦受到《2000年調查權力規管法令》的規管。

---

10 《2000年調查權力規管法令》並非只涉及截取通訊。該法例亦規管其他調查權力，包括對住宅處所或私人車輛施予具侵犯私隱性質的監視、在特定行動中暗中監視、使用特務刺探情報，以及取覽加密資料。請參閱《2000年調查權力規管法令》第II及III部。

11 《2000年調查權力規管法令》第2條。

12 《2000年調查權力規管法令》第2(7)條及內政部(2002年)第5至6頁。

2.2.4 《2000年調查權力規管法令》與《1998年人權法令》同步實施，後者把《歐洲人權公約》納入英國法例中。[13] 《2000年調查權力規管法令》必須反映《歐洲人權公約》第八條的規定，並實施歐洲議會及歐洲聯盟理事會發出的指令。有關指令規定成員國必須保障通訊的保密。[14]

2.3 《2000年調查權力規管法令》的截取手令制度

2.3.1 《2000年調查權力規管法令》訂立了一套制度，規定合法截取某通訊時必須獲得行政當局發出的手令。

2.3.2 截取手令分為兩類。第一類稱為"*一般手令*"，規定須提供某人姓名或形容某人，作為"*截取對象*"，或提供將有截取活動的處所名單或形容該等處所。[15] 負責截取活動的機構通常會申請此類手令。另一類手令稱為"*具證明書手令*"，規定須具有事務大臣發出的證明書，而且只適用於在英國以外地方發出或接收的"*外地通訊*"。此類手令可獲得多項豁免，包括無須遵守有關指明任何人士或處所的規定。[16]

2.3.3 儘管上述兩類手令在多方面不同，但兩者均受到大致相同的制度規管。

---

13 根據《1998年人權法令》，英國公民可透過國內法庭維護本身按《歐洲人權公約》獲保障的權利，而毋須訴諸歐洲人權法院。進一步資料請瀏覽 http://www.lcd.gov.uk/hract/hramenu.htm。

14 歐洲議會及歐洲聯盟理事會於1997年12月15日發出有關在電訊業處理個人資料及保障私隱的97/66/EC號指令。該指令第5(1)條訂明："*成員國應透過本土規例，確保公眾電訊網絡及公共電訊服務的通訊得以保密，尤其須禁止其他人士在未經有關使用者同意之下，監聽、竊聽、儲存通訊內容，或就通訊進行其他類別的截取或監視，但根據第14(1)條獲得合法授權而進行的則屬例外。*"第14(1)條訂明："*成員國可採取立法措施，限制第5條所訂明責任和權利的涵蓋範圍.....當這些限制在維護國家安全、防衛、公共安全，以至防止、調查、偵查及檢舉刑事罪行或未獲授權使用電訊系統的行為方面，成為一項必要的措施.....*"。

15 《2000年調查權力規管法令》第8(1)、(2)及(3)條。

16 《2000年調查權力規管法令》第8(4)及(5)條。

發出手令的機構

2.3.4 一般手令及具證明書手令均須由事務大臣簽發，即通常由掌管英國治安的內政大臣簽發。即使在緊急情況下高級官員亦可簽發手令，事務大臣仍須在該項手令獲簽發前，審核有關申請，並向簽發官員給予指示。[17]

申請程序

2.3.5 一般手令或具證明書手令的申請[18]，只能由少數高級官員或其代表提出。這些官員包括：[19]

(a) 保安及情報機關的首長，即保安處(軍情五處)處長、秘密情報組織(軍情六處)處長、政府通訊總部部長、國家刑事情報處處長，以及國防情報處處長[20]；及

(b) 執法機關的首長，即首府警務處處長[21]、北愛爾蘭警察署署長、根據《1967年警務(蘇格蘭)法令》運作的任何警隊的警察總長，以及海關關長。

17 根據內政部發布的《截取通訊實務守則》，緊急個案指需要在24小時內取得截取授權的個案。請參閱內政部(2002年)第12、19及20頁。

18 每宗申請必須載有下述資料：涉及有關申請的人士或處所名單；有關將被截取通訊的描述；通訊服務供應商的詳細資料；截取行動的可行性評估；解釋為何有必要截取通訊；手令授權的行為與該行為擬達致的結果為何相稱的考慮；有關任何不尋常程度的侵犯截取對象以外人士私隱的考慮；以及所有被截取材料均會受《2000年調查權力規管法令》保障的保證。此外，申請具證明書手令必須附有事務大臣發出的證明書，而該證明書訂明被截取材料會受審查的程度。請參閱內政部(2002年)第10、11、16及17頁。

19 《2000年調查權力規管法令》第6條。

20 軍情五處負責英國的內部保安，軍情六處則負責英國的對外保安。政府通訊總部主要提供國家安全、軍事行動及執法方面的信號情報。國家刑事情報處提供嚴重及有組織罪行的情報。國防情報處是國防部的一部分，負責就英國及其盟友可能受到的威脅提供策略性防衛情報。

21 首府警務處是現時在大倫敦執行警務的最大規模警隊。

發出手令的理據

2.3.6 發出一般或具證明書手令前，事務大臣必須確保有關申請符合下列規定：[22]

(a) 手令必須"*合乎國家安全的利益*"，或其目的是"*防止或偵查嚴重罪行*"、"*保障英國的經濟福祉*"免受外來威脅，或"*實施任何國際互助協定的條文*";

(b) 獲手令授權的行為必須與該行為擬謀求的結果"*相稱*"；及

(c) 所謀求的資料並不能以其他方式合理地取得。

手令的有效期、終止有效期及續發安排

2.3.7 所有新發出的手令(不論是一般或具證明書手令)，最初有效期通常為3個月。假如繼續需要手令的理由跟最初申請手令的理由相同，手令的有效期可延長。因嚴重罪行而續發的手令，有效期可延長3個月。以國家安全或國家經濟福祉為理由而續發的手令，有效期可延長6個月。除非獲事務大臣續發手令，否則在緊急情況下授權發出的手令，有效期為5個工作天。倘認為有關手令與達致的結果不再相符，及其理由已非必要，則可提早撤銷該項手令。

[22] 《2000年調查權力規管法令》第5條。公民自由團體曾批評部分法定理由含糊不清及未有定義，而且賦予事務大臣過大的酌情權。內政部回應這些批評時表示，法定理由的大部分措辭均來自《歐洲人權公約》第八條(請參閱注釋6)，例如"*必要*"、"*為了國家安全的利益*"及"*經濟福祉*"。此外，除非能證明保障英國經濟利益與國家安全直接有關，否則事務大臣不會只為了保障英國經濟福祉而發出手令。請參閱下議院圖書館(2000年)第28至29頁及內政部(2002年)第8及11頁。

沒有手令下合法截取通訊

2.3.8 《2000年調查權力規管法令》列出一些情況，可在沒有手令下合法截取通訊。這些情況包括：[23]

(a) 有合理理由相信，某一通訊的發送者及預定收受者均同意截取行動；

(b) 某一通訊的發送者或預定收受者已同意截取行動，而有關的截取行動並非由手令授權，[24] 而是被列作監視行動。例如，當綁匪致電人質的親屬，而警方希望紀錄來電內容，以識別或追查綁匪下落，便會採取監視行動；及

(c) 截取行動與服務的提供或營運有關。例如，由於收件人地址不詳，郵遞服務供應商需要開啟郵件以確定收件人的地址。

2.3.9 事務大臣可訂立規例，在合法商業運作的過程中、在醫院，以及根據監獄規則和國際互助協定，容許若干種類的截取行動。[25]

內部保障措施

2.3.10 《2000年調查權力規管法令》規定，截取通訊的機關須就由一般或具證明書手令截取所得的所有材料，訂定內部保障措施。[26]

23 《2000年調查權力規管法令》第3條。

24 《2000年調查權力規管法令》第48 (2)和(4)條。監視行動是一種介入性的監控方法，包括具針對某對象及侵犯私隱性質的監視，以及警方或特務機關可能使用的隱秘式特務技術。

25 《2000年調查權力規管法令》第4條。

26 《2000年調查權力規管法令》第15和16條，以及內政部(2002年)第22至27頁。

使用被截取材料的限制

2.3.11 被截取材料的披露、複印及保存，只限於授權截取所需的最低限度。這些目的包括方便截取通訊專員執行其職能，以及確保檢控工作公正持平。當局亦有額外保障措施，保護按具證明書手令而從外地通訊截取的材料。事務大臣必須確保只有指明的被截取材料，才可供任何人閱讀、查看或聽取。

2.3.12 此外，只有名列截取機關分發名單上的人士，才可接觸被截取的材料，或閱覽任何有關材料的報告。該類人士均須接受適當的審查。[27]

豁除於法律程序以外的被截取材料

2.3.13 在法律程序中，被截取材料不會獲接納為證據。但凡可能會透露截取行動曾展開的盤問、聲稱或披露亦不獲接納為證據。唯一例外是，當檢控官有需要審核全部所得的材料，以確保檢控工作不會有任何偏頗，或檢控官已諮詢主審法官，並獲信納在有關個案的例外情況下，披露所得材料對"*維護司法公正有其必要*"。[28]

<u>司法機構的監察</u>

2.3.14 雖然司法機構並無參與發出截取手令的工作，但《2000年調查權力規管法令》規定，截取通訊專員(須由現時或曾經身居司法要職的人士擔任)必須監察截取權力的使用。[29]

---

27 內政部(2002年)第24頁。

28 《2000年調查權力規管法令》第17及18條、內政部(2002年)第25至27頁，以及政府檢控事務處所發表有關截取電話通訊的法律指引(網址：http://www.cps.gov.uk/legal/section20/chapter_e.html)。

29 截取通訊專員由首相委任，任期3年，並有可能獲委連任。在2003年獲委連任的現任專員是一名退休高等法院法官。請參閱首相府於2003年3月28日所發出有關截取通訊專員的新聞公告(網址：http://www.pm.gov.uk/output/Page3375.asp)。

截取通訊專員

2.3.15 截取通訊專員負責檢討事務大臣處理截取手令的角色、獲取通訊資料制度的運作情況，以及是否有足夠安排，以確保截取所得資料可獲適當處理。[30]《2000年調查權力規管法令》並沒有訂明應如何履行這些職能。現任專員履行職能的方式，是覆核截取機關向事務大臣提交的手令申請。專員會定期走訪有關的公共機構，特別是執法機關，以便與有關的調查人員，抽樣審查截取手令的資料。[31]

2.3.16 所有曾涉及提出、授權或進行截取行動的人士，均須向專員提供讓其履行法定職能所需的任何文件或資料。[32] 專員可在其認為適當的任何時候，向首相報告其工作情況。

2.3.17 專員必須每年向首相提交報告。有關報告將提交議會，然後公開讓公眾查閱。報告內容包括對截取過程的檢討、概述截取行動的價值，以及在不公開發表的機密附件中，交代專員曾覆核的截取手令在行動上已獲得的成果。[33]

---

30 《2000年調查權力規管法令》第57條及上議院(2000年)。

31 截取通訊專員在2003年曾探訪的公共機構有軍情五處、軍情六處、政府通訊總部、國家刑事情報處、首府警務處特別事務部、斯特拉斯克萊德警務處、北愛爾蘭警務處、海關、外交及聯邦事務部、內政部、蘇格蘭行政機關(蘇格蘭政府)及國防部。專員亦曾與內政大臣、北愛爾蘭事務大臣、國防大臣及蘇格蘭國務大臣(蘇格蘭政府首長)會談。請參閱《截取通訊專員2003年報告書》(2004年)第2頁。

32 《2000年調查權力規管法令》第58條。

33 首相倘認為周年報告所發表的任何事宜，會有違公眾利益，或不利於國家安全、不利於防止或偵查嚴重罪行、不利於英國的經濟福祉或不利於任何受專員監察的公共機構繼續履行其職能，首相可從提交議會的報告中剔除有關事宜。

2.3.18 在2003年的周年報告中，截取通訊專員對於所發出手令"*完全符合《2000年調查權力規管法令》的規定，有關方面依循適當程序行事，而有關的保障措施和實務守則亦獲得遵循*"，表示滿意。[34] 專員在其2001年及2002年的周年報告中亦有相同的評論。[35]

立法機關的監察

2.3.19 有關軍情五處、軍情六處及政府通訊總部截取通訊的開支、管理及政策事宜，由一個稱為情報及保安事務委員會的議會委員會監察。

情報及保安事務委員會

2.3.20 根據《1994年情報服務法令》成立的情報及保安事務委員會，由9名成員組成，分別從下議院及上議院選出。該委員會每年向首相提交報告，而首相將報告提交議會前，可以保安理由刪除[36] 報告的任何內容。該委員會亦會不時向首相提交特別報告。

2.3.21 情報及保安機關向情報及保安事務委員會披露資料，須受到《1994年情報服務法令》所限制。這些機關的主管可與情報及保安事務委員會分享敏感資料。然而，取得內政大臣同意後，這些機關可以保安理由拒絕提供資料。

34 《截取通訊專員2003年報告書》(2004年)第2頁。

35 《截取通訊專員2001年報告書》(2002年)第2頁及《截取通訊專員2002年報告書》(2003年)第2頁。

36 情報及保安事務委員會成員由首相徵詢反對黨領袖後委任。現任部長不得出任情報及保安事務委員會成員。該委員會現有6名成員(包括主席)屬工黨成員。該委員會由一名秘書及設於內閣辦事處的秘書處提供支援服務。在1998年，英國政府接納該委員會的建議，委任一名調查員協助該委員會執行職務。該名調查員被確認可接觸各保安及情報機關，但須受到同樣適用於情報及保安事務委員會有關敏感事宜的考慮因素所規限。該調查員其後曾展開多項調查，調查結果已在情報及保安事務委員會的周年報告中反映出來。

公眾監察

2.3.22 任何公眾人士如因截取機關或代表截取機關進行的任何截取活動而感到受屈，可向根據《2000年調查權力規管法令》成立的調查權力審裁處("審裁處")投訴。[37]

調查權力審裁處

2.3.23 審裁處由8名資深的法律界及司法機構人士組成。所有成員均由女皇按《英皇制誥》任命。[38] 審裁處的現任主席是一名上訴法院的常任法官。[39]

2.3.24 審裁處有權就投訴及程序展開聆訊及裁決、判處賠償、撤銷或取消任何手令或授權，以及要求銷毀被截取的材料。審裁處亦可就任何程序、投訴或轉交處理的事宜決定本身的處理程序。所有投訴均保密處理。[40] 審裁處裁定某宗投訴時，其採用的原則，與法庭處理司法覆核申請時所採用的原則相同。投訴人無權取覽有關投訴的檔案。除非事務大臣命令，否則不得就審裁處的裁決提出上訴或在任何法庭提出質疑。

調查權力審裁處所處理的投訴個案數目

2.3.25 自2000年10月2日成立至2001年底為止，審裁處共接獲102宗投訴，在2002及2003年則分別接獲130及109宗新的投訴。在這些投訴當中，審裁處從未裁定任何個案有違反《2000年調查權力規管法令》或《1998年人權法令》。[41] 審裁處的前身(即截取通訊審裁處），在13年運作期間，亦從未裁定任何投訴個案得直。

---

37 《2000年調查權力規管法令》第65至69條。這個審裁處統合並取代了分別根據《1985年截取通訊法令》、《1989年保安處法令》、《1994年情報服務法令》及《1997年警務法令》成立的各個審裁處。

