國立政治大學法學院碩士在職專班

碩士論文

指導教授：楊雲驊 博士

我國情報通訊監察法治之研究

The Legal Ramifications of Intelligence Surveillance

研究生：錢祐萱

中華民國一０一年六月

序言與謝辭

"Those who can give up the essential liberty to obtain a little temporary safety, deserve neither liberty nor safety."

-- Benjamin Franklin, Memoirs of the life and writings of Benjamin Franklin

美國開國元老富蘭克林曾說：「那些可以放棄基本自由權利以獲取些微短暫安全的人，既得不到自由，亦得不到安全。」他認為這些所謂「些微短暫安全」時常是虛無抽象的，但基本自由權利卻是珍貴的，人民在交換的過程中常無法獲得利益。

討論這句弔詭的話重點應在於所謂「些微短暫安全」的程度為何，又「基本自由權利」的範疇何在。「國家安全」一辭絕非可無限上綱而藉以要求人民放棄其基本自由權利，而人民在犧牲什麼程度的自由來換取常是虛無抽象的國家安全概念才是合理，似乎亦無絕對的標準。

美國華盛頓郵報（Washington Post）2012 年 4 月 23 日報導，由於通訊與網路等現代科技可協助民運人士對抗極權政府，但極權政府亦利用監視、封鎖網路或追查反對派人士以箝制異議人士，故美國總統歐巴馬於該日頒布一行政命令，授權美國政府對協助極權政府利用新科技侵犯人權的個人、企業或團體施加制裁，如凍結在美資產或拒絕入境等。但有趣的是，當美國譴責極權國家濫用科技侵犯人權的同時，美國本身在九一一事件後對通訊及網路的監控能量並不在話下，這樣的行政命令似乎有其正義，亦有其諷刺的一面，濫用科技侵犯人權的標準究竟何在？

撰寫本篇論文即想藉由比較我國與外國立法例，其人民自由權在情報通訊監察中退讓之程度，並從中探求相對普世合理的標準。在蒐集論文相關資料的過程

中常會發現，現代科技所能造成人民自由權利的侵犯實不容小覷，這些有趣的新知使長時間的論文撰寫過程平添不少樂趣。

楊雲驊教授對通訊監察之研究相當精深，相關著作極為豐富，很感謝楊老師在繁忙的學術研究當中能撥冗抽空指導我的論文，並在德國法制的部份給予許多輔導，解決我德文上的障礙。感謝我的論文口試委員何賴傑教授與張明偉教授，在口試時非常詳細地提出許多寶貴的建議，使我能以更多面向的思考精進完備論文內容。

感謝我的父親與母親，對我所作的選擇與決定一直都給予無限的支持與關懷，陪伴我經歷生命中許多快樂，也度過試煉人生的逆境。

期望本篇論文未來能夠對我國情報通訊監察法制之研究提供些許貢獻。

錢祐萱　2012 年 6 月 15 日

台北

論文摘要

通訊監察區分爲「犯罪通訊監察」及「情報通訊監察」二大種類，犯罪通訊監察須針對特定犯罪活動而爲之偵查行爲，而情報通訊監察則係針對外國勢力及其工作人員危害國家安全之行爲而爲國家預警情報作爲。世界各民主先進國家在將通訊監察法治化及透過實際案例之修正後，逐步建立起類似之通訊監察立法通則，如比例原則、令狀原則監察、透明化、保護隱私權益、重罪原則、特定性、補充性原則等，幾已成爲犯罪通訊監察法治不可違逆之普世價值； 然在情報通訊監察部分，各國則因歷史背景之不同，其情報通訊監察法治發展是不一而足，其法律保留、授權密度、證據能力、救濟及監督方式皆大相逕庭。

我國情報通訊監察規範於民國 88 年與犯罪通訊監察一併規範於「通訊保障及監察法」中，條文規範略嫌簡略，依據民國 100 年修正之國家情報工作法，立法政策將朝向情報通訊監察單獨立法邁進。

爲探討我國情報通訊監察制度之現存問題，本文研究分析美國「外國情報通訊監察法（The Foreign Intelligence Surveillance Act of 1978,FISA）」及德國「G10 法（Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses,Gesetz zu Artikel 10 Grundgesetz – G10）」之情報通訊監察法治，與我國現行規範加以比較，並對未來設立專法提出建議。

關鍵字：情報通訊監察、國家安全、通訊保障及監察法、外國情報通訊監察法、機動式通訊監察、G10 法、戰略性情報通訊監察、濾蒐、監聽

Abstract

Electronic surveillance can be divided into criminal surveillance and intelligence surveillance. Different from the intelligence surveillance, criminal surveillance should be solely engaged in for specific criminal law enforcement purposes. Intelligence surveillance is directed at the acquisition of the contents of communications transmitted by means of communications used between or among foreign powers for the purpose of national security. Through the electronic surveillance legalization process of the advanced democracy countries, we can summarize a few principles such as the principle of proportionality, warrant, privacy, felony, particularity and complementarity which have became the universal value of the criminal surveillance. Nevertheless, the development of the intelligence surveillance in each country is by no means an isolated case because of the different background. They are different from law reservation, the intensity of judicial review, admissibility and judicial remedy, etc.

In 1999, the rules of intelligence surveillance were regulated in Communication Protection and Monitoring Law with criminal surveillance, and the regulations of the intelligence surveillance are sort of incomplete. According to the amendment of the National Intelligence Services Law of 2011, the independent legislation of intelligence surveillance is imperative in future.

In order to solve the problems of intelligence surveillance in Taiwan, the thesis introduced and compared the "The Foreign Intelligence Surveillance (FISA)" in the U.S.A., and the "Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses,Gesetz zu Artikel 10 Grundgesetz (G10)" in Germany with the Communication Protection and Monitoring Law in Taiwan. Hopefully the thesis could provide the directions of the independent legislation of intelligence surveillance in future.

Keywords:

Intelligence Surveillance, National Security, Communication Protection and Monitoring Law, The Foreign Intelligence Surveillance Act, Roving Surveillance, Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses,Gesetz zu Artikel 10 Grundgesetz, G10, Strategische Beschränkungen, Intelligence Filtering, Wiretapping, Interception

目　　錄

第一章 緒論

第一節　研究動機與目的

強制處分是國家爲訴追犯罪所進行的種種強制措施，可保全被告並取得證據，以利於刑事訴訟程序順利的進行。依刑事訴訟法，傳統強制處分主要包括拘提、通緝、逮捕、羈押、搜索、扣押等手段；但隨著資通訊科技的快速發展普及於一般民眾生活當中，刑事訴追機關開始廣泛使用具隱密性如通訊監查等之新型態偵查方式，嫌犯、被告或第三人甚至無法察覺隱私遭到侵犯。

通訊監察爲掌握犯罪證據、追尋人犯、蒐集情報及防止破壞活動之重要方法，但爲防範國家不當濫用通訊監察此一利器，世界民主國家逐漸將通訊監察法治化及透明化，並禁止任意監察他人之秘密通訊。

我國憲法第 12 條明文規定「人民有秘密通訊之自由」，然而通訊保障和監察之法制化作業卻落後西方國家甚多，遲至 88 年 7 月 14 日始按憲法第 23 條意旨制定「通訊保障及監察法」，正式結束政府長期以行政命令執行侵犯人民基本權之不當行爲。[1]

通訊監察區分爲「犯罪通訊監察」及「情報通訊監察」二大種類，而本文主要探討著重於「情報通訊監察」部分。

犯罪通訊監察須針對特定犯罪活動而爲之偵查行爲，而情報通訊監察則係針對外國勢力及其工作人員危害國家安全之行爲而爲國家預警情報作爲。一般犯罪活動影響的層面通常較爲有限，被害人人數也通常較少。外國勢力危安活動相對

[1] 通訊保障及監察法外國法案介紹，立法院國會圖書館，http://npl.ly.gov.tw/do/www/billIntroductionContent?id=27，2006 年 6 月。

來說，破壞國家安全或利益的活動常常對國民造成極爲廣泛的影響，被害人數也通常遠較一般犯罪爲多。[2]

犯罪通訊監察蒐集所得的資訊，通常是用以作爲認定犯罪事實的證據，在審判期日中提出作爲證明被告之犯罪事實，因犯罪通訊監察係限定針對「特定」重罪案件所爲，所侵害者爲該案特定人之通訊自由。

而情報通訊監察中，以破壞國家安全，侵害國家、社會法益爲主，監察範圍及對象較廣泛且具不特定，不一定會涉及特定的犯罪案件，性質多偏向預防不法活動之發生及抗制可能之危害，多爲外國人或與外國勢力接觸的本國人，其所得的資訊，則多作爲預警、情報分析、危機因應、政策形成或是國防及外交工作之用，因此通訊自由受侵害之人數通常遠比犯罪通訊監察者爲多。[3]且情報通訊監察常係對抗外國對國內之活動及蒐集與國家安全相關外國情資，例如外國人在臺灣從事一般性情報活動不一定構成內亂、外患罪。[4]

定義上情報通訊監察與犯罪通訊監察或許可以清楚的區分，但實際運作上，其概念並非容易區分。情報通訊監察與犯罪通訊監察有極高之同質性。就情報通訊監察中得就影響「國家安全」事項爲通訊監察，而多數國家之犯罪通訊監察中皆能對刑法之重罪包含「內亂」、「外患」等罪加以通訊監察，僅偵查之主體多爲層級較高之情報機關。若事涉刑法上之內亂、外患罪名者，得否規避犯罪通訊監察中所要求之明確性原則及較嚴密之權利保障，而直接以其行爲妨礙「國家安全」爲由直接進行程序、要件相對寬鬆之情報通訊監察？

例如，依我國犯罪通訊監察之標準須爲最輕本刑爲 3 年以上有期徒刑之重罪，若行爲人爲蒐集我國國防秘密資訊之活動，該行爲人乃觸犯我國刑法第 111 條刺探搜集國防秘密罪，爲 5 年以下有期徒刑之罪，故依我國現行通訊保障及監察法規定，並不能對行爲人施以犯罪通訊監察。此時情報機關是否得以合理的臆

[2] 張明偉，監聽風雲—以通訊監察進行國家情報工作之規範檢討，軍法專刊第 56 卷第 6 期，頁 170，2010 年 12 月

[3] 李榮耕，析論我國情報通訊監察法制-以美國法制為比較，軍法專刊，56 卷 5 期，107 頁，2010 年 10 月 1 日

[4] 通訊監察法草案研究制定資料彙編，頁 11，羅明通發言，法務部印行，1992 年。

測其蒐集資訊行爲可能有後續之交付或利用情形，而以妨礙國家安全爲由逕行對其施行情報通訊監察？

又例如，洩漏或交付關於中華民國國防應秘密之文書者，依我國刑法第第109 條洩漏交付國防秘密罪，雖其刑度僅爲一年以上七年以下有期徒刑，但依我國通訊保障及監察法第 5 條另有列舉得對本條文之犯罪爲犯罪通訊監察。此時情報機關是否僅得依規範較爲明確嚴密之犯罪通訊監察，而不得因懷疑其洩漏或交付該秘密文書係爲最終將交付予外國敵對勢力情報網絡，而對其施以情報通訊監察？

更甚者，如刑法第 104 條通謀喪失領域罪，通謀外國或其派遣之人，意圖使中華民國領域屬於該國或他國者，處死刑或無期徒刑。此等外患重罪又是否適合僅以犯罪通訊監察爲調查？

本文另對情報通訊監察相關外國立法例做分析、介紹。世界各民主先進國家在將通訊監察法治化及透過實際案例之修正後，逐步建立起類似之通訊監察立法通則，如比例原則、令狀原則、透明化、保護隱私權益、重罪原則、特定性、補充性原則等，幾已成爲犯罪通訊監察法治不可違逆之普世價值； 然在情報通訊監察部分，各國則因歷史背景之不同，其情報通訊監察法治發展是不一而足，其法律保留、授權密度、證據能力、救濟及監督方式皆大相逕庭。

如美國自詡爲世界警察，對世界各國之騷動皆視爲己務，蒐集各國情報不遺餘力，且在接連的恐怖攻擊事件後，其國內之情報通訊監察需求亦大輻提升，爲避免在這樣大量之監聽需求下犧牲了人權，美國在 1978 年即制定「美國聯邦外國情報通訊監察法（the Foreign Intelligence Surveillance Act of 1978,FISA）」，詳細規定情報通訊監察所需依循之規範；德國則因過去東、西德分裂之背景，而於 1968 年制定「G10 法」(Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses,Gesetz zu Artikel 10 Grundgesetz – G10)，亦縝密規範相關情報通訊監察之保護救濟措施。

我國情報通訊監察，在我國「通訊保障及監察法」中與犯罪通訊監察一同被規範，規範法條相對他國較爲簡略。這樣的規範究竟是過度概括的授權情報機

關，亦或是情報通訊監察均須比照犯罪通訊監察之程序而更爲嚴謹？

本文將比較幾個世界民主先進法治國家之情報通訊監察法治，分析其立法意旨及所欲保護之法益；或許多未爲法律規範之缺漏，其背後隱藏之弊病。

第二節 研究途徑與方法

本論文在第二章到第三章的部分介紹各國及我國之情報通訊監察制度，各該國之情報通訊監察法治將基本區分五大層面剖析：

一、情報通訊監察立法沿革：透過相關案例及立法沿革可以深入瞭解該國情報通訊監察發展之背景，及現有法治所受之影響。

二、情報通訊監察要件：各國通訊監察要件寬鬆不一，限制之方式亦多所不同，何種程度之規範始能在人權保障及公權力之執行取得平衡點？

三、情報通訊監察之救濟：情報通訊監察之救濟措施包括事後的通知、違法通訊監察之相關責任及違法通訊監察所得證據之證據能力等，是否有窮救濟之途完善保障「有侵權即有救濟」之可能性。

四、情報通訊監察之監督：情報通訊監察之監督亦寬鬆有別，有些國家規定了完整的行政、立法、司法監督以避免情報通訊監察之濫用；有些則爲保護情報安全爲由而僅訂定籠統的監督方式規避監督，這樣是否妥適？亦或有更細緻化的方式來區隔，有可能確保在充分的監督下進行情報通訊監察？

五、其他：各國依其國情文化及歷史背景，除了上述共通可供分析之項目外，尚有其他獨有之規範，在論文中亦會一併探討。

第四章主要透過外國立法例分析我國現有情報通訊監察現有規範之不足，並給予情報通訊監察法治未來發展之建議，如修正核發情報通訊監察之組織、強化

情報通訊監察之事後救濟及強化情報通訊監察之監督責任等。

第三節 研究範圍與限制

本論文之研究範圍將限縮著重於通訊監察中之「情報」通訊監察，以比較法學研究各國與我國情報通訊監察法治，並兼顧學理及實務發展，惟相關研究仍有限制如下：

一、 儘管情報通訊監察在學理上之討論爲法學研究之重要根基，惟參照實務見解之發展才能確實瞭解真相，我國情報通訊監察之實務上判決或案例在國內公開者較爲少數，故僅能就少數判決中尋得蛛絲馬跡。在此部分之不足將以司法院公布通訊監察資訊及數據統計資料，及國內相關實務界之研究報告及論文，並輔以參照國外之情報通訊監察案例作爲補充。

二、 本論文探討著重於法理之研究，將不處理細部的監聽技術問題，網路通訊之保密措施及其解密之通訊監察技術日新月異，關於網路通訊監察技術部份在國內亦已有數部科技法律論文作過相關介紹[5]，並非本論文所討論之重點。

三、 情報通訊監察與犯罪通訊監察的部分基礎法理是相通的，如比例原則、書面監察、保護隱私權益、重罪原則、特定性、補充性原則等，國內相關研究更是汗牛充棟亦相當完整，本論文將不另佔篇幅針對上述法理原則作詳細的解釋說明，避免本論文過於冗長而失焦。

[5] 錢世傑，網路通訊監察法制與相關問題研究，中原大學碩士論文，2002 年 7 月；蘇三榮，網路時代通訊監察與個人資料保護之法制研究，國立交通大學碩士論文，2009 年 6 月等。

第二章 外國情報之通訊監察

民主先進國家，有關通訊監察之實施，均以法律明定之。美國於 1968 年間制定有線通訊與口頭對話之截取法，至 1986 年將之修正爲有線與電子通訊之截取及截取口頭對話法，並於 1978 年間制定外國情報監聽法，使其通訊監察有完整之法律依據；德國於 1968 年制定限制書信、郵件及電信秘密之法律，並同時修正刑事訴訟法相爲配合；英國爲符合歐洲人權公約第 8 條規定，於 1985 年制定電信（通訊）攔截法；法國亦爲維護個人通訊自由及履行歐洲人權公約，於 1991 年制定電訊通話秘密法；奧地利、義大利等國，則於刑事訴訟法中明文規定。足見制定通訊監察法律，乃世界潮流所趨。本章將就美國與德國之情報通訊監察法制加以研究與分析。

第一節　美國外國情報通訊監察

第一項　立法沿革

美國早期的通訊監察並非作爲一種獨立偵查手段，而是比照搜查和扣押，依美國憲法第四修正案規範，即「人民之身體、住所、文件及物品有不受不合理搜索與扣押之權利，僅在具有相當理由，並以宣誓或書面確認，且明確記載搜索之處所及扣押之人或物件，始能核發令狀。」[6]

[6] U.S.Const. 4th Amend: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue ,but upon probable cause, supported by Oath or affirmation ,and particularly describing the place to be searched, and the persons or things to be seized.

隨科技發達電子通訊已經成爲犯罪聯繫利器，通訊監察因而成爲美國政府破案之利器，但通訊監察之濫用侵犯公民權利的情況屢屢發生，爲平民怨，1934年美國國會通過了「聯邦通訊法」(The Federal Communications Act of 1934)，該法的第 605 節規定，未經發送者的授權，任何人均不得截取任何通訊及對任何人洩露或公開所截取通訊的內容。

但在1967年Katz v. United States[7]一案中，聯邦調查局人員得知被告常用某一公共電話亭對外聯繫，故爲偵查犯罪於該電話亭裝設竊聽器，並稱其僅在空間外竊聽，未有物理侵入，但最高法院認爲憲法第四修正案保護的是個人「對隱私權的合理期待」，認若某人「願意」將己之談話暴露於外，即使於住家或辦公室亦不受保障；但若已表現出主觀隱私之期待，並欲保有其私密性，則即使於公共場所亦應受到保護。

在本案中，美國聯邦最高法院判決中提到，犯罪通訊監察必須遵守美國聯邦第四修正案的要求，但外國情報通訊監察是否應事先聲請法院令狀則非本案判決所涵括範圍。本案雖未替外國情報通訊監察設下規範，但卻是美國聯邦最高法院首次就判決區分出「犯罪通訊監察」及「外國情報通訊監察」。

因此在Katz v. United States案後，爲強化管制通訊監察規範，該判例促使美國聯邦國會於 1968 年制定「綜合犯罪防制暨街道安全法案」，其中第三篇Title Ⅲ第 2510 條至 2522 條，針對有線通訊（Wire Communications）及口頭通訊(Oral Communications）之通訊監察加以規範[8]，使令狀程序成爲犯罪通訊監察合憲性之前提要件。

但此時對於情報通訊監察之規範卻仍付之闕如，在涉及危害國家安全利益時，偵查人員可無須事先取得法院許可，直接進行監聽，爲實施通訊監察令狀原則之例外。總統得不經國會同意，亦無須取得通訊監察命令，即可就關於國內安全事務授權執行通訊監察，並認爲此乃基於國家安全職責所必要而得爲自由裁

---

[7] Katz v. United State, 389 U.S.347(1967)

[8]至 1986 年美國國會通過「電子通訊法」(The Electronic Communication Act of 1986, ECPA)為規範犯罪通訊監察之重要法規，同時增修 Title Ⅲ，並改名為「有線通訊與電子通訊暨口頭對話截取法」（Wire and Electronic Communications Interception and Interception of Oral Communications, 18 U.S.C.§2510-2522），將電子通訊亦納入規範。

量。

1972 年美國聯邦最高法院首次於United States v.United States District Court[9]案中直接審理關於情報通訊監察議題。本案被告以涉嫌以炸藥破壞公物而被起訴，其一位用炸彈攻擊美國中央情報局，審判中被告主張檢察官對其實施通訊監察未事先經法院授權，所取得之證據違法無證據能力。檢察官主張雖本案之通訊監察未事先獲法院授權，但總統授權之檢察總長有權為維護國家安全而進行情報通訊監察，該監聽應屬使國家免於本國組織的攻擊或顛覆政府體制之必要行為，因此縱無法院事先許可亦屬合法監聽。聯邦地方法院及第六巡迴上訴法院皆主張該通訊監察違法無證據能力，上訴至美國聯邦最高法院後，聯邦最高法院表示政府確實有為國家安全而進行情報通訊監察之權力，但仍屬對人民隱私之嚴重侵害，故針對國內勢力或是國內組織(domestic power or domestic organization)進行情報通訊監察時，仍需遵守憲法第四修正案，但因國家安全事務之特殊性，其要件及程序可較有彈性。[10]不受約束之行政裁量將會過度侵犯個人隱私權與言論自由，法院對於證據取得後再為監督審查並無濟於事，事先審查才能實現憲法第四修正案所保障之個人權利。雖檢方主張國家安全事項過於精細複雜，無法由欠缺該等知識與技巧之法院審查，然聯邦最高法院依然認為對國內所為國家安全調查可能會過於被濫用而侵犯人民憲法保障之權利，更有可能以國家安全名義對付政治上不同意見者。故法院得審查國內之國家安全事務，增加法院令狀之聲請程序雖然會增加檢察總長之負擔，卻是保障自由社會憲法價值必要之不便，亦可減輕事後審查之負擔，並可避免對一般守法之大眾進行大規模之監聽[11]。

United States v.United States District Court 案中涉及以維護國家安全為目的之情報通訊監察，監察對象為單純的國內團體，為避免情報機關意濫用其監察權力，其發動及程序仍須受到邦憲法第四修正案「合理(reasonable)」規範，要有其他機關的制衡，但得以較為彈性的程序來規範，避免發生行政機關以維護國家安全為由進行通訊監察而無須經過司法審查，可能會假借國家安全之名侵害人民隱

---

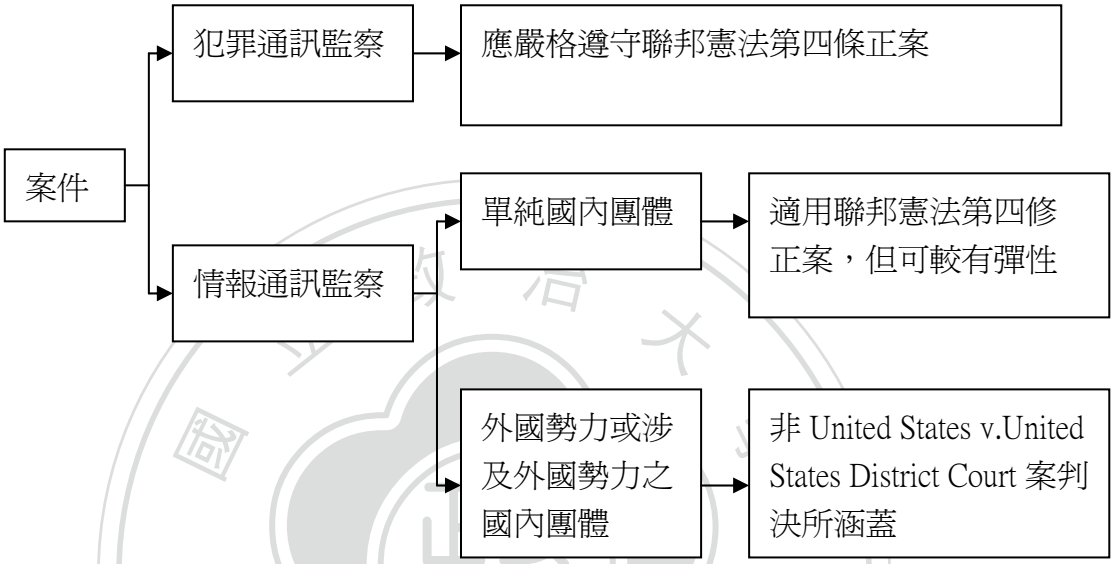
[9] United States v. United States District Court,407 U.S. 297(1972).

[10] 李榮耕，析論我國情報通訊監察法制-以美國法制為比較，軍法專刊，56 卷 5 期，頁 113-115，2010 年 10 月 1 日。

[11] 蔡達智，公權力利用衛星科技對隱私權之影響-以美國法為中心，國立政治大學博士學位論文，頁 95-96，2005 年

私。

至於就外國勢力及涉及外國勢力的國內團體所進行的情報通訊監察，則未為 United States v.United States District Court 案（Keith 案）判決所涵蓋，亦未說明行政權是否有權得不經司法審查便逕行就外國勢力進行通訊監察。



United States v.United States District Court案後犯罪、情報通訊監察區分說明圖[12]

20 世紀 60 年代民權運動及反戰運動期間，美國聯邦調查局以國家安全為名，對黑人民權領袖馬丁・路德金(金恩博士)在內的民權運動及反戰知識份子濫權監聽。其後 1972 年共和黨尼克森總統涉及違法竊聽，由 FBI 人員在華盛頓水門住商大樓內的民主黨全國委員會辦公室裝設竊聽裝置，進行政治竊聽。1974 年

尼克森在 1974 年為此辭任美國總統，結束一場歷時甚久的醜聞。

水門案後，美國聯邦參議員法蘭克.邱吉爾(Frank Church)組成了調查委員會，

[12] 李榮耕，析論我國情報通訊監察法制-以美國法制為比較，軍法專刊，56 卷 5 期，頁 115，2010 年 10 月 1 日。

針對以維護國家安全爲目的所進行的無令狀通訊監察進行研究，最後作成了邱吉爾委員會報告(Church Committee Reports)，說明通訊監察固然能讓行政機關得以取得重要資訊及情報，但同時伴隨濫權且違憲的疑慮。委員會建議聯邦國會應儘速立法建立規範情報通訊監察之機制。這份報告促成了隨後於 1978 年制定了「美國聯邦外國情報通訊監察法(the Foreign Intelligence Surveillance Act of 1978,FISA)」，強化美國境內國家安全領域情報通訊監察的規範及監督，規定了以獲得外國情報資訊爲目的之電子通訊監察，包括對外國勢力或外國勢力工作人員，在美國安全利益及人民隱私權利間求取適當權衡。[13]

1998 年 FISA 修法允許對外國情報核發通訊元件追蹤資訊之令狀（pen/trap orders）以獲得通訊者相關紀錄，使相關資訊之調閱亦須依令狀爲之。

2001 年發生了九一一事件後，美國國會通過了美國愛國者法，大幅擴張情報與治安機關進行通訊監察與資訊獲取權之權力，該法擴大國內恐怖行爲的定義，降低犯罪偵查、強制處分、蒐集情報的程序限制，只須合理懷疑或重要目的即可發動事證調查，並將網路服務業者納入通訊協助法律執行法，擴大個人通訊識資訊如網址、電子郵件地址、個人電腦的識別碼、信用卡號碼與銀行帳戶號碼等皆可依法提供給政府運用。

至 2005 年 12 月 16 日紐約時報(New York Times)揭露國家安全署(National Security Agency, NSA)自 2002 年起即未依FISA規範，而依總統頒布之各項軍事與行政命令，對有任何被懷疑有間接與恐怖份子接觸之美國人民爲無法院令狀之情報通訊監察，而大多數的被監聽人從未有犯罪紀錄。[14] 布希總統於隔日公開承認此事，並主張此爲總統源自憲法之固有權，引起學界及國會爭論。以美國民權聯盟（ACLU）爲首的社會組織認爲無證監聽違反了美國憲法，遂於 2006 年 1 月提起了American Civil Liberties Union v. National Security Agency案[15]。2006 年 8 月，地方法院判決國家安全署的活動違反了美國憲法第一修正案、第四修正案和 1978

---

[13] James G. McAdams, Foreign Intelligence Surveillance Act (FISA):An Overview(2007).

[14] JAMES RISEN and ERIC LICHTBLAU, Bush Lets U.S. Spy on Callers Without Courts ,New York Times(2005.11.26.),http://www.nytimes.com/2005/12/16/politics/16program.html?th

[15] American Civil Liberties Union et al., v. National Security Agency / Central et al., 493 F.3d 644 (6th Cir. 2007).

年國外情報通訊監察法。法官Anna Diggs Taylor在判決書中寫道，“制憲者從來不承認總統有不受控制、肆意妄爲的權力，其不得將權利法案中明文列舉的人民權利棄之不顧”。然而，2007 年 9 月，第六巡迴上訴法院撤銷了該案，理由是由學者、記者和非政府組織構成的原告沒有訴訟資格，因爲他們沒有證據表明其遭受到國家安全署的監聽，因此法院並未對國家安全署的監聽行爲是否違憲做出實質判斷，當然也未支持其合法性。2007 年 10 月ACLU向美國最高法院提起上訴，2008 年 2 月最高法院同樣以原告沒有訴訟資格駁回上訴。

2010 年在Al-Haramain v. Obama[16]案中，聯邦地方法院法官瓦克（Vaughn R. Walker）在判決認定，美國司法部在沒有得到法院令狀的情況下阻截了伊斯蘭慈善機構哈拉曼基金會(Al-Haramain)的通話，以及在 2004 年爲該機構處理事務的兩名律師的通話，違反了 1978 年制定的外國情報通訊監察法。法官判定原告被非法監聽，美國司法部應賠償他們的損失。[17]

國會於 2008 年修正 FISA 制定了「美國聯邦外國情報通訊監察法修正法案(the FISA Amendment Act of 2008,FAA)」，對擴充強化對美國境外及美國人民跨境之情報通訊監察之規範，人權團體認爲其規範侵害權利並對其提出抗議及訴訟，惟其設有落日條款即將於 2012 年 12 月 13 日失效。

以下以 FISA 爲主要研究，分別論述相關法規之重要規範。

第二項　外國情報通訊監察要件

[16] Al-Haramain et. al v. Obama et. al, Case No C 07-0109 VRW (U.S. District Court for the Northern District of California 2010). http://www.wired.com/images_blogs/threatlevel/2010/03/walker.pdf

[17] CHARLIE SAVAGE and JAMES RISEN, Federal Judge Finds N.S.A. Wiretaps Were Illegal, New York Times, http://www.nytimes.com/2010/04/01/us/01nsa.html, (2010.3.31)

美國聯邦外國情報通訊監察法(the Foreign Intelligence Surveillance Act, FISA)[18]是以美國聯邦犯罪通訊監察法(Electronic Communications Privacy Act,1986,ECPA)爲立法參考，但在FISA中，國家安全領域的通訊監聽的目的不是爲了取得刑事訴訟的犯罪証據，而是爲了蒐集有關國家安全的情報資訊，與犯罪偵查有本質上的差異，故部份的規範要件較ECPA爲寬鬆，FISA法院的參與是限縮的。

外國情報通訊監察法非以犯罪嫌疑爲法定要件，而是針對具有特定身分之人執行情報通訊監察，而情報工作的目的並非爲了偵查和起訴犯罪，所以得以適用針對「身分」（外國勢力及其工作人員）而非「行爲」（犯罪）之較低標準來檢視。[19]

一、 外國情報通訊監察之對象

依 FISA 可對危害美國國家安全之「外國勢力」及「外國勢力工作人員」通訊進行情報通訊監察。

所謂「外國勢力」[20]係指：

(1)外國政府或非由美國政府所承認之組成機構，

(2)非實質上由美國人所組成之外國組織，

---

[18] FISA 現已編入美國法典第 50 篇第 36 章（50 USC Chapter 36 – FOREIGN INTELLIGENCE SURVEILLANCE）。

[19] 林俊雄，國家情報工作中通訊監察之探討-以台美兩國法制面之比較為中心，中央警察大學公共安全研究所碩士論文，頁 237，2006 年。

[20] 50 U.S.C. &1801(a) "Foreign power" means -
(1) a foreign government or any component thereof, whether or not recognized by the United States;
(2) a faction of a foreign nation or nations, not substantially composed of United States persons;
(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
(4) a group engaged in international terrorism or activities in preparation therefor;
(5) a foreign-based political organization, not substantially composed of United States persons;
(6) an entity that is directed and controlled by a foreign government or governments; or
(7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

(3)由外國政府公開承認指揮控制之實體，

(4)從事國際恐怖活動或預備爲國際恐怖活動之團體，

(5)非實質上由美國人組成，以外國人爲基礎之政治組織，

(6)外國政府或其所指揮控制之實體。

(7)非美國人所組成從事國際毀滅性武器擴散之實體

「外國勢力工作人員」[21]，係指

（1）非美國人，其

(A)在美國活動，擔任外國勢力之官員或受僱人，或爲第 1804(a)(4)條從事國際恐怖活動或預備爲國際恐怖活動之團體所指外國勢力之成員，

[21] 50 U.S.C. &1801(b). "Agent of a foreign power" means -
(1) any person other than a United States person, who -
(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;
(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;
(C) engages in international terrorism or activities in preparation therefore;
(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or
(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor for or on behalf of a foreign power; or
(2) any person who -
(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

(B)在美國爲外國勢力或代表外國勢力從事秘密情報活動而悖乎美國國家利益之人，或依其所在之週遭情況顯示可能在美國從事上述活動之人，或明知而幫助、策動他人從事上述活動之人，或明知而仍與上述活動之人爲共犯者，

(C)從事國際恐怖活動或預備爲國際恐怖活動之團體，

(D)從事國際大規模毀滅性武器擴散活動或預備爲之者，

(E)代表外國勢力從事國際大規模毀滅性武器擴散活動或預備爲之者。

(2) 任何人（包括美國人），其

(A)明知而爲外國勢力從事秘密情蒐活動，涉及或可能涉及違反美國**刑法**者，

(B)遵從外國勢力之情報服務或外國勢力之網絡之指示，明知而爲外國勢力或代表外國勢力從事其他秘密情報活動，其活動涉及或將涉及違反美國**刑事法律**者，

(C)明知而從事或代表外國勢力從事**顛覆**行爲(sabotage)或**國際恐怖活動**，或預備爲此等行爲者，

(D)明知而從事或代表外國勢力以虛僞身份進入美國，或在美國使用虛僞身份者，

(E)明知而幫助或策動他人爲前述(A)(B)(C)之人所爲活動之共犯者。

「外國勢力」須爲非美國人之政治實體；「外國勢力工作人員」則不區分國籍，但若是美國人，則須限於有事實明知其從事刑法上犯罪行爲或從事顛覆、恐怖活動、代表外國勢力使用虛僞身份時，方可認定其爲外國勢力之工作人員，大幅的限縮了其抽象的空間。此種以國籍作爲區分的方式，可保障具美國國籍之人民權利不受國家以觀念上較模糊之「國家安全」概念爲侵害。

另依通訊監察對象種類之不同，區分了不同程度之監督：

（一）通訊之一方（接收者及發話者）爲美國境內之人：只要通訊之一方爲美國境內之人民，使用有線或無線通訊[22]，對其爲情報通訊監察皆受到FISA之規範，不得爲無法院令狀之外國情報通訊監察。

（二）通訊之一方爲美國人民：受通訊之一方爲美國美國人民，受隱私權之保障，故其在美國境內、跨境、境外之外國情報通訊監察皆有FISA之適用[23]。

（三）美國境外之非美國人：FISA對美國境外之非美國人進行外國情報通訊監察，可由檢察總長(Attorney General)或國家情報首長授權爲一年期之通訊監察，無須有法院令狀。[24]

二、 外國情報通訊監察之程序

依據FISA規定，爲取得外國情報，而對外國勢力及外國勢力工作人員進行外國情報通訊監察，需先行取得法院令狀方得爲之，但在特定情形下，情報機關可進行無令狀情報通訊監察，分別介紹如下。[25]

（一） 無法院令狀之外國情報通訊監察

爲取得外國情報，以下 3 種情狀可不須有法院核發之監察命令，直接由總統授權檢察總長(Attorney General)爲無法院令狀之外國情報通訊監察。3 種情狀分述如下：

---

[22] 50 U.S.C. &1801f(3).

[23] 50 U.S.C. &1801f(1) ; 50 U.S.C. &1881b.c.

[24] 50 U.S.C. &1802f(a)(1)(B); 50 U.S.C. &1881a.

[25] 李榮耕，析論我國情報通訊監察法制-以美國法制為比較，軍法專刊，56 卷 5 期，頁 117，2010 年 10 月 1 日。

1. 經總統授權檢察總長(Attorney General)同意[26]

依據FISA第 1802 條規定，美國總統經書面授權檢察總長，可對合理確信位於美國境外之外國人，進行爲期一年的無法院令狀之外國情報通訊監察。[27]

總統授權，檢察總長必須宣誓以書面保證下列事項[28]：

a. 該外國情報通訊監察單純是爲取得「外國勢力」間的通訊，或僅是爲了從「外國勢力」所支配的處所取得技術情報，而非僅爲取得其個人日常通訊內容。

而該「外國勢力」亦僅限縮於 1801(a)中「外國勢力」7 款定義中的(1)~(3)款，即：外國政府或非由美國政府所承認之組成機構、非實質上由美國人所組成之外國組織，及由外國政府公開承認指揮控制之實體。而「外國勢力」原本即定義排除是美國人民之可能。

b. 任何通訊之一方非爲美國人民。

c. 對個案最小侵害原則符合 FISA 的要求。

檢察總長在完成以上書面宣誓後，仍須將其宣誓書送交外國情報監察法院保存，若事後對此外國情報通訊監察合法性有爭議時可爲審查。

而檢察總長上述之宣誓及其最小侵害原則之判斷標準，須於 FISA 對國會爲半年及年度報告時提出說明，以資檢驗。

2. 緊急情況[29]

---

[26] 50 USC § 1802 - Electronic surveillance authorization without court order; certification by Attorney General; reports to Congressional committees; transmittal under seal; duties and compensation of communication common carrier; applications; jurisdiction

[27] 50 U.S.C.§1802(a)(3)

[28] 50 U.S.C.§1802(a)(1)

在緊急情狀時，檢察總長可以於取得令狀前進行外國情報通訊監察，其要件爲：

a. 檢察總長合理相信有緊急情狀存在而有必要進行外國情報通訊監察

b. 存在合於法院得核發令狀之事實情狀及要件

c. 檢察總長須通知有管轄權的法官，已進行緊急外國情報通訊監察

d. 檢察總長須於 7 日內補行聲請法院令狀

檢察總長於緊急情況下得准予先行執行外國情報通訊監察，但須於 7 日內補行向法院聲請令狀。

若法院拒絕核發令狀，或檢察總長未補行聲請令狀等情形時，情報機關須立即停止該緊急外國情報通訊監察。

法院拒絕核發令狀時，檢察總長得向法院提起抗告。若法院最終仍拒絕核發令狀，則不得於審判程序或任何行政程序中揭露或使用其於緊急外國情報通訊監察中所取得之証據，除非該資訊之不揭露將造成人民死亡或重大傷害則爲例外可使用該資訊。

3. 戰爭時期

FISA規定，在國會通過宣戰案後，總統得經檢察總長，授權進行 15 日以內之外國情報通訊監察[30]。

（二） 有法院令狀之外國情報通訊監察

---

[29] 50 U.S.C.§1805(e)Emergency Orders

[30] 50 USC § 1811 - Authorization during time of war

爲取得外國情報，除了以上得爲無法院令狀外國情報通訊監察之情況，其他外國情報通訊監察皆須先依 FISA 規範聲請取得外國情報監察法院核發的監察令狀。明確的說，對危害美國國家安全之「外國勢力」（1801(a)中「外國勢力」定義中的(4)~(7)款，非美國人）及「外國勢力工作人員」（1801(b)，不排除美國人）爲外國情報通訊監察，不得無法院令狀。因「外國勢力」之定義排除了美國人的可能，故此等區別，可確保美國人民若涉「外國勢力工作人員」而受外國情報通訊監察時，皆須有法院令狀始能爲之。

有法院令狀的外國情報通訊監察須由聯邦官員或國家全安行政長官[31]提出聲請，備齊審查資料後，由聯邦檢察總長、副檢察總長[32]審核批准後，得向法院提出聲請外國情報通訊監察聲請書。

1. 聲請

一般案件乃由聯邦行政官員或國家安全行政長官提出聲請案件，交檢察總長、副檢察總長審核批准後，得向法院提出聲請外國情報通訊監察聲請書。聲請權人身份之限制乃爲外國

[31] 50 U.S.C.§1804(a)(7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate –

(A) that the certifying official deems the information sought to be foreign intelligence information;

(B) that a significant purpose of the surveillance is to obtain foreign intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; and

(E) including a statement of the basis for the certification that –

(i) the information sought is the type of foreign intelligence information designated; and

(ii) such information cannot reasonably be obtained by normal investigative techniques;

(F) a statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;

[32] 50 U.S.C. § 1801(g) "Attorney General" means the Attorney General of the UnitedStates (or Acting Attorney General) or the Deputy Attorney General.

情報通訊監察設定了較高層級的聲請門檻，減少浮濫運用的機會。

聲請須提供下列資料：[33]

(1) 實際提出聲請的聯邦官員人別資料。

(2) 受監察之對象，但若監察對象不明時，得不予記載；或對特定監察標的之敘述。即當不知受監察對象之真實姓名時，得依其暱稱等取代。

(3) 聲請人必須對其所依據之事實與情狀予以陳述，相關事實使檢察總長相信監察對象爲外國勢力及其工作人員，及受監察的處所或設備現爲或即將爲外國勢力或其工作人員所使用。

(4) 已踐行「最小侵害程序」(minimization procedures)之具體說明。例如對無關之對話進行最小可能性之截聽，並避免截取到享有不受通訊監察權利之對特定關係人間對話如律師與客戶、夫妻間、醫病間等。[34]

(5) 所欲取得的情報類型及種類。

(6) 美國總統國家安全事務助理（即廣泛被大眾所稱之國家安全顧問）[35]或負責國家安全情報事務之行政官員[36]所提出之聲請須具保證書（Certification）。

---

[33] 50 U.S.C. § 1804 Applications for court orders (a)Submission by Federal lfficer; approval of Attorney General

[34] Michael R. Sklaire, Minimization, United States Attorney's Bulletin,頁 27, 1997 年 9 月

[35] 美國總統國家安全事務助理（Assistant to the President for National Security Affairs），又稱國家安全顧問（National Security Advisor），是美國總統在國家安全相關事項的主要參謀。國家安全顧問隸屬總統辦公室國安會。總統無須經由參議院同意即可任命國家安全顧問。因此他們與官僚體系的國防部無關，可以提供超然獨立之意見。但各任國家安全顧問的權利與角色卻不競相同。

[36] 參照 50 USC § 1804(d)(1)(A)可知其機關包括聯邦調查局局長、國防部部長、美國國務卿、美國國家情報總監(總統之情報顧問，負責領導協調美國國家安全局等十六個情報機構)、中央情報局局長等所下轄之國家安全情報事務行政官員。

國家安全事務助理執行機關官員、或由總統指派國家安全領域事務長官且經參議院同意之官員，以保證書擔保以下之事項：

（A）該官員認爲所欲截取的資料爲外國情報資料[37]。

（B）監察之重要目的(a significant purpose)係爲取得外國情報資料。

（C）該資料無法以一般調查方式取得。

（D）該外國情報資料屬於 FISA 第 1801 條第 e 款所規範之種類。

（E）對於所欲取得之資料爲外國情報資料，以及必須說明該資料不能以一般調查方式取得之事實。

該情報長官依上述要求提出聲請後，須先由檢察總長審查其是否符合FISA規範對象之要件，並決定是否得向法院提出聲請[38]。

(7) 使用之監察方式，及是否需進入一定處所。

(8) 對於聲請書所載之同一受監察人、設備、處所，先前曾經向法官提出聲請之相關事項，以及依該先前聲請書所採取之行動等事實，均予以陳述。

(9) 情報通訊監察期間。對曾執行過之外國情報通訊監察續次執行時，依所蒐集之情資性質於首次通訊監察獲得之情資，於續次執行時亦可獲得同類型情資者之事實均需陳述。

(10) 檢察總長得視個案情況而要求提出額外之證明書(affidavit or

[37] 「外國情報資訊」係指該資訊侵害美國人民之(A)外國勢力或外國勢力工作人員之實際或潛在攻擊或其他重大敵對行為，(B)外國勢力或外國勢力工作人員之破壞行為或國際恐怖活動，(C)外國勢力或外國勢力工作人員之情治單位或通訊網之秘密情報活動。或該資訊為外國勢力或外國領域侵害美國人民之(A)美國國防或國家安全，(B)美國外交行為。參照 50 U.S.C. &1801(e).

[38] 50 USC § 1804(d) Personal review by Attorney General

certification)。

(11) 法官亦得視個案情況而要求提供額外之資訊以協助其作成決定。

2. 審查

（1） 由外國情報監察法院(Foreign Intelligence Surveillance Court)審查

FISA 以外國情報監察法院專責審查外國情報通訊監察聲請書(foreign intelligence electronic surveillance order)，其法官由聯邦最高法院院長選任 11 個聯邦地方法院法官，任期 7 年每年選任 1 位，其中 3 名法官的住居所與哥倫比亞特區距離須少於 20 英里，以確保於緊急時，法官得迅速抵達法院審理聲請案。

在審級方面，另設有外國情報監察上訴法院[39]，由聯邦最高法院院長自聯邦地方法院或巡迴法院中任命 3 名法官組成。若法院駁回情報機關的聲請應以書面說明理由，當情報機關不服外國情報監察法院的駁回時，可向FISA上訴法院提出救濟，則外國情報監察法院須將該理由書送交外國情報監察上訴法院。

此外，若對外國情報監察上訴法院之決定仍有不服，政府可再上訴於聯邦最高法院[40]。

---

[39] 50 U.S.C. § 1803(b)

[40] 50 U.S.C. § 1803(b) Court of review; record, transmittal to Supreme Court
The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals who together shall comprise a court of review which shall have jurisdiction to review the denial of any application made under this chapter. If such court determines that the application was properly denied, the court shall immediately provide for the record a written statement of each reason for its decision

（2） 審查內容

當法院審酌政府官員之陳述，認爲符合以下下列之情況者，即應頒發領狀權電子監察之實施：[41]

a. 總統授權之檢察總長批准對於外國情報資料進行通訊監察之聲請書。

b. 該聲請書係由聯邦官員所製成並經檢察總長批准。

c. 依聲請書，有相當理由（probable cause）足以認定電子監察之標的爲外國勢力或其工作人員，且電子監察所截取之每一設備或處所正被或將要被外國勢力或其工作人員所使用。

d. 必須遵守 FISA 第 1804 條第 h 項所規範之最小侵害原則。對某一通訊監察案件監控其一個以上之通訊工具時，對於每一通訊工具所取得之情資應注意最小侵害原則之適用。

e. 若受監察人爲美國人民，則依該法第 1804 條第 a 項(7)款之(e)所爲之陳述，或依本法第 1804 條第 d 項所提出

---

and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

[41] 50 U.S.C. § 1805(a) Necessary findings, Upon an application made pursuant to section 1804 of this title, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that -

(1) the application has been made by a Federal officer and approved by the Attorney General;

(2) on the basis of the facts submitted by the applicant there is probable cause to believe that -

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(3) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title; and

(4) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) (!1) of this title and any other information furnished under section 1804(d) (!1) of this title.

之資料必須無顯然之錯誤。

此外，外國情報監察法院於個案中審查是否有相當理由（probable cause）時，應考量監察對象過去、現在或未來的行爲一切事實及情狀，如線民的信用性、線民取得線報的整體情狀、線民提供線報後到官員提出情報通訊監察聲請所經過的時間、及有無其他足以佐證該線報的資訊等。[42]

3. 外國情報通訊監察之法院令狀

若外國情報通訊監察法院經法官審核無誤後，即需核發通訊監察書，其中通訊監察書內必須記載下列事項[43]：

(1) 受監察對象的人別資料或對其之描述。

(2) 受監察之處所或設備。若無法確知時則得不予記載，但若未記載而針對新的地點或設備進行機動式通訊監察(roving surveillance)時，則須於 10 日內通知法院，有正當理由則得延長至 60 日。[44]

(3) 受監察之通訊或是活動之類型，以及所欲取得資訊之類型。

(4) 監察方式，及是否必須進入到特定處所進行情報通訊監察。

---

[42] 50 U.S.C.§1805 (b) Determination of probable cause -- In determining whether or not probable cause exists for purposes of an order under subsection (a)(2) of this section, a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.

[43] 50 U.S.C.§1805

[44] 50 U.S.C.§1805(c)(3) Special directions for certain orders--An order approving an electronic surveillance under this section in circumstances where the nature and location of each of the facilities or places at which the surveillance will be directed is unknown shall direct the applicant to provide notice to the court within ten days after the date on which surveillance begins to be directed at any new facility or place, unless the court finds good cause to justify a longer period of up to 60 days,

(5) 監察期間。[45]

一般外國情報通訊監察期間爲至多 90 日；若監察對象爲協助外國勢力或組織之非美國人民，監察期間至多 120 日；若監察對象爲非美國人民之外國勢力或組織人員，監察期間可達 1 年。

若要聲請延長外國情報通訊監察，聲請人得以原命令爲基礎，因發現與原命令之同一事實聲請發給延期命令，但對於非美國人之外國勢力監聽，若法官認爲延長監聽不致監聽至美國人民之私人通訊時，得發給不超過一年期限之延期命令。

法院同時應就是否被獲得美國人民資訊等情況，評估其是否遵守最小侵害原則，考量通訊監察是否能達其目的。

(6) 指示應遵守之最小侵害程序。若聲請人向法院請求，法院得命通訊服務業者、場所所有人或其他特定人提供必要資訊及協助，並保管相關紀錄，以利進行外國情報通訊監察。並應指示聲請人對協助義務人之補償義務。[46]

法院之權限不僅存在於核發外國情報通訊監察書時，在通訊監察期間結束前，法官對於蒐獲關於美國人之情資是否得使用、保留或傳遞，得對其情狀重新爲評估，確認其是否符合最小侵害原則。[47]

---

[45] 50 U.S.C.§1805 (d) Duration of order; extensions; review of circumstances under which information was acquired, retained or disseminated
(1) An order issued under this section may approve an electronic surveillance for the period necessary to achieve its purpose, or for ninety days, whichever is less, except that (A) an order under this section shall approve an electronic surveillance targeted against a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title, for the period specified in the application or for one year, whichever is less, and (B) an order under this chapter for a surveillance targeted against an agent of a foreign power who is not a United States person may be for the period specified in the application or for 120 days, whichever is less.

[46] 50 U.S.C. § 1805(c)(2)

[47] 50 U.S.C.§1805 (d) (3) At or before the end of the period of time for which electronic surveillance is

4. 外國情報通訊監察法院對聲請案件極少否決

依據 FISA 對於外國情報通訊監察書之審查規範，相較犯罪通訊監察而言，法官對於外國情報通訊監察聲請是否核發監察命令時，審查權大幅限縮。只要外國情報通訊監察命令之核發符合法條內標準與程序，並使相信監察對象係屬外國勢力或其工作人員，以及監察處所正被或將被監察對象所使用外，僅以行政或情報機關所提供的 50 USC § 1804(c)其他宣誓書 及(d)其他參考資訊，來證明有相當理由爲監察之必要。因此，在大多數情況下法官僅能審查聲請書的形式。

在美國實務運作上，法官對於聲請機關所提出之證明書幾乎僅審酌其偵察對象是否爲美國公民；又由於法院之審查案件鮮少直接以美國人民爲調查對象，故實務上法院幾乎難以駁回外國情報通訊監察命令的聲請，雖法院同意核發通訊監察書應依據各項規範審核，惟法院僅能就聯邦行政機關所呈資料作形式上審查，因此極少否決其聲請，法院易淪爲橡皮圖章。據統計，自 1979 年至 2004 年的 25 年間，法院發出過 1 萬 8,761 份外國情報通訊監察書，僅有 5 案被否決，足見美國在外國情報通訊監察中法院審酌餘地較少。[48]

雖情報機關不服外國情報監察法院之駁回時，可向外國情報監察上訴法院提出救濟，若對上訴法院之決定仍有不服，政府可再上訴於聯邦最高法院，惟如此上訴之案件極爲少數，外國情報監察上訴法院首件上訴案件發生於 2002 年[49]，係外國

---

approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

[48] John Diamond，NSA's surveillance of citizens echoes 1970s controversy，USA TODAY，http://www.usatoday.com/news/washington/2005-12-18-nsa-70s_x.htm ,(2005.12.18)

[49] In re Sealed Case No. 02-001, 310 F.3d 717 (FISCR 2002).

情報監察法院對該外國情報通訊監察是否符合「最小侵害原則」有所疑慮，惟最後外國情報監察上訴法院仍以因愛國者法案之擴權，而幾乎可認定只要符合確定其為「蒐集外國情報」即可同意其聲請[50]，該判決遭法界人士批評法院審查過於寬鬆。

此為法院自成立 24 年來的第一次上訴案件，絕大部份的案件在第一審級外國情報監察法院即予以核准進行外國情報通訊監察。

第三項　情資之使用、通知、救濟與罰則

在 FISA 之規範下，情資之使用、通知與救濟三者間關係密不可分。

一、 情資之使用

FISA所獲情資若係關於美國人民者，若情報單位要使用其情資須確認其使用符合最小侵害程序，並使用於合法的目的。[51]

但若為執法之目的而須揭露外國情報通訊監察所獲情資，僅限於「刑事」訴追所需，始能在檢察總長授權下進行。

若一旦確認外國情報通訊監察所獲得之內容與情報監察目的無關，且收發話雙方皆位於美國境內時，應立即銷毀該資料。但檢察總長認其涉及他人

[50] Foreign Intelligence Surveillance Court of Review, http://legal-dictionary.thefreedictionary.com/Foreign+Intelligence+Surveillance+Court+of+Review

[51] 50 USC § 1806 – Use of Information

生命或身體重大危害時，時下令不予立即銷毀。[52]若由無法院令狀外國情報通訊監察所獲資訊則得保存 10 年。[53]

二、 通知與救濟

在 FISA 之規範下，通知與救濟間關係密不可分。通知乃爲使被通訊監察人得爲後續之救濟程序。

政府機關若要將所蒐情資轉爲刑事訴訟證據或揭露於審判程序、聽證會、行政部門等時，爲保障正當法律程序及對質詰問之權利，政府機關應事先通知受外國情報通訊監察之人，向其揭示聲請書、外國情報通訊監察書及是否獲得相關情資等資訊。[54]

通知之目的在於使受監察之人得在該情資被使用及揭露前，若被通訊監察人認爲外國情報通訊監察有以下不合法之情事時，得聲請地方法法院排除該資訊及其衍生證據[55]：

（一）非法之通訊監察。

（二）通訊監察之授權或許可之形式要件不完備。

由於外國情報通訊監察之重要目的是爲獲取情報資訊，而非以有犯罪要件存在爲前提，但若外國情報通訊監察之中取得刑事犯罪證據時，該證據在經過檢察總長授權通知受監察人並保障其救濟權利後，在刑事審判程序中仍得有證據能力。

若檢察總長提出具結書宣示（affidavit under oath）說明相關資訊揭示或

---

[52] 50 USC § 1806(i) Destruction of unintentionally acquired information

[53] 50 USC § 1805 (g) Retention of certifications, applications and orders--Certifications made by the Attorney General pursuant to section 1802 (a) of this title and applications made and orders granted under this subchapter shall be retained for a period of at least ten years from the date of the certification or application.

[54] 50 USC § 1806(c)(d) –Notification

[55] 50 USC §1806(e) – Motion to suppress.

兩造辯論將有害於國家安全，則地方法院應以秘密及一造方式審查系爭外國情報通訊監察是否被合法的授權與執行，亦可經衡酌，可採適當安全程序、保護令後爲適當部分通知。[56]若該地方法院審查後認爲該外國情報通訊監察不合法，則應排除其證據能力，但該法院判決得爲上訴。[57]

外國情報通訊監察僅在要揭露運用外國情報通訊監察所獲情資，使其成爲刑事訴訟證據時，始有通知義務，在未面臨上述情形時受通訊監察者並不會被通知，故無法依據司法程序提出異議。故上述檢察總長提出具結書宣示，再由地方法院爲確認是否合法授權與執行，於特殊情況下替代受監察人主張權利。

然而在緊急外國情報通訊監察中，情報機關於事後向法院補行聲請而法院未予核可時，法院得斟酌通知被監察人：[58]

（一） 受外國情報通訊監察事宜

（二） 受情報通訊監察期間

（三） 期間是否獲得相關情資

法院亦得決定該通知是否得延後至長 90 日，或若檢察總長補足正當理由後則得不爲通知。

三、 罰則

受違法監聽者可向法院主張違反本法通訊監察或揭露所蒐情資之刑事處罰[59]（五年以下有期徒刑或科或併科美金 1 萬元以下罰金），及民事賠償，包括：損害賠償、懲罰性賠償及相關訴訟費用。[60]

---

[56] 50 USC §1806(f) – In camera and ex parte review by district court

[57] 50 USC §1806(g) –Suppression of evidence; denial of motion，50 USC §1806(h) –Finality of orders

[58] 50 USC §1806(j) –Notification of emergency employment of electronic surveillance; contents; postponement, suspension or elimination

[59] 50 USC § 1809 – Criminal sanctions

[60] 50 USC § 1810 – Civil Liability

第四項　　情資傳遞之限制

在外國情報通訊監察所蒐獲之情資，除了如前所述經通知被監察人之程序後，得爲刑事訴追之證據外，FISA對情資傳遞予其他機關僅作簡單之規範。執行外國情報通訊監察所蒐獲之情資，得就其中關於「國家安全事務」，與相關聯邦執法單位、行政機關傳遞運用，其範圍如下:[61]

一、外國勢力及其工作人員實質上或預謀之攻擊。

二、外國勢力及其工作人員從事顛覆活動、國際恐怖活動、毀滅性武器擴散。

三、外國勢力及其工作人員爲其情報組織及網絡暗中從事情報活動。

第五項　　外國情報通訊監察之監督

美國外國情報通訊監察之監督分爲司法行政及國會監督，分述如下：

一、 司法行政監督

每年四月，聯邦檢察總長應向聯邦法院行政處及國會報告年度之(a)聲請外國情報通訊監察及延期通訊監察之總數及(b)對聲請案及延期聲案之同意、修正及駁回之總數。

[61] 50 USC §1806(k) – Coordination with law enforcement on national security matters

二、 國會監督[62]

（一）、半年報告

檢察總長應至少每半年一次，向聯邦眾議情報委員會(the House Permanent Select Committee on Intelligence)、參議院情報委員會(the Senate Select Committee on Intelligence)及參議院司法委員會(the Senate Select Committee on Intelligence)提出報告，說明外國情報通訊監察的執行狀況。

報告的內容包括：

（一） 外國情報通訊監察及其延期通訊監察之數目，及其許可、修改或拒絕之總數。

（二） 外國情報通訊監察獲得之證據使用於刑事訴訟之情況。

（三） 臨時僱用翻譯通訊監察內容人員總數及通訊監察聲請許可與否之總數。

（四） 而檢察總長上述之宣誓及其最小侵害原則之判斷標準，須於FISA對國會爲半年及年度報告時提出說明，以資檢驗。[63]

（二）、年度報告

每年 10 月 25 日，參、眾議院情報委員會應就外國情報通訊監察的執行情形向參議院及眾議院作成報告。報告內容應包括FISA應否修正、應否廢止或應依原規定授權進行外國情報通訊監察之分析及建議[64]。

---

[62] 50 USC § 1808 - Report of Attorney General to Congressional committees; limitation on authority or responsibility of information gathering activities of Congressional committees; report of Congressional committees to Congress

[63] 50 USC § 1802(a)(2)

[64] 50 USC § 1808(b)

此種監督機制，由行政機關就執行通訊監察之情形，向司法機關及國會報告，做爲日後修訂法令的參考依據，使權力均衡符合憲政原理，避免行政權濫用通訊監察而對人民權利的過度侵害之情形。[65]

第六項　美國愛國者法案(U.S.A. Patriot Act)之擴權

2001 年「九一一事件」後，反恐、確保國家安全成爲超越一切價值衡量標準，美國執法部門開始加強犯罪之「預防」。爲了防範可能出現之恐怖襲擊，「九一一事件」後 6 週即頒布的「愛國者法案」，大大加強了對美國境內人民及機構之情報偵察力度。

在 2001 年發生「九一一事件」後，美國布西總統即在 2001 年 10 月 26 日簽署頒布國會法案，正式的名稱爲「使用適當之手段來阻止或避免恐怖主義以團結並強化美國的法律」(Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001)，取英文原名的首字縮寫簡稱爲「USA PATRIOT Act」，亦即所謂的「美國愛國者法案」。

此法案以防止恐怖主義爲目的，共修正 15 部法律，其中包括「電子通訊法(ECPA)」及「外國情報監察法(FISA)」等，賦予美國執法機構和國際情報機構更廣泛的權力，以防止、偵破與打擊恐怖主義活動。根據法案的內容，降低犯罪偵查、強制處分、蒐集情報之程序限制，只須合理懷疑(reasonable doubt)或明顯目的(significant purpose)即可發動調查，不須憲法第四條要求搜索扣押須符合之可能懷疑(probable cause)及合理搜索(reasonable search)等要件。並將網路服務業者納入通訊協助法律執行法，擴大個人通訊識別資訊(call-identifying information)如網址、電

[65] 林俊雄，國家情報工作中通訊監察之探討-以台美兩國法制面之比較為中心，中央警察大學公共安全研究所碩士論文，頁 110，2006 年。

子郵件地址、個人電腦識別碼、信用卡號碼與銀行帳戶號碼皆可提供給政府或任何第三人。

本法案延伸了恐怖主義之定義，在該法案第 802 條部份將恐怖主義定義爲「指任何活動： a.涉及觸犯美國或任何州之刑法，足以危及他人生命之行爲。 b.以恐嚇及強制手段影響政府政策。 c.大規模破壞、暗殺、綁架以影響政府之行爲。」[66]

本法案修正外國情報通訊監察法規之規範，其中在該法案第二章「強化監聽程序」（Enhanced Surveillance Procedures），給予了執法機關執行外國情報通訊監察上有更大的權力監聽、監測電子郵件等，其中較重要之措施如下：[67][68]

一、 增加得通訊監察罪名之範圍。對非法製造、取得化學武器及其他恐怖活動之犯罪嫌疑行爲，執法機關可向法院聲請核准對其實施外國情報通訊監察。[69]

二、 任何有關恐怖犯罪之通訊監察所獲資訊，得於美國各情報機關、司法審判等機關間相互分享。[70]不但情報機關與執法機關間資訊可互相分享，且外國政府所蒐獲之情報資訊亦可與美國情報機關分享，此規範擴大運用外國情報通訊監察情資，惟本修本使美國政府得利用此一漏洞，由外國政府進行相關情報蒐集行爲，美國政府再向該外國政府取得相關情報資訊，輾轉蒐集美國人民之情報，因追查不易，使美國人民之基本權利遭到無法迴避之侵害。[71]

---

[66] Usa Patriot Act of 2001 SEC.802. DEFINITION OF DOMESTIC TERRORISM

[67] 廖元豪，美國反恐怖主義相關法律措施之簡介與評論，月旦法學雜誌，第 80 期，頁 274，2002 年 1 月。

[68] 蔡庭榕，論反恐怖主義行動法制與人權保障，刑事法雜誌第 47 卷第 4 期，頁 48-50，2003 年 10 月。

[69] Usa Patriot Act of 2001 SEC.201. AUTHORITY TO INTERCEPT WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS RELATING TO TERRORISM

[70] Usa Patriot Act of 2001 SEC. 203. AUTHORITY TO SHARE CRIMINAL INVESTIGATIVE INFORMATION

[71] 錢世傑，網路通訊監察法制與相關問題研究，中原大學財經法律學系碩士論文，頁 64，2002

三、 授權聯邦調查局可迅速僱用反恐怖調查行動之翻譯人員，使程序不受聯邦人事法規之拘束。美國爲各種族溶合的國家，使用各種語言，故爲通訊監察時爲大量翻譯外國情報通訊監察所得之情資，須迅速僱用各種語言之翻譯人員。[72]

四、 機動式通訊監察(roving surveillance authority)[73]：原本在FISA中，執法機關通訊監察須針對特定線路之通訊，但本法明定，若法院認定受監察對象有任何妨礙執法機關辨認身分之行爲，則可擴張監察範圍，原本僅能針對「特定線路」爲通訊監察，現在可針對「特定人」爲之，以增加執法機關通訊監察之機動性。因在行動電話之取得方便、丟棄容易的時代，聲請限定某組號碼通訊監察的方式，已不敷使用。[74]在網際網路上之機動性更爲重要，因犯罪嫌疑人爲逃避追蹤，可能以任何方式逃避執法機關之追查，例如更換帳號、使用公用網路電腦，或不斷聲請免費電子郵件帳號等。[75]惟FISA對機動式通訊監察規範亦設有一定之限制。在法院同意爲機動式通訊監察後，當發現並開始對新的通訊工具或新的地點爲通訊監察時，則應在 10 日內須通知法院其新通訊工具或新地點、相當事實使聲請單位足認其爲被監察人所使用、已採行之最小侵害措施，及核准增加機動式通訊監察之設備總數。有正當理由則得延長至 60 日。[76]相關規定並已配合修正FISA中 50U.S.C. §1805(c)中，其中 50USC§1805(c)(2)(b)更規範若受監察人有妨礙執法機關辨認身分之行爲時，電信公司應提供進行機動式通訊監察所須之資訊及協助。

年。

[72] Usa Patriot Act of 2001 SEC. 205. EMPLOYMENT OF TRANSLATORS BY THE FEDERAL BUREAU OF INVESTIGATION

[73] Usa Patriot Act of 2001 SEC. 206. ROVING SURVEILLANCE AUTHORITY UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

[74] 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學位論文，頁 49，2009 年。

[75] 錢世傑，網路通訊監察法制與相關問題研究，頁 58，中原大學財經法律學系碩士論文，2002 年。

[76] 50 U.S.C.§1805(c)3　Special directions for certain orders

五、 延長FISA對於非美國人民之外國勢力工作人員通訊監察期間至 120 日。[77]

六、 對語音信箱資訊之外國情報通訊監察。原本通訊監察僅限於電子通訊紀錄，現執法機關可依據法院核發之令狀，向電信事業索取語音信箱之通訊紀錄。[78]

七、 執法機關可經由法院許可，就有關犯罪偵查事項，裝置設施以監測電訊通訊者姓名、地址、電話通連紀錄、談話時間、服務期間、服務型態、付款方式（包括信用卡或銀行帳號）、收發端電話號碼、IP位置等身份訊息[79]。政府就取得情報或犯罪資訊進一步擴大將網路服務業者納入規範，如網路資訊服務業者如認爲有犯罪嫌疑，可自願或採行簡易程序的法院許可，將非通訊內容的資料例如網址、電子郵件地址、個人電腦的識別碼提供給政府。要求電信業者提供通訊識別資訊，包括電話付費方式及來源，如信用卡號碼以及銀行的帳戶，從而瞭解個人電子交易狀況。[80]因此，大部分的非通訊內容資訊，只要確認有進行犯罪偵查必要，不論是通訊地點、數位號碼，網路郵件、網址、電腦辨識碼，都能爲政府輕易監控，而且任何執法機關取得他人之通訊資訊，可與其他機關相互運用。[81]

八、 若電子通信業者和遠端電腦服務商合理相信有對任何人生命造成危險或嚴重身體傷害之緊急情況下，應立即向政府部門揭露相關用戶電子通信記錄。[82]

九、 對疑似恐怖份子者可進行電話或電腦、電子通信之通訊監察，以調閱其特

---

[77] Usa Patriot Act of 2001 SEC. 207. DURATION OF FISA SURVEILLANCE OF NON-UNITED STATES PERSONS WHO ARE AGENTS OF A FOREIGN POWER.

[78] Usa Patriot Act of 2001 SEC. 209. SEIZURE OF VOICE-MAIL MESSAGES PURSUANT TO WARRANTS.

[79] Usa Patriot Act of 2001 SEC. 216. MODIFICATION OF AUTHORITIES RELATING TO USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES.

[80] 蔡達智，公權力利用衛星科技對隱私權的影響-以美國法為中心，國立政治大學法律係博士學位論文，頁 117-119，2006 年。

[81] 吳兆琰，論網路環境下的通訊監察法制，科技法律透析，17 卷 2 期，頁 46-47，2005 年 2 月。

[82] Usa Patriot Act of 2001 SEC. 212. EMERGENCY DISCLOSURE OF ELECTRONIC COMMUNICATIONS TO PROTECT LIFE AND LIMB.

定商業紀錄。[83]

「美國愛國者法案」部分條款擴張外國情報通訊監察權力而引發爭議[84]，如「美國愛國者法案」將FISA中聲請要件之一的「以獲取外國情報資訊爲目的」(a purpose of the surveillance is to obtain foreign initelligence information)改爲「以獲取外國情報資訊爲重要目的」(a significant purpose of the surveillance is obtain foreign intelligence information)，[85]然而何謂「重要」目的，其範圍模糊並抽象，在外國情報通訊監察上訴法院In re: Sealed Case No. 02-001 判決表示，由於犯罪通訊監察與外國情報通訊監察之界線難以區隔，故不論針對犯罪之目的爲多或針對情報蒐集之目的爲多，只要能確定其獲取之資訊爲外國情報者，幾乎皆有獲取外國情報資訊之目的[86]，而不像修法前法院還須衡量是否應爲犯罪通訊監察或外國情報通訊監察。唯法界人士批評這樣的判決，將使執法人員規避犯罪通訊監察而濫用外國情報通訊監察，使外國情報通訊監察大大的擴張權力。[87]

儘管「美國愛國者法案」部分條款存有爭議，但在「九一一」事件強力震撼下，美國國會僅 45 天就批准了該法案。「美國愛國者法案」犧牲了公民的某些自由，其中部分賦予情報、執法機構過大權力之條款引發人權爭議，國會爲求在國家安全與人權間求得平衡，給予這些條款附加上廢止期限。但出於對美國國家

---

[83] Usa Patriot Act of 2001 SEC. 217. INTERCEPTION OF COMPUTER TRESPASSER COMMUNICATIONS

[84] 廖元豪，多少罪惡假國家安全之名而行？-簡介美國反恐措施對人權之侵蝕，月旦法學，第 131 期，頁 40，2006 年 4 月。

[85] Usa Patriot Act of 2001SEC. 218. FOREIGN INTELLIGENCE INFORMATION

[86] In re Sealed Case that there had never been a primary purpose requirement. Id. at 723-27. The court reasoned that, because the statute's definition of "foreign intelligence information" necessarily included evidence of crimes, such as espionage, sabotage, and terrorism, it was "virtually impossible to read the 1978 FISA to exclude from its purpose the prosecution of foreign intelligence crimes, most importantly because, as we have noted, the definition of an agent of a foreign power--if he or she is a U.S. person--is grounded on criminal conduct." Id. at 723. http://epic.org/privacy/terrorism/fisa/FISCR_opinion.pdf

[87] Elizabeth B. Bazan, The Foreign Intelligence Surveillance Act: An Overview of the Satatutory Framework and Recent Judicial Decisions, CRS Report for Congress. 57-87 (2004)

安全之保障，國會兩次延長了「美國愛國者法案」的期限，布希總統並於 2006 年 3 月 9 日將其中即將到期的 14 項條款將永久化，另三項較有爭議之條款效期將延長 4 年。

「美國愛國者法案」此三項核心條款合稱「反恐監視權」（counter-terrorism surveillance powers），賦予中央情報局、聯邦調查局等政府機構以下三項特權：[88]

一、 調取商業記錄條款（Business Records provision）：愛國者法案第 215 條授權聯邦政府可以在不知會嫌疑人的情況下，查扣對調查行動攸關緊要的私人或公司檔案資料，獲取嫌疑人商業記錄等資訊的權力。

二、機動式通訊監察（Roving Wiretaps provision）：愛國者法案第 206 條授權機動式通訊監察，在嫌疑人更換手機改變通訊工具後，可以繼續監聽嫌疑人的通信，無需重新再向法庭聲請授權。

三、 獨狼條款（Lone Wolf provision）：獨狼係指從事或預備爲國際恐怖活動之非美國人民，2004 年情報改革及反恐法第 6001 條（Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004）擴充FISA之規範，修法將獨狼列入50 U.S.C.§1801(b)(1)(C)外國勢力之定義，授權FISA可以在沒有證據的情況下，允許相關部門對非隸屬某一恐怖組織，疑爲獨自犯案的外國恐怖主義嫌疑人的非美國公民進行電子監聽[89]。

在該三項爭議性條款效期屆期之際，美國總統歐巴馬於 2011 年 5 月 26 日再對此三項有爭議性的條款簽署延長了四年，未來是否能永久立法則就須再視屆時之反恐氣氛及民意而定了。

---

[88] Eric Rosenbach, “The USA-Patriot Act”, Confrontation or Collaboration? Congress and the Intelligence Community, Belfer Center for Science and International Affairs, Harvard Kennedy School. 92-95 (2009)

[89] Elizabeth B. Bazan, Intelligence Reform and Terrorism Prevention Act of 2004: “Lone Wolf” Amendment to the Foreign Intelligence Surveillance Act, CRS Report for Congress 5 (2004)

第七項　外國情報通訊監察法 2008 年修正案

國會於 2008 年修正FISA制定了「美國聯邦外國情報通訊監察法修正法案(the FISA Amendment Act of 2008,FAA)」[90]強化原本FISA規範之不足，並設有落日條款即將於 2012 年 12 月 13 日失效。

FAA強化對美國境外非美國人民之外國情報通訊監察規範。原本依FISA第 1802 條規範得爲長達一年期之無法院令狀之通訊監察對象，僅限於對「外國勢力」7 款定義中前 3 款 1801 (a)(1)(2)(3)外國政府、組織、實體間之通訊，對象較爲限縮，但依FAA第 702 條[91]規定，檢察總長及國家情報總監(DNI)[92]得共同授權對美國境外之非美國人爲情報通訊監察，僅要求「合理確信」其監察對象爲美國境外之非美國人，亦即僅要求不得明知爲境內之美國人而故意爲之，而不要求確信該對象爲外國勢力，在符合最小侵害原則，有取得外國情報之重要目的（如同愛國者法案，僅要求重要目的significant purpose，而不要求爲唯一目的purpose），即可授權爲長達一年期之外國情報通訊監察，惟對以上認定應出具證明書交由外國情報通訊監察法院確認同意後始得爲之。

FAA並強化對境外美國人民通訊之規範，在FAA第 703-704 條[93]確認不論是在美國境內對境外美國人民、或其他方式對境外美國人民所爲之通訊監察，皆應取得外國情報通訊監察法院之令狀後始能爲之，且其監察期間不得超過 90 日，且

---

[90] The FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2463 ; 50 USC Chapter 36, Subchapter VI – ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES, 2008 年。

[91] 50 USC §1881a. Procedures for targeting certain persons outside the United States other than United States persons

[92] Director of National Intelligence，DNI，直接受美國總統的指揮，根據2004 年情報改革及反恐法案(Intelligence Reform and Terrorism Prevention Act of 2004)而設立的，為美國總統、美國國家安全會議與美國國土安全會議在關係到國家安全的情報事務上的主要諮詢對象，統領包括 16 個組織的美國情報體系，統籌指導美國國家情報計畫

[93] 50 USC §1881b. Certain acquisitions inside the United States targeting United States persons outside the United States ; §1881c. Other acquisitions targeting United States persons outside the United States

需注意者爲該許可對境外美國公民的通訊監察，一旦發現該美國公民返回美國時，即必須停止監察，惟仍不須有合理確認其是否爲外國勢力之依據。

依FAA所爲之外國情報通訊監察亦須受國會監督[94]，檢察總長須每半年向參議院及眾議院情報、司法委員會報告執行情形，包括：

1. 外國人於境外通訊監察中，認定境外通訊監察之理由依據、最小侵害手段、司法審查等證明之標準。
2. 美國人民於境外通訊之申請及核准總數。
3. 依 FAA 爲緊急通訊監察之申請及核准總數。

FAA 並且也提供了在 2001 年 9 月 11 日到 2007 年 1 月 17 日之間配合美國政府命令進行監聽的電信公司對該修正案具有溯及既往的豁免權。

輿論認爲FAA是爲過去布希時代依行政命令所爲之違法通訊監察賦予正式法律依據，其規定擴張了情報通訊監察權限。人權團體ACLU於法案修正 2008 年同年即提出訴訟Amnesty et al. v McConnell Complaint案[95]，認爲該修正案使政府不須合理確認通訊監察對象是否爲外國勢力，也不須確認使用設備、地點等，亦未有對所蒐集資訊使用及傳遞之規範，而以收蒐裝置(dragnet surveillance)大量擷取美國人民之國際通訊，可能嚴重違法侵害美國人民權益[96]。然而法院以該人權團體並無法確認其是否受通訊監察，而以訴訟當事人不適格駁回訴訟，但該案 2012 年在上訴法院逆轉判決，目前等待最高法院作出裁決。[97]

FAA 即將於 2012 年 12 月 13 日失效，未來修法方向須再觀察。

---

94 50 USC §1881f. Congressional oversight

95 Amnesty et al. v McConnell Complaint, http://www.aclu.org/pdfs/safefree/faa_complaint_20080710.pdf ,Page 3. (2008)

96 Jessica LoConte, FISA Amendments Act 2008:Protecting Americans by Monitoring International Communication—Is It Reasonable?, Pace International Law Review Online Companion, 2010.1.1., Page 8.(2010)

97 ACLU Argues Dragnet Surveillance of Americans Is Unconstitutional, ACLU, http://www.aclu.org/national-security/obama-administration-asks-supreme-court-dismiss-aclu-challenge-warrantless , (2012.2.17.)

第八項　　小結

綜觀 FISA 之特色可發現在某些部分之立法是相當具體的，例如在 FISA 50 U.S.C.&1801 中詳細具體定義了許多法律用語，如：

一、「外國勢力」"Foreign power"及「外國勢力之工作人員」" Agent of a foreign power"[98]。

其「外國勢力」除包括外國政府、機關、組織或國家、政治實體等，但限於非美國國民。而「外國勢力工作人員」則包括美國國民或非美國國民，但若對象是美國國民時，「外國勢力」須爲非美國人之政治實體；「外國勢力工作人員」則不區分國籍，但若是美國人，則須**限於有事實明知其從事刑法上犯罪行爲或從事顛覆、恐怖活動、代表外國勢力使用虛僞身份時**，方可認定其爲外國勢力之工作人員，抽象的空被大幅的限縮。以國籍區分可保障具美國國籍之人民權利不受國家以觀念上較模糊之「國家安全」概念爲侵害。

二、「最小侵害程序」"Minimization procedures"在FISA中有非常詳盡的規定及定義[99]，即在執行通訊監察時，應對本案無關之對話進行最小可能性之通訊監察。無論有無法院令狀之外國情報通訊監察都須遵守本原則。其中包括：

(7) 程序必須合理、並說明採取何種具體的方式以確保爲對美國人民侵害最小、資料保全不濫用、如何避免取得不相關資訊、時間限制，以及非外國情報資訊之銷毀等，並由檢察總長制定就相類似案件制定一致性的準則。

(8) 除非爲評估外國情報資訊，否則在受監察之美國人民同意前，其非

[98] 50 U.S.C. § 1801(a)(b)

[99] 50 U.S.C. § 1801(h) "Minimization procedures"

公開及非屬外國情報之資訊不會被散布或利用。

(9) 除非涉及已發生或即將發生之犯罪，否則不得保存或散布與外國情報無關之資訊。

(10) 無法院令狀之外國情報通訊監察若通訊之一方爲美國人民，則取得之美國人民通訊資訊，非經法院事後核發令狀或檢察總長認爲其關係他人生命或重大身體危險，不得保存或散布。

(11) 外國情報監察法院必須審查聲請人所指示提出的具體措施，是否符合最小侵害程序準則，若不符合，則可選則駁回聲請，或是要求變更其最小侵害程序，或要求聲請人提出更多的相關資訊以決定是否核發令狀[100]。

此外，美國 FISA 特有的保證書制度，要求在有法院令狀之外國情報通訊監察中，國家安全行政長官提出外國情報通訊監察時，應出具保證書(Certification)保證其認爲該截取爲外國情報資料，並符合不得以一般調查方式取得等事項；在無法院令狀之外國情報通訊監察中，檢察總長亦須宣誓以書面保證(Certifies in Writing under Oath)該監察對象非美國人、爲單純外國勢力間通訊及符合最小侵害原則等。

此等保證書制度，或 FISA 中要求聲請書中須明載實際提出聲請之聯邦官員人別資料等類似規範，其立法目的在於使檢察總長或行政機關提出外國情報通訊監察之聲請時，保證其聲請乃有相當之依據與確信。美國 FISA 外國情報通訊監察制度雖對外國情報通訊監察設有許多如最小侵害程序及判斷可能性之規範設計，惟經愛國者法案明文擴張其權利，僅要求以獲取外國情報資訊爲「重要目的」即可爲監察，常使法院之審查流於形式，最後幾乎僅要求確認其係爲搜集外國情報即可爲通訊監察，故是否能證實該情報屬外國情報則須仰賴行政或情報機關在保證書上說明並宣誓所提供資訊爲真，此種制度之設計乃加重檢察或行政機關在提出外國情報通訊監察聲請時之責任，並若日後發生違法通訊監察爭議時，亦得較清楚的釐清相關行政或法律責任歸屬，藉以彌補司法審查「國家安全」抽象界

[100] 50 U.S.C §1804(b)、(C)、(d)

線時之先天缺陷。

此外 FISA 允許「機動式通訊監察(roving surveillance)」以符合效率及實際需求；以及繁複之「外國情報通訊監察法院」設立規範等制度，皆值得參考。

2002 年 11 月 25 日美國國會通過「國土安全法」，使網際網路的監控更爲嚴密，規範有關監控網際網路和懲治駭客的條款。該法將美國境內外的所有情報組織統一爲一個在總統領導下的情報網絡，使美國情報機關擁有完全的自由可以收集美國境內任何人的任何資訊，並且可以與盟國合作以收集世界上任何地方任何人的任何資訊。

有了「外國情報通訊監察法」、「愛國者法案」及「國土安全法」三部法案，形塑了美國情報通訊監察及網際網路管制之全貌，在法規詳盡的規範之下，一方面保障人民在受情報通訊監察時應享有的程序利益及合障，但另一方面卻也在某些規範中開了後門，使公眾在網路上的一切私人資訊在必要情況下都可以受到監視，人民之權益在國家安全之下作了讓步。

第二節　德國情報通訊監察

第一項　立法沿革

電訊通訊技術發明後不久，德國在 1919 年威瑪憲法第 117 條對人民秘密通訊之自由賦予憲法層次之保障，規定對於秘密通訊監察須依法律之始能爲之，惟其後均未通過准許電話監聽之法律[101]。在 1933 年納粹時期，德國制定通過帝國總統爲保護民族與國家條例(Verordnung des Reichspräsidenten zum Schutz von Volk und Staat)，該條例第 1 條規定使威瑪憲法第 117 條規定失去效力，人民秘密通訊之自由不再受憲法之保障。[102]

德國二次世界大戰後，爲保障人民之秘密通訊自由，德國基本法第 10 條規定「書信秘密、郵件與電信之秘密不可侵犯。前項限制僅得依據法律爲之。如限制係爲保護自由民主之基本原則，或爲保護聯邦或各邦之存在與安全，則法律得規定該等限制不須通知當事人，並由國會指定或輔助機關所爲之事後審查代替救濟途徑。」

秘密通訊自由非不可限制之基本權，惟其限制須以法律爲之。基本法第 10 條第 2 項第 1 句係般法律保留原則，因此無論是爲了犯罪訴追或危害防止而有對前述權利予以限制者，均應以法律定之。

1945 年二次世界大戰結束後，1949 年成立德意志聯邦共和國並通過德國基本法，基本法第 10 條規定郵政秘密與電信秘密不可侵犯，秘密通訊自由重新獲得憲法保障，惟此時德國由英、美、法三國派遣軍隊佔領，依依「德意志聯邦共和國與三國關係條約(Deutschlandvertrag)」第 5 條第 2 項規定，西德政府僅獲得有限度的主權，美、英、法 3 國盟軍爲保衛其在聯邦共和國駐軍武裝部隊之安全，

---

[101] Vgl. Gabriele Gross-Spreitzer, Die Grenzen der Telefonüberwachung nach §100a,100b stop unten Berücksichtigung der Aussageverweigerungsrechte im Strafprozess, Diss. Heidelberg, 1987, S. 7-10

[102] 江舜明，刑事偵查監聽容許界限之研究，國立臺北大學法律系博士論文，頁 98-99，2004 年。

於基於軍事之目的得對書信、郵件及電信進行通訊監察，俟德意志權責機關能立法以有效保障三軍駐軍之安全並能處理公與安全與秩序之重大破壞時，上述保留權始失效[103]。在西德尚未立法前，因受基本法第 10 條之拘束，訴追機關僅能依電信設備法第 12 條查詢電話通聯紀錄，不得進行電話之通訊監察。

爲免除此項限制，西德政府自 1968 年依據基本法第 10 條制定「限制書信、郵件及電信秘密法」，賦予情報機關對書信、郵件及電信之監察權限。由於該法係依據基本法第 10 條而來，因此又稱爲基本法第 10 條法，簡稱G10 法(Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses,Gesetz zu Artikel 10 Grundgesetz – G10)，爲德國進行情報通訊監察之依據。本法一方面要應付東西德緊張關係，另一方面爲解除英美法三國駐軍保留權以回復戰敗後受壓抑之主權。[104]

G10 法非僅合法化國家情報機關干預人民基本權，由於本法立法當時，發生許多綁架兒童案件嫌疑人使用電話勒贖，爲有效訴追重大犯罪，立法者認有擴大刑事訴訟之干預權限，經由增訂刑事訴訟法第 100 條a、第 100 條b及修改第 101 條，明文授權准許對重大犯罪進行犯罪通訊監察。[105]自此，爲打擊犯罪所執行犯罪通訊監察由刑事訴訟法規範；而情報機關所執行之情報通訊監察則由G10 法規範。

G10 法自 1968 年制定以來經過無數次修正，基本上並無太大的變動，其中一次重要的變革是配合 1994 年 10 月 28 日「刑法、刑事訴訟法及其他法律部份修正法律(Gesetz zur Anderung des Strafgesetzbuches, der Strafprozebordnung und anderer Gestze – Verbrechensbekampfungsgesetz)」對G10 法的部份修正。此次修正主要針對 90 年代以來組織犯罪及跨國性犯罪之興起，爲有效防制犯罪，擴大了情報報機關通信密的限制範圍。此次修正目的有二：其一、若某組織團體成立之目的係以危害自由民主之基本秩序，或爲保護聯邦或各邦之存在與安全，爲了解

---

103 Vgl. Hermann Borgs-Maciejewski/Frank Ebert, Das Recht der Geheimdienste-Kommentar zum Bundesverfassungsschutzgesetz sowie zum G10,1986,S.139.