38 《2000年調查權力規管法令》並沒有訂明審裁處成員的數目及任期。審裁處於2000年成立時，獲委成員的任期為5年。

39 調查權力審裁處，網址：http://www.homeoffice.gov.uk/inside/pubapps/ipt.html。

40 調查權力審裁處：《2000年調查權力規管法令》，網址：www.dumgal.gov.uk/services/depts/tradstds/TribunalInfo.pdf。

41 請參閱截取通訊專員於2001、2002及2003年提交的報告書。

實施法例的行政酌情權權限

2.3.26 在英國，首相及部長並無酌情權，決定某項法令在議會通過後開始實施的日期。原則上，任何法令獲御准後均會即時生效。實際上，某法令可賦權部長藉命令使之開始實施，但不一定須要所有條文同時開始生效。換言之，法令的部分條文可能會在稍後時間才開始生效，亦有可能在被廢除前從未開始實施。就《2000年調查權力規管法令》而言，並非所有條文均在該法令2000年通過時同時開始實施，原因不在於該法令執行上有困難，而在於部分條文實施前需要較長時間預備。

2.4 與"911"事件及通訊科技發展有關的法例修訂

2.4.1 英國政府近年開展了多項有關截取通訊的立法措施。部分措施着眼於加強《2000年調查權力規管法令》的實施，以便更有效配合通訊科技及服務的發展，另一些措施則因應"911"事件而加強政府的調查權力。

《截取通訊實務守則》

2.4.2 內政部於2002年7月按《2000年調查權力規管法令》的要求，根據《2002年調查權力規例(截取通訊：實務守則)令》發表了《截取通訊實務守則》。該守則的擬稿在上、下議院通過前曾諮詢公眾。[42]

[42] 《2000年調查權力規管法令》第71(4)條和《2002年調查權力規例(截取通訊：實務守則)令》的擬稿，以及下議院有關授權法例的第三個常設委員會2002年5月21日的會議紀要，網址：http://www.publiscations.parliament.uk。

2.4.3 該守則詳細訂明了公共機關獲授權申請截取手令，以及在指定情況下沒有手令而合法進行截取活動所須遵從的程序。該守則亦就執行手令、被截取材料的披露、複印、保存，以及處理被截取材料的其他必要保障措施，提供指引。根據《2000年調查權力規管法令》，任何行使截取權力及履行截取職務的人士均須顧及實務守則的規定，而有關守則在刑事及民事訴訟程序中均可獲接納為證據。然而，任何人士如未有遵從守則，此行為本身並不會導致該人士須負上受刑事或民事追究的責任。

通訊服務供應商的截取能力

2.4.4 在2002年，《2002年調查權力規例(維持截取能力)令》按《2000年調查權力規管法令》第12條實施[43]，內政大臣藉此可向通訊服務供應商(例如郵務、電訊或互聯網公司)發出通知，要求它們維持其截取能力。[44] 通訊服務供應商有責任協助截取手令的執行。這些責任包括向有關機構提供被截取的材料、維持有關材料的保安及保密，以及協助截取通訊專員執行其職能。至於因履行這些責任而招致的開支，英國政府根據與所有提供截取服務的通訊服務供應商訂立的協議，將有責任"*公平地分擔部分*"款項，以應付所需開支。[45]

設立技術諮詢委員會

2.4.5 通訊服務供應商如接獲提供協助截取通訊的通知，並認為遵從該項通知要求而引致的技術或財務影響不合理，可將有關事宜轉交技術諮詢委員會處理。[46] 技術諮詢委員會由英國政府及通訊業的代表組成，負責就任何轉交其處理的通知是否合理一事，向內政大臣提供意見。事務大臣經考慮技術諮詢委員會的報告後，可撤回有關通知，或再發出經修改或未經修改的通知，以確認先前發出通知的效力。[47]

43 2002年第1931號立法文件，網址：http://www.hmso.gov.uk/si/si2002/20021931.htm。

44 授權法例委員會的辯論。有關授權法例的第十個常設委員會。《調查權力規例(維持截取能力)令》的擬稿。下議院。2002年6月18日。

45 《2000年調查權力規管法令》第14條。

46 2001年第3734號立法文件。技術諮詢委員會在2001年11月根據《2001年調查權力規例(技術諮詢委員會)令》成立。

47 授權法例委員會的辯論。有關授權法例的第十個常設委員會。《調查權力規例(維持截取能力)令》的擬稿。下議院。2002年6月18日。

《2001年反恐怖活動、罪行和保安法令》

2.4.6 《2001年反恐怖活動、罪行和保安法令》於2001年12月制定，作為緊急的反恐怖主義活動法例的一部分。該法令旨在確保英國政府擁有必需的權力，對付任何對英國的威脅。根據該法令第11部，內政大臣可發出有關通訊服務供應商保存通訊資料的實務守則。

2.4.7 通訊資料是通訊服務供應商所持有涉及其客戶所作通訊的資料，其中包括分項開列的帳單、通訊路線資料及用戶詳情，但不包括任何通訊的內容。根據該法令，通訊服務供應商可獲准保存這些資料，保存期限可超過其本身業務用途所需的時間，以便執法及保安機關可以國家安全和防止罪行為理由，根據《2000年調查權力規管法令》取覽有關資料。

第3章 —— 美國

3.1 背景

3.1.1 在美國，政府截取通訊的活動有很長歷史。自電報通訊於1844年發明以來，執法機關一直有截取電報的活動；自十九世紀90年代初，亦有截聽電話的活動。[48]

3.1.2 禁止非法截取通訊的州法例早於1862年已制定[49]，但往後數十年，卻未見有制定任何聯邦法例針對截取通訊。在1928年，最高法院在Olmstead v. United States一案裁定，聯邦探員利用竊聽裝置截取電話交談內容，並不算是《美國憲法第四修正案》[50] 所指的搜查或查封。其主要論據是根據《第四修正案》，免受不合理搜查及查封的保障只適用於人或物件，而不適用於無形之物，例如電話交談。

3.1.3 在1934年制定的《1934年聯邦通訊法令》，是禁止未經發送者同意下截取及洩露電話交談內容的首條聯邦法例。該法令亦限制以被截取材料作為法律程序上的可接納證據。然而，該法令的效力很快便被行政權力侵蝕。隨後30年間，聯邦調查機關繼續運用酌情權截取通訊，主要是根據總統保障國家安全的憲法權力，針對有嫌疑的外國情報人員截取通訊。[51]

3.1.4 在60年代，最高法院限制基於截取通訊而提出的檢控，以謀求保障個人免受不合理的搜查及查封。在1967年的Katz v. United States這個經典案例中，法庭裁定沒有手令的截取違反了《第四修正案》，並藉此建立了私隱權的合理期望原則。此項裁決推翻了1928年Olmstead一案的裁決，法庭並裁定截取通訊行動須符合憲法才可進行。

---

48 Boucher, Cotler and Larson (2001年)第3頁、Edwardson (1999年)第1頁，以及《新大英百科全書》(1994年)第437頁。

49 《新大英百科全書》(1994年)第437頁。

50 《美國憲法第四修正案》訂明，"*不得違反個人所享有在其人身、住所、文件及財物不會受到不合理搜查及查封的權利；除非基於很可能成立的因由，並由宣誓或誓章支持，以及特別說明將會被搜查的地點和人士或被查封的物件，否則不得發出任何手令。*"

51 Boucher, Cotler and Larson (2001年)第3及14頁，以及《新大英百科全書》(1994年)第437頁。

3.1.5 美國國會在1968年制定《1968年安全街道及罪行管制綜合法令標題III》(一般稱為《標題III》)，在聯邦層次訂立了首個截取通訊的具體法律架構。此後，國會曾多次修訂及更新有關截取的法例。《外國情報監視法令》("《情報監視法令》")、《電子通訊私隱法令》("《通訊私隱法令》")及《通訊協助執法法令》("《協助執法法令》")，分別於1978、1986及1994年制定。最近一次對截取法例的重要修訂，是在2001年"911事件"發生後一個半月制定的《提供必要的阻截恐怖主義的合適工具以團結和增強美國法令》("《愛國者法令》")。

3.2 法律架構

3.2.1 截取通訊的聯邦法律架構由3個主要部分組成:

(a) 載於《美國法典》第18篇第2510至2522條的《標題III》，以及《通訊私隱法令》對《標題III》的修訂；

(b) 載於《美國法典》第50篇第1801至1811條的《情報監視法令》；及

(c) 載於《美國法典》第18篇第3121至3127條的《標題18》有關通訊紀錄器及監測追蹤裝置的一章("《通訊紀錄／監測法規》")。

《1968年安全街道及罪行管制綜合法令標題III》

3.2.2 《標題III》是為執法目的而規管即時從電信及口頭通訊"*收集實際內容*"的最重要聯邦法規。[52] 此處所指的"*內容*"包括"*有關此類通訊所涉各方身份的任何資料，或該項通訊的存在、內容、大意或涵義的資料*"。[53] 該項法規於1986年被《通訊私隱法令》修訂，以包括截取電子通訊的事宜。[54]

3.2.3 根據《標題III》，"*截取*"指"*透過使用任何電子、機械或其他裝置，聽取或取得任何電信、電子或口頭通訊的內容*"。據司法部詮釋，"*截取*"的涵義"*限於在獲得通訊傳遞的同時取得其內容*"，而不包括取得已儲存的電信或電子通訊的行為。[55] 因此，《標題III》只適用於規管截取即時進行的通訊，而不適用於規管截取儲存的通訊。

《1978年外國情報監視法令》

3.2.4 《情報監視法令》訂定條文，規管截取在美國境內的外國勢力[56] 或其代理人的通訊以獲取外國情報資料的行為。此類資料從美國國家安全的角度來界定，包括保護國家免受實際或潛在的攻擊、破壞、國際恐怖主義及秘密情報活動的威脅等。

---

52 司法部(2002年)第76至77頁。根據《標題III》，口頭通訊指"*某人士說出的言詞，並顯示該人士期望該項通訊在合乎該期望的環境下不會被截取*"。電信通訊指"*通訊的來源點與接收點之間(包括來源點與接收點)任何一處包含人的聲音的通訊傳遞*"，而該項通訊的全部或部分必須"*借助電信設備、電纜或其他類似接駁裝置*"發送。一般而言，電話交談屬電信通訊。請參閱《標題III》第2510條及司法部(2002年)第81頁。

53 《標題III》第2510(8)條。

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

55 司法部(2002年)第82至83頁。

56 根據《情報監視法令》第1801(a)條，"外國勢力"包括外國政府或其組成部分；並非主要由美國人組成的外地國家的派系；正在或將會受到外國政府指示及控制的實體；從事國際恐怖主義活動的組織；以及以外國為基地而並非主要由美國人組成的政治組織。

3.2.5 與《標題III》相似的是，《情報監視法令》也是規管對通訊實際"*內容*"的截取。[57] 與《標題III》不同的是，《情報監視法令》的監視目標，必須是美國境內的外國勢力或其代理人，或所監視的設施正在或將會被外國勢力或其代理人使用。所截取的通訊無須與任何罪行有關，然而所得資料可能會提供刑事檢控的證據。儘管如此，監視的其中一個重要目的，必須是獲取外國情報資料，而非進行執法行動。

《標題18》有關通訊紀錄器及監測追蹤裝置的一章

3.2.6 與《標題III》或《情報監視法令》不同，《通訊紀錄／監測法規》所規管的，是對電信及電子通訊"*發訊對象及其他不涉實際內容資料*"的即時收集行為，例如撥出電話號碼及來電號碼的資料。[58]

3.2.7 據司法部所稱，"*通訊紀錄器*"及"*監測追蹤裝置*"的定義很廣泛，以致截取裝置可以是任何實物工具或軟件程式，或可安裝在各式各樣的通訊科技設施中，包括手提電話、互聯網用戶帳戶或電子郵件帳戶。這些裝置亦可記錄或解譯通訊中幾乎所有不涉*實際*內容的資料。[59]

3.3 《1968年安全街道及罪行管制綜合法令標題III》的法院命令制度

3.3.1 根據《標題III》，聯邦調查或執法人員獲准可依據法院命令截取通訊。

---

57 《情報監視法令》第1801(n)條。《情報監視法令》有關"*內容*"的定義基本上與《標題III》的相同。

58 同上。根據《通訊紀錄／監測法規》，"*通訊紀錄器*"指"*記錄或解譯從傳遞電信或電子通訊儀器或設施發出的撥號、發訊路線、發訊對象或信號資料的裝置或過程*"，但這些資料"*不包括任何通訊的內容*"。該詞亦不包括用作記帳或成本會計的裝置或過程。"*監測追蹤裝置*"指"*獲取正輸入的電子或其他脈衝資料的裝置或過程，以識別來源號碼或其他撥號、發訊路線、發訊對象或信號資料，而這些資料可合理地有可能識別某一電信或電子通訊的來源*"，這些資料"*不包括任何通訊的內容*"。

59 司法部(2002年)第104至105頁。

發出法院命令的機構

3.3.2 《標題III》的法院命令必須由美國地方法院或美國上訴法院的一名法官發出。[60]

申請程序

3.3.3 每宗申請在提交法官核准前，均須先獲下列其中一名司法部高級官員授權[61]：

(a) 司法部長；

(b) 副司法部長；

(c) 高級助理司法部長；或

(d) 任何助理司法部長、任何署理助理司法部長或任何特別指定的副助理司法部長。

3.3.4 每宗申請均須以書面向法官提出，並須宣誓或提交誓章。[62]如有需要，申請人或須向法官提交額外證供或檔案證據，以支持其申請。

發出法院命令的理據

3.3.5 只有為了調查《標題III》所列的嚴重罪行，才可發出法院命令。此類罪行包括謀殺、綁架、搶劫、勒索、賄賂、性侵犯兒童、毒品罪行、危害國家安全的罪行，以及可判處死刑或監禁超過1年的罪行。[63]

---

60 《標題III》第2510(9)條。

61 《標題III》第2516條。

62 《標題III》第2518條。每宗申請均須包括下列資料：(a)提出申請的調查或執法人員的身份，以及授權提出申請的人員的身份；(b)申請人賴以證明其有理據相信必須發出法院命令的事實及客觀情況。這些事實包括已觸犯、正在觸犯或將會觸犯的罪行的詳情；說明將進行截取通訊的設施或地點的性質及位置，以及將被截取的通訊類別；觸犯有關罪行及其通訊將被截取的人士的身份(如已知悉)；(c)是否已嘗試採取其他調查程序但告失敗，或為何合理地確定即使嘗試採取該些程序亦不大可能會成功，或認為採取該些程序過於冒險；(d)須持續截取通訊的期限；及(e)所有過往申請的詳細資料。

63 《標題III》第2516(1)(a)至(r)條。

3.3.6 此外，申請人必須證明有"*很可能成立的因由*"，使法院相信[64]：

(a) 某人士正觸犯、已觸犯或將觸犯《標題III》所列的某項罪行；

(b) 透過該截取行動將可獲得與該項罪行有關的通訊內容；及

(c) 將會在某設施或地點截取電信、口頭或電子通訊，而該設施或地點被該人士正在使用、將會使用或經常使用。

3.3.7 有關申請亦須證明截取行動會"*盡量減少截取若無必要不應被截取的通訊*"[65]，例如與行動目標無關、不切題及不涉刑事罪行的通訊，無論是截取對象或申請中並無提及的其他人士的通訊。[66]