104 謝佑平、謝立軍，德國的秘密偵查制度，甘肅政法學院學報 2011 年第 6 期，頁 51-53，2011 年。

105 江舜明，刑事偵查監聽容許界限之研究，國立臺北大學法律系博士論文，頁 100，2004 年。

其成員之行動，得限制其通信秘密權。其二、爲獲取國際恐怖活、入境德國之毒品走私、非法武器交易、國際性僞造貨幣及洗錢等情報，得監聽國際電話。由於此次修法，大幅擴張聯邦情報局之職權，引發情報機關警察化之批判，遭提起憲法訴願，聯邦憲法法院於 1999 年 7 月作出一項影響深遠的判決，宣告G10 法部份條文違憲，聯邦政府遂依聯邦憲法法院判決意旨，於 2001 年 6 月對G10 法進行修正。其後僅有細節性修正，以下僅就G10 法重要內容簡介如下。[106]

第二項　德國情報通訊監察要件

G10 法乃爲防止危害自由民主基本秩序、聯邦或邦之存續安全，及駐守於德國境內之北大西洋公約組織軍隊之安全，而賦予聯邦及各邦憲法保護局(Bundesamt für Verfassungsschutz, BFV)、軍事情報局(Militärische Abschirmdienst, MAD)及聯邦情報局(Bundesnachrichtendienst,BND)得對電信通訊進行監聽與錄音，亦可開啓及檢視書信及郵件。[107]

情報機關得依 G10 法聲請進行情報通監察，並依其性質不同區分爲「個案情報通訊監察」及「戰略性情報通訊監察」，分別介紹如下：

一、 個案情報通訊監察

依 G10 法情報機關爲偵查重大犯罪行爲，得提出針對個人之個案情報通

[106]周治平，情報機關通訊監察權之研究--德國法之啟示，警大法學論集第 15 期，頁 260-262，2008 年 10 月。

[107] G10, Abschnitt 1: Allgemeine Bestimmungen § 1 Gegenstand des Gesetzes

訊監察之聲請，經其管轄之最高行政機關下達，送 G10 委員會同意後，得執行個案情報通訊監察。

（一） 個案情報通訊監察之聲請機關

1. 聯邦情報局(Bundesnachrichtendienst,BND)：直屬總理辦公室之下(Kanzleramt)，主要負責國外有關外交，政治，軍事，科技，軍備及恐怖分子活動情蒐分析的工作，以供政府擬定外交政策的參考，從事境外電訊監聽工作。
2. 邦及聯邦憲法保護局(Bundesamt für Verfassungsschutz, BFV)：聯邦政府及各邦政府內政部之下均設有憲法保護局，主要負責德國境內安全情報工作，尤其是負責監視德國境內出現的違反民主自由基本憲政秩序之活動。
3. 軍事情報局(Militärische Abschirmdienst, MAD)：軍事情報局隸屬於國防部，爲德國最高軍事情報和反間諜機關，負責與軍事相關之保防，軍事外原則上非屬其管轄範圍。

（二）個案情報通訊監察之監察對象

上述情報機關可依G10 法對於危害自由民主基本秩序、危害聯邦或邦之存續安全之犯罪行爲，並有事實足認某人有涉嫌計劃、實行或完成下列所列舉各款犯罪之嫌疑者，或爲其組織成員者，得向法院聲請進行個案情報通訊監察。[108]

1. 危害和平或內亂罪（刑法第 80-83 條）
2. 危害民主法治國家罪（刑法第 84-86、87-89 及結社法第 20 條第 1 項第 1 至 4 款）

[108] G10, Abschnitt 3: Strategische Beschränkungen

3. 叛國或對國家安全之危害行爲（刑法第 94-96、97a-100a）

4. 危害國防罪（刑法第 109 條 e-g）

5. 危害駐守德國境內之北大西洋公約國軍隊之安全罪（刑法第 87、89、94、98-100、109e-g、北大西洋公約國軍隊保護法第 1 條）

6. 其他刑法重罪[109]

7. 居留法第 95 條第 1 項第 8 款

8. 海關法第 23 條 a 項 1.3 項

（三）個案情報通訊監察之監察限制

1. 一般限制

因通訊監察之偵察手段對人權侵害較大，故如同犯罪通訊監察一般，G10規範中亦要求需在不能或極難以其他方法調查事實，始得爲個案情報通訊監察；且個案情報通訊監察之對象限於法律上之犯罪嫌疑人，或依一定事實足認爲與犯罪嫌疑人聯繫之人。惟德國聯邦眾議院及各邦議會之議員之郵件則有排除本規範之適用，不得對其爲個案情報通訊監察。

2. 私人生活不可侵犯之核心領域及合法拒絕證言權

聯邦憲法法院於德國1983年人口普查法判決[110]後建立了訊息自決

[109] G10, § 3 (1) 6. Straftaten nach
a)den §§ 129a bis 130 des Strafgesetzbuches sowie
b)den §§ 211, 212, 239a, 239b, 306 bis 306c, 308 Abs. 1 bis 3, § 315 Abs. 3, § 316b Abs. 3 und § 316c Abs. 1 und 3 des Strafgesetzbuches, soweit diese sich gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes richten, oder

[110] 1 BvR 209/83 u.a., BVerfGE 65, 1, Dezember 1983。該判決之中譯，詳見蕭文生，關於「一九八三年人口普查法」之判決，收錄於西德聯邦憲法法院裁判選輯(一)，司法週刊雜誌社，第 288 頁以下，1990 年 10 月。

權的概念；此權利是從自我表現權延伸而來，得對抗國家無限制的調查、儲存、使用與傳遞個人信息，以是否侵犯人性尊嚴核心領域，作爲是否禁止信息傳遞連結的基準。但在重大公共利益的前提下,個人必須忍受其權利的限制,而國家對此權利的限制則必須符合法律保留原則與比例原則。其後在2004年德國聯邦憲法法院對刑事訴訟法第100條ｃ大監聽作出限制[111]，強調即便是爲了重大公益的需求監聽行爲不應損及「私人生活不可侵犯之核心領域」，如果長時間且毫無限制的全面監視，可能因觸及私人生活核心領域而侵犯人性尊嚴，當監聽發生未預期之情況以侵犯此一核心領域時，應該立刻停止監聽，取得之資訊應加以銷毀並禁止使用。

另在「私人生活不可侵犯之核心領域」中可能涉及最具私人性質之談話者，應注意其談話內容中應依拒絕證言權人之保護，對於因侵入「不可侵犯之核心領域」所得資料禁用並銷毀。[112]

爲符合上述相關原則，G10法亦增修了第3條ａ、ｂ。

（１）在第3條ａ的部份保障了私人生活不可侵犯之核心領域，個案情報通訊監察之措施不得侵犯私人生活核心領域。

執行個案情報通訊監察中，若有事實足認其通訊監察所得內容包含了私人生活核心領域時，須以機器自動爲紀錄者始得以繼續實施通訊監察。該自動紀錄應即提交G10委員會判斷情資是否可以運用或應銷毀。畢竟機器自動所爲之紀錄在經G10委員會確認後始有被利用之可能，對人權侵害程度較小。

（２）保護「職業上負保密義務者」合法拒絕證言權之權利

G10法保障若可預見個案情報通訊監察之行爲將獲取原依刑事訴訟法享有拒絕證言權人如神職人員、被告的辯護律師、議員等人之資訊時，則不得爲之。若有取得相關資訊亦不得使用，並

111 BVerfGE 109, 279 (2004).

112 楊雲驊，保障「私人生活不可侵犯之核心領域」--德國聯邦憲法法院對於「住宅內監聽」（大監聽）違憲審查判決簡評，財團法人民間司法改革基金會電子報，2006 年 6 月 25。

應銷毀。

若是可預見將獲取律師、公證人、會計師、醫師等專業人員等專業人員個人資訊，則須比例原則，權衡公益及信任知悉他人事務保密義務之公益，決定是否使用該資訊。

若有事實足認合法拒絕證言之人乃係依本法得爲個案情報通訊監察之犯罪嫌疑人，或爲幫助犯者，則不受上述之保護。

（四）個案情報通訊監察之執行[113]

1. 情報機關於執行情報通訊監察期間之自我審查

情報機關於執行個案情報通訊監察 6 個月內，就所蒐集之個人資料，在自身職務範圍內，隨時審查資料確認是否有符合第 1 條第 1 項第 1 款「防止危害自由民主基本秩序、聯邦或邦之存續或安全之規範目的」而有通訊監察之必要性。

若不符合上述目的，且情資亦無傳遞他機關之必要時，應立即在具有法官資格之公務員之監督下予以銷毀，並作成紀錄。但若爲履行對於受通訊監察人之事後告知義務，或對於本通訊監察行爲適法性審查具重要性時，不得銷毀，但不得爲其他目的再爲利用。剩餘之情資並應予以標示後始得利用。

2. 所蒐獲情資之標識與運用

個案情報通訊監察經情報機關將所獲情資中，與監察目的無關之部分銷毀後，確認剩餘部份符合執行通訊監察之目的時，該剩餘部份須經進行標識後，再予情報單位運用，或傳遞予與情資內容相關主管機關運用。

[113] G10, Abschnitt 2: Beschränkungen in Einzelfällen § 4 (1)

（五）情資傳遞之限制[114]

執行個案情報通訊監察所得之情資，在符合「防止危害自由民主基本秩序、聯邦或邦之存續或安全」之規範目的，若爲其他機關履行職務所需要，而爲防止或調查該犯罪，或有特定事實根據足認某人涉嫌實行或完成該等犯罪而欲追訴之，符合涉嫌下列列舉之犯罪，始得傳遞予其他機關：

1. 爲防止或調查符合 G10 法第 3 條個案情報通訊監察所列舉之重罪（如刑法內亂罪、危害民主法治國家罪、判國罪、危害國防罪等）；
2. 有特定事實足認某人涉嫌計劃或實施 G10 法第 7 條戰略性情報通訊監察所得內容得傳遞其它單位之舉列重罪（如犯罪集團、僞造貨幣、僞造有價證券、洗錢等）

在以上列舉之犯罪之外，另規範了爲準備及實施基本法中關於違憲政黨或社團法中相關規定時，亦得爲傳資之傳遞。

此外，在得傳遞利用之情報通訊監察情資若結合了當事人與第三人之通訊內容，而無法將其分離，或分離須花費鉅額費用時，得在傳遞機關內具有法官資格之公務員決定後一併傳遞，但關於第三人之部份則不得運用。

受領機關僅得就其職務範圍內，符合該資料傳遞目的下加以利用，並於 6 個月內審查其受領之必要性，或無受領必要時亦須銷毀並通知傳遞機關。

二、 戰略性情報通訊監察

[114] G10, Abschnitt 2: Beschränkungen in Einzelfällen § 4 (4) Die Daten dürfen nur übermittelt werden

所謂戰略性情報通訊監察(Strategische Beschränkungen)，乃聯邦情報局(Bundesnachrichtendienst,BND)爲察覺及防止重大國際犯罪之危險，得對「國際電信通訊」，非針對個人，而係針對事件進行之戰略性情報通訊監察，排除個別化要件[115]。聯邦情報局得透由通訊監察設備以獲得大批的通訊內容，並經議會監督委員會之同意設定關鍵字後，對大批的通訊內容就關鍵字爲搜尋，並得將資訊於法規限制內與其他政府機關傳遞分享。[116]。

在數個情報機關中，僅有聯邦情報局有聲請戰略性情報通訊監察之權限，此乃因聯邦情報局在德國情報機關的任務分配中，是涉外情報蒐集與評估之專責機關。爲獲取對於德國外交或國家安全政策具有重要性之涉外情報，依據聯邦情報局法(BND-Gesetz)第 12 條規定，聯邦情報局需向聯邦總理府秘書長(Chef des Bundeskanzleramtes)報告其工作狀況，故由聯邦情報局提出戰略性情報通訊監察之聲請，聯邦總理府主任認可後，經聯邦議會監督委員會同意後，得爲戰略性情報通訊監察。[117]

（一）通訊監察對象

聯邦情報局得爲及時察覺、防止下列犯行而蒐集通訊資訊，得提出戰略性情報通訊監察之聲請。[118]

1. 對德意志聯邦共和國的武力攻擊
2. 與德意志聯邦共和國直接有關的國際恐怖攻擊
3. 軍事武器管制法所指之國際武器擴散，及重要的商品、資訊處理程

---

115 G10, Abschnitt 3: Strategische Beschränkungen § 5 Voraussetzungen

116 Nicole E. Jacoby, Alston & Bird, LLP, Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and the United States, Berkeley Electronic Press, http://law.bepress.com/expresso/eps/1515/, Page.36, 2006

117 周治平，情報機關通訊監察權之研究--德國法之啟示，警大法學論集第 15 期，頁 265-267，2008 年 10 月。

118 G10, Abschnitt 3: Strategische Beschränkungen § 5 (1)

式及高科技之非法跨國交易

4. 未經許可將大量毒品攜入德意志聯邦共和國

5. 在國外僞造貨幣，而損害歐元流通區的貨幣安定性

6. 重大國際組織洗錢活動

7. 外國人對歐盟地區之重大組織性國際走私活動

（二）情報通訊監察之執行[119]

1. 得設定「關鍵字搜尋」

G10 法明文規範聯邦情報局可依其情蒐任務之必要使用「關鍵字搜尋」(Suchbegriffe)，設定特定「關鍵字」，對通訊內容進行特定及適當之自動搜尋。

聯邦情報局得透由通訊監察設備以獲得大批尚未有任何犯罪嫌疑之通訊內容，並經議會監督委員會之同意設定關鍵字後，對大批的通訊內容就關鍵字爲搜尋，例如設定關鍵字「恐怖攻擊」加上關鍵字「蓋達組織」，對網路通訊或語音通訊自動搜尋，可迅速在成千上萬的通訊內容中快速篩出特定通訊後再爲檢視利用。

惟戰略性情報通訊監察此種排除個人化通訊監察要件之設定，亦非針對特定人爲通訊監察，故在使用「關鍵字搜尋」進行戰略性情報通訊監察時，若關鍵字設定不當或過於籠統空泛，便可能侵害廣泛人民之隱私權[120]，故G10 法對該關鍵字設定後，下命實施前須得到議會監督委員會之同意，且該鍵字之設定仍設有下列限制：

（１） 若該國際通訊之經常使用者爲德國人時，其關鍵字不得包

[119] G10, Abschnitt 3: Strategische Beschränkungen § 5 (2)

[120] Kim Lane Scheppele, Other People's Patriot Acts: Europe's Response to September 11, Scholarship at Penn Law,Page.115 , 2004.10.1

含：

a.可導出個人身分特徵之特定目標。如個人電話號碼或使用者人姓名等。[121]

b.私人生活不可侵犯之核心領域。

（２） 若該國際通訊之經常使用者爲非德國人時，其關鍵字則不受上述規範之限制。

2. 私人生活核心領域保護之限制

爲戰略性情報通訊監察蒐集資訊，不得包含私人生活核心領域之通訊內容。[122]若取得該資訊則亦不得加以運用，並應在有法官資格之公務員的監督之下予以銷毀。其規範適用個案情報通訊監察對私心生活核心領域之保護。

3. 情報機關於監察期間之自我審查

同個案情報通訊監察，G10 亦要求情報通訊監察所獲情資之運用，須有自我審查機制，在蒐集到的資料在 6 個月內在自身職務範圍內對資料隨時審查是否符合戰略性情報通訊監察之必要性。若該資料已不符其必要性時，亦無傳遞至其他機關之必要時，應即在具有法官資格之公務員之監督下予以銷毀並作成紀錄。但若爲履行對於受通訊監察人之事後告知義務，或對於本通訊監察行爲適法性審查具重要性時，不得銷毀，但不得爲其他目的再爲利用。

---

121 Nicole E. Jacoby, Alston & Bird, LLP, Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and the United States, Berkeley Electronic Press, http://law.bepress.com/expresso/eps/1515/, Page.35, 2006.

122 G10, Abschnitt 3: Strategische Beschränkungen § 5a Schutz des Kernbereichs privater Lebensgestaltung

（三）資訊交叉比對[123]

爲強化情資之運用，若在自動化設備蒐集下所得之戰略性情報通訊監察情資，若有事實足認將危害國家，則得依聯邦情報局之聲請，將經由自動化設備所獲得之電話號碼，與現行政府所有之資訊，或要求民間機構提供之其他特定特徵資料，進行交叉比對。比對之電話號碼或其他特定特徵資料，聯邦情報局得於國內運用，但不得列爲戰略性情報通訊監察中「關鍵字詞組」再爲搜尋。該比對資訊應做成紀錄，並於保護目的範圍內方得利用，該紀錄應於年度結束時予以銷毀。

（四）情資傳遞之限制[124]

1. 對國內各機關之情資傳遞

依戰略性情報通訊監察所蒐集之個人相關資料，經依聯邦情報局法第 12 條規定，向聯邦政府各權責部會部長就G10 法第 5 條中列舉得爲戰略性情報通訊監察之危險事項進行報告後[125]，方得傳遞。此爲G10 法之特殊證據排除規定，依情報通訊監察所獲取之證據只能被用以偵查或指控上述危害國家安全之犯罪等，而不能用於其他目的，若取得之情資非爲上述犯罪，即使通訊監察過程完全遵守合法程序，該證據亦應被排除。[126]

若符合上述得傳遞之情資，依下列情況須分別指定傳遞至不同單位：

（１）若有事實根據足認有於境內使用暴力行爲而侵害聯邦憲

123 G10, Abschnitt 3: Strategische Beschränkungen § 6 (3)

124 G10, Abschnitt 3: Strategische Beschränkungen § 7 Übermittlungen durch den Bundesnachrichtendienst

125 BNDG§12：聯邦情報局需向聯邦總理府秘書長報告其工作狀況。除此之外，聯邦情報局透過其工作所獲得之情事亦需直接向各相關權責聯邦政府各部會部長報告後，得傳遞相關個人資料。

126 秦策，德國刑事訴訟中的證據禁止：理論、規則與司法技術，法術現代化研究第 9 卷，2004 年。

法保護法第 3 條 1.3.4 款，而其資料對憲法保護局之情報蒐集或分析確有必要時，得傳遞予聯邦或各邦之憲法保護局；若該情資有事實根據足認危害安全或爲外國勢力從事間諜行爲之嫌疑者，則得傳遞予聯邦或各邦憲法保護局或軍事保護局。

（２）得傳遞情資若是爲調查是否符合從事國際貿易、出口之法律或義務時，得傳遞予聯邦經濟及出口管制局(BAFA)。

（３）G10 法在第 7 條第 4 項亦列舉刑法、外貿法、軍事武器管制法及麻醉藥品法等法規內之部份罪名，如犯罪集團、僞造貨幣、僞造有價證券或洗錢等，得將該情資傳遞予警察機關。

相同地，在得傳遞利用之情報通訊監察情資若結合了當事人與第三人之通訊內容，而無法將其分離，或分離須花費鉅額費用時，得在傳遞機關內具有法官資格之公務員決定後一併傳遞，但關於第三人之部份則不得運用。

受領機關僅得就其職務範圍內，符合該資料傳遞目的下加以利用，並於 6 個月內審查其受領之必要性，或無受領必要時亦須銷毀並通知傳遞機關。

2. 對外國政府爲國際情資之傳遞

G10 法第 7 條a中有一較爲特殊之規定，明文對德國聯邦情報局若要將戰略性情報通訊監察情資傳遞予外國政府機關時之規範。[127]

非所有之戰略性通訊監察所得資訊皆得傳遞予他國，而僅限於依通訊監察目的乃爲發覺國際恐怖攻擊、國際武擴散及歐盟區組織性走私者，該等情資符合以下列情形者，得經聯邦總理府同意及聯

[127] Q10,§ 7a Übermittlungen durch den Bundesnachrichtendienst an ausländische öffentliche Stellen

邦情報局內具有法官資格之公務員而爲傳遞行爲：

（１）對維護德國外交或安全政策利益，或對外國政府之安全有顯著影響所必須。

（２）不應損及當事人應被保護之利益，並確認外國政府對情資之保護能力完善，並能以符合法治國家之原則來使用該個人情資。

（３）爲維持平等互惠原則

受領機關有傳遞之情資僅能在傳遞之目的範圍內使用之義務，並保持標識，亦需回覆聯邦情報局對資料運用之查詢。

主管之聯邦部會每月需將相關情資傳遞情形告知 G10 委員會；並於至遲 6 個月內告知國會監督委員會。

（五）情報機關審查及銷毀之義務[128]

聯邦情報局就所蒐集之個人情資，應在 6 個月內，就自身職務範圍內隨時審查其是否合 G10 法第 5 條第 1 項第 3 款所規範戰略性通訊監察目的之必要性，若無必要且也無傳遞之必要時，應即在具有法官資格之公務員的監督下予以銷毀，並作成紀錄。若情資係爲依 G10 法履行告知義務者，或對監察之適法性司法審查有重要性時，不得銷毀。於此情形，該資料不得再予運用，僅得在前揭目的範圍內予以利用。剩餘的情資須予以標示後方得利用。

（六）爲保護在外國之人生命身體危險所執行之戰略性情報通訊監察

戰略性情報通訊監察原本乃非爲針對個案爲通訊監察，惟在 2001

[128] G10,§6(1)(2) Prüf-, Kennzeichnungs- und Löschungspflichten, Zweckbindung

年修法增設另一種針對純屬保護個人法益之通訊監察規範[129]，起因於2000年德國人在菲律賓遭回教激進份子綁架，國會監督委員會迅速授權對其進行戰略性情報通訊監察[130]；修法後，因此在個案中為及時知悉或防止身處國外之人民身體或生命之危害（不問是否具有德國國籍），並以特殊形式直接影響德國利益，於不能或極難以其他方法調查事實時，聯邦情報局亦得聲請為最長為期2個月之戰略性情報通訊監察，但須經「國會監督委員會」三分之二多數同意。[131]此類型通訊監察，亦得使用「關鍵字搜尋」以獲取情報，此將有助於即時危機處理。[132]

第三項　聲請情報通訊監察之程序及其期間

依G10法情報通訊監察執行，須由聯邦憲法保護局、各邦憲法保護局、軍事反情報局及聯邦情報局之首長或其代理人，以書面提出聲請，而有權下達情報通訊監察者，依聲請單位不同而有異：[133]

1. 各邦憲法保護局提出聲請時，由各邦最高行政機關同意。
2. 聯邦憲法保護局提出聲請時，由聯邦內政部長同意。
3. 軍事反情報局提出聲請時，由聯邦國防部長同意。
4. 聯邦情報局提出聲請時，由聯邦總理府主任同意。

---

[129] Huber, Das neue G10-Gesetz, NJW 2001, S.3300.

[130] Alexander Boulerian, Germany: new law allows more extensive government monitoring of phone calls and email, http://www.wsws.org/articles/2001/feb2001/germ-f20.shtml, 2001.2.20.

[131] G10, Abschnitt 3: Strategische Beschränkungen §8 Gefahr für Leib oder Leben einer Person im Ausland

[132] 周治平，情報機關通訊監察權之研究--德國法之啟示，警大法學論集第15期，頁267，2008年10月。

[133] 周治平，情報機關秘密情報蒐集之法律問題，東吳法研論集第五卷，頁149，2009年12月。

相關單位應以書面提出聲請，內容須明示命令之根據及有權執行通訊監察之機關，明定情報通訊監察之類別、範圍及期間。[134]

對個案情報通訊監察之聲請應明示限制之對象、電話號碼或通訊聯繫之標識。對戰略性情報通訊監察，由聲請應將所欲搜尋之關鍵字明定於聲請書內，並載明範圍及方式。

同意執行情報通訊監察之期限，不論是個案情報通訊監察，或戰略性情報通訊監察，皆不得超過 3 個月，但如通訊監察之前提要件仍持續存在時，得聲請延長，每次延長期限亦不得超過 3 個月。

同意執行情報通訊監察後，由聲請機關在具有法官資格之公務員的監督下執行。

第四項　德國情報通訊監察之監督

在 G10 法中，監督情報通訊監察之機關有三，一為聯邦議會監督委員會(Das Parlamentarische Kontrollgremium, PKGr)，一為 G10 委員會(G10 Kommission)，一為各邦議會，分別介紹如下：

一、聯邦議會監督委員會

聯邦議會監督委員會乃屬聯邦議院監督委員會之特設委員會，依據「國會聯邦情報工作監督法」(Gesetz uber die parlamentarische Kontrolle nachrichtendienstlicher Tatigkeit des Bundes)，聯邦議會監督委員會監督聯邦憲法保護局、軍事反情報局及聯邦情報局等德國聯邦所有情報機關之工作。委員會由 9 位聯邦議會議員組成，依議會黨團大小做比例分配選出。

[134] G10, Abschnitt 4 :Verfahren§ 10 Anordnung

[135]

依G10 法規範第 5 條第 1 項規定，聯邦情報局進行戰略性情報通訊監察前，須經聯邦議會監督委員會同意。至於個案情報通訊監察之執行，有權核准通訊監察之聯邦部會，應每隔最長 6 個月內向本委員會報告執行情形。關於其對外國政府之情報傳遞亦應於傳遞後 6 個月內告知國會監督委員會。聯邦議會監督委員會每年應就G10 法之通訊監察種類、範圍及執行情形，向聯邦議會進行報告。[136]

二、G10 委員會[137]

G10 委員會爲G10 法中最主要之監督機關，設於聯邦議會監督委員會下。G10 委員會乃一具有司法權性質之特殊獨立外部監督機關，委員會由主席、3 名委員及 4 名副委員組成。[138]主席須具有法官身份，委員則爲政黨提名各別獨立行使職權之法律專家，經聯邦政府實施聽證後，由聯邦議會監督委員會任命之，不需爲議員，以聯邦議會任期爲期。主席不參與表決，但表決同數時由主席決定之。G10 委員會採秘密方式進行審議，委員對任職期間所知悉事項負保密義務，離職後亦同。

委員會至少每個月召會一次，以秘密方式審議下列事項：

（一） 就個案決定是否執行情報通訊監察：聯邦情報權責機關每月就自己所下令所爲之情報通訊監察措施，在執行前向 G10 委員會報告。唯有經委員會正式決議後，方能執行情報通訊監察。若委員會認爲情報通訊監察之合法性及合目的性均有欠缺時，權責機關即不得爲之。對於已經執行之情報通訊監察，委員會不允許或認無必要時，應立即停止。若情況緊急，可於報告前先命執行，但若 G10 委員會

---

[135] 周治平，情報機關通訊監察權之研究--德國法之啟示，警大法學論集第 15 期，頁 268-272，2008 年 10 月。

[136] G10, Abschnitt 5: Kontrolle § 14 Parlamentarisches Kontrollgremium

[137] G10, Abschnitt 5: Kontrolle § 15 G 10-Kommission

[138] Kim Lane Scheppele, Other People's Patriot Acts: Europe's Response to September 11, Scholarship at Penn Law,Page.111, 2004,10.1.

不同意或認爲無必要時，亦應立即停止。

（二） 審查聯邦各情報機關是否遵守 G10 法之相關情資處理運用之全般規範。

（三） 決定是否將情報通訊監察事宜於事後通知當事人：聯邦權責機關每月應就通知情形，或不予通知之理由向 G10 委員會報告。若 G10 委員會認爲有告知之必要時，權責機關應立即報告。

G10 委員會爲 G10 法中最主要之監督機關，可在個案情報通訊監察預先進行合法性及合目的性之監督。關於對外國政府之情報傳遞情形亦應於告知 G10 委員會。

G10 委員會爲發揮其準司法權之監督調查功能，得針對每一項細節向相關機關詢問、調查，閱覽全般資料，並得隨時進入執行處所。

三、各邦議會

各邦憲法保護局聲請之個案情報通訊監察案件，由各邦議會爲審查及監督，並由各邦立法機關定之。只有經各邦立法機關就個人資料處理及運用已制定監督機制者，方得將資料傳遞予其行政機關。[139]

第五項　德國情報通訊監察之通知與救濟

一、 通知[140]

個案情報通訊監察在監察終止後，應通知受監察人。若在戰略性情報通訊監察中獲取個人情資者，若未立刻銷毀者亦同。換句話說，戰略性情報通訊監察所獲取了個人情資，若立刻將其銷毀者，則不須通知當事人。

[139] G10, Abschnitt 4: Verfahren§ 12 Mitteilungen an Betroffene

[140] G10, Abschnitt 5: Kontrolle§ 16 Parlamentarische Kontrolle in den Ländern

但若情報通訊監察目的之危害尚未結束；或是通知將可預期對聯邦或邦之福祉造成不利益者，得不予通知。

但若在情報通訊監察結束後的 12 個月內仍不通知受監察人時，須經 G10 委員會同意下延長不通知的期限，期限之長短亦應一併審查。

有下列情形者，經 G10 委員會一致同意者，得不通知當事人。

1. 情報通訊監察之要件於 5 年內仍存在。
2. 情報通訊監察之要件於未來仍很有可能存在。
3. 執行機關或受領機關依法有銷毀之義務。

通知義務人爲聲請機關，若情資被傳遞者，其通知應經受領機關同意。

二、 救濟

在情報通訊監察通知當事人前，並不提供任何救濟途徑。[141]然而在通訊監察後如無礙國家安全應通知當事人，此時，受監察人得向法院提請救濟，審查監察措施之合法性[142]。依德國刑事訴訟法上所有干預人民基本權利之強制處分，原則上皆得提起法律救濟，即便已經終結之強制處分，只要有確認利益，亦得請求法院確認該處分之違法性，即可就確認強制處分違法進行確認之訴，以排除證據能力及國家賠償責任。

[141] G10, Abschnitt 4: Verfahren § 13 Rechtsweg

[142] 林鈺雄，論通訊之監察—評析歐洲人權法院相關裁判之發展與影響，東吳法律學報十九卷第四期，頁 138，2008 年 4 月。

第三節　小結

本章中選擇對美國及德國此二具有較嚴格、明確之情報通訊監察法律規範之國家，進行較深入之探究，發現此兩國情報通訊監察法治之基本原則，除共同皆要求遵循部份與犯罪通訊監察相同之比例原則、重罪原則、最後手段原則（不能或難以其他方法蒐集或調查證據）、關聯性原則（有相當理由信其通訊內容與本案有關）、一定期間原則等法治國重要原則外，其他對於不論情報通訊監察限制對象、罪名之列舉、國際間情資傳遞利用之規範、核准及救濟機關等之立法規範方式皆大相競庭，以下略作相關之分析比較。

一、 情報通訊監察限制對象：

依情報通訊監察要件之寬鬆區別，美國 FISA 區分爲要件較嚴格之「有法院令狀之情報通訊監察」及要件較爲寬鬆之「無法院令狀之情報通訊監察」；德國則區分爲要件較嚴格之「個案情報通訊監察」及要件較爲寬鬆之「戰略性情報通訊監察」。

就情報通訊監察限制要件作比較，美國 FISA 以「是否具有美國國籍」之比例原則區別保護程度，若具美國國籍者，不但須要有事實明知其從事違法或犯罪行爲時，且須經外國情報監察法院核發通訊監察書，方可對其實施情報通訊監察；相反的，未具美國國籍者，則可直接由檢察總長授權爲無法院令狀之情報通訊監察。此種以國籍作爲區分的方式，可保障具美國國籍之人民權利不受國家以觀念上較模糊之「國家安全」概念爲侵害。

德國 G10 法之情報通訊監察要件不區分國籍，而以針對個人所爲之「個案情報通訊監察」與對不特定個人所爲之「戰略性情報通訊監察」區分保護的程度。若要針對個人爲個案情報通訊監察，需有事實足認某人涉嫌 G10 法列舉之刑法或其他法規之重罪者，且經準司法性質之獨立機關 G10 委員會核准，始得爲之。但若對不特定個人所爲之通案戰略性情報通訊監察，得就影響國家安全事項爲情蒐，且須經立法性質之議會監督委員會同意。

德國 G10 法中唯一使德國國籍人享有較高保障者是進行「關鍵字搜尋」時，若經常使用者爲德國人時，其關鍵字之設定不得包含個人身分特徵及私人生活核心領域；對非德國籍之外國人則無限制。

二、 罪名之列舉：

美國 FISA 爲確保其外國情報通訊監察之特質，完全與刑事犯罪通訊監察切割，其有法院令狀及無法院令狀之外國情報通訊監察，皆不列舉任何應爲監察之罪名，僅須符合其有詳細定義之「外國勢力」及「外國勢力之工作人員」，並由檢察總長或行政機關出具保證書，得向法院提出聲請監察。

德國 G10 法在戰略性情報通訊監察中有列舉得爲蒐情之國家安全要項，如武力、恐怖攻擊、軍事武器擴散、毒品、洗錢等，雖廣泛但相較於美國之無法院令狀外國情報通訊監察，仍爲更詳盡的規範，更遑論 G10 法規範的個案情報通訊監察，須爲其所詳盡一一列舉之刑法等法律犯罪之嫌疑犯，始得爲個案情報通訊監察之聲請。

三、 國際間情資傳遞利用之規範：

美國情報機關長久以透過國際情報交換，取得、交換他國爲國際通訊監察所獲之國際情資，規避 FISA 中如對國籍要求之規範等，一直爲人所詬病。然德國 G10 法中反倒是在修訂法條時於第 7 條 a 項直接明文規範國際間情資傳遞利用之程序、內容及監督方式，似乎能在情資傳遞行爲中提供較完善之保護。

四、 核准及救濟機關：

美國 FISA 中有法院令狀之外國情報通訊監察，其核發通訊監察書之機關爲外國情報監察法院，其制度依權能區分，爲行政機關提出聲請，由專責司法機關審核；德國 G10 法則是由情報機關提出聲請，向有準司法性質

之獨立機關「G10 委員會」報告後，由最高行政機關下達執行，但因 G10 委員會得依職權調查後決定是否要求停止執行，故 G10 委員會爲實際審核機關。

惟依此制度，當被監察人面對違法情報通訊監察時，美國可依 FISA 向專責之外國情報監察法院提出救濟及上訴，但德國 G10 委員會則未規範此等救濟制度。

美國與德國之情報通訊監察法制皆爲依其原本之司法體系及刑事通訊監察制度而立法，爲各自之固有法，非繼受模仿而來。整體而言，美國 FISA 著重於保障擁有美國國籍之人，強調在「國家安全」這頂大帽子下，無論如何，至少美國人民得較外國人受到更嚴密之保護措施；而德國 G10 法則重於將情報機關之強化情蒐管道如「關鍵字搜尋」、情資交叉比對、情資之國際間傳遞運用等措施明定於法條，並將何種罪行可爲要見較嚴格之個案情報通訊監察，何種罪行可爲要件較寬鬆之戰略情報通訊監察，爲非常詳盡之列舉，看似其情報機關之通訊監察權限大，惟與其不明文規範而於暗中進行情報工作，不如直接立法明定所有擴權措施應遵守之界限，並加強保護私人生活核心領域，才更符合法治國原則。

第三章 我國情報通訊監察

第一節 立法沿革

我國關於通訊監察之法令，在威權時期，於 1948 年曾制定「戡亂時期郵電抽查條例」，但因內容不合時宜從未實施；而依據國家總動員法所訂定之「動員時期電信監察實施辦法」，因 1991 年動員戡亂時期終止而廢止，亦有引用國際電信公約、電信法等而爲之。戒嚴後，實務上爲因應實際需要，1992 年及 1993 年法務部訂頒「檢察機關實施通訊監察應行注意要點」[143]及「國內犯罪案件通訊監察作業執行要點」，是爲規範司法機關執行通訊監察作業而頒行的行政命令。

在我國通訊保障及監察法尚未公布施行前，偵查機關違法監聽層出不窮，但其是否具證據能力實務上爭執不休，直至最高法院 87 年台上字第 4025 號判決，對於違法監聽所取得之證據是否應該排除指出：『刑事訴訟的目的，固在發現真實，藉以維護社會安全，其手段目的應合法純潔，公正公平，以保障人權，倘證據之取得非依法定程序，而若容許該項證據作爲認定犯罪事實之依據，而有害公平正義時，因已違反憲法第 8 條、第 16 條所示應依正當法律程序保障人身自由、貫徹訴訟基本權之行使及受公平審判權利之保障等旨意，自應排除其證據能力。準此，實施刑事訴訟之公務員對被告或訴訟關係人施以通訊監察，如非依法定程序而有妨害憲法第十二條所保障人民秘密通訊自由之重大違法情事，且從抑制違法偵查之觀點衡量，容許該通訊監察所得資料作爲證據並不適當時，當應否定其證據能力』始爲我國刑事審判對違法通訊監察取證採行證據排除立下重要里程碑。[144]

其後，爲確保憲法賦予人民之秘密通訊自由和隱私權受法律保留之保障，迄

---

[143] 檢察制度世紀回顧，台灣高等法院檢察署網站 http://www.tph.moj.gov.tw/ct.asp?xItem=198649&ctNode=28712, 資料最後更新日期:2011 年 12 月 21 日

[144] 周雯蘭，違法監聽所取得證據之證據能力，司法新聲，2490 頁，2007 年。

1999 年 6 月 22 日立法院三讀通過「通訊保障及監察法」全文 34 條，規範對象包括犯罪監察及情報監察，於同年 7 月 14 日公布施行。2007 年司法院釋字第631號解釋以民國 88 年制定之通訊保障及監察法，其通訊監察書，偵查中由檢察官核發，未要求通訊監察書原則上應由客觀、獨立行使職權之法官核發，而使職司犯罪偵查之檢察官與司法警察機關，同時負責通訊監察書之聲請與核發，難謂爲合理、正當之程序規範，而與憲法第 12 條保障人民秘密通訊自由之意旨不符，因此於同年修正公布部分條文，將通訊監察書完全移由法官核發。情報通訊監察之同意權亦由最高法院檢察署之檢察官移至高等法院專責法官。

另我國於 2005 年公布實施國家情報工作法，規範政府情報蒐集活動，使情報機關（國家安全局、國防部軍事情報局、國防部電訊發展室、國防部軍事安全總隊等[145]）及主管有關國家情報事項範圍內視同情報機關（行政院海岸巡防署、國防部總政治作戰局、國防部憲兵司令部、內政部警政署、內政部入出國及移民署及法務部調查局）基於職權，對「足以影響國家安全或利益之資訊」，應進行之蒐集、研析、處理及運用。[146]國家情報工作法規定蒐集上述資訊，必要時得採

---

[145] 國家情報工作法第 3 條:

一、本法用詞定義如下：

1. 情報機關：指國家安全局、國防部軍事情報局、國防部電訊發展室、國防部軍事安全總隊。

二、行政院海岸巡防署、國防部總政治作戰局、國防部憲兵司令部、內政部警政署、內政部入出國及移民署及法務部調查局等機關，於其主管之有關國家情報事項範圍內，視同情報機關。

[146] 國家情報工作法第 7 條:

一、情報機關應就足以影響國家安全或利益之下列資訊進行蒐集、研析、處理及運用：

1、涉及國家安全或利益之大陸地區或外國資訊。

2、涉及內亂、外患、洩漏國家機密、外諜、敵諜、跨國性犯罪或國內外恐怖份子之滲透破壞等資訊。

3、其他有關總體國情、國防、外交、兩岸關係、經濟、科技、社會或重大治安事務等資訊。

二、前項資訊之蒐集，必要時得採取秘密方式為之，包括運用人員、電子偵測、通（資）訊截收、衛星（光纖）偵蒐（照）、跟監、錄影（音）及向有關機關（構）調閱資料等方式。

三、情報機關執行通訊監察蒐集資訊時，蒐集之對象於境內設有戶籍者，其範圍、程序、監督及應遵行事項，應以專法定之；專法未公布施行前，應遵守通訊保障及監察法等相關

取秘密方式爲之，包括運用人員、電子偵測、通（資）訊截收、衛星（光纖）偵蒐（照）、跟監、錄影（音）及向有關機關（構）調閱資料等方式。情報機關爲維護國家安全與利益並進行安全預警，有必要蒐集相關資訊，但爲保障人民權益並兼顧情報工作之特殊性，若情報機關執行通訊監察蒐集資訊時，蒐集之對象於境內設有戶籍者，其範圍、程序、監督及應遵行事項，目前應先遵守通訊保障及監察法等相關法令之規定始能爲之。

故在上述之「通訊保障及監察法」及「國家情報工作法」中，共同建構了我國基於維護國家安全、自由民主的基本秩序所爲之情報通訊監察架構。

我國通訊保障及監察法所規範之客體包括有線及無線電信、郵件書信、言論談話等[147]，立法者在 1995 年立法時即將通訊監察分爲犯罪通訊監察及情報通訊監察兩種形式，本無意以同一套標準作爲規範。

情報通訊監察乃蒐集外國勢力或境外敵對勢力情報，以作爲國家安全預警情報，得依通訊保障及監察法中情報通訊監察之相關規範爲之。以下針對情報通訊監察事宜爲說明。

第二節 情報通訊監察之對象

依通訊保障與監察法第 7 條規定，爲避免國家安全遭受危害，以蒐集外國勢力或境外敵對勢力情報之必要者，得對其爲核發情報通訊監察書：[148]

1. 外國勢力、境外敵對勢力或其工作人員在境內之通訊。
2. 外國勢力、境外敵對勢力或其工作人員跨境之通訊。
3. 外國勢力、境外敵對勢力或其工作人員在境外之通訊。

法令之規定。

四、外國人或大陸地區人民來臺從事與許可停留、居留目的不符之活動或工作者，主管機關得協調內政部警政署、內政部入出國及移民署或法務部調查局，對其實施查（約）訪。拒絕接受查（約）訪者，移請權責機關依法令處理。

147 我國通訊保障及監察法第 3 條

148 我國通訊保障及監察法第 7 條

而所謂「外國勢力」或「境外敵對勢力」之包括：[149]

1. 外國政府、外國或境外政治實體或其所屬機關或代表機構。
2. 由外國政府、外國或境外政治實體指揮或控制之組織。
3. 以從事國際或跨境恐怖活動爲宗旨之組織。

「外國勢力或境外敵對勢之工作人員」則爲：[150]

1. 爲外國勢力或境外敵對勢力從事秘密情報蒐集活動或其他秘密情報活動，而有危害國家安全之虞，或教唆或幫助他人爲之者。
2. 爲外國勢力或境外敵對勢力從事破壞行爲或國際或跨境恐怖活動，或教唆或幫助他人爲之者。
3. 擔任外國勢力或境外敵對勢力之官員或受僱人或國際恐怖組織之成員者。

第三節 情報通訊監察之聲請

依國家情報工作法第 7 條規範，情報機關應就足以影響國家安全或利益之下列資訊進行蒐集、研析、處理及運用：

1、涉及國家安全或利益之大陸地區或外國資訊。

2、涉及內亂、外患、洩漏國家機密、外諜、敵諜、跨國性犯罪或國內外恐怖份子之滲透破壞等資訊。

[149] 我國通訊保障及監察法第 8 條

[150] 我國通訊保障及監察法第 9 條

3、其他有關總體國情、國防、外交、兩岸關係、經濟、科技、社會或重大治安事務等資訊。

國家情報工作法規定蒐集上述資訊，必要時得採取秘密方式爲之，包括運用人員、電子偵測、通（資）訊截收、衛星（光纖）偵蒐（照）、跟監、錄影（音）及向有關機關（構）調閱資料等方式。情報機關爲維護國家安全與利益並進行安全預警，有必要蒐集相關資訊，但爲保障人民權益並兼顧情報工作之特殊性，若情報機關執行通訊監察蒐集資訊時，蒐集之對象於境內設有戶籍者，其範圍、程序、監督及應遵行事項，目前應先遵守通訊保障及監察法等相關法令之規定始能爲之。

而何者爲該條文中所指之「情報機關」？依國家情報工作法第 3 條規範，情報機關係指：

2. 國家安全局
3. 國防部軍事情報局
4. 國防部電訊發展室
5. 國防部軍事安全總隊

另下列機關於其主管之有關國家情報事項範圍內，視同情報機關

1. 行政院海岸巡防署
2. 國防部總政治作戰局
3. 國防部憲兵司令部
4. 內政部警政署
5. 內政部入出國及移民署
6. 法務部調查局等機關

故上述機關皆有權依通訊保障及監察法第 7 條之規定，爲避免國家安全遭受危害，而以蒐集外國勢力或境外敵對勢力情報之必要者，得向綜理國家情報工作機關首長聲請核發情報通訊監察書。

第四節 情報通訊監察書之核發

第一項 有法院令狀之情報通訊監察

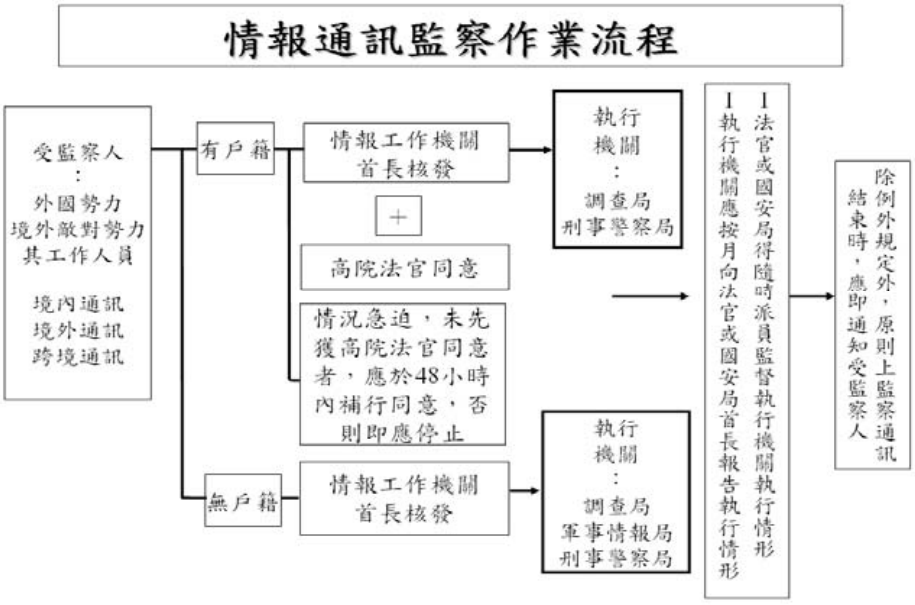
在情報通訊監察中，綜理國家情報工作機關首長，得核發情報通訊監察書。依通訊保障及監察法施行細則第 9 條規定，綜理國家安全情報工作機關係指國家安全局。故國家安全局局長有權得核發情報通訊監察書。

然而若受監察人在我國境內設有戶籍，則爲保障我國人民權益，該情報通訊監察書須由該管高等法院專責法官同意，使能爲之。高等法院爲唯一行使同意權之法院，若情報機關不服並無其他上訴管轄法院，僅能就不足之資訊補足後再送高等法院。

在我國通訊保障及監察法原本情報通訊監察書之同意權由最高法院檢察署之檢察官行使，自民國 96 年修正通過後，該同意權改交由臺灣高等法院法官行使，概檢察官與情報機關原同屬行政體系，將通訊監察書之同意權交予具中立色彩的法官較合適。因此情報通訊監察亦如同犯罪通訊監察一般，回歸如同刑事訴訟法對強制處份所要求之絕對法官保留。

而以戶籍作爲是否經由法院之同意要件乃參照美國外國情報通訊監察法之立法例，且依我國通訊保障及監察法民國 86 年立法說明可知，以戶籍爲區別乃爲保障臺灣地區人民之權益，且亦先推定非本國籍人從事非屬犯罪而爲危害國家安全之可能性較大。反之，若受監察人在我國境內未設有戶籍，綜理國家安全局局長即可以逕自核發通訊監察書。

在情況急迫時，得依國家安全局局長核發之情報通訊監察書先行爲情報通訊監察，唯國家安全局局長應即將通訊監察書核發情形，通知該管高等法院專責法官補行同意，其未在 48 小時內獲得同意者，應即停止監察。



情報通訊監察作業流程圖[151]

情報通訊監察聲請書狀應就下列事項詳實記載，包括：[152]

（一） 案由：在犯罪通訊監察中，除案由外另須載明涉嫌觸犯法條以供審查；惟情報通訊監察爲蒐集國家安全預警情報之用，故不須載明涉嫌觸犯法條。

---

[151] 通訊監察作業專案調查報告，國家安全局，http://www.nsb.gov.tw/documents/%e9%80%9a%e8%a8%8a%e7%9b%a3%e5%af%9f%e4%bd%9c%e6%a5%ad%e5%b0%88%e6%a1%88%e8%aa%bf%e6%9f%a5%e5%a0%b1%e5%91%8a.PDF，2009年10月12日。

[152] 我國通訊保障及監察法施行細則第 12 條：綜理國家情報工作機關依本法第七條第二項及第三項規定，通知高等法院專責法官同意通訊監察者，應備聲請書並記載下列事項：一、案由。二、監察對象及其境內戶籍資料。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、監察理由及其必要性。六、監察期間。七、監察方法。八、執行機關。九、建置機關。

（二） 監察對象及其境內戶籍資料：確認監察對象是否爲同法所定義之外國勢力、境外敵對勢力或其工作人員。

（三） 監察通訊種類及號碼等足資識別之特徵：依同法第 2 條規定，監察通訊種類包括有線及無線電信、言論及談話、郵件及書信，故依其種類需填寫明列通訊監察之電話號碼、網路電信之ADSL帳號、電子郵件帳號、第２類電信如VOIP網路電話號碼等。（電腦對電話之網路電話通訊須經我國電信業者，業者受國內「第２類電信事業管理規則」規範須設置通訊監察設備。惟在第２類電信如skype電腦對電腦之網路電話等，因純粹爲外國公司提供之網路服務，不受第２類電信事業管理規則」規範，故技術上無法爲通訊監察。[153]）

（四） 受監察處所

（五） 監察理由及其必要性：本項亦須依比例原則審查，確認是否有相當理由可信其通訊內容與本案有關，不能或難以他方式蒐集者，始得爲情報通訊監察。惟其未如犯罪通訊監察要「有事實足認有犯嫌」之要件要求，雖不要求具體事證將使審查要件趨向抽象空泛，但因情報通訊監察之實施乃爲蒐集國家安全預警情報[154]，故在本質上其要件本較犯罪通訊監察爲彈性、寬鬆。

（六） 監察期間：情報通訊監察期間，每次不得逾一年；若有繼續監察之必要者，得於期間屆滿前，重新聲請。若於期間屆滿前由國家安全局局長認定已無監察必要者，應停止監察。[155]

---

153 連耀南，新世代通訊網路導論－從法規面與技術面看網路電話的前景，國立政治大學行動計算與網路通訊實驗室（二）研究成果，
http://www.cs.nccu.edu.tw/~lien/Writing/NGN/ch2.htm。

154 我國通訊保障及監察法第 10 條：依第七條規定執行通訊監察所得資料，僅作為國家安全預警情報之用。但發現有第五條所定情事者，應將所得資料移送司法警察機關、司法機關或軍事審判機關依法處理。

155 我國通訊保障及監察法第 12 條：一、…第七條之通訊監察期間，每次不得逾一年；其有繼續

（七） 監察方法：依通訊保障與監察法第 13 條規定，監察通訊是以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似方法爲之，但不得於私人處所裝置竊聽器、錄影設備或其他監察器材。[156]

（八） 執行機關：指蒐集通訊內容之機關。

（九） 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。

依通訊保障及監察法第 2 條規定，不論情報通訊監察或犯罪通訊監察，除爲確保國家安全、維持社會秩序所必要者外，不得爲之（適合性）。且不得逾越所欲達成目的之必要限度（狹義比例原則），且應以侵害最少之適當方法（必要性）爲之。故當國家安全局局長核發通訊監察書及高等法院行使同意權時，除須就聲請書狀記載之客觀形式要件爲審查，另外亦應一併確認是否符合通訊保障及監察法第 2 條所述比例原則之實質要件。

第二項　無法院令狀之情報通訊監察

依我國通訊保障及監察法第 7 條規定，爲避免國家安全遭受危害，而有監察外國勢力、境外敵對勢力或其工作人員在境內、跨境、境外之通訊，以蒐集外國勢力或境外敵對勢力情報之必要者，若受監察人「在境內未設有戶籍」者，綜理國家情報工作機關首長－國家安全局局長得核發通訊監察書。

另對受監察人在境內設有戶籍者，原本其情報通訊監察應依法院令狀執行之情報通訊監察，但在有急迫之情況者，亦得先爲無法院令狀之情報通訊監察，

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。…三、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。

156 我國通訊保障及監察法第 13 條

惟應即通知高等法院專責法官補行同意，其未於 48 小時內獲同意者，應即停止監察。本款規定於 96 年修正前，對外國勢力、境外敵對勢力或其工作人員「境外」之通訊，不論受監察之對象是否具我國國籍，一律皆可進行無法院令狀之情報通訊監察，修法後只要在境內設有戶籍者，不分境內、跨境、境外之通訊皆需法院審查同意取得令狀始能實施。

並違反上述規定進行監聽行爲所取得之內容或所衍生之證據，於司法偵查、審判或其他程序中，均不得採爲證據。

第五節　情報通訊監察之通知

第一項　通知義務

依通訊監察之透明化原則，通訊監察結束後，應讓受監察人得知已受監察之情況，並使其有加以救濟之機會，因此於條文中明定執行機關於監察通訊結束時，應即請通訊監察書核發人許可後，通知受監察人。若有妨害監察目的之虞或不能通知者，於原因消滅後，應補行通知。

告知義務屬於憲法第 8 條第 2 項正當法律程序的重要內容之一，目的在於使被告有行使防禦權的機會。

我國對通訊監察結束後的告知基本上採「強制通知原則」，對於情報通訊監察，通訊保障及監察法第 15 條規定，情報通訊監察案件之執行機關於監察通訊結束時，應即敘明受監察人之姓名、住所或居所報由國家安全局，陳報法院通知受監察人。如認通知有妨害監察目的之虞或不能通知者，應一併陳報。法院對於上述陳報，除認通知有妨害監察目的之虞或不能通知之情形外，應通知受監察人。若不通知之原因消滅後，執行機關應報由國家安全局陳報法院補行通知。

依該規定，情報通訊監察應由國家安全局局長爲初步審核決定是否通知，但決定不通知時，仍應經法官許可。

通訊保障及監察法施行細則第 27 條並規定，執行機關應於通訊監察結束後 7 日內以書面載明情報通訊監察相關事項，報由國家安全局於收文後 5 日內陳報法院審查，法院審查後通知受監察人，其通知內容包括：

一、通訊監察書核發機關及文號。

二、案由。

三、監察對象。

四、監察通訊種類及號碼等足資識別之特徵。

五、受監察處所。

六、監察期間及方法。

七、聲請機關。

八、執行機關。

九、有無獲得監察目的之通訊資料。

第二項　不通知案件之持續檢討

就情報通訊監察而論，通訊保障及監察法施行細則第 27 條第 4 項規定，執行機關認通知有妨害監察目的之虞或不能通知之情形，依本法第 15 條第 1 項陳報之案件，經法院據以不通知受監察人者，執行機關應每 2 月檢討通知有妨害監察目的之虞或不能通知之情形是否消滅，報由國家安全局陳報法院審查。但受監察人實際上無從通知或其不通知原因短期內無法消滅者，得經法院同意，不為定期檢討或延長其檢討期限。

通訊保障及監察法施行細則第 28 條並規定，法院審查執行機關之陳報，如認通知無妨害監察目的之虞或無不能通知之情形，得逕通知國家安全局局長。依本條文可知，對執行機關所陳報不通知之案件，法院須為實質審查其不通知是否

合宜，若認通知並無妨害監察目的之虞或無不能通知之情形，得逕通知受監察人，並副知執行機關及國家安全局局長。[157]

此外，司法院另發布之「法院辦理通訊監察案件應行注意事項」第 24 項規定，國家安全局陳報不通知受監察人，由法院依具體個案情形，本於職權獨立判斷，不受陳報機關意見之拘束。法院若認通知無妨害監察目的之虞或無不能通知之情形，於逕行通知前，宜先徵詢國家安全局局長之意見。

依法院辦理通訊監察案件應行注意事項第 25 項，法院對於國家安全局陳報通知有妨害監察目的之虞或不能通知之情形，應詳爲審查，妥適決定，並注意有無確實執行檢討。

第六節　情報通訊監察之傳遞與救濟

第一項　情資之傳遞

情報通訊監察所得資料，僅作爲國家安全預警情報之用。但若發現有犯罪事實，應將所得資料傳遞移送司法警察機關、司法機關或軍事審判機關依法處理，惟該犯罪案件須符合通訊保障及監察法第 5 條所規範之重罪案件始得爲移送[158]，此規定可避免情報機關以情報通訊監察之名，而行一般犯罪案件調查之實，以免失去立法者爲權衡人民權益而限定重罪案件始得爲犯罪通訊監察之原意。

除了情資得傳遞予司法機關外，若符合本法犯罪通訊監察或情報通訊監察之「監察目的」或其他法律另有規定者，本法監察通訊所得之資料，得提供傳遞

---

[157] 我國通訊保障及監察法施行細則第 28 條：法院審查執行機關依本法第十五條第一項之陳報，如認通知無妨害監察目的之虞或無不能通知之情形，得逕通知受監察人，並副知執行機關、檢察官或綜理國家情報工作機關首長。

[158] 我國通訊保障及監察法第 10 條：依第七條規定執行通訊監察所得資料，僅作為國家安全預警情報之用。但發現有第五條所定情事者，應將所得資料移送司法警察機關、司法機關或軍事審判機關依法處理。

予其他機關、團體或個人。[159]

第二項　救濟

我國最高法院以87年度台上字第4025號刑事判例中明確揭示違法通訊監察取證之證據無證據能力後，違反情報通訊監察程序時，有證據排除法則及毒樹果實理論之適用。從刑事政策的角度觀之，爲抑制國家機關在受監察人不知情的情況下所進行的濫權和違法偵查，若對於違法通訊監察所得的資料不能排除其證據能力，只能於事後追究相關執行人員的民刑事責任，將無法有效抑制違法監察之情事。故違法之情報通訊監察亦可主張無證據能力以爲救濟。

違反通訊保障及監察法之情報通訊監察取得在我國境內設有戶籍者，其所取得之內容或所衍生之證據，於司法偵查、審判或其他程序中，均不得採爲證據。[160]藉由這樣的規定，可以確保情報工作機關確實遵守程序規定，避免濫用情報通訊監察權限，恣意侵害人民通訊隱私。基於保護人權隱私權益原則，通訊監察所得之資料，若涉及我國國民隱私，除於監察目的相關者，得提供予相關機關外，其餘資料應予銷毀，不得外洩；與監察目的相關之資料除予以封緘保存外，於保存期限經過後，亦須加以銷毀。

違法監察他人通訊或洩漏、提供、使用監察通訊所得之資料者，除刑事責任外，亦擔負民事及國家賠償賠償責任。我國通訊保障及監察法中，對「違法通訊監察」之責任規範相當細緻，在違法情報通訊監察可能會觸犯之

---

159 我國通訊保障及監察法第18條：依本法監察通訊所得資料，不得提供與其他機關（構）、團體或個人。但符合第五條或第七條之監察目的或其他法律另有規定者，不在此限。

160 我國通訊保障及監察法第7條第4項：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。

罪名，不論是公務員違法通訊監察、違法洩漏提供使用監察通訊所得之資料、執行或協助執行通訊監察之公務員或從業人員假借職務或業務上之權力機會或方法爲違法通訊監察、明知爲違法監察通訊所得之資料而無故洩漏或交付者或意圖營利者、公務員或曾任公務員之人因職務知悉或持有通訊監察情資而無故洩漏或交付等，該等行爲相關不論損害賠償民事責任、國賠責任、公務員或從業人員刑責，及違法洩漏或交付資訊者之刑責等，故恫嚇違法通訊監察之規範相當縝密。[161]惟對於「形式上合法」之情報通訊監察，即涉我國人民之情報通訊監察案件，若形式上由國家安全局局長核准通訊監察，亦由高等法院法官同意後，受監察之人並未明文規範其救濟管道。

第七節　情報通訊監察之監督

第一項　原則不受立法院監督

依國家情報工作法第 4 條規定，國家情報工作，應受立法院之監督。主管機關首長，應於立法院每一會期率同各情報機關首長向相關之委員會做業務報告，並應邀列席做專案報告。同法第 20 條則規定，主管機關每年應就情報工作之執行成效及興革意見，完成年度總結報告，並送立法院備查。惟通訊保障及監察法中並未明文規範對立法院之報告義務。

爲彰顯對人民負責的權利分立與民主政治精神，情報工作應依國家情報工作法受立法院之監督。惟在通訊保障及監察法規範中，並未規範情報通訊監察事項對立院之報告義務，亦即情報通訊監察事項及執行情形原則上無須向立法院報告，自通訊保障及監察法施行以來，國家安全局僅於民國 98 年間依總統指示[162]，對情報通訊監察相關執行事項及統計數據向立法院外交

[161]我國通訊保障及監察法第 19 至 31 條

[162] 國安局：馬總統上台 監聽量少 7 成，中央社，http://news.rti.org.tw/index_newsConten

及國防委員會作出專案調查報告，並將相關資訊公佈於國家安全局網站。[163]

第二項　行政機關自我監督責任

除不通知案件由法院於事後定期審查是否符合不通知之要件，與法院之線上查核系統外，我國通訊保障及監察法之規範將情報通訊事項監督責責交予綜理國家情報工作機關--國家安全局，依我國通訊保障與監察法第 16 條第 1 項規定:「執行機關於監察通訊後，應按月向檢察官、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報告執行情形。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並得隨時命執行機關提出報告。」

本條文的最初的行政院草案說明中表示「按月報告執行情形」乃指該執行機關當月執行通訊監察的總件數以及各件執行情形之綜合報告。[164]大致區分爲通訊監察綜合報告及對監察設備執行情形之報告。

一、通訊監察綜合報告

通訊監察綜合報告義務區分爲期中、期末與即時報告。

（一）期中報告

關於期中報告，乃通訊監察期間內每月固定之報告，依我國通訊保障與監察法施行細則第 29 條規定：「執行機關依本法第十六條第一項規定按月向檢察官、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報告通訊監察執行情形，應於次月七日前以書面載

---

t.aspx?nid=217412&id2=1，2009 年 9 月 28 日。

[163] 通訊監察作業專業調查報告，國家安全局，國家安全局網站，http://www.nsb.gov.tw/documents/%e9%80%9a%e8%a8%8a%e7%9b%a3%e5%af%9f%e4%bd%9c%e6%a5%ad%e5%b0%88%e6%a1%88%e8%aa%bf%e6%9f%a5%e5%a0%b1%e5%91%8a.PDF，2009 年 10 月 12 日。

[164] 通訊保障及監察法行政院提案（民 81.11.30），通訊保障及監察法案(下)「法律案專輯. 第 274 輯, 司法; 24」,立法院司法委員會編輯，P.563，2001 年。

明第二十七條第一項各款事項報告之。」亦即須報告包括：

1.通訊監察書核發機關及文號。

2.案由。

3.監察對象。

4.監察通訊種類及號碼等足資識別之特徵。

5.受監察處所。

6.監察期間及方法。

7.聲請機關。

8.執行機關。

9.建置機關。

10.監察通訊所得內容及有無獲得監察目的之相關資料。

11.其他相關事項及附件。

（二）期末報告

而期末報告乃於該案通訊監察期間結束後之總體報告，依我國通訊保障與監察法施行細則第 30 條規定：「執行機關依本法第七條之通訊監察書爲通訊監察者，應於通訊監察結束或停止後七日內，以書面向綜理國家情報工作機關首長提出報告。」

此條規定亦可在一情報通訊監察案結束後，重新審視該案以該種通訊監察方式是否能正確取得情資，或手段是否有效、得宜，下次案件聲請情報通訊監察時得以作爲參照，亦爲情報機關自我監督之一種機制。

（三）即時報告

除以上期中、期末報告義務外，國家安全局局長依通訊保障與

監察法第 16 條及通訊保障與監察法施行細則第 30 條後段規定，尚得命執行機關為即時報告。

另依我國監察法施行細則第 18 條規定，執行機關於執行通訊監察時，發現有應予扣押之物或有迅速處理之必者者，亦應即報告國家安全局局長，以利情資之即時利用。

上述期中、期末及即時報告義，乃賦予國家安全局局長應就報告內容，判斷該情報通訊監察是否有監察之必要，若在通訊監察期間屆滿前，綜理國家安全局局長認已無監察之必要者，則應依同法第 12 條立即停止監察。此種情報機關自我審查之方式，乃因情報通訊監察在本法中允許的監察期間最長可達一年之久，故經常對已為之監察內容檢視與確認，可減少對隱私過度之侵害以符合比例原則，並避免不必要的通訊監察成本浪費。

二、監察設備執行情形之報告

通訊保障與監察法第 16 條第 2 項規定，情報通訊監察之監督，由綜理國家情報工作機關，派員至建置機關，或使用電子監督設備，監督通訊監察執行情形。偵查中案件，法院得隨時派員監督執行機關執行情形。

除上以報告義務外，情報通訊監察所得資料應加封緘、標識，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 5 年，逾期予以銷毀。若監察通訊所得資料全部與監察目的無關者，執行機關應即報請國家安全局局長許可後銷毀之。[165]

[165]我國通訊保障及監察法第 17 條

一、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，逾期予以銷毀。

二、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法官或綜理國家情報工作機關首長許可後銷毀之。

第八節 小結

爲維護國家安全利益，情報通訊監察須系統地分析與蒐集情報資訊，如軍隊部署、外交政策、恐怖主義等情資，因此我國情報通訊監察法治類似美國FISA，對於境內未設戶籍外國人之境外、跨境、境內通訊得進行審查要件寬鬆之無法院令狀情報通訊監察。

第四章 我國情報通訊監察現存問題研究及未來發展之建議

第一節 獨任法官制審查情報通訊監察之障礙

美國聯邦最高法院於 1948 年 Johnson v. U.S.判例中指出，若簽發令狀者與令狀之簽發具有利害關係時，可能無法以中立超然之地位爲之。依我通訊保障及監察法第 7 條規定，爲避免國家安全遭受危害，而有監察外國勢力、境外敵對勢力或其工作人員在境內、跨境、境外之通訊，以蒐集外國勢力或境外敵對勢力情報之必要者，國家安全局局長得核發通訊監察書。受監察人在境內設有戶籍者，其通訊監察書之核發，應先經國安局該管高等法院專責法官同意。

爲保障人民權益，「通信保障及監察法」規範了法官審查同意制度。情報通訊監察書之核發權歸屬行政體系之國家安全局局長，然同意權自民國 96 年修法後，由最高法院檢察署之檢察官移交予獨立、客觀行使職權之臺灣高等法院法官行使。法官具中立色彩，惟仍有部份因素可能影響法官的審查密度。

第一項 「國家安全」既存之模糊界限

一定程序之概括授權在情報法制體系乃不可避免的必要之惡，但如何認定國家安全遭受危害，在我國通訊保障及監察法中無明確規範，不符立法要求之特定性及規範明確性。

我國通訊監察區分爲「犯罪通訊監察」及「情報通訊監察」。犯罪通訊監察蒐集所得的資訊，通常是用以作爲認定犯罪事實的證據，在審判期日中提出作爲

證明被告之犯罪事實，因犯罪通訊監察係「限定」針對特定重罪案件所為，所侵害者為該案特定人之通訊自由。情報通訊監察中，以破壞國家安全，侵害國家、社會法益為主，監察對象較廣泛且具不特定，不一定會涉及特定的犯罪案件，多為外國人或與外國勢力接觸的本國人，其所得的資訊，則多作為預警、情報分析、危機因應、政策形成或是國防及外交工作之用，因此通訊自由受侵害之人數通常遠比犯罪通訊監察者為多。[166]

定義上情報通訊監察與犯罪通訊監察或許可以清楚的區分，但實際運作上其概念並非容易區分，因情報通訊監察與犯罪通訊監察有極高之同質性。就情報通訊監察中得就影響「國家安全」事項為通訊監察，而犯罪通訊監察中對刑法之重罪包含「內亂」、「外患」等罪亦符合犯罪通訊監察要件，僅偵查之主體多為層級較高之情報機關。若事涉刑法上之內亂、外患罪名者，得否規避犯罪通訊監察中所要求之明確性原則及較嚴密之權利保障，而直接以其行為妨礙「國家安全」為由直接進行程序、要件相對寬鬆之情報通訊監察？

例如，依我國犯罪通訊監察之標準須為最輕本刑為 3 年以上有期徒刑之重罪，若行為人為蒐集我國國防秘密資訊之活動，該行為人乃觸犯我國刑法第 111 條刺探搜集國防秘密罪，為 5 年以下有期徒刑之罪，故依我國現行通訊保障及監察法規定，並不能對行為人施以犯罪通訊監察。此時情報機關是否得以合理的臆測其蒐集資訊行為可能有後續之交付或利用情形，而以妨礙國家安全為由逕行對其施行情報通訊監察？

又例如，洩漏或交付關於中華民國國防應秘密之文書者，依我國刑法第 109 條洩漏交付國防秘密罪，雖其刑度僅為一年以上七年以下有期徒刑，但依我國通訊保障及監察法第 5 條另有列舉得對本條文之犯罪為犯罪通訊監察。此時情報機關是否僅得依規範較為明確嚴密之犯罪通訊監察，而不得因懷疑其洩漏或交付該秘密文書係為最終將交付予外國敵對勢力情報網絡，而對其施以情報通訊監察？

更甚者，如刑法第 104 條通謀喪失領域罪，通謀外國或其派遣之人，意圖使中華民國領域屬於該國或他國者，處死刑或無期徒刑。此等外患重罪又是否適合

[166] 析論我國情報通訊監察法制-以美國法制為比較，李榮耕，2010.10.1.，軍法專刊，107 頁。

僅以犯罪通訊監察爲調查？

此外，是否應防止情報機關以要件較寬鬆之情報通訊監察做爲例行性的犯罪偵察預防呢？

在美國外國情報通訊監察上訴法院In re: Sealed Case判決曾說明，法條中規範要求之外國情報資訊必然包含了如間諜活動、 顛覆活動或恐怖活動，實質上根本不可能將犯罪偵察排除於情報通訊監察之外，若該外國勢力工作人員爲美國人，則實質即爲進行犯罪行爲。由於犯罪通訊監察與情報通訊監察之界線難以區隔，故不論針對犯罪之目的爲多或針對情報蒐集之目的爲多，只要能確定其獲取之資訊爲外國情報者，幾乎皆有獲取外國情報資訊之目的[167]。

所謂「另案監聽」係指偵查機關實施合法監聽時，「意外發現」屬於另案之證據。依最高法院 97 年度台上字第 2633 號判決，「另案監聽」所取得之證據，如若係執行監聽機關自始即僞以「本案監聽」之罪名而聲請核發通訊監察書，於其監聽過程中發現另案之證據者，因該監聽自始即不符正當法律程序，且執行機關惡性重大，則其所取得之監聽資料及所衍生之證據應予絕對排除，不得作爲另案之證據使用；倘若屬於本案依法定程序爲監聽中偶然獲得者，得爲另案證據[168]。在犯罪通訊監察中，倘若「另案監聽」亦屬於通訊保障及監察法第 5 條第 1 項規定得受監察之犯罪，或雖非該條項所列舉之犯罪，但與本案即通訊監察書所記載之罪名有關聯性者，自應容許將該「另案監聽」所偶獲之資料作爲另案證據使用。

而情報通訊監察常令人擔心的便是以常態性的「本案」情報通訊監察，作爲「另案」犯罪偵查之手段。依通訊保障及監察法第 10 條規定，情報通訊監察所得資料中發現得爲犯罪通訊監察之重大犯罪而將資料移送司法機關。然此在情報

---

167 In re: Sealed Case No. 02-001, 310 F.3d 717 (FISCR 2002). ,Foreign Intelligence Surveillance Court of Review ，…Moreover, the court found that the USA PATRIOT Act allows the government to conduct wiretaps and searches of U.S. citizens and to share these results with prosecutors. The only requirement under the act is that the government must allege that a significant purpose in the investigation is to gather foreign intelligence information. ， http://legal-dictionary.thefreedictionary.com/Foreign+Intelligence+Surveillance+Court+of+Review

168 楊雲驊，另案監聽—評最高法院 97 年台上字第 2633 號判決，台灣法學第 116 期，頁 170-173，2008 年 11 月 15 日。

通訊監察中，若依美國外國情報通訊監察上訴法院 In re: Sealed Case 判決之見解，似乎難以主張執行監聽機關自始即僞以「本案」監聽（情報通訊監察）之罪名而聲請核發通訊監察書，以發現「另案」犯罪證據，因犯罪通訊監察與情報通訊監察之界線難以區隔。

其實情報通訊監察之本質在於就可疑處蒐集國家安全預警情報，而「國家安全」亦不如刑法犯罪一般有清楚的構成犯罪要件，原本即爲較具抽象性質之詞彙而使情報機關擁有彈性較大的運用空間，此種情況在美國的 FISA 與德國的 G10 法雖無不同，但皆有略加限縮其要件範圍。

依美國 FISA 得對「危害美國國家安全」之外國勢力及外國勢力工作人員通訊進行情報通訊監察，「外國勢力」須爲非美國人之政治實體，先排除美國人以障具美國國籍之人民權利不受國家以觀念上較模糊之「國家安全」概念爲侵害；其次「外國勢力工作人員」則不區分國籍，但若是美國人，則須限於「有相當理由可信」其從事刑法上犯罪行爲或從事顛覆、恐怖活動、代表外國勢力使用虛僞身份時，方可認定其爲外國勢力之工作人員，雖仍有抽象的空間，但已被稍稍作限縮。

在德國G10 法在個案情報通訊監察中，列舉了刑法中等法律中得爲情報通訊監察之犯罪，如危害和平及內亂罪、危害民主法治國家罪、叛國或對國家安全之危害罪、危害國防罪等，係針對與國家安全有關之刑法犯罪等爲通訊監察，而刑法等法律已就個該犯罪定有其犯罪要件，審查其要件尚可稱明確，且明確賦予情報機關以調查與國家安全有關之刑法犯罪得依個案情報通訊監察之手段爲之，不受限於犯罪通訊監察，其立法方式亦堪稱較爲細膩。在戰略情報通訊監察中，亦列舉得爲蒐情之國家安全要項，如爲及時察覺、防止對德國的武力攻擊、國際恐怖攻擊、國際武器擴散、重要非法跨國交易、大量毒品攜入、僞造貨幣、重大國際洗錢、重大組織性國際走私活動，其監察者非爲法律所訂犯罪行爲，雖要件較有模糊空間，惟仍訂有明確方向。且德國G10 法對於通訊監察要件，除爲維護德國聯邦之安全存續爲前提外，更需有事實根據（tatsächliche anhaltspunkte）足認某人涉嫌計畫、實行或完成相關犯罪之嫌疑，始可爲通訊監察，在戰略性情報通訊

監察中，亦須爲及時察覺上述特定犯罪之危險而蒐集必要之資訊。[169]

除了美國 FISA 在要件上之限縮，與德國 G10 法除限縮要件外立法直接賦予情報機關得就刑法上國家安全相關罪行進行情報通訊監察之權力，終究，「國家安全」性質上本就無法與犯罪明確切割，能做到的僅是使其形式上立法使其合理、合法，及實質上的加強要件限縮減少侵害人民權益。

上述的提問，在觸犯我國刑法第 111 條刺探搜集國防秘密罪、第 109 條洩漏交付國防秘密罪、第 104 條通謀喪失領域罪等，是否對國家安全之造成危害，須以其他要件限制，例如是否「有事實或有相當理由足認」其行爲係爲交付予敵對勢力，或進而列舉就刑法犯罪中得爲情報通訊監察之條文，以避免對「國家安全」不必要之濫用。

然上述之建議，僅能在情報通訊監察上「國家安全」之定義及「合理確信」爲最初步的限縮，故既然「國家安全」之本質存有模糊空間，故應就另從審查機關著手，即對審查是否符合「國家安全」而進行情報通訊監察之同意機關，是否具有中立、是否有完善之組織，及是否賦予其權能使其得進行實質審查相關事項。

第二項　審查之要件空泛

依通訊保障及監察法第 2 條規定，不論情報通訊監察或犯罪通訊監察，除爲確保國家安全、維持社會秩序所必要者外，不得爲之（適合性）。且不得逾越所欲達成目的之必要限度（狹義比例原則），且應以侵害最少之適當方法（必要性）爲之。故當高等法院行使同意權時，除須就聲請書狀記載之客觀形式要件爲審查，如被監察人是否爲外國勢力、境外敵對勢力或其工作人員等，另外亦應一併確認是否符合通訊保障及監察法第 2 條所述比例原則之實質要件。

---

[169] 周治平，情報機關通訊監察權之研究—德國法之啟示，警大法學論集第 15 期，頁 287，2008 年 10 月。

究竟何爲通訊保障及監察法第 7 條所謂「爲避免國家安全遭受危害」而有蒐集其情報之必要？第 2 條「爲確保國家安全所必要者」、「不得逾越所欲達成目的之必要限度」及「以侵害最少之適當方法爲之」之衡量標準何在？

依我國通訊保障及監察法規範，情報機關對我國境內設有戶籍者進行情報通訊監察前，由國家安全局局長核發通訊監察書，但須由高等法院專任法官進行同意。該同意權之性質爲何？法院究竟有無實質審核權限？然該審核權是否僅審核形式上之要件，或能否爲實質要件審查？

基於強制處分之事前審查權限，爲保護我國國民權益，如同羈押、搜索票之核發、或犯罪通訊監察須由檢察官提出聲請並由法官核發通訊監察書一般，其審查權已回歸處於中立第三人地位之法官，故依相同法理，通訊保障及監察法明文規定，情報通訊監察須先由法院行使同意權後，再由國家安全局局長核發通訊監察書，故應解釋爲法院行使之同意權應以中立之身份，就其聲請爲實質審查，賦予法院對國家情報機關進行情報工作時監督節制，避免情報機關爲偵查國家安全事項而陷入單向思考之危險，始符合法治原則。

法院就通訊監察之令狀審查程序，應審查其發動通訊監察有無合理根據（probable cause），此乃合法性的核心問題，「合理根據」具體內涵，可以細分爲三，同時具備始合乎合理根據之通訊監察門檻，始能發動通訊監察[170]：

1. 存在犯罪或安全顧慮嫌疑之合理根據（爲何認爲存有嫌疑）
2. 存有通訊監察標的之合理根據（爲何認爲存有應受通訊監察之人）
3. 存於通訊監察範圍之合理根據（爲何認爲應受通訊監察之物爲該人所擁有）

上述之「合理根據」之審查要件對犯罪通訊監察可爲較明確之審查，惟在情報通訊監察中，基於「國家安全」界限之模糊，對是否存有安全顧慮嫌疑之合理根據似難依上述審查標準，且對「國家安全」情資之蒐整如何能符合最小侵害原則，在本法亦未有明確定義，使高等法院在審查情報通訊監察同意與否時確有

[170] 林鈺雄，刑事訴訟法上，頁 337-338，2001 年。

其限制。

第三項　建議修正核發情報通訊監察書之組織

通訊保障及監察法對於在我國境本設有戶籍之人民爲情報通訊監察之最終同意機關爲具中立性之高等法院獨任法官，然而參考美國 FISA 規範則是以另行成立專責之外國情報通訊監察法院合議爲之，並設有上訴法院，法官選任規定亦相當明確規範於 FISA 法規中，相較於我國僅規範須由高等法院「專責」獨任法官爲之，其在核發通訊監察之組織上似比我國更爲謹慎。

另在德國 G10 法之情報通訊監察則以設於聯邦議會監察委員會下之獨立機關 G10 委員會爲獨立審查機關。此乃德國專家參審制度之實現，因國家安全情報事項確有其相當之專業性，然爲防止濫權又不宜交由情報機關自爲決定，故設立一獨立之合議審查機構，可透由政黨依比例選任法律專家等 8 人組成 G10 委員會，委員們具有準司法權之監督調查功能，得對相關機關爲詢問、調查，閱監資料等以進行實質審查，爲一專業並兼具代表人民爲監督之中立機關，更客觀、有效且經常性地控制情報通訊監察。

因此，我國情報通訊監察書之同意權行使機關，除可考量採外國立法例，法院改採合議制審查使審查之組織更爲謹慎，亦可考慮設立由專家組成（包括具法官身份者）、具準司法色彩之獨立機關，對情報通訊監察進行實質審核，以善盡審查之功能。

第二節　情報通訊監察之事後救濟

通訊監察是在受監察者不知不覺狀況下進行的干預措施，有別於諸如拘提、逮捕、羈押、搜索、扣押等傳統型態的干預處分，正因不知不覺的特

性，所以受監察者事先、事中皆無法防範，即便事先採行法官保留原則，也難以完全取代事後權利救濟的必要性。換言之，事後有無請求法院救濟的可能，成爲監察措施能否有效控制的最後一道防線，但我國通訊保障及監察法未規劃事後指摘違法監察之法院救濟途徑。[171]

亦即，我國通訊保障及監察法中，對「違法通訊監察」之責任規範相當縝密，在違法情報通訊監察行爲將涉及通訊保障及監察法第 19 至 31 條包括民事損害賠償責任、國家賠償責任或刑事責任等，惟對於符合形式要件而有「形式上合法」之情報通訊監察，即對我國境內設有戶籍人民爲情報通訊監察，若形式上由國家安全局局長核准通訊監察，亦由高等法院法官同意，程序正當後，是否得就其核發情報通訊監察書之「實質正當性」由事後法院加以審查，而確認原本執行之通訊監察爲違法繼而可能請求證據排除或國家賠償？

在犯罪通訊監察中，法官在核發通訊監察書時未依法定原則加以審核，例如非法條所列重罪案件亦予核發通訊監察書，縱以形式上合法之通訊監察書執行通訊監察，亦屬違法通訊監察無疑[172]。唯情報通訊監察，要判斷其實質審核是否符合較抽象之必要性、最小侵害、比例原則等，非同犯罪通訊監察般明確。

首先，要探求事後救濟形式，須先確認核發情報通訊監察書之性質爲何。依通訊保障及監察法第 7 條規定，受監察人在境內設有戶籍者，通訊監察係由法院行使同意權後，再由國家安全局局長核發通訊監察書。若認爲國家安全局局長乃實際核發人而核發通訊監察書之行爲爲行政上之事實行爲[173]，則應爲行政訴訟中的確認公法上法律關係不成立之訴訟；然參照民國 96 年修法意旨將同意權由檢方轉至法院以確保憲法正當程序之要求，可見法院同意權乃執行情報通訊監察最後實質決定程序，不應拘泥於核發與同意之用

---

171 林鈺雄，論通訊之監察—評析歐洲人權法院相關裁判之發展與影響，東吳法律學報十九卷第四期，頁 146，2008 年 4 月。

172 徐智明，通訊監察之保障及規範，國立中正大學法學研究所碩士論文，頁 102，民國 93 年 6 月。

173 臺北高等行政法院 95 年度訴字第 04088 號裁定，2007 年 12 月 31 日。

語，該法院之裁定應以地方法院爲事後救濟之審查法院，類似如美國FISA 50 USC § 1806(f)亦以地方法院爲事後審查。

我國情報通訊監察案件於通知當事人後，當事人提出救濟者，目前僅有主張通訊監察不當而提出國家賠償訴訟數件，尚無在刑事訴訟程序中主張不得採爲證據之案件，本節將探討相關內容。

某週刊記者於 97 年間受情報通訊監察近一年時間，經受高院通知後，該記者以情報通訊監察不當而向臺灣臺北地方法院提出國家賠償之訴訟。地方法院作出民事判決 100 年度國字第 39 號判決表示，高等法院同意核發通訊監察書後，應認高等法院在同意核發時已對其必要性、比例原則等進行實質審查，故若其他形式要件具備，原告又未指稱或提出證據證明有足以影響同意機關決定之情事存在，應認被告本件聲請高等法院專責法官同意核發之通訊監察書應已符合通保法規定之要件。

關於強制處分之監督，基本上有分成兩大方向，一爲從證據禁止法則著手，亦即禁止使用因爲違法強制處分所得的證據；二是從強制處分本身的設計著手，也就是設定強制處分事前以及事後的審查機制。

我國通訊保障及監察法第 7 條第 4 項對違法通訊監察所取得之內容或所衍生之證據，於司法偵查、審判或其他程序中均不得採爲證據，爲證據禁用法則。而對於通訊監察之事前審查機制，目前採法官保留原則，雖審查密度較低，但仍不失其中立性。惟在事後審查救濟機制之規範顯有欠缺。

事後審查機制是指於強制處分決定後並執行中或執行後由某個國家機關來審查強制處分之決定與執行是否合法，或者容許受處分之關係人對強制處分之合法性問題提起救濟。關於強制處分之事後審查，我國目前僅有抗告制度容許撤銷或變更違法或不當之強制處分，[174]然我國刑事訴訟法對羈押、搜索等強制處分可適用抗告之制度以救濟對原法院裁定不服[175]，但卻未將通

[174] 林鈺雄，刑事訴訟法上冊，頁 260-262，2001 年。

[175] 刑事訴訟法第 404 條：對於判決前關於管轄或訴訟程序之裁定，不得抗告。但下列裁定，不在此限：一、有得抗告之明文規定者。二、關於羈押、具保、責付、限制住居、搜索、扣押或扣押物發還、因鑑定將被告送入醫院或其他處所之裁定及依第一百零五條第三項、第四項

訊監察明定爲得救濟之措施，造成僅救濟小干預而不救濟大干預的顛倒現象[176]。

相較於德國法制，德國刑事訴訟法上所有干預人民基本權利之強制處分，原則上皆得提起法律救濟，即便已經終結之強制處分，只要有確認利益，亦得請求法院確認該處分之違法性，即可就確認強制處分違法進行確認之訴。在德國，爲增加對強制處份之救濟途徑，德國法創「刑事訴訟法的確認訴訟」，於刑事程序引進如行政訴訟的確認之訴（確認已經終結之行政處分違法），讓法院可以用事後審查的方法，確認已終結之強制處分「違法」，其確認利益即在於其確認其違法後可排除其證據能力及將來得提出之國家賠償責任。[177]然司法監督在秘密情報領域，實屬於低密度審查範疇[178]，因情報手段之秘密性，人民無法知悉詳細的蒐情行爲，以及找出侵害之機關，另也擔心訴訟後，將再次向法院公開其私領域事務，因此實際上能提起行政救濟之情形甚少，是以事前監督機制更顯其重要性。[179]

第一項　美國 United States v. Holy Land Foundation for Relief and Development案

由於美國FISA第 50 U.S.C.§1806(f)賦予地方初審法院得判斷原實行之外國情報通訊監察是否合法之權，在美國 2011 年United States v. Holy Land Foundation for Relief and Development案[180]中，被告對原FISA法院核發之情報通訊監案書是否合FISA所規範之要件有所疑義，主張其核發未具相當理由（probable cause）認其外國勢力之工作人員，故在地方初審法院受審判時，

所為之禁止或扣押之裁定。三、對於限制辯護人與被告接見或互通書信之裁定。

176 林鈺雄，論通訊之監察—評析歐洲人權法院相關裁判之發展與影響，東吳法律學報十九卷第四期，頁 146，2008 年 4 月。

177 林源湧，違法搜索之救濟，政治大學法學院碩士論文，頁 91-92，2007 年。

178 Schlink, a. a. O.(Fn.14), S.553.

179 周治平，情報機關秘密情報蒐集之法律問題，東吳法研論集第 5 集，頁 156，2009 年 12 月。

180 United States v. Holy Land Foundation for Relief and Development, No.09-10875, 664 F.3d 467, 2011 U.S. App. LEXIS 24216, (5th Cir. 2011)

依FISA第 1806(f)向地方初審法院主張其通訊監察不合法，並主張應依「法蘭克斯審訊（Franks hearing）」原則開啓一證據審訊程序，給予其機會挑戰核發法院令狀之依據內容真實性[181]。

一、 法蘭克斯審訊

在瞭解United States v. Holy Land Foundation for Relief and Development案前，須先說明何謂「法蘭克斯審訊（Franks hearing）」。「法蘭克斯審訊」係指被告有權開啓一證據審訊程序，決定警方爲取得搜索票獲得犯罪證據所提供之宣誓書，是否係基於警方虛僞之陳述。「法蘭克斯審訊」一詞來自Franks v. Delaware[182]案，其判決肯認被告有權去挑戰法院令狀同意搜索人、文件或其他對其不利之事務。該案法院判決肯認在某些特定情況下，被告有權挑戰具形式上合法宣誓書（a facially sufficient affidavit)之法院令狀。若要取得這個確認宣誓書正當性之證據審訊程序，必需釋明：

2. 被告釋明其聲請搜索票之宣誓書中口供有故意虛僞之陳述，或有重大過失罔顧真實之情況，且須附上相關證據之細節。
3. 被告須顯示該錯誤的資訊爲主要影響是否具「相當可能」（probable cause）之判斷。若法院發現排除該錯誤陳述後，宣誓書仍有其他足夠的內容支撐法院令狀判斷其具「相當可能」者，則不須爲該審訊程序。

被告若對上述兩部份爲釋明，則獲得舉行審訊程序之資格。在此審訊程序中，被告有義務證明其主張有證據優勢（即可能多於不可能）。若經審

---

[181] United States v. Holy Land Foundation for Relief and Development, No.09-10875,…2. Suppression of FISA intercepts…. Second, they contend that the Government failed to establish probable cause that the target of the FISA warrant was "a foreign power or an agent of a foreign power." Finally, the defendants contend that the district court should have granted them an evidentiary hearing under Franks v. Delaware, 438 U.S. 154, 98 S. Ct. 2674, 57 L. Ed. 2d 667 (1978), at which they could challenge the veracity of the information in the FISA warrant applications.(2011).