3.3.8 根據《標題III》[67]，截取機關可申請進行"*無固定截取*"，意思是他們可向法院取得沒有指明某一特定電話線或電郵帳戶的截取命令，藉以容許他們可截取涉嫌人士使用的任何電話線、手提電話或互聯網帳戶。若有很可能成立的因由，相信截取對象試圖避開當局從指定設施截取通訊的行動，例如轉換電話以逃避截取，法院便會批准進行無固定截取。

3.3.9 在申請人要求下，法院命令可要求有關第三者(如通訊服務供應商及業主)提供所需的資料、設施及技術援助，以不顯眼及對有關服務干擾最少的方式完成截取行動。該項命令亦可要求有關第三者遵守《執法協助法令》就截取通訊能力的規定。[68] 根據《執法協助法令》，有關第三者因提供上述設施及技術援助而招致的開支，將獲合理賠償。

---

64 《標題III》第2518(3)條。

65 Kerr (2000年)第2頁及第2518(5)條。

66 同上。

67 《標題III》第2518(11)(b)條。無固定截取較為罕見。在2003年，根據《標題III》就刑事個案批准無固定截取的申請只有6宗。在該6宗申請中，有一宗是讓聯邦政府進行毒品調查。其餘5宗則屬州政府的調查：其中3宗涉及敲詐勒索案調查，一宗涉及毒品調查，一宗涉及謀殺案調查。請參閱《2003年竊聽行動報告書》(2004年)。

68 同上。

法院命令的有效期、終止有效期及續發安排

3.3.10 法院命令必須"*盡量減少截取通訊*"，意味截取行動的時間不得"*超逾授權擬達到的目的所需的任何時間，或在任何情況下不得超逾30天*"。[69] 法院可批准將命令續期，但續發命令的期限不得超過30天，並須在達到授權目的時終止。

沒有法院命令下合法截取通訊

3.3.11 《標題III》訂明，在取得法院命令前，司法部長、副司法部長或高級助理司法部長所指定的執法人員，可在涉及以下緊急情況展開截取行動[70]：

(a) 可導致任何人死亡或嚴重損傷的即時危險；

(b) 威脅國家安全的陰謀活動；或

(c) 具有組織罪行特點的陰謀活動。

3.3.12 儘管如此，上述人員必須在截取行動已發生或開始發生後的48小時內，向法院申請簽發法院命令。若未有申請或申請被拒，有關的截取行動必須立刻終止，而該行動會被視為非法。[71]

69 《標題III》第2518(5)條。

70 《標題III》第2518(7)(a)條及Schott(2003年)。

71 《標題III》第2518(7)(b)條。法院已明確指出，在某些地方如囚室、巡邏車及審問室，個人並無享有私隱的合理期望。因此，即使無人同意將對話內容記錄下來，在這些地方可毋須申請截取手令而暗中錄取對話內容。根據《第四修正案》，政府人員不得在侵擾個人合理期望所享有的私隱下，進行搜查行動。請參閱Schott(2003年)。

內部保障措施

盡量減少截取行動

3.3.13 為了限制侵犯個人私隱，《標題III》規定須實施最低限度截取的程序。通常來說，當執法人員在聽到法院命令涵蓋範圍以外的內容時，關掉截取通訊器材，並定時重開截聽器材以確定是否有法院命令所涵蓋的內容，將會被視為符合最低限度截取的規定。[72]

記錄被截取的通訊

3.3.14 被截取的通訊必須以錄音帶或其他相若工具記錄下來，以保障所錄取的內容不會被剪輯或修改。在截取通訊的期限屆滿時，這些紀錄必須立刻送交發出有關命令的法官，並在其指示下密封。除非發出命令或不接納申請的法官頒令，否則不得銷毀這些紀錄，並須將之保存10年。[73]

保障受監視人士的權益

3.3.15 在法院命令終止後的一段合理時間(但不多於90日)內，發出命令的法官有責任確保法院命令的簽發對象，以及被認為有利於司法公正的其他各方人士，均獲提供一份詳盡報表，當中載有截取活動日期的通知，以及通訊有否被截取。若有關人士提出申請，法官可向受影響人士提供部分被截取材料、截取申請文件及法院命令，以供查閱[74]。

提交定期報告

3.3.16 發出截取令的法官通常會要求截取機關提交定期報告，一般是每7至10天提交一次，以交代截取行動的進展。[75]

---

72 伊利諾斯理工學院研究所(2000年)第3-1至3-2頁。
73 《標題III》第2518(8)(a)及(b)條。
74 《標題III》第2518(8)(d)條。
75 Kerr(2000年)第2頁。

證據的可獲接納程度

3.3.17 被截取材料可被接納為法庭證據，但有關各方均須在審訊當日的不少於10天前，獲提供截取令及其申請文件的文本。如法官認為，有關各方不會因延遲接獲這些資料而致利益受損，則可批准豁免該10天期限。[76]

司法機構的監察

3.3.18 在法院命令(或續發命令)的有效期屆滿(或拒絕發出命令)後30天內，發出或拒絕發出命令的法官須向美國法院行政管理局("行政管理局")[77] 提交報告。報告須包括下列資料[78]：

(a) 申請該項命令官員及授權申請人士的身份；

(b) 調查中的罪行；

(c) 截取裝置的類別及這些裝置的一般所在位置；及

(d) 法院命令授權進行的截取行動期限。

[76] 《標題III》第2515及2518(9)條。

[77] 行政管理局是在1939年根據法例(《美國法典》第28篇第601條)成立。行政管理局局長及副局長由美國首席法官經諮詢美國司法會議後委任。該局負責處理美國法院的非司法及行政事務，請瀏覽以下網址：http://www.uscourts.gov/contact.html。

[78] 《標題III》第2519(1)條。

3.3.19 每年一月，在剛過去一年曾申請法院命令的檢控當局亦須向行政管理局提交報告。報告須包括下列資料[79]：

(a) 上一段(a)至(d)項的資料；

(b) 可入罪及不可入罪截取材料的性質，以及截獲此類材料的次數；

(c) 被截取通訊人士的數目；

(d) 在執行時遇到加密通訊的法院命令的數目，以及此類加密通訊有否令執法人員無法取得被截取通訊的原文；

(e) 用於截取行動的人力及其他資源的性質、數量和成本；及

(f) 截取行動所導致的逮捕、審訊及定罪個案數目。

立法機關的監察

3.3.20 除了司法機構的監察，國會亦可循多個途徑對截取通訊持續監察。

國會委員會

3.3.21 司法及情報委員會可舉行聆訊及提出由調查或執法機關回覆的書面質詢。截取活動亦可由眾議院的情報事務常設專責委員會，以及參議院的情報事務專責委員會監察。該兩個委員會負責確保情報資源不被誤用，以及有關當局的情報活動合法進行。[80]

[79] 《標題III》第2519(2)條。

[80] 請瀏覽該兩個委員會的網址：http://intelligence.house.gov/AboutTheCommittee.aspx及http://intelligence.senate.gov/juris.htm。

向國會提交報告

3.3.22 每年4月，行政管理局局長須向國會匯報剛過去一年的截取申請數目、獲發出或拒絕發出法院命令的個案數目、獲批准或拒絕延展命令有效期的個案數目，以及對這些數據的分析。[81]

公眾監察

3.3.23 任何人士屬於被截取通訊所涉一方或截取行動所涉目標的一方，均可在任何法律程序中，申請禁止披露任何被截取通訊的內容或來自有關內容的任何證據。可提出此類申請的理由包括：有關通訊被非法截取；批准截取的法院命令有不足之處；以及該項截取行動不符合法院命令[82]。

3.4 《1978年外國情報監視法令》的法院命令制度

3.4.1 根據《情報監視法令》，監視目標必須是在美國境內的外國勢力或其代理人，而受監視的設施正在或將會被外國勢力或其代理人使用。若截取行動涉及取得美國境內任何美國人的通訊資料，該行動必須取得法院命令。[83]《情報監視法令》有關獲取法院命令的規定較《標題III》的寬鬆。

81 《標題III》第2519(3)條。

82 《標題III》第2518(10)(a)條。

83 根據行政命令第12333號，總統在沒有法院命令下，可授權截取外國勢力及其代理人的通訊，以取得與美國人活動無關的情報資料。

發出法院命令的機構

3.4.2 《情報監視法令》的命令必須由稱為外國情報監視法院的特別法院發出。該法院由11名地方法院法官組成，他們是由最高法院首席法官從全美11個司法區的其中7區委任出來。外國情報監視法院具有獨有的司法管轄權，負責就美國境內任何地方的電子監視行動申請進行聆訊，以及發出命令批准該項監視行動。外國情報監視法院的法官不得就已被另一法官拒絕的同一項申請進行聆訊。[84]

申請程序

3.4.3 每宗申請均須由聯邦人員宣誓或提交誓章後，以書面向發出命令的法官提出，並須獲司法部長批准。[85]

3.4.4 有關申請必須載有一份資料。該份資料與根據《標題III》提出的申請所載相若。此外，《情報監視法令》規定有關申請須包括一份證明書，證明"*監視的一個重要目的是獲取外國情報資料*"。[86] 該證明書必須由負責國家安全事務的總統助理發出，或由總統指定一名行政機關官員發出，該名官員是總統徵詢參議院意見及同意後委任的行政官員之一。

發出法院命令的理據

3.4.5 法官一般會在下列情況發出命令[87]：

(a) 總統已授權司法部長批准有關申請；

(b) 有關申請由聯邦人員提出，並獲司法部長批准；

---

84 《情報監視法令》第1803條。若任何法官拒絕某項發出法院命令的申請，他或她必須就該項決定的理由提供書面陳述，以供記錄在案，有關紀錄將送交覆核法院審理。覆核法院由3名法官組成，他們均由首席法官從美國地方法院或上訴法院委任出來。該法院有司法管轄權覆核遭拒絕的法院命令申請。若覆核法院裁定拒絕有關申請是恰當的，便須就該項決定的理由提供書面陳述，以供記錄在案，而有關決定可由最高法院進一步覆核。雖然在2003年以前，外國情報監視法院從未拒絕任何簽發法院命令的申請，但在2003年，該法院卻拒絕了4項此類申請，而美國政府並沒有就該法院任何一項有關決定提出上訴。另請參閱司法部長於2004年4月30日根據《情報監視法令》向美國法院行政管理局提交的2003年報告書。

85 《情報監視法令》第1804(a)條。

86 《情報監視法令》第1804(a)(7)(B)條。

87 《情報監視法令》第1805(a)條。

(c) 具有很可能成立的因由，相信受電子監視的美國人是外國勢力或其代理人，而監視所針對的設施或地點正在或將會由外國勢力或其代理人使用。外國勢力的代理人包括在知情下從事，或在知情下協助或教唆他人暗中從事情報活動、陰謀破毀或國際恐怖主義活動的人士；及

(d) 截取機關已承諾採取最低限度截取的程序，以取得、保留或傳布截取所得的資料。

3.4.6 《愛國者法令》制定後，法院可根據《情報監視法令》，按《標題III》所訂理由批准進行無固定截取。

法院命令的有效期、終止有效期及續發安排

3.4.7 一般而言，根據《情報監視法令》發出的命令，最初有效期最長為90天。如針對外國勢力，命令的有效期可長達一年。若對象是外國勢力的代理人，命令的有效期可長達120天。法院若接獲有關命令的續期申請，以及按申請原有命令的同一方式提出新資料，即可根據發出原有命令的相同理據，將該項命令續期。

沒有法院命令下合法截取通訊

3.4.8 根據《情報監視法令》，總統可透過司法部長授權，在沒有法院命令下進行可長達一年的電子監視行動，藉以取得外國情報資料，但司法部長須為下述事宜提供證明：

(a) 監視行動旨在純粹獲取只在外國勢力之間傳遞的通訊內容；或從外國勢力公開及單獨控制的物業或處所獲取技術情報；及

(b) 監視行動並不涵蓋有"*美國人*"[88] 屬所涉一方的通訊；及

[88] 根據《情報監視法令》第1801(i)條，"美國人"指美國公民、獲合法認許在美國永久居留的外籍人士、成員主要是美國公民或合法居留外籍人士的非法團組織，或在美國成立為法團，但不包括屬外國勢力的法團或組織。

(c) 截取機關已承諾實施最低限度截取的程序，而司法部長須於這些程序的生效日期前最少30天，向眾議院的情報事務常設專責委員會及參議院的情報事務專責委員會，匯報這些程序。[89]

內部保障措施

3.4.9 比起《標題III》，《情報監視法令》的法院命令的內部保障措施較為寬鬆。[90]

披露及使用資料的限制

3.4.10 與《標題III》不同，《情報監視法令》並未規定須通知監視對象其通訊已被截取。聯邦人員可按合法理由使用及披露涉及任何美國人的被截取材料，而無須先徵得該美國人同意，但使用及披露這些材料時須遵守最低限度截取的程序。

在法院使用被截取材料

3.4.11 獲得司法部長批准後，被截取材料可在法庭上獲接納為證據。使用這些材料前，政府必須通知被告人。若有關證據是循非法途徑得來，被告人有權採取行動禁止披露這些證據。但是，若司法部長證明發放有關命令及其申請文件會損害國家安全，被告人將被禁止取閱這些文件。

司法機構的監察

3.4.12 類似《標題III》，《情報監視法令》同樣規定司法部長須每年向行政管理局提交報告。與《標題III》不同的是，根據《情報監視法令》截取而可披露的資料很有限。司法部長僅須提供有關批准電子監視及搜查行動而提出的法院命令申請及命令續期申請的總數，以及申請分別獲批准、經修訂後批准及遭拒絕的個案數目。其他所有有關《情報監視法令》的資料均屬機密。

---

89 若司法部長決定即時採取行動，他或她必須即時通知該兩個委員會將會採取最低限度截取的程序，以及作出決定的理由。

90 《情報監視法令》第1806條。

立法機關的監察

3.4.13 司法部長亦須每年向國會提交報告。此外，司法部長須就有關情況每年兩次"*充分告知*"眾議院情報事務常設專責委員會及參議院情報事務專責委員會。所提供的資料必須包括說明每宗刑事個案曾為執法目的而使用被截取資料或獲授權在審訊中使用被截取資料的情況。

3.5 《標題18》有關通訊紀錄器及監測追蹤裝置的一章的法院命令制度

3.5.1 《通訊紀錄／監測法規》的法院命令制度，其規定的嚴格程度不及《標題III》或《情報監視法令》所訂的制度。

發出法院命令的機構

3.5.2 《通訊紀錄／監測法規》的命令須由美國地方法院(包括一名此類法院的裁判官)或美國上訴法院發出。此外，發出命令的法院必須有就所查罪行的司法管轄權。[91]

申請程序

3.5.3 有關命令可由任何律師代聯邦政府提出申請。此外，沒有任何特別的授權安排。[92]

發出法院命令的理據

3.5.4 只要申請人證明將有可能被截取的資料，涉及正在進行的刑事調查，法院便會批准申請。法院並無責任就申請所載事實的真確性，進行獨立的司法研訊。

3.5.5 與《標題III》的命令相若，《通訊紀錄／監測法規》的命令同樣可要求第三者提供截取協助，以及遵守《執法協助法令》所訂截取通訊能力的規定。

---

91 《通訊紀錄／監測法規》第3122及3127(2)條。

92 《通訊紀錄／監測法規》第3122條。有關申請必須包括申請人的身份資料和正在調查的執法機關的身份資料，以及申請人提交的證明書，以證明將有可能取得的資料，涉及該機關正在進行的刑事調查。