[182] Franks v. Delaware, 438 U.S. 154 (1978).

訊程序認爲被告有證據優勢，則該令狀必須被廢除（voided），其所得之證據或證言亦將被排除。[183]

回到United States v. Holy Land Foundation for Relief and Development案中，美國聯邦上訴法院第五巡迴審判庭做出判決[184]，認爲：

1. 外國情報通訊監察法院秘密審理 FISA 聲請案時，聲請者提供許多機密的資訊以獲得 FISA 法院令狀之核發，我們認爲政府已達具「相當理由」（probable cause）的要求，包括相信監察目標爲外國勢力之工作人員、被監視處所爲外國勢力之工作人員所用。
2. 被告也未能出示爲得爲「法蘭克斯審訊」的依據。在Franks v.

[183] Franks hearing law and legal definition, http://definitions.uslegal.com/f/franks-hearing/, 最後參照日期 2012 年 2 月 2 日。

[184] United States v. Holy Land Foundation for Relief and Development, No.09-10875,…Similarly, we reject the defendants' argument that the FISA warrant applications did not establish the requisite probable cause in this case. Upon careful *in camera* review of the challenged FISA orders and applications, and the classified materials in support of the applications, we conclude that the Government demonstrated the requirements for probable cause, including the belief that the targets of the surveillance were agents of a foreign power and that the place of surveillance was being used, or was about to be used, by an agent of a foreign power. *See* 50 U.S.C. § 1804(a)(3).
For the same reasons, the defendants have also failed to show a basis for a Franks hearing. A defendant, upon a proper preliminary showing, may obtain an evidentiary hearing to challenge the truthfulness of statements made in an affidavit supporting a warrant. Franks, 438 U.S. at 155-56. A defendant is entitled to a Franks hearing if he shows "that (1) allegations in a supporting affidavit were deliberate falsehoods or made with a reckless disregard for the truth, and (2) the remaining portion of the affidavit is not sufficient to support a finding of probable cause." United States v. Brown, 298 F.3d 392, 395 (5th Cir. 2002). We find no basis to conclude that the statements relied upon by the defendants were made with reckless disregard for the truth. Nor do we find that the statements were necessary to the finding of probable cause. We agree with the district court's conclusion that probable cause was satisfied even absent the erroneous statements. We therefore affirm the district court's denial of the suppression motion.(2011)

Delaware[185]判決中指出，被告若釋明宣誓爲虛僞之證據，則可獲得一個證據審訊程序以挑戰令狀核發依據之宣誓其陳述真實性。在United States v. Brown[186]案中，被告得爲「法蘭克斯審訊」若其（1）主張宣誓書有故意說謊(deliberate falsehoods)的事實或有重大過失罔顧真實(a reckless disregard for the truth)，且（2）宣誓書的其餘部分無法足以支持發現「相當理由」。惟在本案中並未發現任何基礎事實可認聲請者的陳述有重大過失罔顧真實。我們同意地院的結論，就算除去錯誤陳述的部份，其他陳述仍使法院相信具「相當理由」得爲核發FISA令狀。因此，我們肯定地院拒絕證據禁用。

依據該案判決可得知，美國法院得爲審查FISA令狀之是否符合50 U.S.C. § 1801 以下有關外國情報通訊監察條文中「適當性」之要件，惟若要挑戰外國情報通訊監察法院所核發之令狀，然而若未出示足夠的證據釋明其有權得開啓法蘭克審訊，則其提交予法院之陳述與所出示之證明支持其聲請FISA令狀，應被上級審法院推定爲有效的。

二、 保證書制度

執行通訊監察之合法性與正當性，部分來自於明確規範聲請通訊監察人員之責任。法院係就情報機關所檢送之基礎事實爲最重要之審核依據，亦爲同意進行情報通訊監察之心證基礎。

此制度乃參照美國法官對於美國司法警察聲請搜索票（一般犯罪通訊監察亦屬於搜索之範圍），爲確保所提供之資料係屬正確，必須在治安法官面前宣示並以本人名義提出「保證書」（affidavit），除宣誓所述爲真外，另須記載下列事項以保證其書面及口頭說明均有事實根據。

1. 聲請人本身觀察之「具體事實」：其敘述必須是基於其本人觀察之

185 Franks v. Delaware, 438 U.S. 155-56 (1978)

186 United States v. Brown, 298 F.3d 392, 395 (5th Cir. 2002)

具體事實，例如「我於何時以臥底探身分進入甲住處客廳後看到白色粉末，依我所信該粉末應爲毒品。」而非僅是結論如「依我多日觀察結果，甲應有販賣毒品之犯行。」

2. 轉述線民之觀察：須轉述同上之具體事實且須說明該線民何以得知該消息，及該線民之可信度。

若上述記載涉有不實陳述，來日將須負僞證罪之刑責，故法官在進行審核時，一般均假設警察之說明爲真實，再以該等事實做基礎，以審核是否有合理依據。[187]

美國FISA亦規範了相關宣誓及保證書制度，目的在於要求偵查機關對其聲請通訊監察之行爲負責，不得發生虛僞或不實聲請之情事[188]。參照美國FISA行政機關聲請爲外國情報通訊監察時，聲請書上須記載實際提出聲請的聯邦官員之人別資料，聲請人須對其所依據之事實與情狀予以陳述。若由國家安全行政官員提出之聲請須另具保證書（Certification），擔保「該官員認爲所截取之資料爲外國情報資料」、及「該資料不能以一般調查方式取得等事實情狀」等，以上措施皆爲使聲請機關負起擔保其說明之確實性，送出聲請書尚須經檢察總長審查批准後始送至FISA法院，日後若發現有虛僞情事，可釐清相關公務員責任歸屬。

第二項　我國事後救濟相關判決

一、臺灣高等法院民事 99 年度上國字第 15 號判決

除本節初提到的地院判決外，以下討論另案已受三審判決確定較爲完整案件。某週刊記者於民國 91 年至 93 年間連續分別依 3 次通訊監察書受情報通訊 2 年，該記者向法院主張其通訊監察書之 3 次核發不符比例性、必要性原則並請求國家賠償。

---

187 林鈺雄，刑事訴訟法上，頁 339，2001 年。

188 曾正一，台美通訊監察制度之比較研究，釋字 631 號解釋與監聽法制評析學術研討會論文集，頁 58，2008 年。

該案臺灣高等法院民事判決 99 年度上國字第 15 號相關主要意旨如下：

1. 最高法院檢察署檢察官依聲請機關聲請同意時聲請意旨、釋明事證審核後爲同意之表示後，除有特別情事（如聲請機關或所屬人員有刑事犯罪情形），致影響同意機關之決定者外，應非得由民事法院事後另行就最高法院檢察署檢察官同意之當否再爲審查。

2. 被上訴人聲請最高檢檢察官同意核發系爭通訊監察書時，最高檢檢察官自係實質審核[189]，而非形式審核，亦非備查。與通保法規定之法定程序無違，應認被上訴人核發三次通訊監察書監聽上訴人，符合通保法之法定要件。

3. 已依法定程序經最高法院檢察署檢察官或高等法院專責法官所爲之同意所爲通訊監察，解釋上即非通保法第 24 條第 1 項規定之「違法監察他人通訊」，亦非同法第 19 條第 1 項規定之「違反本法或其他法律之規定監察他人通訊」。上訴人自不得事後以通訊監察無結果或其他情事，要求民事法院審核系爭通訊監察是否符合實質要件。

4. 被上訴人依法定程序對上訴人所爲通訊監察，並無違反通保法及其他法律之規定。且系爭通訊監察書之核發，是否符合法定要件、比例原則、必要原則等，係由最高檢檢察官審核，制度設計上，非由民事法院就被上訴人核發通訊監察書是否符合法定要件審查。故本院就被上訴人連續核發三次通訊監察書，是否符合必要性原則及比例原則等實質要件，自毋庸併予審究。

該案於上訴最高法院後受裁定駁回[190]，並再次確認最高法院檢察署檢察官依聲請機關聲請意旨、釋明事證，審核後爲同意之表示，除有特別情事（如聲請機關或所屬人員有刑事犯罪情形），致影響同意機關之決定者外，應非

[189] 96 年 7 月 1 日修正前通保法第七條第二項既已規定是否符合通訊監察要件之司法審查，專屬最高法院檢察署檢察官。

[190] 最高法院民事裁定 100 年度台上字第 2184 號，100 年 12 月 21 日。

得由民事法院事後另行就最高法院檢察署檢察官同意之當否再爲審查。

二、比較 United States v. Holy Land Foundation for Relief and Development 案

比較本案法院意見與上述美國 United States v. Holy Land Foundation for Relief and Development 案，可發現法院原則上皆推定原核發通訊監察書爲有效合法，在美國「除有得開啓法蘭克斯審訊之發動要件」，或在我國「除有發現聲請機關或所屬人員有刑事犯罪情形」。而所謂「聲請機關或所屬人員有刑事犯罪情形」者，應指如聲請人員僞證罪等。

然在刑事訴訟制度上要舉證其爲僞證等犯罪行爲時，除非在被通訊監察人受通知時，其通知書有詳細記載其通訊監察之聲請人、受通訊監察之監察理由，包括所涉案件、不能或難以其他方法蒐集調查證據之具體理由等[191]，否則在我國缺乏如美國「宣誓書」制度要求特定人員詳述相關事由並予以作證之制度[192]，受監察人不但訴訟對象不明，且實際上亦難以舉證，未來應可考慮賦予聲請通訊監察人具結義務以保障人權[193]。

另本案高等法院民事 99 年度上國字第 15 號判決中要求若要主張原情報通訊監察書不合法，須舉證聲請機關或所屬人員有刑事犯罪行爲，參照美國法蘭克斯審訊之原則，並考量情報通訊監察案件當事人確有其舉證之困難，若將該舉證降爲如本節最初所提及之臺灣臺北地方法院 100 年度國字第 39 號民事判決中「提出證據證明有足以影響同意機關決定之情事存在」似乎較爲合理。

然須注意的是，雖然在United States v. Holy Land Foundation for Relief and Development案認爲若被告有提示相關事證則有可能獲得重新審查FISA核發

---

191 依據通訊保障及監察法施行細則第 27 條要求法院審查後通知受監察人之內容僅包括一、通訊監察書核發機關及文號 二、案由 三、監察對象 四、監察通訊種類及號碼等足資識別之特徵 五、受監察處所 六、監察期間及方法 七、聲請機關 八、執行機關 九、有無獲得監察目的之通訊資料，上述資訊實難為相關舉證。

192 陳瑞仁，如何由法制面提升警察辦案品質，月旦法學，第 56 期，頁 58，2000 年 10 月。

193 王兆鵬，刑事訴訟講義（一），頁 85，2003 年。

令狀之合法性，惟依 1982 年哥倫比亞上訴法院曾作出之判決[194]，在重新審查外國情報通訊監察之合法性時，若檢察總長出示證明出表示公開審訊或揭露資訊將有害國家安全時，則其過程法院得爲一造秘審審查，因外國情報有其較複雜細緻之處，並非皆可爲公開審訊。

此外，由 United States v. Holy Land Foundation for Relief and Development 案可看出美國 FISA 保證書制度加重了行政機關及其人員之責任，司法機關係就行政機關所呈資訊爲獨立判斷，行政機關提供資訊正確與否是影響法官審查之重要依據，且我國通訊保障及監察法對具我國籍人民爲情報通訊監察之期間最長可達一年，故在討論事後司法審查機制時，亦一併著重強化我國行政機關事前之證明責任，及事後情報監督責任，相關論述於下一節中討論。

第三節　強化情報通訊監察之行政、國會、司法監督

第一項　強化行政機關責任

一、強化情報機關提出情報通訊監察之自我節制或聲請程序

情報機關提出情報通訊監察聲請時，除上述司法審查機制外，應再強化行政機關之自我審查責任，由情報機關自我節制。

依情報通訊保障及監察法規範，對具我國國籍人民之情報通訊監察時，因事涉國人基本權之侵害，故由法院作爲最後審核同意之機關，惟國家安全一辭抽象模糊，故在行使同意權時自有其限制。此時，應加強前階

194 United States of America v. David Belfield, Aka Daoud Salahuddin Ali Abdul-Mani, Aka Lee Curtis Manning, Appellant; United States of America v. David Belfield, Aka Daoud Salahuddin Horace Anthony Butler, Aka Ahmed Rauf, Appellant, Nos.81-2152,81-2155. United States Court Of Appeals For the District Of Columbia Circuit, 1982.11.5.

段情報機關責任，由情報機關就國家安全保障部份提出具情報專業判斷，及正確無誤之說明，並提出充份證明，法院始能依其資訊實質審核，決定是否同意該情報通訊監察。情報機關所提出之資訊應儘量提供明確之事證以利法官判斷，不得僅以列舉法條即為聲請，若提出不確定法律概念時，行政機關必須擔保其涵攝判斷正確[195]，因為行政機關判斷錯誤可能導致司法判斷之不當。

執行通訊監察之合法性與正當性，部分來自於明確規範聲請通訊監察人員之責任。法院係就情報機關所檢送之基礎事實為最重要之審核依據，亦為同意進行情報通訊監察之心證基礎。

依據本文前節所述，參照美國 FISA 行政機關聲請為情報通訊監察時，聲請書上須記載實際提出聲請的聯邦官員之人別資料，國家安全行政官員提出之聲請須另具保證書（Certification），擔保該官員認為所截取之資料為外國情報資料、及該資料不能以一般調查方式取得等。該制度係使聲請機關負起擔保其說明之確實性，日後若發現有虛偽情事，可明確釐清公務員責任歸屬，亦可使聲請為情報通訊監察時更為嚴謹。

且美國 FISA 在行政官員提出外國情國通訊監察之聲請後，尚須經檢察總長之審核後始能送至 FISA 法院，故檢察總長在該制度下的角色便如前述加強行政機關之「自我節制」功能，在第一道關口先為把關後，再送至 FISA 法院核可，非如同國內係由高等法院法官同意後由情報體系之國家安全局核發。

二、情報機關之事後監督責任

獲得法院審核同意而核發之情報通訊監察書後，目前專由情報機關就執行情報通訊監察事項負事後監督責任。通訊保障及監察法第 16 條賦予國家安全局局長對通訊監察可要求執行機關進行期中、期末、即時報告進行監督。

[195] 李惠宗，行政法院裁判系列研究（十）行政法院有關不確定法律概念判斷之審查，96年度國科會研究計畫精簡報告，2007年。

預測的越遠，其準確度必將減少。我國有令狀情報通訊監察時間單次聲請可長達一年，相較美國若依 FISA 對美國人進行之情報通訊監察期限爲 90 日，通訊監察期間顯然長很多，對國人之隱私權侵害亦較大。依現行規範，若情報通訊監察聲請時皆已具備相關法定要件，仍需有賴國家安全局局長（或未來修法授權於法院或其他中立機關）依通訊保障及監察法第 16 條規定，於執行機關按月向其報告執行情形時，就其已獲之資訊，審查是否仍有繼續監察之必要。若所得資訊明顯與監察目的顯然無關，則應依通訊保障及監察法第 12 條第 3 項之規定，於通訊監察期間屆滿前認已無監察必要者即停止監察，以限縮隱私權之侵害之範圍，使經法院同意所爲之情報通訊監察，在後續通訊監察中更能符合比例原則。

第二項　強化司法於通訊監察中之監督角色

一、 執行機關對司法機關之報告義務

依前節所述，目前在獲得情報通訊監察書而執行情報通訊監察之後，法院除得審核暫不通知受監察人之聲請是否合宜外，其他事後監督責任專屬情報機關。通訊保障及監察法第 16 條賦予國家安全局局長對通訊監察可要求執行機關進行期中、期末、即時報告進行監督，惟執行機關對法院則無報告義務。情報通訊監察執行前乃先經法官審查同意後，故若法院對執行後之各階段若亦能定期負監督之責，對同意監聽之裁定爲指揮執行，可避免情報機關單向思考之弊。

參考美國FISA規範 50 U.S.C.§1805 (d) (3)法院之權限不僅存在於核發外國情報通訊監察書時，在通訊監察期間結束前，法官對於蒐獲關於美國人之情資是否得使用、保留或傳遞，得對其情狀重新爲評估，確認其是否

符合最小侵害原則。[196]

由於我國情報通訊監察單次聲請最長可達一年，若賦予執行機關於期中每月定期向法院報告執行情形，當發現有明顯不必要之通訊監察時即可即時終止監察，中立之審查可確保情報通訊監察符合比例原則及最小侵害原則。

二、 司法機關年度統計數據

司法院自 96 年 12 月 11 日起修正通訊保障及監察法將偵查中案件通訊監察書改由法官核發，對本國籍人民為情報通訊監察書之同意核發權改由高等法院專責法官審查後，雖通訊保障與監察法中未規範，但司法院仍將通訊監察相關統計資料與其他司法統計數據一併揭露於年度司法統計年報中，並公開於司法院網站。[197]

通知比率數據為監督情報通訊監察是否浮濫最重要之數據，因受通知者於通知後可知悉被監察事宜進而主張其權利，未受通知者則無法知曉其權力受侵害。然而司法院統計年報中，通知比率數目卻未針對情報通訊監察與犯罪通訊監察加以區隔，以致無法明確得到數據並加以分析比較，僅能從高等法院之通知率略為比較，因情報通訊監察由高等法院行使同意權，然仍摻雜犯罪通訊監察，建議相關數據皆能區隔情報通訊監察與犯罪通訊監察。但參考高等法院之案件通知率遠低於地方法院之通知率，此現象應予觀注。

另在過去較受眾人注意之數據為通訊監察之核可率，自民國 96 年修法改由法官為通訊監察之核可後，獨立行使職權之法官核發之通訊監察書應較客觀，故核准率之參考重要性略減。國內司法院統計數據並未公布情

---

[196] 50 U.S.C. § 1805 (d) (3) At or before the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

[197] 中華民國 99 年司法統計年報，司法院，2010 年，http://www.judicial.gov.tw/juds/year99/contents_table_ch.htm

報通訊監察核准率，參考美國FISA因加重情報機關聲請時之證明責任，情報機關送出聲請書尚須經檢察總長批准，多一道檢審程序先爲審查要否符合相關要件，聲請書始送至FISA法院，且在FISA施行多年來法治概念修正形塑下，使法院核可率幾乎高達 99%[198]。惟我國尚未有較明確證明責任，且在聲請案送高等法院同意爲情報通訊監察前不須如美國FISA規範先經檢察總長核閱，使情報機關提出聲請案時仍有可能陷入單向思考之盲點，故仍使人民對通訊監察之核可率有所要求。

相較之下，情報通訊監察年度核准件數數量增減之比較，反而更具指標性之意義。年度情報通訊監察數量之增減可比較情報通訊監察之發展係擴張或限縮。美國FISA統計數據可看出，自 1978 年立法以來，其聲請案件數量逐漸攀升，至 911 事件後更是迅速成長，至 2008 年國會再次修正限縮相關FISA及愛國者法案後，其聲請數量才又大幅減少。[199]我國情報通訊監察自民國 96 年改由高等法院法官審查後，亦逐年降低情報通訊監察聲請件數。[200]

此外，犯罪通訊監察得以「是否自該通訊監察中獲得相關犯罪證據」、是否起訴或是否判決有罪，爲事後檢討核發是否符合比例原則，情報通訊監察亦應可是「是否自該通訊監察中獲得相關參考情資」爲事後檢討依據。

然而情報通訊監察常因其隱密性而須迴避相關數據之揭露，我國目前在司法院統計年報中有明確之公布之情報通訊數據僅有核可件數、終結件數、未結件數及期滿續監案件數，未顯示聲請數量或未通知數量等。

---

198 Applications made to the foreign intelligence surveillance court during calendar year 2002-2010，U.S. Department of Justice Office of Legislative Affairs，http://www.fas.org/irp/agency/doj/fisa/2010rept.pdf ~ http://www.fas.org/irp/agency/doj/fisa/2010rept.pdf

199 Foreign Intelligence Surveillance Act Court Orders 0979-2010，Electronic Privacy Information Center，2011 年，http://epic.org/privacy/siretap/stats/fisa_stats.html

200 通保新制上路 2 年 具體成效頗可觀，司法週刊電子報第 1471 期，http://www.judicial.gov.tw/ jw9706/1471_main.html#2，2009 年 12 月 17 日。

第三項　強化國會監督

依國家情報工作法第 4 條規定，國家情報工作，應受立法院之監督。為彰顯對人民負責的權利分立與民主政治精神，情報工作應依國家情報工作法受立法院之監督，不因情報工作之隱匿及機密性而有例外[201]。

我國依 2009 年 1 月修正之「立法院組織法」第 10 條第 1 項規定，於立法院設置內政、外交及國防、經濟、財政、教育及文化、交通、司法及法制、社會福利及衛生環境等 8 個委員會。同條第 2 項規定立法院於必要時，得增設特種委員會。由於情報工作重視隱密性，多數國家之國會對情報工作之監督都以成立特別委員會之方式進行。然而，立法院並未設立情報監察委員會專責監督情報工作事宜。[202]

目前我國情報工作係向外交及國防委員會報告，惟在通訊保障及監察法規範中，並未規範任何對立院之報告及監督義務，故每會期之報告內容並不包括情報通訊監察執行情形。

參考美國 FISA 在國會監督上，檢察總長須向對參眾議院情報永久特設委員會及司法委員會，對外國情報通訊監察執行事項為半年度報告，公布聲請之件數與核可之件數、依 FISA 所取得之證據使用於刑事訴訟之情形、檢察總長認定最小侵害原則之標準等，及對 FISA 是否修正等建議之「年度報告」。

德國G10 法則要求戰略性情報通訊監察前須經聯邦議會監督委員會同意、對外國政府之情報傳遞亦應於傳遞後 6 個月內告知聯邦議會監督委員會，聯邦議會監督委員會每年應就G10 法執行情形再向聯邦議會報告，亦為法律明文之國會報告義務。再參考德國G10 之 2007 年對外揭露之年度報告[203]，內容長達 8 頁，公佈

---

201 林進財，我國情報通訊監察之研究，淡江大學國際事務與戰略研究所碩士論文，頁 112，2007 年。

202 賴建宏，論情報法制與情報監督-英國與我國之制度比較，中央警察大學外事警察研究所碩士學位論文，頁 101，2009 年。

203 德國聯邦議院發佈 16 / 11559 文件(Deutscher Bundestag Drucksache 16/11559)，2007 年度德國聯邦議會監督委員會年度報告，2009 年 1 月。http://dipbt.bundestag.de/dip21/btd/16/115/1611559.pdf。

相關數據，並於報告最後提供修法建議等，內容可謂相當完善。

我國亦可考慮在立院設置情報委員會，並於法規上明文訂定情報通訊監察之國會監督義務，以情報委員會作爲情報機關通訊監察監督機關，情報機關定期向其報告相關執行情形，確保相關工作得在均衡定期的監督下執行。

第四節　例外不通知之規範過於空泛

我國情報通訊監察依通訊保障及監察法第 15 條規定，情報通訊監察案件之執行機關於監察通訊結束時，應即敘明受監察人之姓名、住所或居所報由國家安全局，陳報法院通知受監察人。如認通知有妨害監察目的之虞或不能通知者，應一併陳報。法院對於上述陳報，除認通知有妨害監察目的之虞或不能通知之情形外，應通知受監察人。若不通知之原因消滅後，執行機關應報由國家安全局陳報法院補行通知。

情報通訊監察完畢後之通知爲人民權利保障重要依據，受通知後人民始有能力事後救濟，亦可防止機關浮濫聲請，是正當法律程序之核心內容。

司法院並未就情報通訊監察之通知率與犯罪通訊監察區隔另爲統計，然仍區分地方法院與高等法院所核發，而高院核發之通訊監察一部份爲情報通訊監察，參考民國 99 年統計數據[204]可發現高等法院通訊監察案件核發通知書之比率僅 64.1%，即暫不通知案件高達 35.9%，而暫不通知之原因皆非「不能通知」，全數爲「通知有妨害監察目的之虞」。比較同年犯罪通訊監察通知率[205]爲 80.12%，情報通訊監察之通知率偏低。

---

[204] 99 年高等法院暨分院通訊監察案件核發通知書及暫不通知情形，司法院中華民國 99 年司法統計年報，2010 年，http://www.judicial.gov.tw/juds/year99/06/32.pdf

[205] 99 年地方法院暨分院通訊監察案件核發通知書及暫不通知情形，司法院中華民國 99 年司法統計年報，2010 年，http://www.judicial.gov.tw/juds/year99/09/123.pdf

再看民國 98 年數據，高等法院通訊監察案件核發通知書之比率[206]僅31.25%，不通知案件亦全數爲「通知有妨害監察目的之虞」，而非「不能通知」。

通訊保障及監察法施行細則第 27 及 28 條規定，執行機關認通知有妨害監察目的之虞或不能通知之情形依法陳報，經法院據以不通知受監察人者，執行機關應每 2 月檢討通知有妨害監察目的之虞或不能通知之情形是否消滅，報由國家安全局陳報法院審查。法院審查執行機關之陳報，如認通知無妨害監察目的之虞或無不能通知之情形，得逕通知國家安全局局長後，通知受監察人。

1. 何謂「妨害監察目的」和「不能通知」等要件並無法指涉具體事實。

司法院「法院辦理通訊監察案件應行注意事項」第 24、25 項規定，國家安全局陳報不通知受監察人，由法院依具體個案情形，應詳爲審查，妥適決定，本於職權獨立判斷，不受陳報機關意見之拘束。法院若認通知無妨害監察目的之虞或無不能通知之情形，於逕行通知前，宜先徵詢國家安全局局長之意見。法院並應注意有無確實執行檢討。

依前揭司法院統計年報報表可知，法院將「暫不通知理由」區分爲「通知有妨礙監察目的之虞」、「不能通知」，惟依實際數據可知暫不通知者皆爲「通知有妨礙監察目的之虞」。不能通知在理解上尚能明確，若受監察人在境外難以通知者應屬不能通知，然「通知有妨礙監察目的之虞」則難以明確易受濫用，情報機關應說明爲何將妨礙通訊監察，交由法院各案審查，而非僅以通知有妨礙監察目的之虞爲由主張暫不通知；即應提出原因說明如何造成了「有妨礙監察目的之虞」的結果，原因與結果不可錯置，避免實務運作上由例外變爲原則，致使事後告知之規定流於形式，妨害被監聽人請求救濟之機會。[207]

---

[206] 98 年高等法院暨分院通訊監察案件核發通知書及暫不通知情形，司法院中華民國 98 年司法統計年報，2009 年，http://www.judicial.gov.tw/juds/year98/06/33.pdf

[207] 陳運財，「通訊之監察」，何賴傑、林鈺雄、陳運財合著「刑事訴訟實例研習」，73 頁，2000 年 6 月。

參考美國FISA規範，檢察總長可提出具結書宣示（affidavit under oath）說明相關資訊揭示或兩造辯論將有害於國家安全，則地方法院應以秘密及一造方式審查系爭外國情報通訊監察是否被合法的授權與執行及是否通知，若無法通知時亦可替代受監察人主張權利。[208]

2. 通訊保障及監察法施行細則第 27 條第 4 項但書規定，受監察人實際上無從通知或其不通知原因短期內無法消滅者，得經法院同意，不爲定期檢討或延長其檢討期限，而「不爲定期檢討」亦未明確規範。不爲定期檢討應指不隨同他案每 2 月檢討，但仍應設定下次檢討時間，而不通知原因短期無法消滅時之「短期期限」無法確認時，應僅能延長檢討期限，而不得選擇不爲定期檢討。

嚴格詳實審查不通知事由，定期檢討不通知原因是否消滅，係落實大法官釋字第 631 號解釋，嚴謹審核，隨時監督，保障人民秘密通訊自由之意旨。

第五節　擴充情報通訊監察手段之節制

第一項　機動式通訊監察機制

爲符合明確性原則(particularity requirement)，原本通訊監察書之核發須記載特定門號，但由於通訊技術進步，犯罪嫌疑人可能不停更換新行動電話門號，甚至利用僞造或變造的證件申辦門號規避通訊監察，美國規範犯罪通訊監察之「美國聯邦電子通訊隱私法」（The Electronic Communications Privacy Act, ECPA）首先於 1986 年增訂了「機動式通訊監察（Roving Surveillance）」，授權偵查機關在符合

[208] 50 USC §1806(f)~(h)

一定要件時，經法院許可後，可以針對特定對象之所有通訊進行監察，[209]但未適用於情報通訊監察FISA之規範中。但美國發生九一一事件後，FISA透過愛國者法案擴充外國情報通訊監察權，使FISA亦有使用機動式通訊監察之權限。原本FISA外國情報通訊監察對象僅得針對「特定線路」之通訊，機動式通訊監察在「受監察人有妨礙通訊監察之行爲」之客觀事實時，則可僅針對「特定人」之所有通訊而爲監察，增加執行通訊監察之機動性。[210]

行動電話門號取得容易，聲請限定某組號碼通訊監察之方式將造成不必要之程序延宕，爲避免受監察人以不斷更換行動電話號碼等方式，以妨礙通訊監察目的之執行。機動式通訊監察在網路通訊中更爲重要，因受監察人可不斷重複註冊數個帳號，亦可使用不同處所之公用網路電腦而變換不同IP位址等，其犯罪成本極低。[211]

爲配合執行機動式通訊監察，FISA 規範 50U.S.C.§1805(c)(2)(B)並規範要求電信業者提供執行機動式通訊監察所須相關資訊。然而機動式通訊監察可對受監察人使用之任何電腦網路設備進行通訊監察，可能造成許多不相干第三人之權益損害，若遭誤用時亦同，故愛國者法案中亦設有限制—在法院同意爲機動式通訊監察後，當發現並開始對新的通訊工具或新地點爲通訊監察時，應在 10 日內通知法院其新通訊工具或新地點、相當事實使聲請單位足認其爲被監察人所使用、對於每一通訊工具所取得之情資應注意最小侵害原則之適用，及核准增加機動式通訊監察之設備總數，有正當理由者可延長至 60 日，使法院以資監督。

機動式通訊監察未特定通訊監察號碼是否能符合通訊保障及監察法中「明確性原則」？美國聯邦上訴法院曾在數判決中確認機動式通訊監察之合憲性[212]，因偵查機關仍須描述特定且明確之通訊監察對象，確認是否符合最小侵害原則，有

---

[209] 李榮耕，特定明確原則與機動性通訊監察，政大法學評論第 126 期，頁 129，2012 年 4 月。

[210] Peter M. Thomson, White Paper on The USA PATRIOT Act’s “Roving” Electronic Surveillance Amendment to the Foreign Intelligence Surveillance Act, The Federalist Society for Law and Public Policy Studies. 2-14 (2004)

[211] 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學位論文，頁 49，2009 年。

[212] Hermanek, supra note 15; United States v. Bianco, 998 F.2d 1112 (2d Cir. 1993); United States v. Gaytan, 74 F.3d 545 (5th Cir. 1996); Petti, infra note 61.

相當理由可信受通訊監察者使用該通訊設備；且並非所有通訊監察皆可由偵查機關任意爲機動式通訊監察，須法院認定受監察人有相當理由可信其有妨礙通訊監察之行爲時，始得依令狀之記載爲之。

我國通訊保障及監察法規定通訊監察書須記載「監察通訊種類及號碼及號碼等足資識別之特徵」，無機動式通訊監察之適用，每一通訊監察線路、門號皆須個別列述以獲得法院令狀。

若有充分之監督機制配套下，例如聲請機動式通訊監察前須先提出有相當理由可信受監察人有妨礙通訊監察之事實，由法院認定後依令狀爲之，並在對新通訊設備爲通訊監察後的一定期限內，對該新通訊設備之監察須即送法院爲審查是否符合小侵害原則，以確保情報機關謹慎提出機動式通訊監察，不濫用此權力，未來應可考慮修正相關規範，概使通訊監察法治能跟得上科技與時代變化之腳步。

第二項　濾蒐情報通訊監察

我國通訊保障及監察法不分情報通訊監察或犯罪通訊監察，皆要求通訊監察書須記載特定監察對象後始能爲通訊監察，而始有後續利用通訊監察所獲資訊。

依通訊保障及監察法第 10 條規定，情報通訊監察所得資料，僅作爲國家安全預警情報之用。然而國家安全預警情報工作除了具有預先調查影響國家安全之重大犯罪之作用外，尚包含關係國家安全之外國情報蒐集，若要再加強規範國家安全預警情報工作之功能，應可考慮允許立法規範另一種濾蒐通訊監察，未設定特定通訊監察對象，而以自動化設備，對大量通訊內容如語音通訊或電子郵件等，以關鍵字爲濾蒐。對不特定人爲短暫之通訊資訊擷取，無可疑即可忽略，無持續長時間侵害人民權益，與一般通訊監察之侵害有程度上之不同。

然而濾蒐通訊監察，此種非針對特定人，而係針對特定事件而爲通訊監察方式，若未搭配其他要件之設限，是不會受一般犯罪通訊監察法規所承認。犯罪通訊監察規範仍須要求監察對象之特定性，而不容許一般性、無區別性之探查行

爲。在歐洲執委會與歐洲議會主導下，於 2001 年 11 月 23 日通過全球國際性的網路犯罪公約(Convention of Cybercrime)亦闡明不容許執法機關進行普遍或任意性的通訊監察，也不容許大量蒐集通訊資料。[213]

濾蒐情報通訊監察行爲應受核准目的之拘束，以避免成爲不設界限之「總括式之通訊監察（pauschale kommunikationsüberwachung）」[214]，逾越了比例原則而過度侵犯人權，參考前述第二章所提及德國G10 法中之戰略性情報通訊監察，其核准目的即係針對事件，賦予聯邦情報局得非對個人，而係對事件設定「關鍵字」，並限於對「國際電信通訊」進行過濾，只要涉及特殊字串如關於恐怖活動或重大武器擴散之相關概念詞組等，經由過濾，即可蒐集獲得特定資訊。

在以細緻審查保障人權著稱的歐洲人權法院（European Court Of Human Rights）在 2006 年Gabriele Weber and Cesar Richard Saravia v. Germany案中[215]，曾對德國G10 法戰略性情報通訊監察的適法性作出裁決。告訴人Gabriele Weber及Cesar Richard Saravia向歐洲人權法院主張德國G10 法中關於戰略性情報通訊監察係對普遍未有明確罪嫌者爲通訊監察行爲，其程序不合法，且亦未對受戰略性情報通訊監察者給予事後通知[216]；此外特別是依G10 法第 5 條第 1 項第 4~7 款所爲之戰略性情報通訊監察如毒品運販、僞造貨幣、洗錢、組織犯罪等相關行爲，對公眾建構的危險程度並不足正當化如此嚴重的侵權行爲。然而歐洲人權法院作出長達 37 頁的判決就G10 法中戰略性情報通訊監察之規範逐條分析，認爲戰略性情報通訊監察雖可對未有明確罪嫌者即可藉由關鍵字(Catchwords)進行監察，然該因該監察方式爲保障民主社會、防制犯罪而有其必要性，並亦以法律規範，且該通訊監察係依該關鍵字之「令狀」爲之，明訂監察期限（每次 3 個月之期限）、設有審

---

213 馮震宇，網路犯罪與網路犯罪公約（下），月旦法學教室，第 5 期，頁 119，2003 年 3 月。周玄明，隨機性國際通訊情報偵蒐法制研究，國防大學法學系碩士學位論文，頁 12，2010 年 1 月。

214 詹鎮榮，秘密通訊自由，法學講座，21 期，頁 13，2003 年 9 月。

215 European Court Of Human Rights Third Section Decision as to The Admissibility of Applicatio no. 54934/00 by Gabriele Weber and Cesar Richard Saravia against Germany, (2006).

216 依 G10 法第 12 條第 2 項規定，戰略性情報通訊監察中獲取個人情資者，若未立刻銷毀者則須通知當事人。換句話說，戰略性情報通訊監察所獲取了個人情資，若立刻將其銷毀者，則不須對當事人為通知。

查機制（聯邦議會監督委員會），限制其對象、使用（不得導出針對德國人個人身份特徵，對外國人則排除此限制等）、儲存（每 6 個月定期檢討其儲存情資）及傳遞情資程序，事後情資資訊之刪除亦設有規範，故認其規範應符合最低保障的限度防止濫權監聽而不違法。

但需注意者，德國戰略性情報通訊監察亦同樣須依G10 法第 14 條，受聯邦議會監督委員會嚴格之年度報告所監督，參考其 2007 年公布數據[217]，291 萬 3,812 筆通訊被德國聯邦情報局(BND)以關鍵字偵測到符合第 5 條第 1 項第 1、2 款之「國際恐怖行動」，經追蹤後發現只有 4 筆通訊與外國情報相關，另有 234 萬 3,252 筆通訊符合第 5 條第 1 項第 3 款之「武器擴散」，370 筆實際與武器擴散相關。83 筆通訊符合第 5 條第 1 項第 4 款之「毒品販運」，未有一筆實際符合。參照上述資訊，亦有輿論批評該數據無法證明戰略性情報通訊監察此一情報蒐集管道對德國之國家安全有何正面的貢獻，反而在初期攔截到大量的資訊包含了近九成之垃圾信件，使國家尚須投入大量人力於後續追蹤縮小監察範圍，就算經篩選後符合爲其所須之情報者，其最後轉介於開啓刑事犯罪偵查者更是極少[218]。

美國在九一一事件前，曾有報導揭露了美國國家安全署計劃之梯隊計劃（Echelon）[219]由電腦軟體分析衛星訊號，使其可依聲紋及關鍵字等方式分辨衛星電話通訊，以獲取外國情報。[220]據稱布希政府曾大規範對不特定人所爲之秘密通訊監察方式來蒐集大量情資。[221]新型衛星通訊截收系統使用自動通訊監察設備，

---

[217] 德國聯邦議院發佈 16 / 11559(Deutscher Bundestag Drucksache 16/11559)，2007 年度德國聯邦議會監督委員會年度報告，頁 8，2009 年 1 月。http://dipbt.bundestag.de/dip21/btd/16/115/1611559.pdf。

[218] Norbet Putter, Statewatch Analysis Germany - The Federal Republic's security services from the Cold War to the "new security architecture", Statewatch Journal, vol 19 no 4., http://www.statewatch.org/analyses/no-102-germany-security-services.pdf , Page.5, (2009).

[219] 錢世傑，網路通訊監察法制與相關問題研究，中原大學財經法律學系碩士學位論文，頁 181-183，2002 年。

[220] Edited by Jeffery Richelson and Thomas Blanton, Electronic Surveillance From the Cold War to Al-Qaeda, National Security Archive Electronic Briefing Book No.178, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB178/index.htm

[221] Jason Leopold, Revisiting Echelon: The NSA's Clandestine Data Mining Program, http://pubrecord.org/nation/2290/revisiting-echelon-nsas/ (2009.7.15.).