法院命令的有效期、終止有效期及續發安排

3.5.6 《通訊紀錄／監測法規》命令的有效期不超過60天。如有需要，法院可基於最初發出命令的理由，延長該命令的有效期。每次續發命令的期限不得超過60天。[93]

沒有法院命令下合法截取通訊

3.5.7 和《標題III》相若，《通訊紀錄／監測法規》亦容許司法部高層官員所指定的調查或執法人員在緊急情況下，展開沒有法院命令的截取行動，但有關人員必須在展開行動後48小時內，向法院提出簽發命令的申請。儘管如此，《通訊紀錄／監測法規》所訂緊急情況的定義，較《標題III》的簡單，僅涉及導致任何人死亡或身體受到嚴重損傷的即時危險，或具有組織罪行特點的陰謀活動，而不涉及威脅國家安全的陰謀活動。

內部保障措施

限制使用截取科技

3.5.8 《通訊紀錄／監測法規》訂有條文，限制截取機關使用通訊紀錄／監測裝置科技。對電子或其他脈衝通訊的記錄或解譯工作，必須局限於撥號、發訊路線、發訊對象及信號資料，以便任何通訊的內容不會被包括在內。[94]

不得披露通訊紀錄／監測裝置的存在

3.5.9 法院命令必須密封，直至發出命令的法院頒令解封為止。向申請人提供截取協助的第三者亦不得向任何人披露通訊紀錄／監測裝置的存在，除非或直至法院頒命可披露爲止[95]。

司法機構的監察

3.5.10 若通訊紀錄／監測裝置與任何竊聽裝置一併使用，截取機構必須向行政管理局匯報。除此之外，截取機構毋須向行政管理局提交報告。

---

93 《通訊紀錄／監測法規》第3123(c)條。
94 《通訊紀錄／監測法規》第3121(c)條。
95 《通訊紀錄／監測法規》第3123(d)條。

立法機關的監察

3.5.11 司法部長必須每年向國會提交報告。報告內容必須包括[96]：

(a) 有關命令授權的截取行動期限、該命令獲續期的次數及續期期限；

(b) 有關申請及命令或續發命令所指明的罪行；

(c) 涉及的調查行動數目；

(d) 受影響設施的數目和性質；及

(e) 提出申請的調查或執法機關的身份(包括所屬地區)，以及授權發出命令的人員的身份。

3.6 實施法例的行政酌情權權限

3.6.1 美國的行政機關可酌情決定應否開始實施某項法例，但這項權力受立法機關規限。《美國憲法》第1條第7款訂明，"*每項須經眾議院及參議院通過的法案在成為法例前，均須提交美國總統。*"總統有10天時間決定是否簽署該法案。若總統簽署該法案，該法案便成為法例。若總統否決該法案，便須將該法案發還國會，並說明他不批准該法案的原因。國會可重新研究及修改該法案，然後再提交總統。若總統在10天內不簽署或發還該法案，該法案將自動成為法例。若法案在參、眾兩院獲得三分之二的大多數議員支持，國會可推翻總統的否決，進而在總統否決該法案的情況下簽署該法案，使之成為法例。就截取法例的制定，行政機關在取得國會大多數議員支持以及在實施上，並未遇到困難，但倡議公民自由的組織曾抨擊有關法例大幅擴大當局的權力，令公民的私隱受侵犯。

[96] 《通訊紀錄／監測法規》第3126條。.

3.7 與"911"事件及通訊科技發展有關的法例修訂

3.7.1 美國國會近期的法例修訂大多與"911"事件有關，而非關乎通訊科技的發展。

《提供必要的阻截恐怖主義的合適工具以團結和增強美國法令》

3.7.2 "911"事件後，國會因應恐怖主義活動威脅國家安全，通過了多項法例，為打擊恐怖主義活動提供了新的工具。其中最具爭議性的法令是《愛國者法令》。該法令修訂了多項現行法規，並訂有涵蓋廣泛事務的新條文。該法令就有關截取通訊的聯邦法例的主要修訂綜述如下。這些修訂旨在賦予聯邦人員更大權力截取通訊，以達致執法及蒐集外國情報之目的。[97]

對《標題III》的修訂

3.7.3 《愛國者法令》在《標題III》的指定罪行名單中，加入了網絡罪行如電腦欺詐，以及數項恐怖主義罪行，例如化學武器的罪行、使用大殺傷力武器、跨境恐怖主義暴力行為、與支持恐怖分子的國家有財務交易、對恐怖分子提供實質支持，以及對恐怖分子組織提供實質支持。[98]

3.7.4 《愛國者法令》在《標題III》加入新條文，容許調查或執法人員在沒有法院命令下，截取"*受保護電腦*"系統內侵入者的通訊。此類電腦系統包括作州際或外國商業或通訊用途的電腦，或聯邦政府或金融機構使用的電腦。截取行動必須只限於侵入者向、透過或從被入侵電腦傳遞的通訊[99]。

[97] 詳情請參閱Doyle(2001年)及(2002年)。
[98] 《愛國者法令》第201及202條。
[99] 《愛國者法令》第217條。

3.7.5 《愛國者法令》亦在《標題III》引入一項新條文[100]，容許調查或執法人員與其他聯邦執法官員、情報人員、保衞人員、移民官員、國家防衞官員或國家安全人員，共用被截取通訊的內容(包括外國情報)，以協助該等官員履行其公務職責。

對《情報監視法令》的修訂

3.7.6 在《愛國者法令》制定前，《情報監視法令》規定為截取通訊而提出的法院命令申請，必須載有由行政機關指定人員發出的證明書，證明監視的"*唯一目的*"是取得外國情報資料。《愛國者法令》以"*重要目的*"取代"*唯一目的*"。[101]

3.7.7 為促進執法人員與外國情報調查員的合作，《愛國者法令》訂明，情報人員可共用包含外國情報或反情報資料的刑事調查資料，包括竊聽資料。

對《通訊紀錄／監測法規》的修訂

3.7.8 根據以往所訂的《通訊紀錄／監測法規》，授權使用通訊紀錄／監測裝置的法院命令，主要適用於電話線，儘管不少法院曾將之應用於電腦網絡通訊。此外，通訊紀錄／監測裝置曾一度只限於在發出命令的司法區管轄區內使用。據司法部所稱，此項限制浪費時間及資源，因為執法人員追蹤在多個司法管轄區活動的疑犯，須在每一涉案司法管轄區重複申請有關命令。根據《愛國者法令》，《通訊紀錄／監測法規》的命令不但可用來截取電腦網絡對話(例如電子郵件)的來源及收件人資料，對被調查罪行擁有司法管轄權的法院，更可發出可在美國境內任何地方執行的截取命令。[102]

[100] 《愛國者法令》第203條。
[101] 《愛國者法令》第218條。
[102] 《愛國者法令》第216條、Doyle(2002年)第5至6頁，以及Mueller (2004年)第2頁。

第4章 —— 澳洲

4.1 背景

4.1.1 在1960年之前，澳洲並未有任何聯邦法例禁止截取通訊。政府的截取活動是以行政措施的方式進行。自1950年起，政府便訂有總理指示，規管此種行政權力的使用。這些指示只授權當局就有關間諜、破壞及顛覆活動的個案截取通訊。[103]

4.1.2 於1960年制定的《1960年電話通訊(截取)法令》，是首次以法定方式規管截取通訊。該法令把截取電話通訊定為刑事罪行，但在兩種情況下除外。[104] 該法令亦不准許為執法目的而截取電訊。

4.1.3 上述於1960年制定的法令其後被廢除，並以《1979年電訊(截取)法令》("《截取法》")取代。《截取法》增訂了*"聯邦政府具合法截聽電話的獨有權力"*的規定，以及訂立了把有關權力授予州政府合資格機構的架構。[105] 根據《截取法》，執法機關如澳洲聯邦警察及州政府警隊首次獲准在若干情況下截取電話通訊。

4.1.4 自1979年起，《截取法》一直是截取電訊的主要法律架構。藉着對《截取法》的修訂，可利用截取手令調查的罪行數目倍增；獲授權申請截取手令的機關數目有所增加；使用被截取材料以達到之目的亦日趨廣泛。

---

[103] 《1994年電訊(截取)修訂法案》的摘要說明第2頁。

[104] 第一種情況是由郵政署以技術理由或為了追查非法來電(如騷擾電話)而截取。第二種情況是根據總檢察長以國家安全為理由而向保安部門發出截取手令，或由保安事務長在緊急情況下發出短期的截取手令。

[105] 《1994年電訊(截取)修訂法案》的摘要說明第3頁。

4.2 法律架構

4.2.1 《截取法》的法定基礎來自《澳洲聯邦憲法法令》第51條。該條文訂明澳洲議會有權就"*郵遞、電報、電話及其他相若服務*"，"*為聯邦政府的和平、秩序及良好管治制定法例*"。

4.2.2 《截取法》的重點有二。首先是"*為了保障使用澳洲電訊系統人士的私隱，而把截取經該電訊系統傳送的通訊定為罪行*"。[106]《截取法》第6(1)條把"*截取*"界定為"*包括在發出通訊者不知情的情況下，以任何方法收聽或記錄正透過該電訊系統傳送的通訊*"。根據《截取法》，儲存的通訊亦受到保障而不得被截取，因為"*透過.....傳送*"一語包括"*暫時儲存於*"電訊系統的含義。澳洲政府近年一直嘗試向澳洲國會提出法例修訂，以刪除《截取法》對儲存通訊的保障。

4.2.3 《截取法》的第二個重點是"*訂明可合法截取的情況*"。[107]該法令訂明根據何種目的可以申領截取手令、誰人可申領及發出此類手令、手令申請的格式及內容、在發出手令前必須符合的準則、手令的涵蓋範圍，以及備存紀錄和報告的規定。

4.3 《1979年電訊(截取)法令》的截取手令制度

4.3.1 截取手令分為兩類，即"*電訊服務手令*"及"*具名人士手令*"。前者是就某一項指明的電訊服務而發出的手令，後者是就某一具名人士正在使用或可能使用的任何電訊服務而發出的手令。

---

[106] 總檢察長部(2004年)第8頁。此項重點載於《截取法》第7(1)條，該條文訂明"*任何人士不得截取，或授權、容許或准許另一人截取，或作出任何行為或事情使他／她或另一人可截取經電訊系統傳送的通訊*"。

[107] 總檢察長部(2004年)第8頁及《截取法》第7(2)(b)條。

發出手令的機構

4.3.2 上述兩類手令均可以國家安全或執法為理由而發出。

總檢察長及保安事務長

4.3.3 國家安全手令一般由聯邦政府總檢察長("總檢察長")發出，他是負責處理警務、法律事務及澳洲保安情報組織("保安情報組織")[108] 事務的部長。總檢察長由總理委任，而按照慣例，總理是眾議院擁有最多議席的政黨或執政聯盟的領袖。

4.3.4 在少數情況下，保安情報組織內向總檢察長匯報的保安事務長可發出有效期不超過48小時的國家安全手令。這些情況包括[109]：

(a) 總檢察長在之前3個月內並未拒絕發出保安事務長所要求發出的手令；及

(b) 保安事務長信納受調查個案的事實有充分理據支持總檢察長發出手令，而要等待總檢察長決定是否發出手令，將會或相當可能會嚴重損害國家安全。

4.3.5 發出手令時，保安事務長必須向總檢察長提交該手令的副本，以及發出手令理由的聲明。總檢察長可在有關手令有效期屆滿前隨時將之撤銷。[110]

[108] 保安情報組織的職能詳載於《1979年澳洲保安情報組織法令》。該組織主要負責蒐集資料及提供情報，以便就可能危害澳洲國家安全的活動或情況，向政府發出預警。請瀏覽以下網址：http://www.asio.gov.au/About/Content/what.htm。

[109] 《截取法》第10(1)條。

[110] 《截取法》第10條。

合資格法官及獲提名的行政上訴審裁處成員

4.3.6 執法手令必須由一名合資格法官或獲提名的行政上訴審裁處("審裁處")成員發出。[111]

4.3.7 合資格法官指澳洲國會設立的法院法官，而該名法官已同意總檢察長的提名，並獲總檢察長宣布為合資格法官。[112] 目前，合資格法官分別來自澳洲聯邦法院、澳洲家庭法院及聯邦裁判法院。

4.3.8 獲提名的審裁處成員是指獲得總檢察長提名而可簽發截取手令的審裁處副主席、全職或兼職資深成員或一般成員。[113] 根據《1975年行政上訴審裁處法令》第7條，審裁處副主席必須為曾在州或地區政府的高等法院、聯邦法院或最高法院，有不少於5年經驗的法律執業者，而資深成員則可以是法律執業者或在其他範疇有專業知識的人士。除非審裁處一般成員或兼職資深成員擁有與副主席相同的司法資歷，否則將不符合可獲提名簽發手令的資格。[114] 獲提名的審裁處成員被政府視為獨立，可如法官一樣不偏不倚地評估證據。[115]

111 根據《1975年行政上訴審裁處法令》成立的審裁處，獲賦權覆核各部長及政府官員和公共機構所作範圍廣泛的行政決定，以確定這些決定是否恰當。審裁處亦會覆核若干非政府組織的行政決定。審裁處由一名主席、主席任命的成員(包括法官及副主席)、資深成員及一般成員組成。主席必須由澳洲聯邦法院的法官擔任。審裁處須向總檢察長匯報其工作。請瀏覽以下網址：http://www.aat.gov.au/AboutTheAAT/IntroductionToTheAAT.htm。

112 《截取法》第6D條。

113 《截取法》第6DA(1)條。

114 《截取法》第6DA(2)條。

115 Tom Sherman AO (2003年)第11頁。近年大部分執法手令均由獲提名的審裁處成員簽發。在2002至03年度，審裁處成員曾發出2 788項手令，佔共發出3 058項手令中約91%。其餘手令的簽發當局分別為家庭法院法官(206項或7%)、聯邦法院法官(7項或0.2%)及聯邦裁判法院法官(57項或1.9%)。請參閱總檢察長部(2000年)、(2001年)、(2002年)、(2003年)及(2004年)。

4.3.9 把簽發截取手令的權力賦予獲提名的審裁處成員，源自高等法院在1995年就Grollo一案提出的關注。[116] 法院在該案裁定簽發截取手令不僅是一種不屬於司法範疇的權力，而且帶有侵犯私隱及秘密性質，可能會削弱公眾對司法機構獨立公正的信心。法院亦裁定，未經法官同意下，不得向法官賦予司法以外的職能，而各類審裁處、聯邦政府的法律人員及退休法官亦是負責簽發手令的適當人選。

申請程序

4.3.10 國家安全手令的申請，只可由保安情報組織的保安事務長提出，而執法手令申請則可由下列合資格機構提出[117]：

(a) 澳洲聯邦警察；

(b) 澳洲罪行委員會；或

(c) 有部長宣言生效的州政府或北部地區政府的合資格機構。[118]

4.3.11 國家安全手令的申請須以書面提出，並述明申領該手令的理由及發出該手令所預期達致的效果。

4.3.12 執法手令申請亦須以書面提出。此外，每宗申請須附上一份誓章，述明該項申請以何種事實及理由為根據，以及該手令的有效期。[119]

---

116 Bruno Grollo v. 澳州聯邦警務處長Michael John Palmer及其他F.C.95/032，網址：http://www.newcastle.edu.au/school/law/course_resources/laws5018_media_law/aOJContempt/OJAccess/Html/aCases/Grollo95.html。

117 《截取法》第5、34及39條和總檢察長部(2004年)第9頁。

118 《截取法》把合資格機構界定為州政府或北部地區政府的警務當局。這些機構亦包括廉政公署、新南威爾斯罪行委員會、警務人員操守委員會、昆士蘭州罪行及不當行為委員會、西澳洲反貪污委員會、警務人員操守委員會監察長及皇家西澳洲警隊調查委員會。

119 《截取法》第42(1)、(2)及(3)條。

發出手令的理據

國家安全理由

4.3.13 發出電訊服務或具名人士的國家安全手令前，總檢察長必須考慮若干法定準則，尤其須信納[120]：

(a) 發出手令的對象正從事或被合理地懷疑正從事損害國家安全的活動；或

(b) 擬取得的外國情報對澳洲國防或澳洲國際事務的運作很重要。

4.3.14 倘手令申請的目標是某一具名人士，總檢察長必須進一步信納截取某人通訊是必要的，而倚賴電訊服務手令取得有關情報將不能有效達到該目的。

執法理由

4.3.15 執法手令只可為調查"*一級*"及"*二級*"罪行而發出。

4.3.16 一級罪行包括謀殺、綁架、毒品罪行及恐怖活動，亦包括其他主要一級罪行的從屬罪行，例如協助、教唆及串謀觸犯有關罪行。[121]

4.3.17 二級罪行包括涉及人命損失、嚴重人身傷害、嚴重縱火、販毒、嚴重詐騙、賄賂、貪污、清洗黑錢、網際罪行等。在大部分情況下，有關罪行必須是可被判處終身監禁或最少監禁7年。這些主要罪行的從屬罪行亦屬二級罪行。[122]

4.3.18 就一級及二級罪行發出手令的法定準則大致相同。特別是，合資格法官或獲提名的審裁處成員必須考慮有關的執法機關有多少其他調查方法可供採用，或已使用其他調查方法的程度。

120 《截取法》第9、9A、11A、11B及11C條。
121 《截取法》第5(1)條。
122 《截取法》第5D條。

4.3.19 就一級及二級罪行簽發手令的理由有些少差異，是基於一級罪行較二級罪行嚴重。[123] 兩者的最主要差別在於，就二級罪行簽發手令前，法官或獲提名的審裁處成員必須考慮有關罪行的嚴重程度，以及對任何人私隱的侵擾程度。就一級罪行簽發手令則無此項規定。

手令的有效期、終止有效期及續發安排

4.3.20 國家安全手令的有效期不得超過6個月，而總檢察長可在有關手令有效期屆滿前隨時將之撤銷。[124] 執法手令的有效期最長有90天，並可按申請原有手令的同一方式延展有效期。

沒有手令下合法截取通訊

4.3.21 根據《截取法》，只有澳洲聯邦警察或州政府警隊才可在下述情況，於沒有手令下截取通訊[125]：

(a) 負責截取的警務人員或另一警務人員是被截取通訊的一方，或接收通訊的人士同意其通訊被截取；

(b) 有合理理由懷疑通訊所涉的另一方，其行為已導致或可能導致人命損失、嚴重人身傷害或財產嚴重損毀，或同意其通訊被截取的人士，相當可能會收到由一名已導致或可能導致人命損失、嚴重人身傷害或財產嚴重損毀的人士所發出的通訊；及

(c) 截取的需要已很迫切，無法在合理可行的情況下申請手令。

4.3.22 截取通訊後，有關機構的人員必須在切實可行的情況下盡快提出手令申請。倘有關申請被拒絕，截取行動必須終止。

123 《截取法》第45、45A、46及46A條。
124 《截取法》第9B、11D及13條。
125 《截取法》第7(4)及(5)條。

內部保障措施

4.3.23 《截取法》對領有手令的截取電訊行動施加了多項保障。

總手令登記冊

4.3.24 澳洲聯邦警務處長("處長")必須備存一份總手令登記冊，列述每項執法手令的詳細資料[126]，並每3個月向總檢察長提交該份登記冊，以供查閱。

特別手令登記冊

4.3.25 處長亦須備存一份特別手令登記冊，列述根據被截取資料而未能向某人提出刑事訴訟的各項手令或續發手令的詳細資料。該登記冊所載的詳細資料與總手令登記冊所載的資料相若。處長必須每3個月將特別登記冊連同總登記冊一併呈交總檢察長，以供查閱。

在法庭使用被截取材料的限制

4.3.26 根據《截取法》[127]，合法截取的資料不得傳送予其他人士或在法律程序中被呈交作為證據，但若干情況可獲豁免。該些豁免情況包括：在"獲豁免程序"中使用有關資料，例如就"指明罪行"(即一級及二級罪行)提出檢控；或為了"*獲認許之目的*"(例如調查"*指明罪行*")而將有關資料傳送予另一人。此外，根據其他豁免安排，某些人士可在已指定的情況下披露有關資料，他們包括截取人員、截取機關的主管及警隊成員。

[126] 《截取法》第81A條。有關的詳細資料包括：(a)發出手令的日期；(b)負責簽發手令的法官或獲提名審裁處成員；(c)獲發手令的機關；(d)手令過去或現時的有效期；(e)該手令涉及的電訊服務；(f)手令指明現正或可能會使用有關電訊服務的人士的姓名；及(g)簽發手令的法官或獲提名審裁處成員審批手令申請時信納的每項嚴重罪行。

[127] 《截取法》第67、68及74條。

行政機關的監察

申訴專員報告書

4.3.27 根據《截取法》[128]，申訴專員[129] 在每一財政年度須就澳洲聯邦警察及澳洲罪行委員會("罪行委員會")簽發手令及截取行動的紀錄，最少查核兩次。罪行委員會是有資格申領執法手令的機構之一。查核紀錄的目的之一，是確定記入總手令登記冊及特別手令登記冊的資料均準確無誤。另一目的是監察該兩個機關有否遵守法定的備存紀錄規定。在每一財政年度結束後3個月內，申訴專員必須向總檢察長書面匯報其查核結果。如有需要，申訴專員可隨時進行這類查核，並向總檢察長報告。

4.3.28 查核時，申訴專員獲賦權，在通知有關執法機關的首長後，可進入該機關佔用的處所。申訴專員有權自由取覽該機關有關紀錄的全部內容、複印該些紀錄或從該些紀錄摘取部分內容。申訴專員亦可要求該機關的首長在指明的期限或時間，前往指明的地點與指明的查核人員會面，以回答與查核有關的問題。

立法機關的監察

4.3.29 澳洲國會設有兩個法定委員會及兩個常設委員會，監察與截取通訊有關的事宜。

[128] 《截取法》第79至89條。

[129] 聯邦政府申訴專員一職是根據《1976年申訴專員法令》成立。申訴專員由總督委任。申訴專員的活動受到多項法例規管，包括《1979年電訊(截取)法令》。

澳洲罪行委員會聯合法定委員會

4.3.30 根據《1984年國家罪行管理局法令》成立的澳洲罪行委員會聯合法定委員會[130]，負責審閱罪行委員會提交的周年報告，並就任何與罪行委員會履行職能有關的事宜，向澳洲國會報告。然而，該委員會未獲賦權調查涉及有關犯罪活動的事宜，亦無權重新研究罪行委員會就某項調查工作所得的查核結果。

保安情報組織、澳洲秘密情報處及國防通訊事務部議會聯合委員會[131]

4.3.31 立法機關對情報及保安組織截取通訊的監察，由根據《2001年情報事務法令》設立的保安情報組織、澳洲*秘密*情報處及國防通訊事務部議會聯合委員會("聯合委員會")負責。[132] 聯合委員會負責審查上述3個機構的管理及開支，並檢討由有關事務的部長，或參議院或眾議院通過的決議轉交處理有關該3個機構的任何事宜。聯合委員會不能主動就任何事宜展開檢討，但可要求負責有關事務的部長，將某項事宜轉交該委員會檢討。聯合委員會須向澳洲國會及負責有關事務的部長匯報其意見及建議，並擬備及提交周年報告予澳洲國會。然而，聯合委員會不得調查該3個機構的若干事宜，包括情報蒐集工作的先後次序、情報來源及其他運作上的協助或方法、特定的行動及個別投訴。

[130] 該委員會由10名委員組成，計有由執政黨黨鞭提名的3名眾議院議員；由反對黨黨鞭或獨立議員提名的2名眾議院議員；由參議院內執政黨領袖提名的2名參議院議員；由參議院內反對黨領袖提名的2名參議院議員；以及由少數黨或獨立參議員提名的1名參議員。

[131] 澳洲秘密情報處負責蒐集海外情報。國防通訊事務部是負責訊號情報及資料保安事宜的澳洲國家機構。

[132] 該委員會由7名委員組成，包括3名參議院議員及4名眾議院議員。按慣例，其中4名委員來自組成澳洲政府的黨派，其餘3名委員則來自反對黨。

法律及憲制事務常設委員會

4.3.32 眾議院設有一個可關注廣泛事宜的調查委員會，名為法律及憲制事務常設委員會。[133] 這個委員會負責調查由眾議院或負責有關事務的部長轉交處理的事宜，及有關政府部門在其提交的周年報告中提出的事宜，包括有權以國家安全理由發出截取手令的總檢察長所發表的周年報告。

4.3.33 與眾議院法律及憲制事務常設委員會相比，參議院法律及憲制事務常設委員會的職權範圍較為狹窄。該委員會專責調查由參議院轉交處理的法案或部分法案內容。在2004年，該委員會曾多次調查有關截取電訊的法案。

總檢察長提交的周年報告

4.3.34 《截取法》規定總檢察長須擬備周年報告，載述為執法而截取電訊的詳情，並把報告提交國會參眾兩院省覽。該報告必須包括下述資料[134]：

(a) 手令申請的數目及發出手令的數目；

(b) 發出手令時所指明的手令有效期，以及有關手令的實際有效期；

(c) 根據被截取資料而拘捕、檢控及入罪的個案數目；

(d) 任何機關在緊急情況下未有手令而截取通訊的次數；

(e) 每項手令的總開支和平均開支；及

(f) 是否由法官簽發手令，以及在多大程度上由獲提名審裁處成員簽發手令的情況。

[133] 該委員會由10名眾議院議員組成，其中6名由組成澳洲政府的黨派提名，另外4名由在野黨派提名。

[134] 《截取法》第100至103A條及總檢察長部(2004年)第16頁。《截取法》訂明，每一個有資格申領手令的機構均須在其報告內列述有關資料。有關資料亦須以總計方式詳細顯示截取電訊工作的程度及成效。

法例實施的行政酌情權權限

4.3.35 在澳洲，總理及其他部長均沒有押後實施或不實施某一法令的酌情權。自1989年採用的一般做法，是在法例中訂定生效日期條文，訂明有關法例將於何時自動開始生效。另一做法是在生效日期條文中訂明，如在某日期前沒有公告有關法例，該法例會視作已被廢除。

4.4 與"911"事件及通訊科技發展有關的法例修訂

4.4.1 在澳洲，大部分與截取通訊有關的法例修訂，均屬澳洲政府一系列反恐怖主義活動法例的一部分。在這些修訂中，只有少數條文涉及通訊科技的發展。

《2002年截取電訊法例修訂法令》

4.4.2 當局於2002年7月制定《2002年截取電訊法例修訂法令》("《截取修訂法》")。《截取修訂法》修訂《截取法》以擴大政府的監視權力。有關修訂包括把涉及恐怖主義、兒童色情物品及嚴重縱火的罪行，訂為可容許申領截取電訊服務手令的罪行。[135]

4.4.3 《截取修訂法》獲通過時的條文，並未包括政府擴大執法機關權力的建議。根據該項建議，執法機關可在沒有截取手令的情況下，取覽"*儲存*"或"*延遲取用*"的通訊的內容。[136] 政府該項建議遭否決，因為公眾廣泛批評有關建議會削弱通訊私隱的保障。[137]

[135] 《2002年截取電訊法例修訂法案》，議會事務部議會圖書館資料及研究服務處的《法案匯編》第121號(2001至02年)第7頁，以及總檢察長(2004年)第14頁和(2003年)第9至10頁。

[136] 這些內容指在傳送期間暫時儲存於服務供應商通訊儀器中的通訊，亦即電子郵件、話音通訊、短訊服務等。

[137] 參議院法律及憲制法例委員會(2002年)和澳洲電子領域(2002年)。

《2004年電訊(截取)修訂法令》

4.4.4 當局於2004年4月制定《2004年電訊(截取)修訂法令》("《2004年法令》")。《2004年法令》旨在就下述各方面修訂《截取法》[138]：

關於截取目的之新罪行

4.4.5 《2004年法令》將最近納入《聯邦刑事法典》的具體恐怖主義罪行，加入《截取法》所訂的"*一級*"罪行名單內，該名單原先只採用了"*恐怖主義行為*"這個頗為一般性的用語。具體的恐怖主義罪行包括使用炸藥或致死裝置的恐怖分子活動；提供或接受與恐怖主義行為有關的訓練；擬備有可能助長恐怖主義行為的文件；就恐怖主義組織的活動給予指示；及籌集資金以協助或從事恐怖主義行為。《2004年法令》賦權執法人員及保安情報組織人員申請截取手令，以便調查澳洲境內的具體恐怖活動。

4.4.6 此外，《2004年法令》將各種"*網際*"罪行和"*火器及軍備交易*"納入《截取法》所訂的"*二級*"罪行名單內。此項修訂清楚訂明，當局可發出截取手令，協助調查《截取法》所訂涉及火器或軍備交易的罪行。

"*截取*"*一詞的較廣泛定義*

4.4.7 《2004年法令》修訂了《截取法》有關"*截取*"通訊的定義，使之不僅包括"*收聽及記錄*"，亦同時包括"*閱讀或觀看*"，從而擴大了對截取行為的禁制。此舉旨在配合近年的科技發展，因為有關發展可令電訊用書寫文字的方式傳送，例如電子郵件或圖像，令"*收聽*"的概念不再適用。

[138] 《2004年電訊(截取)修訂法令》，2004年第55號，網址：http://scaleplus.law.gov.au/html/comact/11/6810/0/CM000020.htm。《2004年電訊(截取)修訂法案》，《法案匯編》第111號(2003至04年)，以及總檢察長部就《2004年電訊(截取)修訂法案》提交的摘要說明。

沒有手令下記錄傳送至保安情報組織公用線路的通訊

4.4.8 《2004年法令》在《截取法》中訂定新的條文，容許保安情報組織收聽、記錄、閱讀或觀看循該組織的公開電話號碼聯絡該組織的來電。這些電話號碼讓公眾人士可與保安情報組織聯絡，並載列於可供公眾查閱的電話簿或電話號碼資料庫。

容許未經通知電訊傳送者而截取通訊

4.4.9 《2004年法令》修訂《截取法》，刪除有關保安情報組織須通知電訊傳送者的規定，使該組織在已發出向傳送者營辦電訊服務截取通訊的手令，及毋須取得傳送者協助執行手令的情況下，毋須通知傳送者。然而，執法機關如須截取電訊傳送者所營辦網絡上的通訊，即使毋須該傳送者協助，仍須通知該傳送者。

《2004年電訊(截取)修訂(儲存通訊)法案》

4.4.10 眾議院於2004年6月通過《2004年電訊(截取)修訂(儲存通訊)法案》("《2004年法案》")。《2004年法案》修訂《截取法》，使取覽儲存通訊的行為免除現行有關截取通訊的禁制，為期12個月，以等待總檢察長部就取覽儲存通訊及澳洲的截取通訊制度是否切合時宜進一步檢討的結果。