攔截鉅量之電話、傳真、電子郵件、網路電話、衛星電話等資訊，然後透過聲紋、語音辨識及關鍵字搜尋等方式可即時蒐整出情報，然而這樣的通訊常可能截收到美國人民之通訊，應極難符合FISA相關程序之規範，故備受爭議[222]。

另未證實之報導指稱中國某市建立了一套通訊監聽系統，包括對手機、固定電話、IC卡電話等，系統自動控制監聽敏感詞，例如當發現通話中有 3 個「法」字，電話內容會被自動記錄下來，並將被調查追蹤。[223]

暫不論以上報導內容是否屬實或其程序是否妥適，但以目前科技進步之發展，上述濾蒐技術應非難事，參照歐洲人權法院曾作出之見解，通訊監察就是國家機關之干預，後來使用與否都不會影響這個判斷的結果[224]，故若放任法規未爲規範而非針對特定人爲普遍通訊監察之濾蒐系統，未在法律明確授權與相關要件限縮及監督之下默默運行，就算未使用該情蒐情資，將很有可能造成政府權力之濫用與對人民權利之侵害。若我國未來立法者有意修法加強規範情報通訊監察中預警情報之功能，應可考慮參考德國G10 法戰略性通訊監察模式及歐洲人權法院意見，以法律規範合理限制其範疇，使濾蒐情報通訊監察亦須依關鍵字來特定事件，以符合通訊保障及監察法之「明確性」原則[225]，在符合最小侵害原則下依令狀爲之，核發令狀須受監督，明訂監察期限、設有審查機制、限制其使用、儲存及傳遞情資程序，並規範事後情資資訊之刪除，防止濫權之手段爲之，以確保人民最大權益之保障，並避免情報通訊監察之過度侵犯人權，畢竟明確授權之規範應較可避免濫權通訊監察之質疑。

---

[222] Echelon And FISA, http://www.moonofalabama.org/2005/12/why_not_to_use_.html ,2005.12.20.

[223] 大陸一市建立電訊監聽 3 個以上“法”字通話成嫌疑，大紀元電子報，2002 年 7 月 9 日，”據明慧網 2002 年 7 月 8 日報導，鞍山已經建立起一套通訊監聽系統，包括對手機、固定電話、IC卡電話等，系統自動控制監聽敏感詞，如：當發現通話中有 3 個“法”字，電話內容會被自動記錄下來，並將被調查追蹤。”http://www.epochtimes.com/gb//2/7/9/n201192.htm

[224] 林鈺雄，論通訊之監察—評析歐洲人權法院相關裁判之發展與影響，東吳法律學報十九卷第四期，頁 128，2008 年 4 月。

[225] 通訊監察所應遵守「特定性原則」之解釋應與搜索扣押不盡相同。參照李榮耕，特定明確原則與機動性通訊監察，政大法學評論第 126 期，頁 125-127，2012 年 4 月。

第六節　情報通訊監察單獨立法

第一項　分別立法以明確規範情報通訊監察

我國通訊保障及監察法於 1995 年立法時即將通訊監察分爲犯罪通訊監察及情報通訊監察兩種形式，屬不同性質，立法者本無意以同一套標準規範其程序與要件。然我國情報通訊監察，在我國「通訊保障及監察法」中與犯罪通訊監察一同被規範，規範法條相對他國較爲簡略。這樣的規範究竟是過度概括的授權情報機關，亦或是情報通訊監察多須要求比照犯罪通訊監察程序而更爲嚴謹？

規範國家情報工作之國家情報工作法第 7 條，於民國 100 年 6 月 3 日增訂了第 3 項：「情報機關執行通訊監察蒐集資訊時，蒐集之對象於境內設有戶籍者，其範圍、程序、監督及應遵行事項，應以專法定之；專法未公布施行前，應遵守通訊保障及監察法等相關法令之規定。」自該增修條文確立了政策將朝向情報通訊監察單獨立法邁進，並爲未來設立專法之依據。

國家安全工作常係以預防發生國家安全事件，蒐集預警情報，不以偵查特定犯罪爲目的，情報通訊監察係爲保障國家安全，屬於危害防禦前階段之行爲，具有高度不確定性以及政治性；而犯罪偵查之通訊監察，係以犯罪之防制、偵查及追訴爲主，兩者之要件、審查、資訊傳遞及監督機制，均應有不同之制度設計。[226]犯罪通訊監察蒐集所得的資訊，通常是用以作爲認定犯罪事實的證據，在審判期日中提出作爲證明被告之犯罪事實。

雖情報通訊監察在與犯罪通訊監察有本質上的差異，惟參照世界各國立法例中，有如美國、德國等國家，將情報通訊監察單獨立法而與犯罪通訊監察依據不同之程序規範；亦有如我國與法國等國家，將情報通訊監察與犯罪通訊監察合併立法。亦有只規範犯罪通訊監察，對情報通訊監察未爲規範者，如日本；甚至有對通訊監察皆未以法令規範者，如新加坡。其區別應主要在於對情報通訊監察規

[226] 周治平，情報機關通訊監察權之研究—德國法之啟示，警大法學論集第 15 期，頁 293，2008 年 10 月。

範要件設定之嚴格性及明確性之差異。

情報通訊監察中，因情報工作有其機動性、多樣性、抽象性，須要較廣泛之裁量權，故應加強其監督機制，分別立法亦得明文使情報通訊監察以更嚴謹之方式受外部監督。[227]故單純考慮是否分別立法其實並非不能完善情報通訊監察，重要的應是在於其立法是否明確完整。現行通訊保障及監察法規對情報通訊監察之規範，相較已分別立法之美國FISA及德國G10 法，實在非常簡略。

例如常受批評之「為避免國家安全遭受危害」的要件相當抽象且廣泛，易受濫用，應賦予較明確定義。參照美國FISA在定義「外國勢力」[228]時，明列其範圍，包括： (1)外國政府或非由美國政府所承認之組成機構，(2)非實質上由美國人所組成之外國組織，(3)由外國政府公開承認指揮控制之實體，(4)從事國際恐怖活動或預備為國際恐怖活動之團體，(5)非實質上由美國人組成，以外國人為基礎之政治組織，(6)外國政府或其所指揮控制之實體，(7)非美國人所組成從事國際毀滅性武器擴散之實體。而「外國勢力工作人員」[229]，係指（1）非美國人，其(A)在美國活動，擔任外國勢力之官員或受僱人，或為第 1804(a)(4)條從事國際恐怖活動或預備為國際恐怖活動之團體所指外國勢力之成員，(B)在美國為外國勢力或代表外國勢力從事秘密情報活動而悖乎美國國家利益之人，或依其所在之週遭情況顯示可能在美國從事上述活動之人，或明知而幫助、策動他人從事上述活動之人，或明知而仍與上述活動之人為共犯者，(C)從事國際恐怖活動或預備為國際恐怖活動之團體，(D)從事國際大規模毀滅性武器擴散活動或預備為之者，(E)代表外國勢力從事國際大規模毀滅性武器擴散活動或預備為之者。(2) 任何人（包括美國人），其(A)明知而為外國勢力從事秘密情蒐活動，涉及或可能涉及違反美國刑法者，(B)遵從外國勢力之情報服務或外國勢力之網絡之指示，明知而為外國勢力或代表外國勢力從事其他秘密情報活動，其活動涉及或將涉及違反美國刑事法律者，(C)明知而從事或代表外國勢力從事顛覆行為(sabotage)或國際恐怖活動，或預備為此等行為者，(D)明知而從事或代表外國勢力以虛偽身份進入美

---

227 曾依璇，情報與犯罪監聽國安局想區隔，中央社，http://n.yam.com/cna/politics/201008/20100822444726.html，2010 年 8 月 22 日報導。

228 50 U.S.C. &1801(a)

229 50 U.S.C. &1801(b).

國，或在美國使用虛僞身份者，(E)明知而幫助或策動他人爲前述(A)(B)(C)之人所爲活動之共犯者。

再參照德國G10 法，區分個案情報通訊監察及戰略性情報通訊監察。個案情報通訊監察之件爲須有下列嫌疑 1、危害和平或內亂罪（刑法第 80-83 條），2、危害民主法治國家罪（刑法第 84-86、87-89 及結社法第 20 條第 1 項第 1 至 4 款），3、叛國或對國家安全之危害行爲（刑法第 94-96、97a-100a），4、危害國防罪（刑法第 109 條e-g），5、危害駐守德國境內之北大西洋公約國軍隊之安全罪（刑法第 87、89、94、98-100、109e-g、北大西洋公約國軍隊保護法第 1 條），6、其他刑法重罪，7、居留法第 95 條第 1 項第 8 款，8、海關法第 23 條a項 1.3 項。而戰略性情報通訊監察[230]則須爲防範 1、對德意志聯邦共和國的武力攻擊，2、與德意志聯邦共和國直接有關的國際恐怖攻擊，3、軍事武器管制法所指之國際武器擴散，及重要的商品、資訊處理程　式及高科技之非法跨國交易，4、未經許可將大量毒品攜入德意志聯邦共和國，5、在國外僞造貨幣，而損害歐元流通區的貨幣安定性，6、重大國際組織洗錢活動，7、外國人對歐盟地區之重大組織性國際走私活動。

再看我國目前通訊保障及監察法對情報通訊監察之規範僅在於第 7 條「爲避免國家安全遭受危害，有蒐集外國勢力或境外敵對勢力情報之必要者」，及第 8 條對外國勢力或境外敵對勢力之定義爲「一、外國政府、外國或境外政治實體或其所屬機關或代表機構。二、由外國政府、外國或境外政治實體指揮或控制之組織。三、以從事國際或跨境恐怖活動爲宗旨之組織。」第 9 條對其工作人員之定義爲「一、爲外國勢力或境外敵對勢力從事秘密情報蒐集活動或其他秘密情報活動，而有危害國家安全之虞，或教唆或幫助他人爲之者。二、爲外國勢力或境外敵對勢力從事破壞行爲或國際或跨境恐怖活動，或教唆或幫助他人爲之者。三、擔任外國勢力或境外敵對勢力之官員或受僱人或國際恐怖組織之成員者。」相較而言，其定義確實較爲不明確。

另我國情報通訊監察目前對不論是否具有我國國籍之通訊監察期間皆相同

[230] G10, Abschnitt 3: Strategische Beschränkungen § 5 Voraussetzungen

長達一年，此種不作區別之立法較爲粗糙，且在部分情況下相較外國立法例顯得監察時間過長，例如前文所提到對某週刊記者之情報通訊監察之 2 案，其監察期間動輒長達 1 至 3 年，建議應將其細緻化區分，不應以一律先同一規範核發一年上限，畢竟預測的時間越長，準確性及必要性皆有可能大幅降低。參考美國FISA對外國勢力得爲一年期之無法院令狀情報通訊監察，而對美國人民則僅得爲依法院令狀最長 90 日之情報通訊監察。[231]再參照德國G10 法，並不以是否具有本國籍爲區隔，但其最長通訊監察期間皆設爲 3 個月[232]，縮短通訊監察之期間，若期限屆至後仍有續監需要時，可重新檢視相關要件，復以前次監察所得內容爲據，使須爲較長期續監之案件更具合理性。故相對於上述法規，對於我國人民之情報通訊監察期間似可再爲研議。另參照美國FISA得爲無法院令狀之情報通訊監察者，除了不得爲美國人民外，其範圍亦僅限縮於其對「外國勢力」7 項定義之前 3 項[233]，非所有非美國國籍者皆得爲無法院令狀之情報通訊監察。而德國G10 法個案情報通訊監察皆須經過G10 委員會同意，戰略性情報通訊監察之關鍵字亦須經國會監察委員會同意。

第二項　單獨立法之困難

2001 年美國發生 911 事件，爲配合世界各國建構反恐怖作爲，行政院曾於 2003 年提出「反恐怖行動法」草案[234]並送立法院審議，至今未完成審查，究其原因除草案許多要件尚欠嚴謹周延外，重點在於難以說服立法院無以反恐造成執法擴權之疑慮[235]而有制定反恐專法之必要性。然而，如 1978 年美國FISA法案通過時透過「最小侵害原則」之設限，使經由外國情報通訊監察所得情資不得轉爲刑

---

231 50 U.S.C.§1805(d)

232 G10, Abschnitt 4 : Verfahren § 10 Anordung

233 50 U.S.C.§1802

234 反恐怖行動法草案，行政院，2003 年，http://www.ey.gov.tw/public/Attachment/20031121180741200.pdf

235 蔡庭榕，論反恐怖主義行動法與人權保障，中央警察大學國境安全與刑事政策學術研討會，頁 25，2003 年。

事審判證據，唯在 911 事件發生後，透過愛國者法案之制訂加強各部門間情報資訊之共享，使情資得轉爲刑事審判證據，以此爲限縮人民權利，但民主法治國家人民於「平時」可能無法容忍政府爲反恐怖行動而侵害人權，若非如美國發生 911 事件如戰時之緊急情況，立法者實難以長期支持此項法規之制定。我國政府依據聯合國決議，未雨綢繆事先擬定政策完備法律規範，實無可厚非，但在我國當前強調人權立國之際，必須思考會不會因爲遏阻少數恐怖份子（或根本不存在恐怖份子）的侵犯人權行爲，反而容許國家機關輕易地侵犯更多無辜人民的基本人權。[236]

相同的，要將情報通訊監察單獨立法，除情報通訊監察之規範及要件審查、監察規範皆需明確周延外，若要擴充情報通訊監察之權力，例如增加類似美國機動式通訊監察等功能，亦須先說服立法者確有此須求，否則將情報通訊監察單獨立法之推動亦可能面臨如同反恐怖行動法草案遭長期擱置之窘境。然而我國既非恐怖分子作業之重要國家，兩岸之形勢也處於相對和緩之態勢，若非有重大事件發生，即難有可用之民氣。美國在 911 事件發生後的 6 週即通過實施了強化情報作爲之愛國者法案，否則立法者亦難以在如此短的時間內同意限縮人民權益。

然而不論是現存體制之加以明確規範或要再擴充其功能，若在立法政策設定合理之限制要件及明確之監督方式，兼顧效率及人權之保障，將細節加以明文規範，才能避免人民對情報機關濫權通訊監察之質疑，亦能真正確實保障人民權益；未明確規範而在模糊範圍中運作之情報工作，才是扼殺人民對情報機關信心的黑手。

[236] 陳青田，反恐怖主義立法與關鍵議題之研究，稻江科技暨管理學院財法，頁 465-476， fel.toko.edu.tw/attachments/144_(465-476).doc，2010 年。

第七節　　小結

我國通訊監察立法政策，採用如重罪原則、最小侵害原則、比例原則、法官保留原則等，已相當符合當代立法趨勢，亦成爲其他通訊監察尚未法制化之國家所效仿參考的對象，惟在情報通訊監察部份之規範，美、德兩國已有長年之情報通訊監察法治之實行與修正，相較而言我國之規範稍嫌簡略。檢討我國情報通訊監察法治面及執行面之現況，應對其詳加規範以增加法明確性，並加強行政、立法、司法監督，以嚴謹之組織審查核發情報通訊監察書，給予受情報通訊監察者適當之救濟管道等，尚爲我國所不足處，應參考外國立法例，配合我國國情，制定完善之情報通訊監察規範，並確實依法執行，方能保障人民權益。

仍須注意者爲，國家情報工作任務爲及早獲取、蒐集與分析涉及國家安全的資訊，以防範並排除實際危害的發生，然而情報蒐集途徑眾多，包括綜整公開資訊、人員佈建、跟監、情資交換合作等，通訊監察僅爲其中一種方式，故在考慮擴充情報通訊監察之功能時，應特別注意是否符合最小侵害原則，例如在做情報決策分析時，以其他如公開情報之蒐集等是否亦能達成目的，而不是僅將情報通訊監察視爲無往不利之利器而予取予求。

第五章 結論

中華人民共和國保守國家秘密法第 28 條規定「網際網路及其他公共信息網絡營商、服務商應當配合公安機關、國家安全機關、檢察機關對洩密案件進行調查；發現利用互聯網及其他公共信息網絡發布的信息涉及洩露國家秘密的，應當立即停止傳輸，保存有關記錄，向公安機關、國家安全機關或者保密行政管理部門報告。」，然而華盛頓時報報導批評中國政府時常利用該條文，以對「國家機密」的廣泛定義來箝制國內的資訊自由。[237]

同樣的，「國家安全」亦不應成爲一個漫無限制的尚方寶劍，在情報通訊法治中，若過度擴張國家安全之定義，將會侵害人民通訊、言論、表現自由，甚至箝制了人民思想。通訊監察法規係保護個人之居住空間與秘密空間，確保個人或人與人之間之安心領域，使無恐懼感，即免於恐懼之自由，對於此種領域，個人得自主決定何時即在何種範圍程度內將個人之生活事務予以公開，亦得自主決定，對之保留不公開，故此種資訊的自主決定權，對於個人自由之保護，具有重大意義。[238]人性尊嚴係核憲法之核心，不得將一個人客體化或物化[239]，不敢表達內心之思想與意見，影響自由意志之交流與形成，侵害人性尊嚴與人格完整發展，[240]應基於人性尊嚴與個人主體性之維護及人格發展之完整，爲保障個人生活私密領域免於他人侵擾及個人資料之自主控制。再看歐洲人權法院案例法所承認的私人生活保障，尤其是在監察脈絡，可以說保障的主要是個人內在與外在世界的關係，當個人不希望時，他有免受外界干擾的自由；當個人意欲時，他有權去

---

[237] Gillian Wong，China set to tighten state-secrets law forcing Internet firms to inform on users, The Washington Post，2010.04.28.

[238] 許宗力，法與國家權力，月旦出版社，頁 215-216，1998 年。

[239] 李震山，警察行政法論-自由與秩序之折衝，元照出照公司，頁 320-323，2007 年 9 月初版。

[240] 張明偉，監聽風雲—以通訊監察進行國家情報工作之規範檢討，軍法專刊第 56 卷第 6 期，頁 168，2010 年 12 月。

建立並發展和其他人的關係，這當然包含任何形式的溝通，如此才能發展並實現個人的人格權。[241]故若過度擴張國家安全之範疇而爲情報通訊監察，嚴重者亦可能侵害人民表現自由及人格權，其中輕重衡量須審慎爲之。

因此情報通訊監察規範除須合理，政策之制定須兼顧國家安全與人民權益，監察要件應盡量符合明確性原則，其手段應有比例原則之適用，資料之傳遞與運用應受目的性原則之拘束，且須有防範恣意與濫用之預防措施，執行上須遵守法令，同時要隨國際情勢變化，及國內政治體制環境的變遷，以國家安全受威脅危害的程度與時空背景來做國家安全蒐情政策的適時轉換，並確認該干預是否符合「急迫的社會需求」，才不會遭到民眾之質疑，以提升人民對情報機關之信賴感。立法政策之過與不及皆爲不當。

檢討我國現行規範，在我國情報通訊監察法治中，現行法規以獨任法官來審查情報通訊監察之聲請案件，審查組織過於簡單可能影響審查密度，建議修正核發情報通訊監察書之組織，使其對情報機關所提出之情報通訊監察案件得以進行實際審核。

另爲使情報通訊監察有完善之事後救濟，應可參考 FISA 於國家安全事務機關提出聲請情報通訊監察時，須提出保證書擔保該情報通訊監察行爲有「相當理由可信」及「最小侵害原則」之確信，日後若發現有虛僞不法之情事時得以釐清相關責任歸屬。

對於情報通訊監察之監督，可強化情報機關提出情報通訊監察之自我節制，可參考美國 FISA 之保證書制度及向法院提出聲請書前須先經檢察總長審核等機制；情報通訊監察之執行增加入對司法機關之報告義務，以強化司法於通訊監察中監督之角色；於情報通訊監察法中明訂情報機關對國會之報告義務以強化國會監督。

對於情報通訊監察中例外不通知之規範應求明確，並加強法院對不通知案件之審核。

另亦可考慮修法增加機動式通訊監察或濾蒐情報通訊監察，以因應科技與時

---

[241] 林鈺雄，論通訊之監察—評析歐洲人權法院相關裁判之發展與影響，東吳法律學報十九卷第四期，頁 121-122，2008 年 4 月。

代變化所需，惟仍須明確設定其要件及監督機制，以避免不當之人權侵害。

在未來情報通訊監察走向分別單獨立法之過程中，應以更明確的條文規範情報通訊監察細節，設定合理之限制要件及明確之監督方式，兼顧效率及人權之保障，才能避免人民對情報通訊監察之質疑，未明確規範而模糊範圍中運作之情報工作才是扼殺人民對情報機關信心的黑手。

現今監視器發達的年代，在電梯與路口安裝監視器被視爲正常，雖有人質疑侵擾人權，但它爲防治犯罪帶來利益，甚至未裝或損壞未修者尚會受指責未善盡職責。[242]由此可見，在限縮部份人權時，若衡定了適當之監控邊界，則其限制並不一定會受到阻抗，但若監視器安裝於他人私宅門口則踰越法規所承認之監控邊界而爲違法。相同的，情報通訊監察法規之制定，立法者亦應衡量情報通訊監察最佳之監控邊界，什麼是最佳之監控邊界可以滿足國家安全之維護，同時又能讓人民欣然同意爲該權利之限縮，尚待學者、立法者與情報機關間之持續溝通研究，並參考外國立法例，期能找出保障人民最大權益之道。

[242] 王俊秀，監控社會與個人隱私：關於監控邊界的研究，天津人民出版社，頁 13，2006 年。周玄明，隨機性國際通訊情報偵蒐法制研究，國防大學法律學系碩士學位論文，註 372，頁 85-86，2010 年 1 月。

參考文獻：

中文文獻

專書

王兆鵬，刑事訴訟講義（一），2003 年。

李震山，警察行政法論-自由與秩序之折衝，元照出照公司，2007 年 9 月初版。

林鈺雄，刑事訴訟法上，2001 年。

陳運財，「通訊之監察」，何賴傑、林鈺雄、陳運財合著「刑事訴訟實例研習」，2000 年 6 月。

通訊保障及監察法行政院提案，通訊保障及監察法案(上) 「法律案專輯. 第 274 輯, 司法; 24」，立法院司法委員會編輯，2002 年 10 月。

通訊監察法草案研究制定資料彙編，法務部印行，1992 年。

期刊論文

王俊秀，監控社會與個人隱私：關於監控邊界的研究，天津人民出版社，2006 年。

李榮耕，析論我國情報通訊監察法制-以美國法制爲比較，軍法專刊，56 卷 5 期，2010 年 10 月 1 日。

李榮耕，特定明確原則與機動性通訊監察，政大法學評論第 126 期，2012 年 4 月。

李惠宗，行政法院裁判系列研究（十）行政法院有關不確定法律概念判斷之審查，96 年度國科會研究計畫精簡報告，2007 年。

吳兆琰，論網路環境下的通訊監察法制，科技法律透析，17 卷 2 期，2005 年 2 月。

林鈺雄，論通訊之監察—評析歐洲人權法院相關裁判之發展與影響，東吳法律學報十九卷第四期，2008 年 4 月。

周霎蘭，違法監聽所取得證據之證據能力，司法新聲，2007 年。

周治平，情報機關通訊監察權之研究--德國法之啓示，警大法學論集第 15 期，2008 年 10 月。

周治平，情報機關秘密情報蒐集之法律問題，東吳法研論集第五卷，2009 年 12

月。
秦策，德國刑事訴訟中的證據禁止：理論、規則與司法技術，法術現代化研究第9卷，2004年。
陳瑞仁，如何由法制面提升警察辦案品質，月旦法學，第56期，2000年10月。
許宗力，法與國家權力，月旦出版社，1998 年。
馮震宇，網路犯罪與網路犯罪公約（下），月旦法學教室，第5期，2003年3月。
張明偉，監聽風雲—以通訊監察進行國家情報工作之規範檢討，軍法專刊第56卷第6期，2010年12月。
曾正一，台美通訊監察制度之比較研究，釋字631號解釋與監聽法制評析學術研討會論文集，2008年。
楊雲驊，保障「私人生活不可侵犯之核心領域」--德國聯邦憲法法院對於「住宅內監聽」（大監聽）違憲審查判決簡評，財團法人民間司法改革基金會電子報，2006年6月25。
楊雲驊，另案監聽—評最高法院97年台上字第2633號判決，台灣法學第116期，2008年11月15日。
詹鎮榮，秘密通訊自由，法學講座，21期，2003年9月。
蔡庭榕，論反恐怖主義行動法制與人權保障，刑事法雜誌第47卷第4期，2003年10月。
廖元豪，美國反恐怖主義相關法律措施之簡介與評論，月旦法學雜誌，第80期，2002年1月。
廖元豪，多少罪惡假國家安全之名而行？-簡介美國反恐措施對人權之侵蝕，月旦法學，第131期，2006年4月。
謝佑平、謝立軍，德國的秘密偵查制度，甘肅政法學院學報，2011年第6期，2011年。
蕭文生，關於「一九八三年人口普查法」之判決，收錄於西德聯邦憲法法院裁判選輯(一)，司法週刊雜誌社，1990年10月。

學位論文

江舜明，刑事偵查監聽容許界限之研究，國立臺北大學法律系博士論文，2004

年。
林俊雄，國家情報工作中通訊監察之探討-以台美兩國法制面之比較爲中心，中央警察大學公共安全研究所碩士論文，2006 年。
林源湧，違法搜索之救濟，政治大學法學院碩士論文，2007 年。
林進財，我國情報通訊監察之研究，淡江大學國際事務與戰略研究所碩士論文，2007 年。
周玄明，隨機性國際通訊情報偵蒐法制研究，國防大學法學系碩士學位論文，2010 年 1 月。
徐智明，通訊監察之保障及規範，國立中正大學法學研究所碩士論文，民國 93 年 6 月。
蔡達智，公權力利用衛星科技對隱私權之影響-以美國法爲中心，國立政治大學博士學位論文，2005 年。
賴建宏，論情報法制與情報監督-英國與我國之制度比較，中央警察大學外事警察研究所碩士學位論文，2009 年。
錢世傑，網路通訊監察法制與相關問題研究，中原大學碩士論文，2002 年 7 月。
蘇三榮，網路時代通訊監察與個人資料保護之法制研究，國立交通大學碩士論文，2009 年 6 月。

網路資訊
中華民國 99 年司法統計年報，司法院，2010 年，
http://www.judicial.gov.tw/juds/year99/contents_table_ch.htm
中華民國 98 年司法統計年報，司法院，2009 年，
http://www.judicial.gov.tw/juds/year98/contents_table_ch.htm
通訊保障及監察法外國法案介紹，立法院國會圖書館，
http://npl.ly.gov.tw/do/www/billIntroductionContent?id=27，2006 年 6 月。
國內犯罪案件通訊監察作業執行要點，
http://mojlaw.moj.gov.tw/LawContent.aspx?id=FL010193
陳青田，反恐怖主義立法與關鍵議題之研究，
fel.toko.edu.tw/attachments/144_(465-476).doc，2010 年。
連耀南，新世代通訊網路導論－從法規面與技術面看網路電話的前景，國立政治

大學行動計算與網路通訊實驗室（二）研究成果，
http://www.cs.nccu.edu.tw/~lien/Writing/NGN/ch2.htm。
國安局：馬總統上台 監聽量少 7 成，中央社，
http://news.rti.org.tw/index_newsContent.aspx?nid=217412&id2=1，2009 年 9 月 28 日。
通訊監察作業專案調查報告，國家安全局，
http://www.nsb.gov.tw/documents/%e9%80%9a%e8%a8%8a%e7%9b%a3%e5%af%9f%e4%bd%9c%e6%a5%ad%e5%b0%88%e6%a1%88%e8%aa%bf%e6%9f%a5%e5%a0%b1%e5%91%8a.PDF，2009 年 10 月 12 日。
通保新制上路 2 年 具體成效頗可觀，司法週刊電子報第 1471 期，
http://www.judicial.gov.tw/ jw9706/1471_main.html#2，2009 年 12 月 17 日。
曾依璇，情報與犯罪監聽國安局想區隔，中央社，
http://n.yam.com/cna/politics/201008/20100822444726.html，2010 年 8 月 22 日報導。
檢察制度世紀回顧，台灣高等法院檢察署網站
http://www.tph.moj.gov.tw/ct.asp?xItem=198649&ctNode=28712,資料最後更新日期:2011 年 12 月 21 日

判決
臺北高等行政法院 95 年度訴字第 04088 號裁定，96 年 12 月 31 日。
最高法院民事裁定 100 年度台上字第 2184 號，100 年 12 月 21 日。

英文文獻
專書
Eric Rosenbach, “The USA-Patriot Act”, Confrontation or Collaboration? Congress and the Intelligence Community, Belfer Center for Science and International Affairs, Harvard Kennedy School.(2009)
Elizabeth B. Bazan, The Foreign Intelligence Surveillance Act: An Overview of the Satatutory Framework and Recent Judicial Decisions, CRS Report for Congress. (2004)
Elizabeth B. Bazan, Intelligence Reform and Terrorism Prevention Act of 2004: “Lone Wolf” Amendment to the Foreign Intelligence Surveillance Act, CRS Report for Congress (2004)

James G. McAdams, Foreign Intelligence Surveillance Act (FISA):An Overview(2007)
Peter M. Thomson, White Paper on The USA PATRIOT Act’s “Roving” Electronic Surveillance Amendment to the Foreign Intelligence Surveillance Act, The Federalist Society for Law and Public Policy Studies. (2004)

期刊論文

Jessica LoConte, FISA Amendments Act 2008:Protecting Americans by Monitoring International Communication—Is It Reasonable?, Pace International Law Review Online Companion, 2010.1.1.(2010)
Norbet Putter, Statewatch Analysis Germany - The Federal Republic’s security services from the Cold War o the “new security architecture”, Statewatch Journal, vol 19 no 4.(2009)

網路資訊

ACLU Argues Dragnet Surveillance of Americans Is Unconstitutional, ACLU, http://www.aclu.org/national-security/obama-administration-asks-supreme-court-dismiss-aclu-challenge-warrantless , (2012.2.17.).
Alexander Boulerian, Germany: new law allows more extensive government monitoring of phone calls and email, http://www.wsws.org/articles/2001/feb2001/germ-f20.shtml, (2001.2.20.)
Applications made to the foreign intelligence surveillance court during calendar year 2002-2010，U.S. Department of Justice Office of Legislative Affairs，http://www.fas.org/irp/agency/doj/fisa/2010rept.pdf ~ http://www.fas.org/irp/agency/doj/fisa/2010rept.pdf
CHARLIE SAVAGE and JAMES RISEN, Federal Judge Finds N.S.A. Wiretaps Were Illegal,New York Times, http://www.nytimes.com/2010/04/01/us/01nsa.html, (2010.3.31)
Edited by Jeffery Richelson and Thomas Blanton, Electronic Surveillance From the Cold War to Al-Qaeda, National Security Archive Electronic Briefing Book No.178, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB178/index.htm
Echelon And FISA,

http://www.moonofalabama.org/2005/12/why_not_to_use_.html ,2005.12.20.
Executive Order 12333,
http://www.archives.gov/federal-register/codification/executive-order/12333.html
Foreign Intelligence Surveillance Court of Review,
http://legal-dictionary.thefreedictionary.com/Foreign+Intelligence+Surveillance+Court+of+Review
Franks hearing law and legal definition, http://definitions.uslegal.com/f/franks-hearing/
Foreign Intelligence Surveillance Act Court Orders 0979-2010，Electronic Privacy Information Center(2011)，http://epic.org/privacy/siretap/stats/fisa_stats.html
Gillian Wong，China set to tighten state-secrets law forcing Internet firms to inform on users, The Washington Post，2010.04.28.
JAMES RISEN and ERIC LICHTBLAU, Bush Lets U.S. Spy on Callers Without Courts, New York Times (2005.11.26.),
http://www.nytimes.com/2005/12/16/politics/16program.html?th
Jason Leopold, Revisiting Echelon: The NSA’s Clandestine Data Mining Program, http://pubrecord.org/nation/2290/revisiting-echelon-nsas/ (2009.7.15.).
John Diamond，NSA's surveillance of citizens echoes 1970s controversy，USA TODAY，
http://www.usatoday.com/news/washington/2005-12-18-nsa-70s_x.htm ,(2005.12.18)
Kim Lane Scheppele, Other People’s Patriot Acts: Europe’s Response to September 11, Scholarship at Penn Law,Page.115 , 2004.10.1
Nicole E. Jacoby, Alston & Bird, LLP, Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and the United States, Berkeley Electronic Press, http://law.bepress.com/expresso/eps/1515/, 2006.
THE ATTORNEY GENERAL'S GUIDELINES FOR. FBI NATIONAL SECURITY INVESTIGATIONS. AND FOREIGN INTELLIGENCE COLLECTION, http://www.fas.org/irp/agency/doj/fbi/nsiguidelines.pdf,(2003.10.31.)

判決

Amnesty et al. v McConnell Complaint, (2008).

United States v. United States District Court,407 U.S. 297(1972).

American Civil Liberties Union et al., v. National Security Agency / Central et al., 493 F.3d 644 (6th Cir. 2007).

Al-Haramain et. al v. Obama et. al, Case No C 07-0109 VRW (U.S. District Court for the Northern District of California 2010).

http://www.wired.com/images_blogs/threatlevel/2010/03/walker.pdf

European Court Of Human Rights Third Section Decision as to The Admissibility of Applicatio no. 54934/00 by Gabriele Weber and Cesar Richard Saravia against Germany, (2006).

Franks v. Delaware, 438 U.S. 154 (1978).

In re Sealed Case No. 02-001, 310 F.3d 717 (FISCR 2002).

Katz v. United State, 389 U.S.347(1967)

United States v. Holy Land Foundation for Relief and Development, No.09-10875, 664 F.3d 467, 2011 U.S. App. LEXIS 24216, (5th Cir. 2011)

United States of America v. David Belfield, Aka Daoud Salahuddin Ali Abdul-Mani, Aka Lee Curtis Manning, Appellant; United States of America v. David Belfield, Aka Daoud Salahuddin Horace Anthony Butler, Aka Ahmed Rauf, Appellant, Nos.81-2152,81-2155. United States Court Of Appeals For the District Of Columbia Circuit, 1982.11.5.

United States v. Brown, 298 F.3d 392, 395 (5th Cir. 2002)

德文文獻

專書

Schlink, a. a. O.(Fn.14), S.553.

期刊論文

Huber, Das neue G10-Gesetz, NJW 2001, S.3300.

Vgl. Gabriele Gross-Spreitzer, Die Grenzen der Telefonüberwachung nach § 100a,100b stop unten Berücksichtigung der Aussageverweigerungsrechte im

Strafprozess, Diss. Heidelberg, 1987, S. 7-10

Vgl. Hermann Borgs-Maciejewski/Frank Ebert, Das Recht der Geheimdienste-Kommentar zum Bundesverfassungsschutzgesetz sowie zum G10,1986,S.139.

三、判決

1 BvR 209/83 u.a., BVerfGE 65, 1, Dezember 1983.

BVerfGE 109, 279 (2004).

四、網路資訊

德國聯邦議院發佈 16 / 11559 文件(Deutscher Bundestag Drucksache 16/11559)，2007 年度德國聯邦議會監督委員會年度報告，2009 年 1 月。

http://dipbt.bundestag.de/dip21/btd/16/115/1611559.pdf。

附錄一：美國外國情報通訊監察法The Foreign Intelligence Surveillance Act of 1978 (FISA)

TITLE 50 - WAR AND NATIONAL DEFENSE

CHAPTER 36 - FOREIGN INTELLIGENCE SURVEILLANCE

SUBCHAPTER I - ELECTRONIC SURVEILLANCE

Sec.

50 USC § 1801 - Definitions

As used in this subchapter:

(a) “Foreign power” means—

(1) a foreign government or any component thereof, whether or not recognized by the United States;

(2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons;

(6) an entity that is directed and controlled by a foreign government or governments; or
(7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.
(b) “Agent of a foreign power” means—
(1) any person other than a United States person, who—
(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;
(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person’s presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;
(C) engages in international terrorism or activities in preparation therefore;
(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or
(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor for or on behalf of a foreign power; or
(2) any person who—
(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).
(c) “International terrorism” means activities that—
(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
(2) appear to be intended—
(A) to intimidate or coerce a civilian population;
(B) to influence the policy of a government by intimidation or coercion; or
(C) to affect the conduct of a government by assassination or kidnapping; and
(3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.
(d) “Sabotage” means activities that involve a violation of chapter 105 of title 18, or that would involve such a violation if committed against the United States.
(e) “Foreign intelligence information” means—
(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
(A) the national defense or the security of the United States; or
(B) the conduct of the foreign affairs of the United States.
(f) “Electronic surveillance” means—
(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person

who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511 (2)(i) of title 18;
(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.
(g) "Attorney General" means the Attorney General of the United States (or Acting Attorney General), the Deputy Attorney General, or, upon the designation of the Attorney General, the Assistant Attorney General designated as the Assistant Attorney General for National Security under section 507A of title 28.
(h) "Minimization procedures", with respect to electronic surveillance, means—
(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802 (a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.
(i) "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101 (a)(20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.
(j) "United States", when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands.
(k) "Aggrieved person" means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.
(l) "Wire communication" means any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.
(m) "Person" means any individual, including any officer or employee of the Federal Government, or any group, entity, association, corporation, or foreign power.
(n) "Contents", when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.
(o) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Trust Territory of the Pacific Islands, and any territory or possession of the United States.
(p) "Weapon of mass destruction" means—

(1) any explosive, incendiary, or poison gas device that is designed, intended, or has the capability to cause a mass casualty incident;
(2) any weapon that is designed, intended, or has the capability to cause death or serious bodily injury to a significant number of persons through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors;
(3) any weapon involving a biological agent, toxin, or vector (as such terms are defined in section 178 of title 18) that is designed, intended, or has the capability to cause death, illness, or serious bodily injury to a significant number of persons; or
(4) any weapon that is designed, intended, or has the capability to release radiation or radioactivity causing death, illness, or serious bodily injury to a significant number of persons.

50 USC § 1802 - Electronic surveillance authorization without court order; certification by Attorney General; reports to Congressional committees; transmittal under seal; duties and compensation of communication common carrier; applications; jurisdiction
(a)
(1) Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that—
(A) the electronic surveillance is solely directed at—
(i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801 (a)(1), (2), or (3) of this title; or
(ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 1801 (a)(1), (2), or (3) of this title;
(B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and
(C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801 (h) of this title; and
if the Attorney General reports such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately.
(2) An electronic surveillance authorized by this subsection may be conducted only in accordance with the Attorney General's certification and the minimization procedures adopted by him. The Attorney General shall assess compliance with such procedures and shall report such assessments to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence under the provisions of section 1808 (a) of this title.
(3) The Attorney General shall immediately transmit under seal to the court established under section 1803 (a) of this title a copy of his certification. Such certification shall be maintained under security measures established by the Chief Justice with the concurrence of the Attorney General, in consultation with the Director of National Intelligence, and shall remain sealed unless—
(A) an application for a court order with respect to the surveillance is made under sections 1801 (h)(4) and 1804 of this title; or
(B) the certification is necessary to determine the legality of the surveillance under section 1806 (f) of this title.
(4) With respect to electronic surveillance authorized by this subsection, the Attorney General may direct a specified communication common carrier to—
(A) furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers; and
(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the surveillance or the aid furnished which such carrier wishes to retain.
The Government shall compensate, at the prevailing rate, such carrier for furnishing such aid.
(b) Applications for a court order under this subchapter are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to the court having jurisdiction under section 1803 of this title, and a judge to whom an application is made may, notwithstanding any other law, grant an order, in conformity with section 1805 of this title, approving electronic

surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information, except that the court shall not have jurisdiction to grant any order approving electronic surveillance directed solely as described in paragraph (1)(A) of subsection (a) of this section unless such surveillance may involve the acquisition of communications of any United States person.

50 USC § 1803 - Designation of judges

(a) **Court to hear applications and grant orders; record of denial; transmittal to court of review**

(1) The Chief Justice of the United States shall publicly designate 11 district court judges from at least seven of the United States judicial circuits of whom no fewer than 3 shall reside within 20 miles of the District of Columbia who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this chapter, except that no judge designated under this subsection (except when sitting en banc under paragraph (2)) shall hear the same application for electronic surveillance under this chapter which has been denied previously by another judge designated under this subsection. If any judge so designated denies an application for an order authorizing electronic surveillance under this chapter, such judge shall provide immediately for the record a written statement of each reason of his decision and, on motion of the United States, the record shall be transmitted, under seal, to the court of review established in subsection (b) of this section.

(2)

(A) The court established under this subsection may, on its own initiative, or upon the request of the Government in any proceeding or a party under section 1861 (f) of this title or paragraph (4) or (5) of section 1881a (h) of this title, hold a hearing or rehearing, en banc, when ordered by a majority of the judges that constitute such court upon a determination that—

(i) en banc consideration is necessary to secure or maintain uniformity of the court's decisions; or

(ii) the proceeding involves a question of exceptional importance.

(B) Any authority granted by this chapter to a judge of the court established under this subsection may be exercised by the court en banc. When exercising such authority, the court en banc shall comply with any requirements of this chapter on the exercise of such authority.

(C) For purposes of this paragraph, the court en banc shall consist of all judges who constitute the court established under this subsection.

(b) **Court of review; record, transmittal to Supreme Court**

The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals who together shall comprise a court of review which shall have jurisdiction to review the denial of any application made under this chapter. If such court determines that the application was properly denied, the court shall immediately provide for the record a written statement of each reason for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

(c) **Expeditious conduct of proceedings; security measures for maintenance of records**

Proceedings under this chapter shall be conducted as expeditiously as possible. The record of proceedings under this chapter, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence.

(d) **Tenure**

Each judge designated under this section shall so serve for a maximum of seven years and shall not be eligible for redesignation, except that the judges first designated under subsection (a) of this section shall be designated for terms of from one to seven years so that one term expires each year, and that judges first designated under subsection (b) of this section shall be designated for terms of three, five, and seven years.

(e) **Jurisdiction and procedures for review of petitions**

(1) Three judges designated under subsection (a) who reside within 20 miles of the District of Columbia, or, if all of such judges are unavailable, other judges of the court established under subsection (a) as may be designated by the presiding judge of such court, shall comprise a petition review pool which shall have jurisdiction to review petitions filed pursuant to section 1861 (f)(1) or 1881a (h)(4) of this title.

(2) Not later than 60 days after March 9, 2006, the court established under subsection (a) shall adopt and, consistent with the protection of national security, publish procedures for the review of petitions filed pursuant to section 1861 (f)(1) or 1881a (h)(4) of this title by the panel established under paragraph (1). Such procedures shall provide that review of a petition shall be conducted in camera and shall also provide for the designation of an acting presiding judge.

(f) **Stay of order**
(1) A judge of the court established under subsection (a), the court established under subsection (b) or a judge of that court, or the Supreme Court of the United States or a justice of that court, may, in accordance with the rules of their respective courts, enter a stay of an order or an order modifying an order of the court established under subsection (a) or the court established under subsection (b) entered under any subchapter of this chapter, while the court established under subsection (a) conducts a rehearing, while an appeal is pending to the court established under subsection (b), or while a petition of certiorari is pending in the Supreme Court of the United States, or during the pendency of any review by that court.
(2) The authority described in paragraph (1) shall apply to an order entered under any provision of this chapter.
(g) **Establishment and transmittal of rules and procedures**
(1) The courts established pursuant to subsections (a) and (b) may establish such rules and procedures, and take such actions, as are reasonably necessary to administer their responsibilities under this chapter.
(2) The rules and procedures established under paragraph (1), and any modifications of such rules and procedures, shall be recorded, and shall be transmitted to the following:
(A) All of the judges on the court established pursuant to subsection (a).
(B) All of the judges on the court of review established pursuant to subsection (b).
(C) The Chief Justice of the United States.
(D) The Committee on the Judiciary of the Senate.
(E) The Select Committee on Intelligence of the Senate.
(F) The Committee on the Judiciary of the House of Representatives.
(G) The Permanent Select Committee on Intelligence of the House of Representatives.
(3) The transmissions required by paragraph (2) shall be submitted in unclassified form, but may include a classified annex.
(h) **Compliance with orders, rules, and procedures**
Nothing in this chapter shall be construed to reduce or contravene the inherent authority of the court established under subsection (a) to determine or enforce compliance with an order or a rule of such court or with a procedure approved by such court.

50 USC § 1804 - Applications for court orders
(a) **Submission by Federal officer; approval of Attorney General; contents**
Each application for an order approving electronic surveillance under this subchapter shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 1803 of this title. Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this subchapter. It shall include—
(1) the identity of the Federal officer making the application;
(2) the identity, if known, or a description of the specific target of the electronic surveillance;
(3) a statement of the facts and circumstances relied upon by the applicant to justify his belief that—
(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and
(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
(4) a statement of the proposed minimization procedures;
(5) a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;
(6) a certification or certifications by the Assistant to the President for National Security Affairs, an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official—
(A) that the certifying official deems the information sought to be foreign intelligence information;
(B) that a significant purpose of the surveillance is to obtain foreign intelligence information;
(C) that such information cannot reasonably be obtained by normal investigative techniques;
(D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801 (e) of this title; and
(E) including a statement of the basis for the certification that—
(i) the information sought is the type of foreign intelligence information designated; and
(ii) such information cannot reasonably be obtained by normal investigative techniques;

(7) a summary statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;
(8) a statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application; and
(9) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this subchapter should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter.
(b) **Additional affidavits or certifications**
The Attorney General may require any other affidavit or certification from any other officer in connection with the application.
(c) **Additional information**
The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 1805 of this title.
(d) **Personal review by Attorney General**
(1)
(A) Upon written request of the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, the Director of National Intelligence, or the Director of the Central Intelligence Agency, the Attorney General shall personally review under subsection (a) of this section an application under that subsection for a target described in section 1801 (b)(2) of this title.
(B) Except when disabled or otherwise unavailable to make a request referred to in subparagraph (A), an official referred to in that subparagraph may not delegate the authority to make a request referred to in that subparagraph.
(C) Each official referred to in subparagraph (A) with authority to make a request under that subparagraph shall take appropriate actions in advance to ensure that delegation of such authority is clearly established in the event such official is disabled or otherwise unavailable to make such request.
(2)
(A) If as a result of a request under paragraph (1) the Attorney General determines not to approve an application under the second sentence of subsection (a) of this section for purposes of making the application under this section, the Attorney General shall provide written notice of the determination to the official making the request for the review of the application under that paragraph. Except when disabled or otherwise unavailable to make a determination under the preceding sentence, the Attorney General may not delegate the responsibility to make a determination under that sentence. The Attorney General shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event the Attorney General is disabled or otherwise unavailable to make such determination.
(B) Notice with respect to an application under subparagraph (A) shall set forth the modifications, if any, of the application that are necessary in order for the Attorney General to approve the application under the second sentence of subsection (a) of this section for purposes of making the application under this section.
(C) Upon review of any modifications of an application set forth under subparagraph (B), the official notified of the modifications under this paragraph shall modify the application if such official determines that such modification is warranted. Such official shall supervise the making of any modification under this subparagraph. Except when disabled or otherwise unavailable to supervise the making of any modification under the preceding sentence, such official may not delegate the responsibility to supervise the making of any modification under that preceding sentence. Each such official shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event such official is disabled or otherwise unavailable to supervise the making of such modification.

50 USC § 1805 - Issuance of order
(a) **Necessary findings**
Upon an application made pursuant to section 1804 of this title, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that—
(1) the application has been made by a Federal officer and approved by the Attorney General;
(2) on the basis of the facts submitted by the applicant there is probable cause to believe that—
(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely

upon the basis of activities protected by the first amendment to the Constitution of the United States; and
(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
(3) the proposed minimization procedures meet the definition of minimization procedures under section 1801 (h) of this title; and
(4) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804 (a)(7)(E) [1] of this title and any other information furnished under section 1804 (d) [1] of this title.
(b) **Determination of probable cause**
In determining whether or not probable cause exists for purposes of an order under subsection (a)(2) of this section, a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.
(c) **Specifications and directions of orders**
(1) **Specifications**
An order approving an electronic surveillance under this section shall specify—
(A) the identity, if known, or a description of the specific target of the electronic surveillance identified or described in the application pursuant to section 1804 (a)(3) of this title;
(B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known;
(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;
(D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance; and
(E) the period of time during which the electronic surveillance is approved.
(2) **Directions**
An order approving an electronic surveillance under this section shall direct—
(A) that the minimization procedures be followed;
(B) that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person, or in circumstances where the Court finds, based upon specific facts provided in the application, that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons, furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;
(C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and
(D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.
(3) **Special directions for certain orders**
An order approving an electronic surveillance under this section in circumstances where the nature and location of each of the facilities or places at which the surveillance will be directed is unknown shall direct the applicant to provide notice to the court within ten days after the date on which surveillance begins to be directed at any new facility or place, unless the court finds good cause to justify a longer period of up to 60 days, of—
(A) the nature and location of each new facility or place at which the electronic surveillance is directed;
(B) the facts and circumstances relied upon by the applicant to justify the applicant's belief that each new facility or place at which the electronic surveillance is directed is or was being used, or is about to be used, by the target of the surveillance;
(C) a statement of any proposed minimization procedures that differ from those contained in the original application or order, that may be necessitated by a change in the facility or place at which the electronic surveillance is directed; and
(D) the total number of electronic surveillances that have been or are being conducted under the authority of the order.
(d) **Duration of order; extensions; review of circumstances under which information was acquired, retained or disseminated**
(1) An order issued under this section may approve an electronic surveillance for the period necessary

to achieve its purpose, or for ninety days, whichever is less, except that
(A) an order under this section shall approve an electronic surveillance targeted against a foreign power, as defined in section 1801 (a)(1), (2), or (3) of this title, for the period specified in the application or for one year, whichever is less, and
(B) an order under this chapter for a surveillance targeted against an agent of a foreign power who is not a United States person may be for the period specified in the application or for 120 days, whichever is less.
(2) Extensions of an order issued under this subchapter may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order, except that
(A) an extension of an order under this chapter for a surveillance targeted against a foreign power, as defined in paragraph (5), (6), or (7) of section 1801 (a) of this title, or against a foreign power as defined in section 1801 (a)(4) of this title that is not a United States person, may be for a period not to exceed one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period, and
(B) an extension of an order under this chapter for a surveillance targeted against an agent of a foreign power who is not a United States person may be for a period not to exceed 1 year.
(3) At or before the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.
(e) **Emergency orders**
(1) Notwithstanding any other provision of this subchapter, the Attorney General may authorize the emergency employment of electronic surveillance if the Attorney General—
(A) reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained;
(B) reasonably determines that the factual basis for the issuance of an order under this subchapter to approve such electronic surveillance exists;
(C) informs, either personally or through a designee, a judge having jurisdiction under section 1803 of this title at the time of such authorization that the decision has been made to employ emergency electronic surveillance; and
(D) makes an application in accordance with this subchapter to a judge having jurisdiction under section 1803 of this title as soon as practicable, but not later than 7 days after the Attorney General authorizes such surveillance.
(2) If the Attorney General authorizes the emergency employment of electronic surveillance under paragraph (1), the Attorney General shall require that the minimization procedures required by this subchapter for the issuance of a judicial order be followed.
(3) In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.
(4) A denial of the application made under this subsection may be reviewed as provided in section 1803 of this title.
(5) In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.
(6) The Attorney General shall assess compliance with the requirements of paragraph (5).
(f) **Testing of electronic equipment; discovering unauthorized electronic surveillance; training of intelligence personnel**
Notwithstanding any other provision of this subchapter, officers, employees, or agents of the United States are authorized in the normal course of their official duties to conduct electronic surveillance not targeted against the communications of any particular person or persons, under procedures approved by the Attorney General, solely to—
(1) test the capability of electronic equipment, if—

(A) it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;
(B) the test is limited in extent and duration to that necessary to determine the capability of the equipment;
(C) the contents of any communication acquired are retained and used only for the purpose of determining the capability of the equipment, are disclosed only to test personnel, and are destroyed before or immediately upon completion of the test; and:
(D) Provided, That the test may exceed ninety days only with the prior approval of the Attorney General;
(2) determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, if—
(A) it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance;
(B) such electronic surveillance is limited in extent and duration to that necessary to determine the existence and capability of such equipment; and
(C) any information acquired by such surveillance is used only to enforce chapter 119 of title 18, or section 605 of title 47, or to protect information from unauthorized surveillance; or
(3) train intelligence personnel in the use of electronic surveillance equipment, if—
(A) it is not reasonable to—
(i) obtain the consent of the persons incidentally subjected to the surveillance;
(ii) train persons in the course of surveillances otherwise authorized by this subchapter; or
(iii) train persons in the use of such equipment without engaging in electronic surveillance;
(B) such electronic surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and
(C) no contents of any communication acquired are retained or disseminated for any purpose, but are destroyed as soon as reasonably possible.
(g) **Retention of certifications, applications and orders**
Certifications made by the Attorney General pursuant to section 1802 (a) of this title and applications made and orders granted under this subchapter shall be retained for a period of at least ten years from the date of the certification or application.
(h) **Bar to legal action**
No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this chapter for electronic surveillance or physical search.
(i) **Pen registers and trap and trace devices**
In any case in which the Government makes an application to a judge under this subchapter to conduct electronic surveillance involving communications and the judge grants such application, upon the request of the applicant, the judge shall also authorize the installation and use of pen registers and trap and trace devices, and direct the disclosure of the information set forth in section 1842 (d)(2) of this title.

50 USC § 1806 - Use of information
(a) **Compliance with minimization procedures; privileged communications; lawful purposes**
Information acquired from an electronic surveillance conducted pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter. No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this subchapter shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.
(b) **Statement for disclosure**
No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.
(c) **Notification by United States**
Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the

Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

(d) **Notification by States or political subdivisions**

Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(e) **Motion to suppress**

Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that—

(1) the information was unlawfully acquired; or

(2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) **In camera and ex parte review by district court**

Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(g) **Suppression of evidence; denial of motion**

If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) **Finality of orders**

Orders granting motions or requests under subsection (g) of this section, decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

(i) **Destruction of unintentionally acquired information**

In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

(j) **Notification of emergency employment of electronic surveillance; contents; postponement,**

suspension or elimination
If an emergency employment of electronic surveillance is authorized under section 1805 (e) of this title and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of—
(1) the fact of the application;
(2) the period of the surveillance; and
(3) the fact that during the period information was or was not obtained.
On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.
(k) **Coordination with law enforcement on national security matters**
(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this subchapter may consult with Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision) to coordinate efforts to investigate or protect against—
(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.
(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 1804 (a)(7)(B) [1] of this title or the entry of an order under section 1805 of this title.

50 USC § 1807 - Report to Administrative Office of the United States Court and to Congress
In April of each year, the Attorney General shall transmit to the Administrative Office of the United States Court and to Congress a report setting forth with respect to the preceding calendar year—
(a) the total number of applications made for orders and extensions of orders approving electronic surveillance under this subchapter; and
(b) the total number of such orders and extensions either granted, modified, or denied.

50 USC § 1808 - Report of Attorney General to Congressional committees; limitation on authority or responsibility of information gathering activities of Congressional committees; report of Congressional committees to Congress
(a)
(1) On a semiannual basis the Attorney General shall fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, and the Committee on the Judiciary of the Senate, concerning all electronic surveillance under this subchapter. Nothing in this subchapter shall be deemed to limit the authority and responsibility of the appropriate committees of each House of Congress to obtain such information as they may need to carry out their respective functions and duties.
(2) Each report under the first sentence of paragraph (1) shall include a description of—
(A) the total number of applications made for orders and extensions of orders approving electronic surveillance under this subchapter where the nature and location of each facility or place at which the electronic surveillance will be directed is unknown;
(B) each criminal case in which information acquired under this chapter has been authorized for use at trial during the period covered by such report; and
(C) the total number of emergency employments of electronic surveillance under section 1805 (e) of this title and the total number of subsequent orders approving or denying such electronic surveillance.
(b) On or before one year after October 25, 1978, and on the same day each year for four years thereafter, the Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence shall report respectively to the House of Representatives and the Senate, concerning the implementation of this chapter. Said reports shall include but not be limited to an analysis and recommendations concerning whether this chapter should be
(1) amended,
(2) repealed, or

(3) permitted to continue in effect without amendment.

50 USC § 1809 - Criminal sanctions
(a) **Prohibited activities**
A person is guilty of an offense if he intentionally—
(1) engages in electronic surveillance under color of law except as authorized by this chapter, chapter 119, 121, or 206 of title 18, or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 1812 of this title;
(2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this chapter, chapter 119, 121, or 206 of title 18, or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 1812 of this title.
(b) **Defense**
It is a defense to a prosecution under subsection (a) of this section that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.
(c) **Penalties**
An offense described in this section is punishable by a fine of not more than $10,000 or imprisonment for not more than five years, or both.
(d) **Federal jurisdiction**
There is Federal jurisdiction over an offense under this section if the person committing the offense was an officer or employee of the United States at the time the offense was committed.

50 USC § 1810 - Civil liability
An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 1801 (a) or (b)(1)(A) of this title, respectively, who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 of this title shall have a cause of action against any person who committed such violation and shall be entitled to recover—
(a) actual damages, but not less than liquidated damages of $1,000 or $100 per day for each day of violation, whichever is greater;
(b) punitive damages; and
(c) reasonable attorney's fees and other investigation and litigation costs reasonably incurred.

50 USC § 1811 - Authorization during time of war
Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress.

50 USC § 1812 - Statement of exclusive means by which electronic surveillance and interception of certain communications may be conducted
(a) Except as provided in subsection (b), the procedures of chapters 119, 121, and 206 of title 18 and this chapter shall be the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted.
(b) Only an express statutory authorization for electronic surveillance or the interception of domestic wire, oral, or electronic communications, other than as an amendment to this chapter or chapters 119, 121, or 206 of title 18 shall constitute an additional exclusive means for the purpose of subsection (a).

附錄二：FISA2008 年修正案（FISA Amendments Act of 2008）

50 USC Chapter 36, Subchapter VI - ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES

50 USC § 1881 - Definitions

(a) **In general**

The terms “agent of a foreign power”, “Attorney General”, “contents”, “electronic surveillance”, “foreign intelligence information”, “foreign power”, “person”, “United States”, and “United States person” have the meanings given such terms in section 1801 of this title, except as specifically provided in this subchapter.

(b) **Additional definitions**

(1) **Congressional intelligence committees**

The term “congressional intelligence committees” means—

(A) the Select Committee on Intelligence of the Senate; and

(B) the Permanent Select Committee on Intelligence of the House of Representatives.

(2) **Foreign Intelligence Surveillance Court; Court**

The terms “Foreign Intelligence Surveillance Court” and “Court” mean the court established under section 1803 (a) of this title.

(3) **Foreign Intelligence Surveillance Court of Review; Court of Review**

The terms “Foreign Intelligence Surveillance Court of Review” and “Court of Review” mean the court established under section 1803 (b) of this title.

(4) **Electronic communication service provider**

The term “electronic communication service provider” means—

(A) a telecommunications carrier, as that term is defined in section 153 of title 47;

(B) a provider of electronic communication service, as that term is defined in section 2510 of title 18;

(C) a provider of a remote computing service, as that term is defined in section 2711 of title 18;

(D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or

(E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).

(5) **Intelligence community**

The term “intelligence community” has the meaning given the term in section 401a (4) of this title.

50 USC § 1881a - Procedures for targeting certain persons outside the United States other than United States persons

(a) Authorization

Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

(b) **Limitations**

An acquisition authorized under subsection (a)—

(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the

United States;
(3) may not intentionally target a United States person reasonably believed to be located outside the United States;
(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and
(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.
(c) **Conduct of acquisition**
(1) **In general**
An acquisition authorized under subsection (a) shall be conducted only in accordance with—
(A) the targeting and minimization procedures adopted in accordance with subsections (d) and (e); and
(B) upon submission of a certification in accordance with subsection (g), such certification.
(2) **Determination**
A determination under this paragraph and for purposes of subsection (a) is a determination by the Attorney General and the Director of National Intelligence that exigent circumstances exist because, without immediate implementation of an authorization under subsection (a), intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order pursuant to subsection (i)(3) prior to the implementation of such authorization.
(3) **Timing of determination**
The Attorney General and the Director of National Intelligence may make the determination under paragraph (2)—
(A) before the submission of a certification in accordance with subsection (g); or
(B) by amending a certification pursuant to subsection (i)(1)(C) at any time during which judicial review under subsection (i) of such certification is pending.
(4) **Construction**
Nothing in subchapter I shall be construed to require an application for a court order under such subchapter for an acquisition that is targeted in accordance with this section at a person reasonably believed to be located outside the United States.
(d) **Targeting procedures**
(1) **Requirement to adopt**
The Attorney General, in consultation with the Director of National Intelligence, shall adopt targeting procedures that are reasonably designed to—
(A) ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and
(B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.
(2) **Judicial review**
The procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).
(e) **Minimization procedures**
(1) **Requirement to adopt**
The Attorney General, in consultation with the Director of National Intelligence, shall adopt minimization procedures that meet the definition of minimization procedures under section 1801 (h) of this title or section 1821 (4) of this title, as appropriate, for acquisitions authorized under subsection (a).
(2) **Judicial review**
The minimization procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).
(f) **Guidelines for compliance with limitations**
(1) **Requirement to adopt**
The Attorney General, in consultation with the Director of National Intelligence, shall adopt guidelines to ensure—
(A) compliance with the limitations in subsection (b); and
(B) that an application for a court order is filed as required by this chapter.
(2) **Submission of guidelines**
The Attorney General shall provide the guidelines adopted in accordance with paragraph (1) to—
(A) the congressional intelligence committees;
(B) the Committees on the Judiciary of the Senate and the House of Representatives; and
(C) the Foreign Intelligence Surveillance Court.
(g) **Certification**

(1) **In general**
(A) **Requirement**
Subject to subparagraph (B), prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall provide to the Foreign Intelligence Surveillance Court a written certification and any supporting affidavit, under oath and under seal, in accordance with this subsection.
(B) **Exception**
If the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2) and time does not permit the submission of a certification under this subsection prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall submit to the Court a certification for such authorization as soon as practicable but in no event later than 7 days after such determination is made.
(2) **Requirements**
A certification made under this subsection shall—
(A) attest that—
(i) there are procedures in place that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court that are reasonably designed to—
(I) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and
(II) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States;
(ii) the minimization procedures to be used with respect to such acquisition—
(I) meet the definition of minimization procedures under section 1801 (h) or 1821 (4) of this title, as appropriate; and
(II) have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court;
(iii) guidelines have been adopted in accordance with subsection (f) to ensure compliance with the limitations in subsection (b) and to ensure that an application for a court order is filed as required by this chapter;
(iv) the procedures and guidelines referred to in clauses (i), (ii), and (iii) are consistent with the requirements of the fourth amendment to the Constitution of the United States;
(v) a significant purpose of the acquisition is to obtain foreign intelligence information;
(vi) the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider; and
(vii) the acquisition complies with the limitations in subsection (b);
(B) include the procedures adopted in accordance with subsections (d) and (e);
(C) be supported, as appropriate, by the affidavit of any appropriate official in the area of national security who is—
(i) appointed by the President, by and with the advice and consent of the Senate; or
(ii) the head of an element of the intelligence community;
(D) include—
(i) an effective date for the authorization that is at least 30 days after the submission of the written certification to the court; or
(ii) if the acquisition has begun or the effective date is less than 30 days after the submission of the written certification to the court, the date the acquisition began or the effective date for the acquisition; and
(E) if the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2), include a statement that such determination has been made.
(3) **Change in effective date**
The Attorney General and the Director of National Intelligence may advance or delay the effective date referred to in paragraph (2)(D) by submitting an amended certification in accordance with subsection (i)(1)(C) to the Foreign Intelligence Surveillance Court for review pursuant to subsection (i).
(4) **Limitation**
A certification made under this subsection is not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under subsection (a) will be directed or conducted.
(5) **Maintenance of certification**
The Attorney General or a designee of the Attorney General shall maintain a copy of a certification made under this subsection.

(6) **Review**
A certification submitted in accordance with this subsection shall be subject to judicial review pursuant to subsection (i).
(h) **Directives and judicial review of directives**
(1) **Authority**
With respect to an acquisition authorized under subsection (a), the Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to—
(A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and
(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain.
(2) **Compensation**
The Government shall compensate, at the prevailing rate, an electronic communication service provider for providing information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).
(3) **Release from liability**
No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).
(4) **Challenging of directives**
(A) **Authority to challenge**
An electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition to modify or set aside such directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.
(B) **Assignment**
The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 1803 (e)(1) of this title not later than 24 hours after the filing of such petition.
(C) **Standards for review**
A judge considering a petition filed under subparagraph (A) may grant such petition only if the judge finds that the directive does not meet the requirements of this section, or is otherwise unlawful.
(D) **Procedures for initial review**
A judge shall conduct an initial review of a petition filed under subparagraph (A) not later than 5 days after being assigned such petition. If the judge determines that such petition does not consist of claims, defenses, or other legal contentions that are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law, the judge shall immediately deny such petition and affirm the directive or any part of the directive that is the subject of such petition and order the recipient to comply with the directive or any part of it. Upon making a determination under this subparagraph or promptly thereafter, the judge shall provide a written statement for the record of the reasons for such determination.
(E) **Procedures for plenary review**
If a judge determines that a petition filed under subparagraph (A) requires plenary review, the judge shall affirm, modify, or set aside the directive that is the subject of such petition not later than 30 days after being assigned such petition. If the judge does not set aside the directive, the judge shall immediately affirm or affirm with modifications the directive, and order the recipient to comply with the directive in its entirety or as modified. The judge shall provide a written statement for the record of the reasons for a determination under this subparagraph.
(F) **Continued effect**
Any directive not explicitly modified or set aside under this paragraph shall remain in full effect.
(G) **Contempt of Court**
Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.
(5) **Enforcement of directives**
(A) **Order to compel**
If an electronic communication service provider fails to comply with a directive issued pursuant to paragraph (1), the Attorney General may file a petition for an order to compel the electronic communication service provider to comply with the directive with the Foreign Intelligence Surveillance

Court, which shall have jurisdiction to review such petition.
(B) **Assignment**
The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 1803 (e)(1) of this title not later than 24 hours after the filing of such petition.
(C) **Procedures for review**
A judge considering a petition filed under subparagraph (A) shall, not later than 30 days after being assigned such petition, issue an order requiring the electronic communication service provider to comply with the directive or any part of it, as issued or as modified, if the judge finds that the directive meets the requirements of this section and is otherwise lawful. The judge shall provide a written statement for the record of the reasons for a determination under this paragraph.
(D) **Contempt of Court**
Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.
(E) **Process**
Any process under this paragraph may be served in any judicial district in which the electronic communication service provider may be found.
(6) **Appeal**
(A) **Appeal to the Court of Review**
The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition with the Foreign Intelligence Surveillance Court of Review for review of a decision issued pursuant to paragraph (4) or (5). The Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this subparagraph.
(B) **Certiorari to the Supreme Court**
The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.
(i) **Judicial review of certifications and procedures**
(1) **In general**
(A) **Review by the Foreign Intelligence Surveillance Court**
The Foreign Intelligence Surveillance Court shall have jurisdiction to review a certification submitted in accordance with subsection (g) and the targeting and minimization procedures adopted in accordance with subsections (d) and (e), and amendments to such certification or such procedures.
(B) **Time period for review**
The Court shall review a certification submitted in accordance with subsection (g) and the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and shall complete such review and issue an order under paragraph (3) not later than 30 days after the date on which such certification and such procedures are submitted.
(C) **Amendments**
The Attorney General and the Director of National Intelligence may amend a certification submitted in accordance with subsection (g) or the targeting and minimization procedures adopted in accordance with subsections (d) and (e) as necessary at any time, including if the Court is conducting or has completed review of such certification or such procedures, and shall submit the amended certification or amended procedures to the Court not later than 7 days after amending such certification or such procedures. The Court shall review any amendment under this subparagraph under the procedures set forth in this subsection. The Attorney General and the Director of National Intelligence may authorize the use of an amended certification or amended procedures pending the Court's review of such amended certification or amended procedures.
(2) **Review**
The Court shall review the following:
(A) **Certification**
A certification submitted in accordance with subsection (g) to determine whether the certification contains all the required elements.
(B) **Targeting procedures**
The targeting procedures adopted in accordance with subsection (d) to assess whether the procedures are reasonably designed to—
(i) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

(ii) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

(C) **Minimization procedures**

The minimization procedures adopted in accordance with subsection (e) to assess whether such procedures meet the definition of minimization procedures under section 1801 (h) of this title or section 1821 (4) of this title, as appropriate.

(3) **Orders**

(A) **Approval**

If the Court finds that a certification submitted in accordance with subsection (g) contains all the required elements and that the targeting and minimization procedures adopted in accordance with subsections (d) and (e) are consistent with the requirements of those subsections and with the fourth amendment to the Constitution of the United States, the Court shall enter an order approving the certification and the use, or continued use in the case of an acquisition authorized pursuant to a determination under subsection (c)(2), of the procedures for the acquisition.

(B) **Correction of deficiencies**

If the Court finds that a certification submitted in accordance with subsection (g) does not contain all the required elements, or that the procedures adopted in accordance with subsections (d) and (e) are not consistent with the requirements of those subsections or the fourth amendment to the Constitution of the United States, the Court shall issue an order directing the Government to, at the Government's election and to the extent required by the Court's order—

(i) correct any deficiency identified by the Court's order not later than 30 days after the date on which the Court issues the order; or

(ii) cease, or not begin, the implementation of the authorization for which such certification was submitted.

(C) **Requirement for written statement**

In support of an order under this subsection, the Court shall provide, simultaneously with the order, for the record a written statement of the reasons for the order.

(4) **Appeal**

(A) **Appeal to the Court of Review**

The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order under this subsection. The Court of Review shall have jurisdiction to consider such petition. For any decision under this subparagraph affirming, reversing, or modifying an order of the Foreign Intelligence Surveillance Court, the Court of Review shall provide for the record a written statement of the reasons for the decision.

(B) **Continuation of acquisition pending rehearing or appeal**

Any acquisition affected by an order under paragraph (3)(B) may continue—

(i) during the pendency of any rehearing of the order by the Court en banc; and

(ii) if the Government files a petition for review of an order under this section, until the Court of Review enters an order under subparagraph (C).

(C) **Implementation pending appeal**

Not later than 60 days after the filing of a petition for review of an order under paragraph (3)(B) directing the correction of a deficiency, the Court of Review shall determine, and enter a corresponding order regarding, whether all or any part of the correction order, as issued or modified, shall be implemented during the pendency of the review.

(D) **Certiorari to the Supreme Court**

The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(5) **Schedule**

(A) **Reauthorization of authorizations in effect**

If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a), the Attorney General and the Director of National Intelligence shall, to the extent practicable, submit to the Court the certification prepared in accordance with subsection (g) and the procedures adopted in accordance with subsections (d) and (e) at least 30 days prior to the expiration of such authorization.

(B) **Reauthorization of orders, authorizations, and directives**

If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a) by filing a certification pursuant to subparagraph (A), that authorization, and any directives issued thereunder and any order related thereto, shall remain in effect, notwithstanding the expiration provided for in subsection (a), until the Court issues an order with

respect to such certification under paragraph (3) at which time the provisions of that paragraph and paragraph (4) shall apply with respect to such certification.

(j) **Judicial proceedings**

(1) **Expedited judicial proceedings**

Judicial proceedings under this section shall be conducted as expeditiously as possible.

(2) **Time limits**

A time limit for a judicial decision in this section shall apply unless the Court, the Court of Review, or any judge of either the Court or the Court of Review, by order for reasons stated, extends that time as necessary for good cause in a manner consistent with national security.

(k) **Maintenance and security of records and proceedings**

(1) **Standards**

The Foreign Intelligence Surveillance Court shall maintain a record of a proceeding under this section, including petitions, appeals, orders, and statements of reasons for a decision, under security measures adopted by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

(2) **Filing and review**

All petitions under this section shall be filed under seal. In any proceedings under this section, the Court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions of a submission, which may include classified information.

(3) **Retention of records**

The Attorney General and the Director of National Intelligence shall retain a directive or an order issued under this section for a period of not less than 10 years from the date on which such directive or such order is issued.

(l) **Assessments and reviews**

(1) **Semiannual assessment**

Not less frequently than once every 6 months, the Attorney General and Director of National Intelligence shall assess compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f) and shall submit each assessment to—

(A) the Foreign Intelligence Surveillance Court; and

(B) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

(i) the congressional intelligence committees; and

(ii) the Committees on the Judiciary of the House of Representatives and the Senate.

(2) **Agency assessment**

The Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community authorized to acquire foreign intelligence information under subsection (a), with respect to the department or element of such Inspector General—

(A) are authorized to review compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f);

(B) with respect to acquisitions authorized under subsection (a), shall review the number of disseminated intelligence reports containing a reference to a United States-person identity and the number of United States-person identities subsequently disseminated by the element concerned in response to requests for identities that were not referred to by name or title in the original reporting;

(C) with respect to acquisitions authorized under subsection (a), shall review the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

(D) shall provide each such review to—

(i) the Attorney General;

(ii) the Director of National Intelligence; and

(iii) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

(I) the congressional intelligence committees; and

(II) the Committees on the Judiciary of the House of Representatives and the Senate.

(3) **Annual review**

(A) **Requirement to conduct**

The head of each element of the intelligence community conducting an acquisition authorized under subsection (a) shall conduct an annual review to determine whether there is reason to believe that foreign intelligence information has been or will be obtained from the acquisition. The annual review shall provide, with respect to acquisitions authorized under subsection (a)—

(i) an accounting of the number of disseminated intelligence reports containing a reference to a United States-person identity;
(ii) an accounting of the number of United States-person identities subsequently disseminated by that element in response to requests for identities that were not referred to by name or title in the original reporting;
(iii) the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and
(iv) a description of any procedures developed by the head of such element of the intelligence community and approved by the Director of National Intelligence to assess, in a manner consistent with national security, operational requirements and the privacy interests of United States persons, the extent to which the acquisitions authorized under subsection (a) acquire the communications of United States persons, and the results of any such assessment.
(B) **Use of review**
The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall use each such review to evaluate the adequacy of the minimization procedures utilized by such element and, as appropriate, the application of the minimization procedures to a particular acquisition authorized under subsection (a).
(C) **Provision of review**
The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall provide such review to—
(i) the Foreign Intelligence Surveillance Court;
(ii) the Attorney General;
(iii) the Director of National Intelligence; and
(iv) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—
(I) the congressional intelligence committees; and
(II) the Committees on the Judiciary of the House of Representatives and the Senate.

50 USC § 1881b - Certain acquisitions inside the United States targeting United States persons outside the United States
(a) **Jurisdiction of the Foreign Intelligence Surveillance Court**
(1) **In general**
The Foreign Intelligence Surveillance Court shall have jurisdiction to review an application and to enter an order approving the targeting of a United States person reasonably believed to be located outside the United States to acquire foreign intelligence information, if the acquisition constitutes electronic surveillance or the acquisition of stored electronic communications or stored electronic data that requires an order under this chapter, and such acquisition is conducted within the United States.
(2) **Limitation**
If a United States person targeted under this subsection is reasonably believed to be located in the United States during the effective period of an order issued pursuant to subsection (c), an acquisition targeting such United States person under this section shall cease unless the targeted United States person is again reasonably believed to be located outside the United States while an order issued pursuant to subsection (c) is in effect. Nothing in this section shall be construed to limit the authority of the Government to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other subchapter of this chapter.
(b) **Application**
(1) **In general**
Each application for an order under this section shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under subsection (a)(1). Each application shall require the approval of the Attorney General based upon the Attorney General's finding that it satisfies the criteria and requirements of such application, as set forth in this section, and shall include—
(A) the identity of the Federal officer making the application;
(B) the identity, if known, or a description of the United States person who is the target of the acquisition;
(C) a statement of the facts and circumstances relied upon to justify the applicant's belief that the United States person who is the target of the acquisition is—
(i) a person reasonably believed to be located outside the United States; and
(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;
(D) a statement of proposed minimization procedures that meet the definition of minimization procedures under section 1801 (h) or 1821 (4) of this title, as appropriate;

(E) a description of the nature of the information sought and the type of communications or activities to be subjected to acquisition;
(F) a certification made by the Attorney General or an official specified in section 1804 (a)(6) of this title that—
(i) the certifying official deems the information sought to be foreign intelligence information;
(ii) a significant purpose of the acquisition is to obtain foreign intelligence information;
(iii) such information cannot reasonably be obtained by normal investigative techniques;
(iv) designates the type of foreign intelligence information being sought according to the categories described in section 1801 (e) of this title; and
(v) includes a statement of the basis for the certification that—
(I) the information sought is the type of foreign intelligence information designated; and
(II) such information cannot reasonably be obtained by normal investigative techniques;
(G) a summary statement of the means by which the acquisition will be conducted and whether physical entry is required to effect the acquisition;
(H) the identity of any electronic communication service provider necessary to effect the acquisition, provided that the application is not required to identify the specific facilities, places, premises, or property at which the acquisition authorized under this section will be directed or conducted;
(I) a statement of the facts concerning any previous applications that have been made to any judge of the Foreign Intelligence Surveillance Court involving the United States person specified in the application and the action taken on each previous application; and
(J) a statement of the period of time for which the acquisition is required to be maintained, provided that such period of time shall not exceed 90 days per application.
(2) **Other requirements of the Attorney General**
The Attorney General may require any other affidavit or certification from any other officer in connection with the application.
(3) **Other requirements of the judge**
The judge may require the applicant to furnish such other information as may be necessary to make the findings required by subsection (c)(1).
(c) **Order**
(1) **Findings**
Upon an application made pursuant to subsection (b), the Foreign Intelligence Surveillance Court shall enter an ex parte order as requested or as modified by the Court approving the acquisition if the Court finds that—
(A) the application has been made by a Federal officer and approved by the Attorney General;
(B) on the basis of the facts submitted by the applicant, for the United States person who is the target of the acquisition, there is probable cause to believe that the target is—
(i) a person reasonably believed to be located outside the United States; and
(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;
(C) the proposed minimization procedures meet the definition of minimization procedures under section 1801 (h) or 1821 (4) of this title, as appropriate; and
(D) the application that has been filed contains all statements and certifications required by subsection (b) and the certification or certifications are not clearly erroneous on the basis of the statement made under subsection (b)(1)(F)(v) and any other information furnished under subsection (b)(3).
(2) **Probable cause**
In determining whether or not probable cause exists for purposes of paragraph (1)(B), a judge having jurisdiction under subsection (a)(1) may consider past activities of the target and facts and circumstances relating to current or future activities of the target. No United States person may be considered a foreign power, agent of a foreign power, or officer or employee of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States.
(3) **Review**
(A) **Limitation on review**
Review by a judge having jurisdiction under subsection (a)(1) shall be limited to that required to make the findings described in paragraph (1).
(B) **Review of probable cause**
If the judge determines that the facts submitted under subsection (b) are insufficient to establish probable cause under paragraph (1)(B), the judge shall enter an order so stating and provide a written statement for the record of the reasons for the determination. The Government may appeal an order under this subparagraph pursuant to subsection (f).
(C) **Review of minimization procedures**
If the judge determines that the proposed minimization procedures referred to in paragraph (1)(C) do

not meet the definition of minimization procedures under section 1801 (h) or 1821 (4) of this title, as appropriate, the judge shall enter an order so stating and provide a written statement for the record of the reasons for the determination. The Government may appeal an order under this subparagraph pursuant to subsection (f).

(D) **Review of certification**

If the judge determines that an application pursuant to subsection (b) does not contain all of the required elements, or that the certification or certifications are clearly erroneous on the basis of the statement made under subsection (b)(1)(F)(v) and any other information furnished under subsection (b)(3), the judge shall enter an order so stating and provide a written statement for the record of the reasons for the determination. The Government may appeal an order under this subparagraph pursuant to subsection (f).

(4) **Specifications**

An order approving an acquisition under this subsection shall specify—

(A) the identity, if known, or a description of the United States person who is the target of the acquisition identified or described in the application pursuant to subsection (b)(1)(B);

(B) if provided in the application pursuant to subsection (b)(1)(H), the nature and location of each of the facilities or places at which the acquisition will be directed;

(C) the nature of the information sought to be acquired and the type of communications or activities to be subjected to acquisition;

(D) a summary of the means by which the acquisition will be conducted and whether physical entry is required to effect the acquisition; and

(E) the period of time during which the acquisition is approved.

(5) **Directives**

An order approving an acquisition under this subsection shall direct—

(A) that the minimization procedures referred to in paragraph (1)(C), as approved or modified by the Court, be followed;

(B) if applicable, an electronic communication service provider to provide to the Government forthwith all information, facilities, or assistance necessary to accomplish the acquisition authorized under such order in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition;

(C) if applicable, an electronic communication service provider to maintain under security procedures approved by the Attorney General any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain; and

(D) if applicable, that the Government compensate, at the prevailing rate, such electronic communication service provider for providing such information, facilities, or assistance.

(6) **Duration**

An order approved under this subsection shall be effective for a period not to exceed 90 days and such order may be renewed for additional 90-day periods upon submission of renewal applications meeting the requirements of subsection (b).

(7) **Compliance**

At or prior to the end of the period of time for which an acquisition is approved by an order or extension under this section, the judge may assess compliance with the minimization procedures referred to in paragraph (1)(C) by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

(d) **Emergency authorization**

(1) **Authority for emergency authorization**

Notwithstanding any other provision of this chapter, if the Attorney General reasonably determines that—

(A) an emergency situation exists with respect to the acquisition of foreign intelligence information for which an order may be obtained under subsection (c) before an order authorizing such acquisition can with due diligence be obtained, and

(B) the factual basis for issuance of an order under this subsection to approve such acquisition exists, the Attorney General may authorize such acquisition if a judge having jurisdiction under subsection (a)(1) is informed by the Attorney General, or a designee of the Attorney General, at the time of such authorization that the decision has been made to conduct such acquisition and if an application in accordance with this section is made to a judge of the Foreign Intelligence Surveillance Court as soon as practicable, but not more than 7 days after the Attorney General authorizes such acquisition.

(2) **Minimization procedures**

If the Attorney General authorizes an acquisition under paragraph (1), the Attorney General shall

require that the minimization procedures referred to in subsection (c)(1)(C) for the issuance of a judicial order be followed.

(3) **Termination of emergency authorization**

In the absence of a judicial order approving an acquisition under paragraph (1), such acquisition shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

(4) **Use of information**

If an application for approval submitted pursuant to paragraph (1) is denied, or in any other case where the acquisition is terminated and no order is issued approving the acquisition, no information obtained or evidence derived from such acquisition, except under circumstances in which the target of the acquisition is determined not to be a United States person, shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such acquisition shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(e) **Release from liability**

No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with an order or request for emergency assistance issued pursuant to subsection (c) or (d), respectively.

(f) **Appeal**

(1) **Appeal to the Foreign Intelligence Surveillance Court of Review**

The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order issued pursuant to subsection (c). The Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this paragraph.

(2) **Certiorari to the Supreme Court**

The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under paragraph (1). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(g) **Construction**

Except as provided in this section, nothing in this chapter shall be construed to require an application for a court order for an acquisition that is targeted in accordance with this section at a United States person reasonably believed to be located outside the United States.

50 USC § 1881c - Other acquisitions targeting United States persons outside the United States

(a) **Jurisdiction and scope**

(1) **Jurisdiction**

The Foreign Intelligence Surveillance Court shall have jurisdiction to enter an order pursuant to subsection (c).

(2) **Scope**

No element of the intelligence community may intentionally target, for the purpose of acquiring foreign intelligence information, a United States person reasonably believed to be located outside the United States under circumstances in which the targeted United States person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes, unless a judge of the Foreign Intelligence Surveillance Court has entered an order with respect to such targeted United States person or the Attorney General has authorized an emergency acquisition pursuant to subsection (c) or (d), respectively, or any other provision of this chapter.

(3) **Limitations**

(A) **Moving or misidentified targets**

If a United States person targeted under this subsection is reasonably believed to be located in the United States during the effective period of an order issued pursuant to subsection (c), an acquisition targeting such United States person under this section shall cease unless the targeted United States person is again reasonably believed to be located outside the United States during the effective period of such order.

(B) **Applicability**

If an acquisition for foreign intelligence purposes is to be conducted inside the United States and could be authorized under section 1881b of this title, the acquisition may only be conducted if authorized

under section 1881b of this title or in accordance with another provision of this chapter other than this section.

(C) **Construction**

Nothing in this paragraph shall be construed to limit the authority of the Government to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other subchapter of this chapter.

(b) **Application**

Each application for an order under this section shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under subsection (a)(1). Each application shall require the approval of the Attorney General based upon the Attorney General's finding that it satisfies the criteria and requirements of such application as set forth in this section and shall include—

(1) the identity of the Federal officer making the application;

(2) the identity, if known, or a description of the specific United States person who is the target of the acquisition;

(3) a statement of the facts and circumstances relied upon to justify the applicant's belief that the United States person who is the target of the acquisition is—

(A) a person reasonably believed to be located outside the United States; and

(B) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;

(4) a statement of proposed minimization procedures that meet the definition of minimization procedures under section 1801 (h) or 1821 (4) of this title, as appropriate;

(5) a certification made by the Attorney General, an official specified in section 1804 (a)(6) of this title, or the head of an element of the intelligence community that—

(A) the certifying official deems the information sought to be foreign intelligence information; and

(B) a significant purpose of the acquisition is to obtain foreign intelligence information;

(6) a statement of the facts concerning any previous applications that have been made to any judge of the Foreign Intelligence Surveillance Court involving the United States person specified in the application and the action taken on each previous application; and

(7) a statement of the period of time for which the acquisition is required to be maintained, provided that such period of time shall not exceed 90 days per application.

(c) **Order**

(1) **Findings**

Upon an application made pursuant to subsection (b), the Foreign Intelligence Surveillance Court shall enter an ex parte order as requested or as modified by the Court if the Court finds that—

(A) the application has been made by a Federal officer and approved by the Attorney General;

(B) on the basis of the facts submitted by the applicant, for the United States person who is the target of the acquisition, there is probable cause to believe that the target is—

(i) a person reasonably believed to be located outside the United States; and

(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;

(C) the proposed minimization procedures, with respect to their dissemination provisions, meet the definition of minimization procedures under section 1801 (h) or 1821 (4) of this title, as appropriate; and

(D) the application that has been filed contains all statements and certifications required by subsection (b) and the certification provided under subsection (b)(5) is not clearly erroneous on the basis of the information furnished under subsection (b).

(2) **Probable cause**

In determining whether or not probable cause exists for purposes of paragraph (1)(B), a judge having jurisdiction under subsection (a)(1) may consider past activities of the target and facts and circumstances relating to current or future activities of the target. No United States person may be considered a foreign power, agent of a foreign power, or officer or employee of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(3) **Review**

(A) **Limitations on review**

Review by a judge having jurisdiction under subsection (a)(1) shall be limited to that required to make the findings described in paragraph (1). The judge shall not have jurisdiction to review the means by which an acquisition under this section may be conducted.

(B) **Review of probable cause**

If the judge determines that the facts submitted under subsection (b) are insufficient to establish probable cause to issue an order under this subsection, the judge shall enter an order so stating and provide a written statement for the record of the reasons for such determination. The Government may appeal an order under this subparagraph pursuant to subsection (e).