4.4.11 《2004年法案》是澳洲政府提出的最新一項立法行動，希望可在沒有截取手令下取覽"*儲存通訊*"。澳洲國會圖書館的資料及研究服務處認為，澳洲政府藉着《2004年法案》，就《截取法》為儲存通訊"*訂定的保障建議提出範圍更廣的豁免，儘管有關豁免僅屬暫時性質*"，其豁免甚至較《2002年法案》[139] 所建議而備受批評的豁免更為廣泛。另一方面，澳洲聯邦警察歡迎當局制定《2004年法案》，並表示"*如不修訂，以便盡快取覽儲存通訊，則可以很容易被任意處置並可輕易被銷毀的證據，便有可能*"在申領截取手令期間"*喪失*"。

[139] 《2002年截取電訊法例修訂法案》，國會事務部議會圖書館資料及研究服務處的《法案匯編》第153號(2003至04年)第7頁。

4.4.12 參議院法律及憲制法例委員會在2004年7月建議將《2004年法案》提交參議院表決，但條件是總檢察長所建議的檢討必須開展以及將檢討結果公開，並具體研究儲存通訊應否免受《截取法》規管的問題。[140]

[140] 法律及憲制法例委員會就《2004年電訊(截取)修訂(儲存通訊)法案》條文所提交的報告。該委員會審議《2004年法案》後，於2004年7月22日提交該報告。

第5章 —— 分析

5.1 引言

5.1.1 根據是項研究的結果，本部集中討論下述事項，以協助議員商議香港特別行政區("香港特區")對截取通訊的規管：

(a) 選定海外司法管轄區截取手令制度的特點；及

(b) 其他司法管轄區因應"911"事件及通訊科技發展而作出的法例修訂。

5.1.2 本部討論這些事項時，參考了香港特區的相關規例及立法建議，計有《電訊條例》(現時規管截取電訊的法例)、《截取通訊條例》(於1997年制定但政府至今尚未實施)，以及《截取通訊條例草案》("《白紙條例草案》")(於1997年2月由政府公布作公眾諮詢，但該條例草案一直未有提交前立法局／立法會)。

5.1.3 為方便議員討論，就研究中3個司法管轄區及香港特區的截取手令制度各項特點的比較表列於附錄I。附錄II列述若干其他海外地區所採用不同類別的截取手令制度。附錄III就美國及澳洲為執法目的而進行的截取行動提供部分詳細資料。3個選定司法管轄區發出截取手令數目的各個圖表載於附錄IV。

5.2 截取手令制度

<u>法律架構</u>

5.2.1 在所研究的3個司法管轄區中，英國及澳洲均採用單一及總括的法規，規管為執法及國家安全而展開的截取通訊行動。該兩個地區的法例不僅規管截取通訊的實際內容，亦規管截取通訊中與內容無關的資料。另一方面，美國則以兩套不同的法規，分別規管為執法及為保障國家安全而展開的截取行動。前者由《標題III》規管，後者則受《情報監視法令》規限。此外，無論是《標題III》或《情報監視法令》，均未有涵蓋通訊中與內容無關的資料的截取行動，此類行動由《通訊紀錄／監測法規》規管。

5.2.2 在香港特區，為防止、調查或偵測嚴重罪行及為香港特區保安而進行的截取通訊，均由單一條例即《電訊條例》規管。《截取通訊條例》及《白紙條例草案》均建議訂立類似的規管模式。

5.2.3 就處理通訊中與內容無關的資料，《電訊條例》容許截取"*任何訊息或任何類別的訊息*"，即容許截取通訊內容，但不包括通訊中與內容無關的資料。《白紙條例草案》同樣規定，"*通訊*"的涵義局限於"*由發訊人藉郵遞或電訊傳送予接收人的通訊的內容*"。[141] 然而，《截取通訊條例》下"*通訊*"的定義，則同時包括通訊內容和與內容無關的資料。[142]

<u>發出手令的機構</u>

5.2.4 3個選定司法管轄區各自訂有不同的截取手令簽發制度。在英國，所有手令均由行政機關(即內政大臣)簽發。在美國，各類授權在美國境內截取通訊的法院命令均由法官簽發。在澳洲，視乎申領手令的目的，可由行政機關或法官(或具備司法資歷的專業人士)簽發手令。正如附錄II所顯示，很多海外地方均採用由法院簽發手令的制度。

5.2.5 在香港特區，只有政府首長(即行政長官)才可下令截取通訊。[143] 然而，《截取通訊條例》則建議一套新的法院手令制度，規定截取手令必須由高等法院法官簽發。《白紙條例草案》亦建議訂立類似的制度。[144]

---

141 《白紙條例草案》訂明，通訊不包括"*所撥的電話號碼、通訊的地址或由藉以傳送該通訊的系統的營運人所保存的紀錄，亦不包括透過電腦網絡傳送的通訊*"。此外，《白紙條例草案》未有涵蓋透過電腦網絡傳送的通訊，因為據政府表示，《電訊條例》所訂一項條文已足以保障該類通訊。

142 根據《截取通訊條例》，"*通訊*"的涵義包括"*電訊*"，後者的涵義與《電訊條例》所訂的相同。《電訊條例》第2條訂明，"*電訊*"指"*藉導向電磁能或無導向電磁能或藉此二者而發送、發射或接收通訊，但擬讓人眼直接接收或看見的任何發送或發射除外*"。在此條文中，"*通訊*"包括"*人與人、物與物或人與物之間的通訊；及通過下述形式進行的通訊：語言、音樂或其他聲音、文字、影像(不論是否活動的)或任何其他形式的訊號或由不同形式的訊號組成的訊號*"。

143 《電訊條例》第33條。

144 《截取通訊條例》第4(1)條及《白紙條例草案》第9條。

授權提出申請

5.2.6 在所研究的各個司法管轄區中，手令申請均須由高層官員提出或授權提出。在英國，此類申請必須由執法或情報機關首長或其代表提出。在美國，只有司法部指明的高層官員才可授權按《標題III》提出手令申請，然後由法官批准該些申請。按《情報監視法令》提出的手令申請，只可由司法部長授權，然後由外國情報監視法庭批准。在澳洲，國家安全手令的申請必須由保安部門首長提出，而執法手令申請須由執法機關當局提出。

5.2.7 在香港特區，《電訊條例》訂明，只有政府首長才可下令或授權公職人員下令截取通訊。另一方面，《截取通訊條例》的擬議安排，則與研究中3個司法管轄區的安排相似。根據《截取通訊條例》，法院命令的申請必須由警司級或以上的警務人員，或其他執法機關的高級人員提出[145]。《白紙條例草案》亦建議，只有政府首長授權的首長級或以上或相等職級的公職人員才可申請手令。[146]

5.2.8 值得注意的是，在所研究的司法管轄區中，只有美國規定法院命令的申請要由司法人員授權提出。在英國、澳洲以至香港特區，司法人員均未有參與手令申請的過程或授權提出申請的事宜。

發出手令的理據

申請國家安全手令的具體規定較少

5.2.9 在所研究的3個司法管轄區中，申請國家安全手令的主要規定，其具體程度不及執法手令的規定。在英國，就被調查而符合發出執法手令規定的嚴重罪行的類別，已有界定，但就國家安全手令所謀求保障的國家安全利益或經濟福祉，則未有界定。在美國，按《標題III》提出的手令申請，必須證明有很可能成立的因由，相信須透過授權的截取行動才可獲得與某罪行有關的通訊，但按《情報監視法令》提出的申請則毋須符合有關規定。在澳洲，如要發出執法手令，簽發機構必須考慮將會截取的資料是否用來調查某指明的罪行。相比之下，簽發國家安全手令的規定則寬鬆得多。

145 《截取通訊條例》第5(1)及(2)條。
146 《白紙條例草案》第5條。

5.2.10 在香港特區，根據《電訊條例》，只要政府首長決定基於公眾利益（有關利益沒有定義）而有截取通訊的需要，即可命令展開截取行動。相反，《截取通訊條例》及《白紙條例草案》就簽發手令均訂有較具體的規定。[147]

使用其他方法

5.2.11 在所研究的司法管轄區中，當截取機關申請執法手令以調查嚴重罪行時，必須證明曾在何種程度上使用其他調查方法或有其他調查方法可供使用。然而，該3個司法管轄區在簽發為國家安全而提出申請的手令時，均未有把此項理由視為必要的考慮因素。只有英國規定有關申請必須證明未能以其他方法合理地獲取所需資料。美國《情報監視法令》的手令申請及澳洲的國家安全手令申請，均未有類似規定。至於香港特區，《截取通訊條例》及《白紙條例草案》所建議的做法與英國的相似。

手令的有效期、終止有效期及續發安排

5.2.12 所研究的3個司法管轄區均就截取手令的有效期施加限制。在英國，無論有關手令謀求達到何種目的，所有手令最初發出時的有效期均不超過30天，但在緊急情況下發出的手令除外。在美國及澳洲，不同種類手令的最初有效期各有不同，而以為國家安全而發出的手令有效期最長。在美國，《標題III》的手令有效期不超過30天，《通訊紀錄／監測法規》的手令有效期較長，但不多於60天。《情報監視法令》的手令有效期最長，可達一年。在澳洲，執法手令的有效期最長為90天，國家安全手令的有效期最長可達6個月。

[147] 根據《白紙條例草案》第6條，只有在"*為了防止、調查或偵測嚴重罪行*"，而有合理因由相信有關截取"*相當可能*"就嚴重罪行"*揭露*"識別疑犯身份或導致逮捕的"*有用資料*"，或"*為了香港的安全*"，而截取行動"*相當可能*"對達致該目的"*有重大價值*"時，才可發出手令。《截取通訊條例》的規定較《白紙條例草案》的更具體。根據《截取通訊條例》第4(2)及(3)條，除非"*有需要為防止或偵查一項嚴重罪行；或為香港的安全的利益*"，否則不可發出法院命令。法官亦須有合理理由相信有人正觸犯、已觸犯或將會觸犯罪行，而透過擬進行的截取行動將可獲得和該罪行有關的資料。此外，法官須有理由相信該項截取行動將導致定罪。

5.2.13 在香港特區，《電訊條例》並未就截取手令的有效期訂定任何限制。根據《截取通訊條例》[148]，法院命令的有效期不超過90天。《白紙條例草案》建議發出手令的最初有效期不應超過6個月。[149]

內部保障措施

5.2.14 3個選定司法管轄區的截取機關均訂有內部保障措施，防止濫用以手令截取通訊的程序。在英國，截取機關必須符合最低程度截取的規定，以限制被截取材料的披露、複印、保存及銷毀。美國及澳洲亦有就以法院命令截取的材料，訂定類似的保障措施。在該3個司法管轄區中，只有澳洲規定聯邦警隊首長備存登記冊，列明每項執法手令詳情，包括未能令截取對象入罪的每項手令的資料或其續期資料。

5.2.15 在香港特區，《電訊條例》沒有就被截取材料提供任何保障。另一方面，《截取通訊條例》及《白紙條例草案》均建議訂定行政安排，限制被截取材料的披露。[150]

行政機關的監察

5.2.16 在所研究的3個司法管轄區中，只有澳洲賦權申訴專員監察及查核執法當局有否遵守就使用截取手令的法定備存紀錄規定。英國及美國均較着重透過司法機制確保截取法例獲得遵從。在香港特區，根據《電訊條例》、《截取通訊條例》或《白紙條例草案》，申訴專員在促請行政機關遵守備存紀錄規定方面，均未有擔當任何角色。雖然如此，《截取通訊條例》及《白紙條例草案》分別較著重透過立法機關及司法機構，監察截取機關有否符合備存紀錄的規定。

148 《截取通訊條例》第6(4)、(5)及(6)條。
149 《白紙條例草案》第8條。
150 《截取通訊條例》第8條及《白紙條例草案》第10條。

司法機構的監察

5.2.17 在所討論的3個司法管轄區中，只有澳洲沒有監察簽發截取手令事宜的司法機制。英國設立了須由高級司法人員擔任的截取通訊專員職位，以監察截取權力的使用。美國規定按《標題III》發出手令的法官須就每項手令申請，向美國法院行政管理局局長提交書面報告。執法機關亦須每年向行政管理局提交其截取活動的報告。

5.2.18 在香港特區，《電訊條例》並無設立截取通訊專員或類似職位。《截取通訊條例》亦未有訂定類似的監察機制。另一方面，《白紙條例草案》建議設立監管監督("監督")一職，由政府首長從首席大法官呈交的提名人選中，委任一名上訴法院大法官擔任該職位。[151] 建議設立的監督職位，其大部分職責與英國截取通訊專員的相若。[152]

5.2.19 監督與截取通訊專員的主要分別，在於監督獲賦權，可接受及審理相信其通訊曾遭截取的公眾人士所提出的投訴。[153] 若發現有任何違規情況，監督有權撤銷有關手令、指示銷毀被截取的材料，以及命令向投訴人給予補償。在英國，聆訊及裁定投訴的權力歸於調查權力審裁處。

[151] 《白紙條例草案》第12及13條。

[152] 與英國截取通訊專員相似，監督：(a)須曾擔任高級司法人員職位，並由政府首長委任；(b)具有下述職能：不斷檢討手令的發出及手令的妥善執行，以及檢討被截取材料的保障安排是否足夠；(c)履行法定職能時可要求有關各方提供全部所需的文件或資料；及(d)每年須向政府首長提交報告，而有關報告其後須提交予立法機關。

[153] 《白紙條例草案》第12至14條。監督的審查範圍局限於確定有關截取行動(如有)是否由手令授權，以及有否違反任何截取法例。審理某項投訴時，監督有權取覽有關手令或申請手令的正式文件，包括被截取的材料。此外，公職人員有責任向監督提供資料。監督須在不公開的情況下審理投訴。監督的決定不被任何法院質疑，亦不接受上訴。

立法機關的監察

議會委員會

5.2.20 所研究的3個司法管轄區均設有議會委員會，監察涉及截取通訊的事宜。在英國，情報及保安事務委員會只會就為國家安全而進行的截取通訊，監察有關的開支、管理及政策事宜。另一方面，美國及澳洲的議會委員會，則同時監察為執法及國家安全而進行的截取通訊。

5.2.21 美國眾議院的司法及情報委員會監察《標題III》手令制度的運作情況。此外，眾議院的情報事務常設專責委員會及參議院的情報事務專責委員會，則特別關注監視外國情報的事宜。

5.2.22 澳洲立法機關的監察主要由兩個法定委員會進行，它們分別是監察涉及執法的截取通訊事宜的澳洲罪行委員會聯合法定委員會，以及純粹處理國家安全事宜的澳洲保安情報組織、澳洲秘密情報處及國防通訊事務部議會聯合委員會。

5.2.23 在香港特區，《電訊條例》沒有訂定任何立法機制以監察政府首長行使截取權力的情況。無論是《白紙條例草案》或《截取通訊條例》，均未有設立一個可要求截取機關交代其工作的議會委員會。儘管如此，《截取通訊條例》賦權立法會可於任何時間要求保安局局長，在任何指定期限內提供特定的資料。《白紙條例草案》只建議政府首長每年將有關發出截取手令的報告，提交立法會會議席上省覽。[154]

向立法機關提交報告

5.2.24 3個選定司法管轄區的截取法例均規定監察當局每年向立法機關提交報告，交代為執法而進行的截取行動。英國的截取通訊專員須每年向首相提交報告，然後將報告提交國會省覽。在美國，美國法院行政管理局局長每年須向國會提交竊聽報告。在澳洲，總檢察長每年須向澳洲國會提交截取電訊的報告，以供省覽。

[154] 《白紙條例草案》第14條。

公開披露涉及截取的資料

5.2.25 3個選定司法管轄區的監察當局就公開披露有關截取行動的資料，程度不一。英國截取通訊專員所擬備的周年報告，只披露發出手令的整體數目。在美國及澳洲，正如附錄III顯示，所披露的資料較具體及實質，不但包括提出及授權的手令申請數目，還包括最初發出手令及續發手令的平均有效期、根據被截取材料而拘捕及定罪的數目，以及有關手令的開支。

5.2.26 正如附錄IV顯示，在所研究的司法管轄區中，向公眾披露截取行動的資料，大多涉及執法而非國家安全的事宜。英國截取通訊專員的周年報告沒有包括任何有關為國家安全或經濟福祉而截取通訊的具體數字。在美國，涉及《情報監視法令》的周年報告只披露截取及實際搜查行動的整體數字。在澳洲，由總檢察長擬備而可供公眾查閱的周年報告，未有提供有關申請及執行國家安全手令的資料。

5.2.27 在香港特區，《電訊條例》沒有就公開披露截取行動資料而訂定條文。《截取通訊條例》建議向立法機關披露有關截取行動的資料，與美國及澳洲的相似。[155] 《白紙條例草案》只規定披露授權發出的手令數目、手令的平均有效期及續期數目。[156]

5.3 與"911"事件及通訊科技發展有關的法例修訂

5.3.1 在3個選定的司法管轄區，近期涉及截取通訊的法例修訂大都源自"911"事件而非通訊科技的發展。一般而言，"911"事件促使該3個司法管轄區賦予執法及保安當局更多調查權力。

[155] 根據《截取通訊條例》第11條，向立法會披露有關截取行動的資料包括：(a)獲授權及被拒絕的截取行動數目；(b)被截取通訊的設備和地方的性質及地點；(c)使用截取方法處理的重要罪行；(d)截取方法的形式；(e)截取行動所導致被逮捕及定罪的人數；(f)每次截取行動的平均期限；及(g)要求續期及被拒續期的次數。

[156] 《白紙條例草案》第14條。

5.3.2 在英國，最近制定的《反恐怖活動、罪行和保安法令》規定，通訊服務供應商須為了國家安全目的而保存客戶的通訊資料。通訊服務供應商亦須向截取機關提供協助，以執行截取手令。此外，當局發出了《截取通訊實務守則》，以便截取機關依法行事。

5.3.3 在美國，《愛國者法令》就截取法例作出了重要修改。例如，當局鼓勵執法機關及情報機關共用被截取材料，以及按《標題III》發出的截取手令，可調查更多恐怖主義罪行。

5.3.4 澳洲政府把就《截取法》作出的若干重大法例修訂，視為一系列反恐怖主義措施的一部分。根據這些修訂，有關當局可用截取手令調查恐怖主義罪行。"*截取*"一詞的定義亦擴闊至一旦涉及恐怖主義罪行，可合法截取電子訊息或圖像。

附錄I

香港特區、英國、美國及澳洲截取通訊手令制度的比較

	手令種類	發出手令的機構
香港特區	• 沒有特別就手令分類。	• 根據《電訊條例》，所有截取行動均由政府首長下令進行；及 • 《截取通訊條例》及《白紙條例草案》均建議，所有截取命令須由高等法院法官簽發。
英國	• 一般手令指明適用於某人或單一組處所；及 • 具證明書手令只適用於在英國以外地方的外地通訊。	• 所有手令均由內政大臣簽發。
美國	• 按《標題III》發出的法院命令授權為執法而截取通訊的內容； • 按《情報監視法令》發出的法院命令授權為國家安全而截取在美國境內外國勢力或其代理人的通訊內容；及 • 按《通訊紀錄／監測法規》發出的法院命令用以截取通訊中與內容無關的資料。	• 按《標題III》及《通訊紀錄／監測法規》發出的命令由美國地方法院或美國上訴法院的法官簽發；及 • 按《情報監視法令》發出的命令由外國情報監視法院簽發。
澳洲	• 執法手令是為了執法而發出；及 • 國家安全手令是為了國家安全而發出。	• 國家安全手令由聯邦政府總檢察長或保安事務長簽發；及 • 執法手令由合資格的法官或獲提名的行政上訴審裁處成員簽發。

附錄I (續)

	申請程序	發出手令的主要理據
香港特區	• 根據《電訊條例》，只有政府首長才可下令或授權任何公職人員下令截取通訊； • 《截取通訊條例》建議須由高級執法人員提出申請；及 • 《白紙條例草案》建議，只有政府首長授權的首長級或以上或相等職級公職人員才可申請手令。	• 根據《電訊條例》，只要政府首長認為基於公眾利益而有需要截取通訊，便可發出手令； • 《截取通訊條例》建議，為防止或偵查嚴重罪案或為了香港特區保安的利益，即有需要發出法院命令；及 • 《白紙條例草案》建議，只有為了防止、調查或偵測嚴重罪行，或為了香港特區的保安，才可發出手令。
英國	• 申請須由執法或保安機關的首長提出。	• 手令申請須符合"*是否必要*"及"*目的與效果是否相稱*"的驗證標準。
美國	• 按《標題III》及《情報監視法令》提出的申請必須獲高層司法官員授權。按《通訊紀錄／監測法規》提出的申請，可由任何律師代聯邦政府提出。	• 按《標題III》及《情報監視法令》提出的申請，必須符合"*很可能成立的因由*"的驗證標準，而按《通訊紀錄／監測法規》提出的申請則毋須符合此項規定。
澳洲	• 執法手令的申請須由合資格機構提出；國家安全手令的申請只可由保安事務長提出。	• 執法手令只可為調查指明罪行而發出。國家安全手令可在截取目標可能從事損害國家安全的活動，或擬取得的資料對國家安全相當重要時發出。

附錄I (續)

	手令的有效期及續發安排	資料披露及接納為證據
香港特區	• 《電訊條例》沒有就此兩項事宜訂定條文； • 《截取通訊條例》建議，新發出的法院命令有效期不超過90天，並可續期一次，為期不超過90天；及 • 《白紙條例草案》建議，新發出手令的有效期最長為6個月，續期次數則無上限。	• 《電訊條例》沒有就此兩項事宜訂定條文； • 《截取通訊條例》建議，被合法截取的材料可在法庭上獲接納為證據；及 • 《白紙條例草案》建議，除非被截取材料是用來證明一項非法的截取行動，否則有關材料在法庭上不會獲接納為證據。
英國	• 新發出手令的有效期不超過3個月；及 • 手令可接連獲得續期。基於嚴重罪行而續發的手令，每次有效期可達3個月。基於國家安全或國家經濟福祉而續發的手令，每次有效期可達6個月。	• 除有限情況外，被截取材料在法庭上不會獲接納為證據。
美國	• 按《標題III》、《情報監視法令》及《通訊紀錄／監測法規》而新發出的命令，有效期分別可長達30天、90天及60天；及 • 上述3類命令均可接連獲得續期，續發期限與原初命令發出的相同。	• 合法截取的材料可在法庭上獲接納為證據。
澳洲	• 新發出的執法手令有效期最長為90天，而新發出的國家安全手令有效期則不超過6個月；及 • 每類法令均可接連獲得續期，續發期限與原初發出的命令相同。	• 合法截取的材料可在指明的法律程序或情況下獲接納為證據。

附錄I (續)

	行政機關的監察	司法機構的監察
香港特區	• 《電訊條例》、《截取通訊條例》或《白紙條例草案》均沒有訂定任何法定的行政機關監察機制。	• 《白紙條例草案》建議設立監管監督一職，由政府首長委任上訴法院大法官擔任。
英國	• 《2000年調查權力規管法令》沒有訂定任何法定的行政機關監察機制。	• 截取機關行使截取權力由截取通訊專員監察，而截取通訊專員由首相委任現職或退休法官擔任。
美國	• 3項截取通訊的法規均沒有訂定任何法定的行政機關監察機制。	• 根據《標題III》，發出或拒絕發出法院命令的法官須向美國法院行政管理局("行政管理局")提交報告。檢控當局亦須每年向行政管理局提交報告，提供有關在剛過去一年提出法院命令申請的資料； • 根據《情報監視法令》，司法部長須每年向行政管理局提交報告，簡述按《情報監視法令》發出手令的資料；及 • 根據《通訊紀錄／監測法規》，若通訊紀錄／監測裝置與任何竊聽裝置一併使用，須將使用這些裝置一事向行政管理局匯報。
澳洲	• 申訴專員每年須就澳洲聯邦警察及澳洲罪行委員會備存的手令紀錄，查核至少兩次，並向總檢察長匯報查核結果。	• 《截取法》沒有訂定任何法定的司法機構監察機制。

附錄I (續)

	立法機關的監察	公眾監察
香港特區	• 《電訊條例》沒有訂定任何立法機關監察機制； • 《截取通訊條例》建議，立法會可要求保安局局長提供政府截取通訊的資料；及 • 《白紙條例草案》建議政府首長每年須將有關發出截取手令的報告提交立法會。	• 《電訊條例》、《截取通訊條例》或《白紙條例草案》均沒有訂定法定的公眾監察機制。
英國	• 涉及保安機關截取通訊的開支、管理及政策事宜，由一個名為情報及保安事務委員會的法定議會委員會監察。該委員會須每年向首相報告，並由首相將有關報告提交國會；及 • 截取通訊專員須每年向首相提交報告，首相其後會將有關報告提交國會。	• 公眾人士如因截取活動而感到受屈，可向調查權力審裁處投訴。審裁處可就投訴展開聆訊及裁決、判處賠償和撤銷手令。
美國	• 行政管理局須向國會提交周年報告，就按《標題III》發出手令的詳情提供資料； • 司法部長須向國會提交有關《情報監視法令》的周年報告，並須每年兩次充分告知眾議院情報事務常設專責委員會及參議院情報事務專責委員會，有關按該法令而採取監視行動的情況；及 • 司法部長須向國會提交周年報告，匯報按《通訊紀錄／監測法規》發出手令的詳情。	• 《標題III》、《情報監視法令》或《通訊紀錄／監測法規》均沒有訂定法定的公眾監察機制。
澳洲	• 澳洲罪行委員會聯合法定委員會有責任審閱可按執法需要而申領截取手令的澳洲罪行委員會("罪行委員會")的周年報告，並向澳洲國會報告罪行委員會的工作情況；及 • 保安情報組織、澳洲秘密情報處及國防通訊事務部議會聯合委員會監察情報及保安機關的截取工作。	• 《截取法》沒有訂定法定的公眾監察機制。

附錄II

部分海外地區採用的截取手令制度的類別

由行政機關發出截取手令的地區	由法院發出截取手令的地區	由行政機關或法院發出截取手令的地區
印度共和國	阿根廷共和國	泰王國
新加坡共和國	比利時	保加利亞共和國
	加拿大	波蘭共和國
	捷克共和國	匈牙利共和國
	法蘭西共和國	以色列國
	德意志聯邦共和國	
	希臘	
	意大利共和國	
	荷蘭王國	
	西班牙王國	
	新西蘭	
	芬蘭共和國	
	冰島共和國	
	菲律賓共和國	
	瑞士	

資料來源： Privacy and Human Rights: An International Survey of Privacy Laws and Practice (2003)。

附錄III

在美國為執法需要而發出的法院命令的具體資料(1996-2003)

	1996	1997	1998	1999	2000	2001	2002	2003
法院命令申請數目	1 150	1 186	1 331	1 350	1 190	1 491	1 359	1 442
被拒絕／撤回的法院命令申請數目	1	0	2	0	0	0	1	0
發出的法院命令數目	1 149	1 186	1 329	1 350	1 190	1 491	1 358	1 442
發出原初法院命令的平均有效日數	28	28	28	27	28	27	29	29
續發的法院命令數目	887	1 028	1 164	1 367	926	1 008	889	1 145
發出續發法院命令的平均有效日數	28	28	27	29	28	29	29	29
根據合法截取的資料而作出的拘捕行動數目	2 464	3 086	3 450	4 372	3 411	3 683	3 060	3 674
以合法截取的資料作為證據的定罪數目	502	542	911	654	736	732	493	843

資料來源： 美國法院行政管理局有關竊聽事宜的周年報告。

附錄III(續)

在澳洲為執法需要而發出的手令的具體資料(1996-2003)

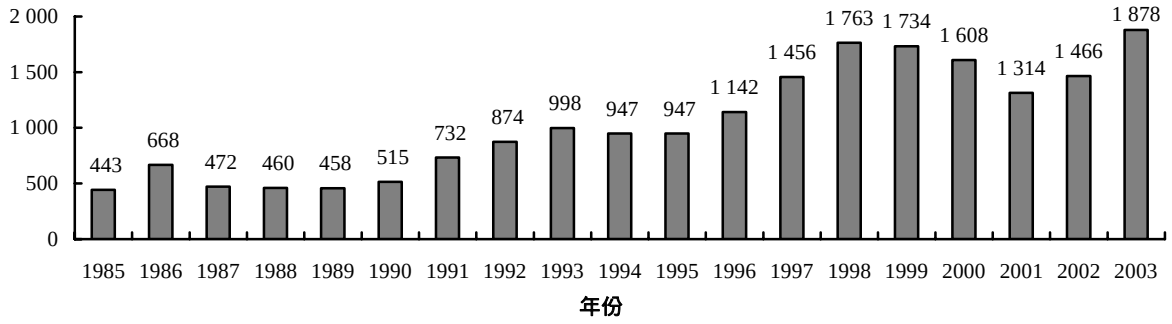
	96/97	97/98	98/99	99/00	00/01	01/02	02/03
手令申請數目	638	684	1 286	1 696	2 164	2 518	3 067
被拒絕／撤回的手令申請數目	11	9	2	7	7	4	9
發出的手令數目	627	675	1 284	1 696	2 157	2 514	3 058
發出原初手令的平均有效日數	44.02	50.24	39.25	37.09	48.18	47.87	44.28
續發的手令數目	137	109	198	270	309	462	736
發出續發手令的平均有效日數	52.65	43.08	50.85	53.18	60.44	66.95	51.52
根據合法截取的資料作出的拘捕行動數目	493	625	633	1 109	1 033	1 479	1 535
以合法截取的資料作為證據的定罪數目	360	330	713	691	623	935	1 125

資料來源： 澳洲政府總檢察長部有關《截取法》的周年報告。

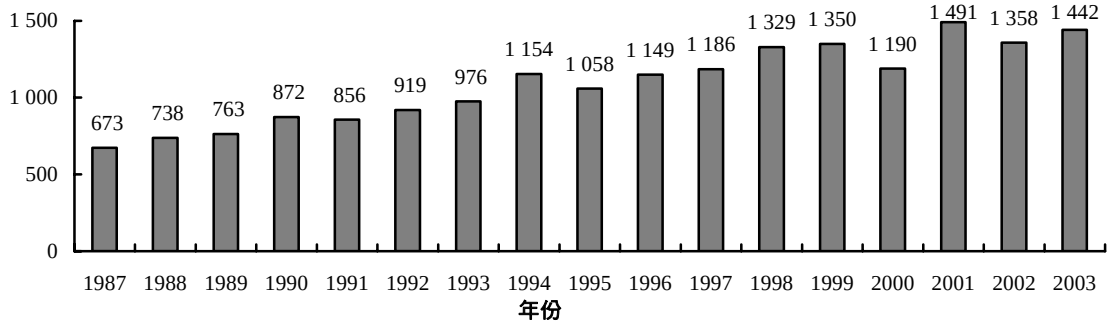
附錄IV

圖1 —— 英國、美國及澳洲發出的截取手令

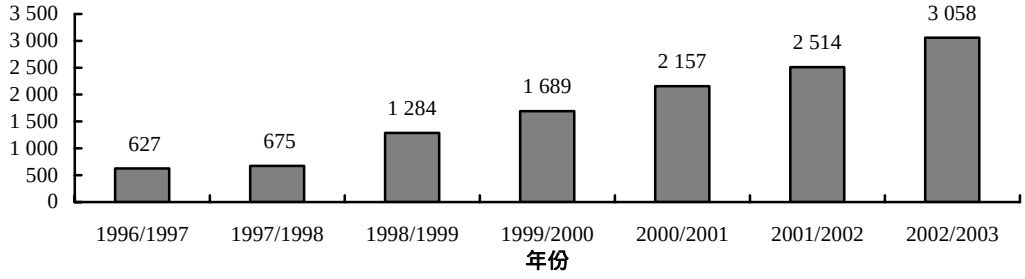
英國 —— 監察機關只披露在英格蘭及威爾士發出所有截取手令的綜合數字(包括為執法及國家安全需要而發出的手令)



美國 —— 監察機關只全面披露按《標題III》發出手令的數字



澳洲 —— 監察機關只披露執法手令的數字



資料來源：

(a) 英國截取通訊專員發表的周年報告；
(b) 美國法院行政管理局有關竊聽事宜的周年報告；
(c) 司法部就《情報監視法令》向美國法院行政管理局提交的周年報告；及
(d) 澳洲政府總檢察長部有關《截取法》的周年報告。

參考資料

英國

1. *Anti-terrorism, Crime and Security Act 2001*. Available from: http://www.legislation.hmso.gov.uk/acts/acts2001/10024--b/htm/ [Accessed January 2005].

2. Broadbrige, Sally. (2001) *The Anti-Terrorism, Crime and Security Bill: Introduction and Summary*. Research Paper 01/101. Available from: http://www.publications.parliament.uk/ [Accessed January 2005].

3. Cyber-rights and Cyber-liberties. *Recent Interception of Communications related to Legal and Policy Developments*. Available from: http://www.cyber-rights.org/interception/ [Accessed January 2005].

4. Danby, Grahame. (2002) *Communications Data: Access and Retention.* Research Paper 02/63. House of Commons Library. Available from: http//www.parliament.uk/parliamentary_publications_and_archives/researchpapers.cfm/ [Accessed January 2005].

5. *European and National Law.* The STOA Program, Directorate A, Directorate General for Research, European Parliament.

6. *Explanatory Notes to Anti-Terrorism, Crime and Security 2001*. Available from: http://www.legislation.hmso.gov.uk/acts/en2001/2001en24.htm/ [Accessed January 2005].

7. *Intelligence and Security Committee Annual Report 2003-2004.*

8. *Intelligence Services Act 1994.* Available from: http://www.legislation.hmso.gov.uk/acts/acts1994/Ukpga_19940013_en_1.htm/ [Accessed January 2005].

9. *Olmstead v. United States, 277 U.S. 438 (1928), Docket No: 493.* Available from: http://www.oyez.org/oyez/resource/case/288/ [Accessed January 2005].

10. *Regulation of Investigatory Powers Act 2000.* Available from: http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm/ [Accessed January 2005].

11. *Regulation of Investigatory Powers Bill. House of Commons Standing Committee Debates.* 14 March 2000. Available from: http://www.publications.parliament.uk/ [Accessed January 2005].

12. *Regulation of Investigatory Powers Bill. House of Commons Standing Committee Debates.* 28 March 2000. Available from: http://www.publications.parliament.uk/ [Accessed January 2005].

13. *Regulation of Investigatory Powers Bill. House of Commons Standing Committee Debates.* 30 March 2000. Available from: http://www.publications.parliament.uk/ [Accessed January 2005].

14. *Regulation of Investigatory Powers Bill. House of Commons Standing Committee Debates.* 4 April 2000. Available from: http://www.publications.parliament.uk/ [Accessed January 2005].

15. *Regulation of Investigatory Powers Bill. House of Commons Standing Committee Debates.* 6 April 2000. Available from: http://www.publications.parliament.uk/ [Accessed January 2005].

16. *Report of the Interception of Communications Commissioner for 2003.*

17. *Report of the Interception of Communications Commissioner for 2002.*

18. *Report of the Interception of Communications Commissioner for 2001*.

19. The Home Office. (1999) *Interception of Communications in the United Kingdom:* A Consultation Paper. Available from:http://www.homeoffice.gov.uk/docs/interint.html/ [Accessed January 2005].

20. The Home Office. (2002) *Interception of Communications Code of Practice.*

美國

1. American Civil Liberties Union. *Surveillance under the USA PATRIOT Act.* Available from:http://www.aclu.org/ [Accessed January 2005].

2. Annual Reports submitted by the U.S. Department of Justice to the Administrative Office of the United States Courts pursuant to the Foreign Intelligence Surveillance Act of 1978, 1997-2004.

3. Boucher, Sarah, et al. (2001) *Internet Wiretapping and Carnivore*. Available from: http://www.google.com.hk/ [Accessed January 2005].

4. Bulzomi, Michael J. (2003) *Foreign Intelligence Surveillance Act: Before and After the USA PATRIOT Act.* Available from: http://www.fbi/publications/leb/2003/june2003/june03leb.htm/ [Accessed January 2005].

5. Centre for Democracy and Technology (2004). *The Nature and Scope of Governmental Electronic Surveillance Activity.* Available from: http://www.cdt.org/wiretap/wiretap_overview.html/ [Accessed January 2005].

6. *Child Sex Crimes Wiretapping Act of 2002.*

7. Collins, Jeffrey G. (2003) *Questions and Answers about the USA PATRIOT ACT*. Available from: http://www.usdoj.gov/usao/mie/ctu/FAQ_Patriot.htm/ [Accessed January 2005].

8. Doyle, Charles. (2002) *The USA PATRIOT Act: A Legal Analysis.* Congressional Research Service, the Library of Congress, 15 April 2002.

9. Doyle, Charles. (2004) *USA PATRIOT Act Sunset: A Sketch.* Congressional Research Service, the Library of Congress, 7 January 2004.

10. Foreign Intelligence Surveillance Act. US Code Collection, Title 50, Chapter 36, Subchapter I, Section 1801–1811. Available from: http://www4.law.cornell.edu/ [Accessed January 2005].

11. Freeh, Louis J. (2000) *Cybercrime*. Testimony submitted to the Senate Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, State, the Judiciary, and Related Agencies. 16 February 2000. Available from: http://www.fbi.gov/congress/congress00/cyber021600.htm/ [Accessed January 2005].

12. Galemore, Gary L. (2000) *Congressional Overrides of Presidential Vetoes*. Congressional Research Service, the Library of Congress, 2 November 2000.

13. Gallagher, Francis A.(2001) *Limited Expansion of the Predicate Offences for Title III Electronic Surveillance.* Available from: http://www.fbi.gov/congress/congress01/gallagher062101.htm/ [Accessed January 2005].

14. IIT Research Institute. (2000) *Independent Review of the Carnivore System – Final Report.*

15. Kennedy, Charles H. and Swire, Peter P. *State Wiretaps and Electronic Surveillance After September 11.*

16. Kerr, Donald M. (2000) *Carnivore Diagnostic Tool.* Testimony presented before the United States Senate, the Committee on the Judiciary. Available from: http://www.fbi.gov/congress/congress00/kerr090600.htm/ [Accessed January 2005].

17. Kerr, Donald M. (2000) Congressional Statement presented before the Committee on the Judiciary Subcommittee on the Constitution, the United States House of Representatives Available from: http://www.house.gov/ [Accessed January 2005].

18. Knowlton, David R. (2000) *Electronic Surveillance.* Testimony made before the House Judiciary Committee, Subcommittee on Crime.

19. Mueller, Robert S. (2004) Congressional statement presented before the National Commission on Terrorist Attacks upon the United States. Available from: http://www.fbi.gov/congress/congress04/mueller041404.htm/ [Accessed January 2005].

20. Regini, Lisa A. (1997) *Searching Pagers Incident to Arrest.* Law Enforcement Bulletin, FBI Publications. Available from:http://www.fbi.goc/publications/leb/1997/jan977.htm/ [Accessed January 2005].

21. Rundquist, Paul S. (1999) *Engrossment, Enrollment, and Presentation of Legislation*. Congressional Research Service, the Library of Congress, 2 March 1999.

22. Schott, Richard G. (2003) *Warrantless Interception of Communications: When, Where, and Why It Can be Done.* Available from:http://www.fbi.gov/publications/leb/2003/jan2003/jan03leb.htm/ [Accessed January 2005].

23. The Attorney General. (2002a) *Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation.*

24. The Attorney General. (2002b) *Guidelines Regarding Prompt Handling of Reports of Possible Criminal Activity Involving Foreign Intelligence Sources.*

25. The Attorney General. (2002c) *Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons.*

26. The Pen/Trap provisions. US Code Collection, Title 18, Part II, Chapter 206, Section 3121–3127. Available from: http://www4.law.cornell.edu/ [Accessed January 2005].

27. *The United States Constitution.* Available from: http://www.house.gov/Constitution/Constitution.html/ [Accessed January 2005].

28. *Title III of the Omnibus Crime Control and Safe Streets Act of 1968.* US Code Collection, Title 18, Part I, Chapter 119, Section 2510–2522. Available from: http://www4.law.cornell.edu/ [Accessed January 2005].

29. *U.S. Constitution: Fourth Amendment.* Available from: http://www.caselaw.1p.findlaw.com/data/constitution/amendment04/index.html. [Accessed January 2005].

30. United States Department of Justice. (2002) *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.* Available from: http://www.cybercrime.gov/s&smanual2002.htm/ [Accessed January 2005].

31. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*. Available from: http://thomas.loc.gov/ [Accessed January 2005].

32. Wiretap Reports. 1998-2003. Administrative Office of the United States Courts. Available from: http://www.uscourts.gov/ [Accessed January 2005].

<u>澳洲</u>

1. Australian Communications Authority. (2000) *Internet Service Providers Interception Obligations.* Available from: http://www.aca.gov.au/ [Accessed January 2005].

2. Australian Labor Party. (2002) *More Telephone Taps in Australian than the United States.* Available from: http://www.alp.org.au/media/0902/20002179.html/ [Accessed January 2005].

3. Branch, Philip. (2003) *Lawful Interception of the Internet.* Issue 1: Spring 2003, Australian Journal of Emerging Technologies and Society. Available from:http://www.swin.edu.au/ajets/ [Accessed January 2005].

4. Ford, Peter. (1999) *Telecommunications Interception Policy Review.* Information and Security Law Division, Attorney-General's Department, the Government of Australia.

5. Hancock, Nathan. (2002) *Terrorism: Legislating for Security.* Research Note No. 25, 2001-02. Available from: http://www.aph.gov.au/library/pubs/rn/2001-02/02rn25.htm/ [Accessed January 2005].

6. Hancock, Nathan. (2002a) *Terrorism and the Law in Australia: Legislation, Commentary and Constraints.* Research Paper No. 12. Available from: http://www.aph.gov.au/library/pubs/rp/2001-02/02rp12.htm/ [Accessed January 2005].

7. Hancock, Nathan. (2002b) *Terrorism and the Law in Australia: Supporting Materials.* Research Paper No. 13. Available from: http://www.aph.gov.au/library/pubs/rp/2001-02/02rp13.htm/ [Accessed January 2005].

8. *Overview of Bill and Effect on Existing Privacy Protections.* Available from: http://www.efa.org.au/Issues/Privacy/tia_bill2002.html/ [Accessed January 2005].

9. *Surveillance Devices Bill (No.2) 2004.* Bills Digest No.24 2004-05. Information and Research Services, Parliamentary Library, Department of Parliamentary Services.

10. *Telecommunications (Interception) Act 1979 Report for the year ending 30 June 1999.*

11. *Telecommunications (Interception) Act 1979 Report for the year ending 30 June 2000.*

12. *Telecommunications (Interception) Act 1979 Report for the year ending 30 June 2001*.

13. *Telecommunications (Interception) Act 1979 Report for the year ending 30 June 2002*

14. *Telecommunications (Interception) Act 1979 Report for the year ending 30 June 2003.*

15. *Telecommunications (Interception) Act 1979.* Available from: http://scaleplus.law.gov.au/html/pasteact/0/464/top/htm/ [Accessed January 2005].

16. *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004 – Question on Notice and Supplementary Submission.* Available from: http://www.privacy.gov.au/publications/senTIAsup.html/ [Accessed January 2005].

17. *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004.* Bills Digest, No. 153 2003-04. Information and Research Services, Parliamentary Library, Department of Parliamentary Services. Available from: http://www.aph.gov.au/publications/index.htm/ [Accessed January 2005].

18. *Telecommunications (Interception) Amendment Act 2004.* No.55. Available from:http://scaleplus.law.gov.au/html/comact/11/6810/0/CM000020.htm/ [Accessed January 2005].

19. *Telecommunications (Interception) Amendment Bill 2004.* Bills Digest, No. 111 2003-04. Information and Research Services, Parliamentary Library, Department of Parliamentary Services.

20. The Senate. (2004) *Legal and Constitutional Legislation Committee. Provisions of the Telecommunications (Interception) Amendments (Stored Communications) Bill 2004.*

香港特別行政區

1. *Interception of Communications Ordinance.* Available from: http://www.justice.gov.hk/ [Accessed January 2005].

2. Ng, Hon Wah. (2003) *Remedies Against Telephone Tapping by the Government.* Hong Kong Law Jorunal, Vol. 33, Part 3. Sweet & Maxwell Asia, pp. 543-567.

3. *Post Office Ordinance.* Available from: http://www.justice.gov.hk/ [Accessed January 2005].

4. Security Branch. (1997) *Consultation Paper on Interception of Communications Bill.*

5. *Telecommunication Ordinance.* Available from: http://www.justice.gov.hk/ [Accessed January 2005].

6. The Law Reform Commission of Hong Kong. (1996) *Report on Privacy: Regulating the Interception of Communications.*

其他

1. Cameron, Iain. (2000) *National Security and the European Convention on Human Rights*. Kluwer Law International, the Netherland.

2. Electronic Surveillance Task Force of the Digital Privacy and Security Working Group. (1997) *Communications Privacy in the Digital Age. Centre for Democracy and Technology.* Available from: http://www.cdt.org/wiretap/9706rpt.html/ [Accessed January 2005].

3. *Privacy and Human Rights: An International Survey of Privacy Laws and Practice (2003)*, published by Global Internet Liberty Campaign. Available from: http://www.gilc.org/privacy/survey/ [Accessed January 2005].

4. Long, Colin D. (1995) *Telecommunications Law and Practice.* Second Edition. Sweet & Maxwell, Australia.

5. *The New Encyclopedia Britannica.* (1994) Encyclopedia Britannica, Inc.