(C) **Review of minimization procedures**
If the judge determines that the minimization procedures applicable to dissemination of information obtained through an acquisition under this subsection do not meet the definition of minimization procedures under section 1801 (h) or 1821 (4) of this title, as appropriate, the judge shall enter an order so stating and provide a written statement for the record of the reasons for such determination. The Government may appeal an order under this subparagraph pursuant to subsection (e).
(D) **Scope of review of certification**
If the judge determines that an application under subsection (b) does not contain all the required elements, or that the certification provided under subsection (b)(5) is clearly erroneous on the basis of the information furnished under subsection (b), the judge shall enter an order so stating and provide a written statement for the record of the reasons for such determination. The Government may appeal an order under this subparagraph pursuant to subsection (e).
(4) **Duration**
An order under this paragraph shall be effective for a period not to exceed 90 days and such order may be renewed for additional 90-day periods upon submission of renewal applications meeting the requirements of subsection (b).
(5) **Compliance**
At or prior to the end of the period of time for which an order or extension is granted under this section, the judge may assess compliance with the minimization procedures referred to in paragraph (1)(C) by reviewing the circumstances under which information concerning United States persons was disseminated, provided that the judge may not inquire into the circumstances relating to the conduct of the acquisition.
(d) **Emergency authorization**
(1) **Authority for emergency authorization**
Notwithstanding any other provision of this section, if the Attorney General reasonably determines that—
(A) an emergency situation exists with respect to the acquisition of foreign intelligence information for which an order may be obtained under subsection (c) before an order under that subsection can, with due diligence, be obtained, and
(B) the factual basis for the issuance of an order under this section exists,
the Attorney General may authorize the emergency acquisition if a judge having jurisdiction under subsection (a)(1) is informed by the Attorney General or a designee of the Attorney General at the time of such authorization that the decision has been made to conduct such acquisition and if an application in accordance with this section is made to a judge of the Foreign Intelligence Surveillance Court as soon as practicable, but not more than 7 days after the Attorney General authorizes such acquisition.
(2) **Minimization procedures**
If the Attorney General authorizes an emergency acquisition under paragraph (1), the Attorney General shall require that the minimization procedures referred to in subsection (c)(1)(C) be followed.
(3) **Termination of emergency authorization**
In the absence of an order under subsection (c), an emergency acquisition under paragraph (1) shall terminate when the information sought is obtained, if the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.
(4) **Use of information**
If an application submitted to the Court pursuant to paragraph (1) is denied, or in any other case where the acquisition is terminated and no order with respect to the target of the acquisition is issued under subsection (c), no information obtained or evidence derived from such acquisition, except under circumstances in which the target of the acquisition is determined not to be a United States person, shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such acquisition shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.
(e) **Appeal**
(1) **Appeal to the Court of Review**
The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order issued pursuant to subsection (c). The Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this paragraph.

(2) **Certiorari to the Supreme Court**
The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under paragraph (1). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

50 USC § 1881d - Joint applications and concurrent authorizations
(a) **Joint applications and orders**
If an acquisition targeting a United States person under section 1881b or 1881c of this title is proposed to be conducted both inside and outside the United States, a judge having jurisdiction under section 1881b (a)(1) or 1881c (a)(1) of this title may issue simultaneously, upon the request of the Government in a joint application complying with the requirements of sections 1881b (b) and 1881c (b) of this title, orders under sections 1881b (c) and 1881c (c) of this title, as appropriate.
(b) **Concurrent authorization**
If an order authorizing electronic surveillance or physical search has been obtained under section 1805 or 1824 of this title, the Attorney General may authorize, for the effective period of that order, without an order under section 1881b or 1881c of this title, the targeting of that United States person for the purpose of acquiring foreign intelligence information while such person is reasonably believed to be located outside the United States.

50 USC § 1881e - Use of information acquired under this subchapter
(a) **Information acquired under section 1881a**
Information acquired from an acquisition conducted under section 1881a of this title shall be deemed to be information acquired from an electronic surveillance pursuant to subchapter I for purposes of section 1806 of this title, except for the purposes of subsection (j) of such section.
(b) **Information acquired under section 1881b**
Information acquired from an acquisition conducted under section 1881b of this title shall be deemed to be information acquired from an electronic surveillance pursuant to subchapter I for purposes of section 1806 of this title.

50 USC § 1881f - Congressional oversight
(a) **Semiannual report**
Not less frequently than once every 6 months, the Attorney General shall fully inform, in a manner consistent with national security, the congressional intelligence committees and the Committees on the Judiciary of the Senate and the House of Representatives, consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution, concerning the implementation of this subchapter.
(b) **Content**
Each report under subsection (a) shall include—
(1) with respect to section 1881a of this title—
(A) any certifications submitted in accordance with section 1881a (g) of this title during the reporting period;
(B) with respect to each determination under section 1881a (c)(2) of this title, the reasons for exercising the authority under such section;
(C) any directives issued under section 1881a (h) of this title during the reporting period;
(D) a description of the judicial review during the reporting period of such certifications and targeting and minimization procedures adopted in accordance with subsections (d) and (e) ofsection 1881a of this title and utilized with respect to an acquisition under such section, including a copy of an order or pleading in connection with such review that contains a significant legal interpretation of the provisions of section 1881a of this title;
(E) any actions taken to challenge or enforce a directive under paragraph (4) or (5) of section 1881a (h) of this title;
(F) any compliance reviews conducted by the Attorney General or the Director of National Intelligence of acquisitions authorized under section 1881a (a) of this title;
(G) a description of any incidents of noncompliance—
(i) with a directive issued by the Attorney General and the Director of National Intelligence under section 1881a (h) of this title, including incidents of noncompliance by a specified person to whom the Attorney General and Director of National Intelligence issued a directive under section 1881a (h) of

this title; and
(ii) by an element of the intelligence community with procedures and guidelines adopted in accordance with subsections (d), (e), and (f) ofsection 1881a of this title; and
(H) any procedures implementing section 1881a of this title;
(2) with respect to section 1881b of this title—
(A) the total number of applications made for orders under section 1881b (b) of this title;
(B) the total number of such orders—
(i) granted;
(ii) modified; and
(iii) denied; and
(C) the total number of emergency acquisitions authorized by the Attorney General under section 1881b (d) of this title and the total number of subsequent orders approving or denying such acquisitions; and
(3) with respect to section 1881c of this title—
(A) the total number of applications made for orders under section 1881c (b) of this title;
(B) the total number of such orders—
(i) granted;
(ii) modified; and
(iii) denied; and
(C) the total number of emergency acquisitions authorized by the Attorney General under section 1881c (d) of this title and the total number of subsequent orders approving or denying such applications.

50 USC § 1881g - Savings provision
Nothing in this subchapter shall be construed to limit the authority of the Government to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other subchapter of this chapter.

附錄三：美國愛國者法案U.S.A Patriot Act Title II

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.

TITLE II--ENHANCED SURVEILLANCE PROCEDURES
SEC. 201. AUTHORITY TO INTERCEPT WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS RELATING TO TERRORISM.
Section 2516(1) of title 18, United States Code, is amended--
(1) by redesignating paragraph (p), as so redesignated by section 434(2) of the Antiterrorism and Effective Death Penalty Act of 1996 (Public Law 104-132; 110 Stat. 1274), as paragraph (r); and
(2) by inserting after paragraph (p), as so redesignated by section 201(3) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (division C of Public Law 104-208; 110 Stat. 3009-565), the following new paragraph:
`(q) any criminal violation of section 229 (relating to chemical weapons); or sections 2332, 2332a, 2332b, 2332d, 2339A, or 2339B of this title (relating to terrorism); or'.
SEC. 202. AUTHORITY TO INTERCEPT WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS RELATING TO COMPUTER FRAUD AND ABUSE OFFENSES.
Section 2516(1)(c) of title 18, United States Code, is amended by striking `and section 1341 (relating to mail fraud),' and inserting `section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse),'.
SEC. 203. AUTHORITY TO SHARE CRIMINAL INVESTIGATIVE INFORMATION.
(a) AUTHORITY TO SHARE GRAND JURY INFORMATION-
(1) IN GENERAL- Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure is amended to read as follows:
`(C)(i) Disclosure otherwise prohibited by this rule of matters occurring before the grand jury may also be made--
`(I) when so directed by a court preliminarily to or in connection with a judicial proceeding;
`(II) when permitted by a court at the request of the defendant, upon a showing that grounds may exist for a motion to dismiss the indictment because of matters occurring before the grand jury;
`(III) when the disclosure is made by an attorney for the government to another Federal grand jury;
`(IV) when permitted by a court at the request of an attorney for the government, upon a showing that such matters may disclose a violation of state criminal law, to an appropriate official of a state or

subdivision of a state for the purpose of enforcing such law; or
`(V) when the matters involve foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in clause (iv) of this subparagraph), to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties.
`(ii) If the court orders disclosure of matters occurring before the grand jury, the disclosure shall be made in such manner, at such time, and under such conditions as the court may direct.
`(iii) Any Federal official to whom information is disclosed pursuant to clause (i)(V) of this subparagraph may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information. Within a reasonable time after such disclosure, an attorney for the government shall file under seal a notice with the court stating the fact that such information was disclosed and the departments, agencies, or entities to which the disclosure was made.
`(iv) In clause (i)(V) of this subparagraph, the term `foreign intelligence information' means--
`(I) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--
`(aa) actual or potential attack or other grave hostile acts of-a foreign power or an agent of a foreign power;
`(bb) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
`(cc) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of foreign power; or
`(II) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--
`(aa) the national defense or the security of the United States; or
`(bb) the conduct of the foreign affairs of the United States.'.
(2) CONFORMING AMENDMENT- Rule 6(e)(3)(D) of the Federal Rules of Criminal Procedure is amended by striking `(e)(3)(C)(i)' and inserting `(e)(3)(C)(i)(I)'.
(b) AUTHORITY TO SHARE ELECTRONIC, WIRE, AND ORAL INTERCEPTION INFORMATION-
(1) LAW ENFORCEMENT- Section 2517 of title 18, United States Code, is amended by inserting at the end the following:
`(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.'.
(2) DEFINITION- Section 2510 of title 18, United States Code, is amended by--
(A) in paragraph (17), by striking `and' after the semicolon;
(B) in paragraph (18), by striking the period and inserting `; and'; and
(C) by inserting at the end the following:
`(19) `foreign intelligence information' means--
`(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--
`(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
`(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
`(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
`(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--
`(i) the national defense or the security of the United States; or
`(ii) the conduct of the foreign affairs of the United States.'.
(c) PROCEDURES- The Attorney General shall establish procedures for the disclosure of information pursuant to section 2517(6) and Rule 6(e)(3)(C)(i)(V) of the Federal Rules of Criminal Procedure that

identifies a United States person, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801)).
(d) FOREIGN INTELLIGENCE INFORMATION-
(1) IN GENERAL- Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.
(2) DEFINITION- In this subsection, the term `foreign intelligence information' means--
(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--
(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--
(i) the national defense or the security of the United States; or
(ii) the conduct of the foreign affairs of the United States.
SEC. 204. CLARIFICATION OF INTELLIGENCE EXCEPTIONS FROM LIMITATIONS ON INTERCEPTION AND DISCLOSURE OF WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS.
Section 2511(2)(f) of title 18, United States Code, is amended--
(1) by striking `this chapter or chapter 121' and inserting `this chapter or chapter 121 or 206 of this title'; and
(2) by striking `wire and oral' and inserting `wire, oral, and electronic'.
SEC. 205. EMPLOYMENT OF TRANSLATORS BY THE FEDERAL BUREAU OF INVESTIGATION.
(a) AUTHORITY- The Director of the Federal Bureau of Investigation is authorized to expedite the employment of personnel as translators to support counterterrorism investigations and operations without regard to applicable Federal personnel requirements and limitations.
(b) SECURITY REQUIREMENTS- The Director of the Federal Bureau of Investigation shall establish such security requirements as are necessary for the personnel employed as translators under subsection (a).
(c) REPORT- The Attorney General shall report to the Committees on the Judiciary of the House of Representatives and the Senate on--
(1) the number of translators employed by the FBI and other components of the Department of Justice;
(2) any legal or practical impediments to using translators employed by other Federal, State, or local agencies, on a full, part-time, or shared basis; and
(3) the needs of the FBI for specific translation services in certain languages, and recommendations for meeting those needs.
SEC. 206. ROVING SURVEILLANCE AUTHORITY UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.
Section 105(c)(2)(B) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(c)(2)(B)) is amended by inserting `, or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons,' after `specified person'.
SEC. 207. DURATION OF FISA SURVEILLANCE OF NON-UNITED STATES PERSONS WHO ARE AGENTS OF A FOREIGN POWER.
(a) DURATION -
(1) SURVEILLANCE- Section 105(e)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(e)(1)) is amended by--
(A) inserting `(A)' after `except that'; and
(B) inserting before the period the following: `, and (B) an order under this Act for a surveillance targeted against an agent of a foreign power, as defined in section 101(b)(1)(A) may be for the period specified in the application or for 120 days, whichever is less'.

(2) PHYSICAL SEARCH- Section 304(d)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1824(d)(1)) is amended by--
(A) striking `forty-five' and inserting `90';
(B) inserting `(A)' after `except that'; and
(C) inserting before the period the following: `, and (B) an order under this section for a physical search targeted against an agent of a foreign power as defined in section 101(b)(1)(A) may be for the period specified in the application or for 120 days, whichever is less'.
(b) EXTENSION-
(1) IN GENERAL- Section 105(d)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(d)(2)) is amended by--
(A) inserting `(A)' after `except that'; and
(B) inserting before the period the following: `, and (B) an extension of an order under this Act for a surveillance targeted against an agent of a foreign power as defined in section 101(b)(1)(A) may be for a period not to exceed 1 year'.
(2) DEFINED TERM- Section 304(d)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1824(d)(2) is amended by inserting after `not a United States person,' the following: `or against an agent of a foreign power as defined in section 101(b)(1)(A),'.
SEC. 208. DESIGNATION OF JUDGES.
Section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a)) is amended by--
(1) striking `seven district court judges' and inserting `11 district court judges'; and
(2) inserting `of whom no fewer than 3 shall reside within 20 miles of the District of Columbia' after `circuits'.
SEC. 209. SEIZURE OF VOICE-MAIL MESSAGES PURSUANT TO WARRANTS.
Title 18, United States Code, is amended--
(1) in section 2510--
(A) in paragraph (1), by striking beginning with `and such' and all that follows through `communication'; and
(B) in paragraph (14), by inserting `wire or' after `transmission of'; and
(2) in subsections (a) and (b) of section 2703--
(A) by striking `CONTENTS OF ELECTRONIC' and inserting `CONTENTS OF WIRE OR ELECTRONIC' each place it appears;
(B) by striking `contents of an electronic' and inserting `contents of a wire or electronic' each place it appears; and
(C) by striking `any electronic' and inserting `any wire or electronic' each place it appears.
SEC. 210. SCOPE OF SUBPOENAS FOR RECORDS OF ELECTRONIC COMMUNICATIONS.
Section 2703(c)(2) of title 18, United States Code, as redesignated by section 212, is amended--
(1) by striking `entity the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber' and inserting the following: `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'; and
(2) by striking `and the types of services the subscriber or customer utilized,'.
SEC. 211. CLARIFICATION OF SCOPE.
Section 631 of the Communications Act of 1934 (47 U.S.C. 551) is amended--
(1) in subsection (c)(2)--
(A) in subparagraph (B), by striking `or';
(B) in subparagraph (C), by striking the period at the end and inserting `; or'; and
(C) by inserting at the end the following:
`(D) to a government entity as authorized under chapters 119, 121, or 206 of title 18, United States Code, except that such disclosure shall not include records revealing cable subscriber selection of video programming from a cable operator.'; and
(2) in subsection (h), by striking `A governmental entity' and inserting `Except as provided in subsection (c)(2)(D), a governmental entity'.

SEC. 212. EMERGENCY DISCLOSURE OF ELECTRONIC COMMUNICATIONS TO PROTECT LIFE AND LIMB.
(a) DISCLOSURE OF CONTENTS-
(1) IN GENERAL- Section 2702 of title 18, United States Code, is amended--
(A) by striking the section heading and inserting the following:
`Sec. 2702. Voluntary disclosure of customer communications or records';
(B) in subsection (a)--
(i) in paragraph (2)(A), by striking `and' at the end;
(ii) in paragraph (2)(B), by striking the period and inserting `; and'; and
(iii) by inserting after paragraph (2) the following:
`(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.';
(C) in subsection (b), by striking `EXCEPTIONS- A person or entity' and inserting `EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS- A provider described in subsection (a)';
(D) in subsection (b)(6)--
(i) in subparagraph (A)(ii), by striking `or';
(ii) in subparagraph (B), by striking the period and inserting `; or'; and
(iii) by adding after subparagraph (B) the following:
`(C) if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay.'; and
(E) by inserting after subsection (b) the following:
`(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS- A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))--
`(1) as otherwise authorized in section 2703;
`(2) with the lawful consent of the customer or subscriber;
`(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
`(4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information; or
`(5) to any person other than a governmental entity.'.
(2) TECHNICAL AND CONFORMING AMENDMENT- The table of sections for chapter 121 of title 18, United States Code, is amended by striking the item relating to section 2702 and inserting the following:
`2702. Voluntary disclosure of customer communications or records.'.
(b) REQUIREMENTS FOR GOVERNMENT ACCESS-
(1) IN GENERAL- Section 2703 of title 18, United States Code, is amended--
(A) by striking the section heading and inserting the following:
`Sec. 2703. Required disclosure of customer communications or records';
(B) in subsection (c) by redesignating paragraph (2) as paragraph (3);
(C) in subsection (c)(1)--
(i) by striking `(A) Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may' and inserting `A governmental entity may require a provider of electronic communication service or remote computing service to';
(ii) by striking `covered by subsection (a) or (b) of this section) to any person other than a governmental entity.
`(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity' and inserting `)';
(iii) by redesignating subparagraph (C) as paragraph (2);
(iv) by redesignating clauses (i), (ii), (iii), and (iv) as subparagraphs (A), (B), (C), and (D), respectively;
(v) in subparagraph (D) (as redesignated) by striking the period and inserting `; or'; and
(vi) by inserting after subparagraph (D) (as redesignated) the following:
`(E) seeks information under paragraph (2).'; and
(D) in paragraph (2) (as redesignated) by striking `subparagraph (B)' and insert `paragraph (1)'.

(2) TECHNICAL AND CONFORMING AMENDMENT- The table of sections for chapter 121 of title 18, United States Code, is amended by striking the item relating to section 2703 and inserting the following:
`2703. Required disclosure of customer communications or records.'.
SEC. 213. AUTHORITY FOR DELAYING NOTICE OF THE EXECUTION OF A WARRANT.
Section 3103a of title 18, United States Code, is amended--
(1) by inserting `(a) IN GENERAL- ' before `In addition'; and
(2) by adding at the end the following:
`(b) DELAY- With respect to the issuance of any warrant or court order under this section, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if--
`(1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705);
`(2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and
`(3) the warrant provides for the giving of such notice within a reasonable period of its execution, which period may thereafter be extended by the court for good cause shown.'.
SEC. 214. PEN REGISTER AND TRAP AND TRACE AUTHORITY UNDER FISA.
(a) APPLICATIONS AND ORDERS- Section 402 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1842) is amended--
(1) in subsection (a)(1), by striking `for any investigation to gather foreign intelligence information or information concerning international terrorism' and inserting `for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution';
(2) by amending subsection (c)(2) to read as follows:
`(2) a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.';
(3) by striking subsection (c)(3); and
(4) by amending subsection (d)(2)(A) to read as follows:
`(A) shall specify--
`(i) the identity, if known, of the person who is the subject of the investigation;
`(ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;
`(iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order.'.
(b) AUTHORIZATION DURING EMERGENCIES- Section 403 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1843) is amended--
(1) in subsection (a), by striking `foreign intelligence information or information concerning international terrorism' and inserting `foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution'; and
(2) in subsection (b)(1), by striking `foreign intelligence information or information concerning international terrorism' and inserting `foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution'.
SEC. 215. ACCESS TO RECORDS AND OTHER ITEMS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT.
Title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) is amended by striking sections 501 through 503 and inserting the following:

`SEC. 501. ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS.
`(a)(1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.
`(2) An investigation conducted under this section shall--
`(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and
`(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.
`(b) Each application under this section--
`(1) shall be made to--
`(A) a judge of the court established by section 103(a); or
`(B) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and
`(2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) to protect against international terrorism or clandestine intelligence activities.
`(c)(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.
`(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).
`(d) No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.
`(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.
`SEC. 502. CONGRESSIONAL OVERSIGHT.
`(a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests for the production of tangible things under section 402.
`(b) On a semiannual basis, the Attorney General shall provide to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period--
`(1) the total number of applications made for orders approving requests for the production of tangible things under section 402; and
`(2) the total number of such orders either granted, modified, or denied.'.
SEC. 216. MODIFICATION OF AUTHORITIES RELATING TO USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES.
(a) GENERAL LIMITATIONS- Section 3121(c) of title 18, United States Code, is amended--
(1) by inserting `or trap and trace device' after `pen register';
(2) by inserting `, routing, addressing,' after `dialing'; and
(3) by striking `call processing' and inserting `the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications'.
(b) ISSUANCE OF ORDERS-
(1) IN GENERAL- Section 3123(a) of title 18, United States Code, is amended to read as follows:
`(a) IN GENERAL-
`(1) ATTORNEY FOR THE GOVERNMENT- Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or

entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served.
`(2) STATE INVESTIGATIVE OR LAW ENFORCEMENT OFFICER- Upon an application made under section 3122(a)(2), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.
`(3)(A) Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public, the agency shall ensure that a record will be maintained which will identify--
`(i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;
`(ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;
`(iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and
`(iv) any information which has been collected by the device.
To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of such device.
`(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof).'.
(2) CONTENTS OF ORDER- Section 3123(b)(1) of title 18, United States Code, is amended--
(A) in subparagraph (A)--
(i) by inserting `or other facility' after `telephone line'; and
(ii) by inserting before the semicolon at the end `or applied'; and
(B) by striking subparagraph (C) and inserting the following:
`(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and'.
(3) NONDISCLOSURE REQUIREMENTS- Section 3123(d)(2) of title 18, United States Code, is amended--
(A) by inserting `or other facility' after `the line'; and
(B) by striking `, or who has been ordered by the court' and inserting `or applied, or who is obligated by the order'.
(c) DEFINITIONS-
(1) COURT OF COMPETENT JURISDICTION- Section 3127(2) of title 18, United States Code, is amended by striking subparagraph (A) and inserting the following:
`(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals having jurisdiction over the offense being investigated; or'.
(2) PEN REGISTER- Section 3127(3) of title 18, United States Code, is amended--
(A) by striking `electronic or other impulses' and all that follows through `is attached' and inserting `dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication'; and
(B) by inserting `or process' after `device' each place it appears.
(3) TRAP AND TRACE DEVICE- Section 3127(4) of title 18, United States Code, is amended--
(A) by striking `of an instrument' and all that follows through the semicolon and inserting `or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;'; and
(B) by inserting `or process' after `a device'.
(4) CONFORMING AMENDMENT- Section 3127(1) of title 18, United States Code, is amended--
(A) by striking `and'; and
(B) by inserting `, and `contents' after `electronic communication service'.
(5) TECHNICAL AMENDMENT- Section 3124(d) of title 18, United States Code, is amended by

striking `the terms of'.
(6) CONFORMING AMENDMENT- Section 3124(b) of title 18, United States Code, is amended by inserting `or other facility' after `the appropriate line'.
SEC. 217. INTERCEPTION OF COMPUTER TRESPASSER COMMUNICATIONS.
Chapter 119 of title 18, United States Code, is amended--
(1) in section 2510--
(A) in paragraph (18), by striking `and' at the end;
(B) in paragraph (19), by striking the period and inserting a semicolon; and
(C) by inserting after paragraph (19) the following:
`(20) `protected computer' has the meaning set forth in section 1030; and
`(21) `computer trespasser'--
`(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and
`(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.'; and
(2) in section 2511(2), by inserting at the end the following:
`(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if--
`(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;
`(II) the person acting under color of law is lawfully engaged in an investigation;
`(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and
`(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.'.
SEC. 218. FOREIGN INTELLIGENCE INFORMATION.
Sections 104(a)(7)(B) and section 303(a)(7)(B) (50 U.S.C. 1804(a)(7)(B) and 1823(a)(7)(B)) of the Foreign Intelligence Surveillance Act of 1978 are each amended by striking `the purpose' and inserting `a significant purpose'.
SEC. 219. SINGLE-JURISDICTION SEARCH WARRANTS FOR TERRORISM.
Rule 41(a) of the Federal Rules of Criminal Procedure is amended by inserting after `executed' the following: `and (3) in an investigation of domestic terrorism or international terrorism (as defined in section 2331 of title 18, United States Code), by a Federal magistrate judge in any district in which activities related to the terrorism may have occurred, for a search of property or for a person within or outside the district'.
SEC. 220. NATIONWIDE SERVICE OF SEARCH WARRANTS FOR ELECTRONIC EVIDENCE.
(a) IN GENERAL- Chapter 121 of title 18, United States Code, is amended--
(1) in section 2703, by striking `under the Federal Rules of Criminal Procedure' every place it appears and inserting `using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation'; and
(2) in section 2711--
(A) in paragraph (1), by striking `and';
(B) in paragraph (2), by striking the period and inserting `; and'; and
(C) by inserting at the end the following:
`(3) the term `court of competent jurisdiction' has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation.'.
(b) CONFORMING AMENDMENT- Section 2703(d) of title 18, United States Code, is amended by striking `described in section 3127(2)(A)'.
SEC. 221. TRADE SANCTIONS.
(a) IN GENERAL- The Trade Sanctions Reform and Export Enhancement Act of 2000 (Public Law 106-387; 114 Stat. 1549A-67) is amended--
(1) by amending section 904(2)(C) to read as follows:
`(C) used to facilitate the design, development, or production of chemical or biological weapons, missiles, or weapons of mass destruction.';
(2) in section 906(a)(1)--
(A) by inserting `, the Taliban or the territory of Afghanistan controlled by the Taliban,' after `Cuba'; and

(B) by inserting `, or in the territory of Afghanistan controlled by the Taliban,' after `within such country'; and
(3) in section 906(a)(2), by inserting `, or to any other entity in Syria or North Korea' after `Korea'.
(b) APPLICATION OF THE TRADE SANCTIONS REFORM AND EXPORT ENHANCEMENT ACT- Nothing in the Trade Sanctions Reform and Export Enhancement Act of 2000 shall limit the application or scope of any law establishing criminal or civil penalties, including any executive order or regulation promulgated pursuant to such laws (or similar or successor laws), for the unlawful export of any agricultural commodity, medicine, or medical device to--
(1) a foreign organization, group, or person designated pursuant to Executive Order 12947 of January 23, 1995, as amended;
(2) a Foreign Terrorist Organization pursuant to the Antiterrorism and Effective Death Penalty Act of 1996 (Public Law 104-132);
(3) a foreign organization, group, or person designated pursuant to Executive Order 13224 (September 23, 2001);
(4) any narcotics trafficking entity designated pursuant to Executive Order 12978 (October 21, 1995) or the Foreign Narcotics Kingpin Designation Act (Public Law 106-120); or
(5) any foreign organization, group, or persons subject to any restriction for its involvement in weapons of mass destruction or missile proliferation.
SEC. 222. ASSISTANCE TO LAW ENFORCEMENT AGENCIES.
Nothing in this Act shall impose any additional technical obligation or requirement on a provider of a wire or electronic communication service or other person to furnish facilities or technical assistance. A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to section 216 shall be reasonably compensated for such reasonable expenditures incurred in providing such facilities or assistance.
SEC. 223. CIVIL LIABILITY FOR CERTAIN UNAUTHORIZED DISCLOSURES.
(a) Section 2520 of title 18, United States Code, is amended--
(1) in subsection (a), after `entity', by inserting `, other than the United States,';
(2) by adding at the end the following:
`(f) ADMINISTRATIVE DISCIPLINE- If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.'; and
(3) by adding a new subsection (g), as follows:
`(g) IMPROPER DISCLOSURE IS VIOLATION- Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a).
(b) Section 2707 of title 18, United States Code, is amended--
(1) in subsection (a), after `entity', by inserting `, other than the United States,';
(2) by striking subsection (d) and inserting the following:
`(d) ADMINISTRATIVE DISCIPLINE- If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.'; and
(3) by adding a new subsection (g), as follows:
`(g) IMPROPER DISCLOSURE- Any willful disclosure of a `record', as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official

functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter.'.
(c)(1) Chapter 121 of title 18, United States Code, is amended by adding at the end the following:
`Sec. 2712. Civil actions against the United States
`(a) IN GENERAL- Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation of this chapter or of chapter 119 of this title or of the above specific provisions of title 50, the Court may assess as damages--
`(1) actual damages, but not less than $10,000, whichever amount is greater; and
`(2) litigation costs, reasonably incurred.
`(b) PROCEDURES- (1) Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code. `(2) Any action against the United States under this section shall be forever barred unless it is presented in writing to the appropriate Federal agency within 2 years after such claim accrues or unless action is begun within 6 months after the date of mailing, by certified or registered mail, of notice of final denial of the claim by the agency to which it was presented. The claim shall accrue on the date upon which the claimant first has a reasonable opportunity to discover the violation.'.
`(3) Any action under this section shall be tried to the court without a jury.
`(4) Notwithstanding any other provision of law, the procedures set forth in section 106(f), 305(g), or 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which materials governed by those sections may be reviewed.
`(5) An amount equal to any award against the United States under this section shall be reimbursed by the department or agency concerned to the fund described in section 1304 of title 31, United States Code, out of any appropriation, fund, or other account (excluding any part of such appropriation, fund, or account that is available for the enforcement of any Federal law) that is available for the operating expenses of the department or agency concerned.
`(c) ADMINISTRATIVE DISCIPLINE- If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the possible violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.
`(d) EXCLUSIVE REMEDY- Any action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section.
`(e) STAY OF PROCEEDINGS- (1) Upon the motion of the United States, the court shall stay any action commenced under this section if the court determines that civil discovery will adversely affect the ability of the Government to conduct a related investigation or the prosecution of a related criminal case. Such a stay shall toll the limitations periods of paragraph (2) of subsection (b).
`(2) In this subsection, the terms `related criminal case' and `related investigation' mean an actual prosecution or investigation in progress at the time at which the request for the stay or any subsequent motion to lift the stay is made. In determining whether an investigation or a criminal case is related to an action commenced under this section, the court shall consider the degree of similarity between the parties, witnesses, facts, and circumstances involved in the 2 proceedings, without requiring that any one or more factors be identical.
`(3) In requesting a stay under paragraph (1), the Government may, in appropriate cases, submit evidence ex parte in order to avoid disclosing any matter that may adversely affect a related investigation or a related criminal case. If the Government makes such an ex parte submission, the plaintiff shall be given an opportunity to make a submission to the court, not ex parte, and the court may, in its discretion, request further information from either party.'.
(2) The table of sections at the beginning of chapter 121 is amended to read as follows:
`2712. Civil action against the United States.'.

SEC. 224. SUNSET.
(a) IN GENERAL- Except as provided in subsection (b), this title and the amendments made by this title (other than sections 203(a), 203(c), 205, 208, 210, 211, 213, 216, 219, 221, and 222, and the amendments made by those sections) shall cease to have effect on December 31, 2005.
(b) EXCEPTION- With respect to any particular foreign intelligence investigation that began before the date on which the provisions referred to in subsection (a) cease to have effect, or with respect to any particular offense or potential offense that began or occurred before the date on which such provisions cease to have effect, such provisions shall continue in effect.
SEC. 225. IMMUNITY FOR COMPLIANCE WITH FISA WIRETAP.
Section 105 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805) is amended by inserting after subsection (g) the following:
`(h) No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act.'.

附錄四：德國G10 法

Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses

(Artikel 10-Gesetz - G 10)

Ausfertigungsdatum: 26.06.2001

Vollzitat:"Artikel 10-Gesetz vom 26. Juni 2001 (BGBl. I S. 1254, 2298), das zuletzt durch Artikel 5 des Gesetzes vom 7. Dezember 2011 (BGBl. I S. 2576) geändert worden ist"

Stand: Zuletzt geändert durch Art. 5 G v. 7.12.2011 I 2576

Hinweis: Mittelbare Änderung durch Art. 6 Nr. 3 Buchst. a G v. 7.12.2011 I 2576 ist berücksichtigt

Fußnote

(+++ Textnachweis ab: 29.6.2001 +++)

Das G wurde als Art. 1 G v. 26.6.2001 I 1254 vom Bundestag beschlossen. Es ist gem. Art. 5 Satz 1 G v. 26.6.2001 I 1254 mWv 29.6.2001 in Kraft getreten.

Abschnitt 1
Allgemeine Bestimmungen

§ 1Gegenstand des Gesetzes

(1) Es sind

1. die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes einschließlich der Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantikvertrages,
2. der Bundesnachrichtendienst im Rahmen seiner Aufgaben nach § 1 Abs. 2 des BND-Gesetzes auch zu den in § 5 Abs. 1 Satz 3 Nr. 2 bis 7 und § 8 Abs. 1 Satz 1 bestimmten Zwecken

berechtigt, die Telekommunikation zu überwachen und aufzuzeichnen, in den Fällen der Nummer 1 auch die dem Brief- oder Postgeheimnis unterliegenden Sendungen zu öffnen und einzusehen.

(2) Soweit Maßnahmen nach Absatz 1 von Behörden des Bundes durchgeführt werden, unterliegen sie der Kontrolle durch das Parlamentarische Kontrollgremium und durch eine besondere Kommission (G 10-Kommission).

§ 2Pflichten der Anbieter von Post- und Telekommunikationsdiensten

(1) Wer geschäftsmäßig Postdienste erbringt oder an der Erbringung solcher Dienste mitwirkt, hat der berechtigten Stelle auf Anordnung Auskunft über die näheren Umstände des Postverkehrs zu erteilen und Sendungen, die ihm zum Einsammeln, Weiterleiten oder Ausliefern anvertraut sind, auszuhändigen. Der nach Satz 1 Verpflichtete hat der berechtigten Stelle auf Verlangen die zur Vorbereitung einer Anordnung erforderlichen Auskünfte zu Postfächern zu erteilen, ohne dass es hierzu einer gesonderten Anordnung bedarf. Wer geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt, hat der berechtigten Stelle auf Anordnung Auskunft über die näheren Umstände der nach Wirksamwerden der Anordnung durchgeführten Telekommunikation zu erteilen, Sendungen, die ihm zur Übermittlung auf dem Telekommunikationsweg anvertraut sind, auszuhändigen sowie die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen. § 8a Absatz 2 Satz 1 Nummer 4 des Bundesverfassungsschutzgesetzes, § 4a des MAD-Gesetzes und § 2a des BND-Gesetzes bleiben unberührt. Ob und in welchem Umfang der nach Satz 3 Verpflichtete Vorkehrungen für die technische und organisatorische Umsetzung der Überwachungsmaßnahme zu treffen hat, bestimmt sich nach § 110 des Telekommunikationsgesetzes und der dazu erlassenen Rechtsverordnung.

(2) Der nach Absatz 1 Satz 1 oder 3 Verpflichtete hat vor Durchführung einer beabsichtigten Beschränkungsmaßnahme unverzüglich die Personen, die mit der Durchführung der Maßnahme betraut werden sollen,

1. auszuwählen,
2. einer einfachen Sicherheitsüberprüfung unterziehen zu lassen und
3. über Mitteilungsverbote nach § 17 sowie die Strafbarkeit eines Verstoßes nach § 18 zu belehren; die Belehrung ist aktenkundig zu machen.

Mit der Durchführung einer Beschränkungsmaßnahme dürfen nur Personen betraut werden, die nach Maßgabe des Satzes 1 überprüft und belehrt worden sind. Nach Zustimmung des Bundesministeriums des Innern kann der Behördenleiter der berechtigten Stelle oder dessen Stellvertreter die nach Absatz 1 Satz 1 oder 3 Verpflichteten schriftlich auffordern, die Beschränkungsmaßnahme bereits vor Abschluss der Sicherheitsüberprüfung durchzuführen. Der nach Absatz 1 Satz 1 oder 3 Verpflichtete hat sicherzustellen, dass die Geheimschutzmaßnahmen nach den Abschnitten 1.1 bis 1.4, 1.6, 2.1 und 2.3 bis 2.5 der Anlage 7 zur Allgemeinen Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen vom 29. April 1994 (GMBl S. 674) getroffen werden.

(3) Die Sicherheitsüberprüfung nach Absatz 2 Satz 1 Nr. 2 ist entsprechend dem Sicherheitsüberprüfungsgesetz durchzuführen. Für Beschränkungsmaßnahmen einer Landesbehörde gilt dies nicht, soweit Rechtsvorschriften des Landes vergleichbare Bestimmungen enthalten; in diesem Fall sind die Rechtsvorschriften des Landes entsprechend anzuwenden. Zuständig ist bei Beschränkungsmaßnahmen von

Bundesbehörden das Bundesministerium des Innern; im Übrigen sind die nach Landesrecht bestimmten Behörden zuständig. Soll mit der Durchführung einer Beschränkungsmaßnahme eine Person betraut werden, für die innerhalb der letzten fünf Jahre bereits eine gleich- oder höherwertige Sicherheitsüberprüfung nach Bundes- oder Landesrecht durchgeführt worden ist, soll von einer erneuten Sicherheitsüberprüfung abgesehen werden.

Abschnitt 2
Beschränkungen in Einzelfällen

§ 3Voraussetzungen

(1) Beschränkungen nach § 1 Abs. 1 Nr. 1 dürfen unter den dort bezeichneten Voraussetzungen angeordnet werden, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand

1. Straftaten des Friedensverrats oder des Hochverrats (§§ 80 bis 83 des Strafgesetzbuches),
2. Straftaten der Gefährdung des demokratischen Rechtsstaates (§§ 84 bis 86, 87 bis 89a des Strafgesetzbuches, § 20 Abs. 1 Nr. 1 bis 4 des Vereinsgesetzes),
3. Straftaten des Landesverrats und der Gefährdung der äußeren Sicherheit (§§ 94 bis 96, 97a bis 100a des Strafgesetzbuches),
4. Straftaten gegen die Landesverteidigung (§§ 109e bis 109g des Strafgesetzbuches),
5. Straftaten gegen die Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantikvertrages (§§ 87, 89, 94 bis 96, 98 bis 100, 109e bis 109g des Strafgesetzbuches in Verbindung mit § 1 des NATO-Truppen-Schutzgesetzes),
6. Straftaten nach
   a)
   den §§ 129a bis 130 des Strafgesetzbuches sowie
   b)
   den §§ 211, 212, 239a, 239b, 306 bis 306c, 308 Abs. 1 bis 3, § 315 Abs. 3, § 316b Abs. 3 und § 316c Abs. 1 und 3 des Strafgesetzbuches, soweit diese sich gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes richten, oder
7. Straftaten nach § 95 Abs. 1 Nr. 8 des Aufenthaltsgesetzes

plant, begeht oder begangen hat. Gleiches gilt, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand Mitglied einer Vereinigung ist, deren Zwecke oder deren Tätigkeit darauf gerichtet sind, Straftaten zu begehen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind.

(1a) Beschränkungen nach § 1 Abs. 1 Nr. 1 dürfen unter den dort bezeichneten Voraussetzungen für den Bundesnachrichtendienst auch für Telekommunikationsanschlüsse, die sich an Bord deutscher Schiffe außerhalb deutscher Hoheitsgewässer befinden, angeordnet werden, wenn tatsächliche Anhaltspunkte bestehen, dass jemand eine der in § 23a Abs. 1 und 3 des Zollfahndungsdienstgesetzes genannten Straftaten plant, begeht oder begangen hat.

(2) Die Anordnung ist nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. Sie darf sich nur gegen den Verdächtigen oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Verdächtigen bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Verdächtige ihren Anschluss benutzt. Maßnahmen, die sich auf Sendungen beziehen, sind nur hinsichtlich solcher Sendungen zulässig, bei denen Tatsachen die Annahme rechtfertigen, dass sie von dem, gegen den sich die Anordnung richtet, herrühren oder für ihn bestimmt sind. Abgeordnetenpost von Mitgliedern des Deutschen Bundestages und der Parlamente der Länder darf nicht in eine Maßnahme einbezogen werden, die sich gegen einen Dritten richtet.

§ 3aSchutz des Kernbereichs privater Lebensgestaltung

Beschränkungen nach § 1 Abs. 1 Nr. 1 sind unzulässig, soweit tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch sie allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erfasst würden. Soweit im Rahmen von Beschränkungen nach § 1 Abs. 1 Nr. 1 neben einer automatischen Aufzeichnung eine unmittelbare Kenntnisnahme erfolgt, ist die Maßnahme unverzüglich zu unterbrechen, soweit sich während der Überwachung tatsächliche Anhaltspunkte dafür ergeben, dass Inhalte, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Bestehen insoweit Zweifel, darf nur eine automatische Aufzeichnung fortgesetzt werden. Automatische Aufzeichnungen nach Satz 3 sind unverzüglich einem bestimmten Mitglied der G10-Kommission oder seinem Stellvertreter zur Entscheidung über die Verwertbarkeit oder Löschung der Daten vorzulegen. Das Nähere regelt die Geschäftsordnung. Die Entscheidung des Mitglieds der Kommission, dass eine Verwertung erfolgen darf, ist unverzüglich durch die Kommission zu bestätigen. Ist die Maßnahme nach Satz 2 unterbrochen worden, so darf sie für den Fall, dass sie nicht nach Satz 1 unzulässig ist, fortgeführt werden. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Beschränkung nach § 1 Abs. 1 Nr. 1 erlangt worden sind, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

§ 3bSchutz zeugnisverweigerungsberechtigter Personen

(1) Maßnahmen nach § 1 Abs. 1 Nr. 1, die sich gegen eine in § 53 Abs. 1 Satz 1 Nr. 1, 2 oder Nr. 4 der Strafprozessordnung genannte Person richten und voraussichtlich Erkenntnisse erbringen würden, über die diese Person das Zeugnis verweigern dürfte, sind unzulässig. Dennoch erlangte Erkenntnisse dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Die Sätze 2 bis 3 gelten entsprechend, wenn durch eine Maßnahme, die sich nicht gegen eine in § 53 Abs. 1 Satz 1 Nr. 1, 2 oder Nr. 4 der Strafprozessordnung genannte Person richtet, von einer dort genannten Person Erkenntnisse erlangt werden, über die sie das Zeugnis verweigern dürfte.
(2) Soweit durch eine Beschränkung eine in § 53 Abs. 1 Satz 1 Nr. 3 bis 3b oder Nr. 5 der Strafprozessordnung genannte Person betroffen wäre und dadurch voraussichtlich Erkenntnisse erlangt würden, über die diese Person das Zeugnis verweigern dürfte, ist dies im Rahmen der Prüfung der Verhältnismäßigkeit unter Würdigung des öffentlichen Interesses an den von dieser Person wahrgenommenen Aufgaben und des Interesses an der Geheimhaltung der dieser Person anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen. Soweit hiernach geboten, ist die Maßnahme zu unterlassen oder, soweit dies nach der Art der Maßnahme möglich ist, zu beschränken.
(3) Die Absätze 1 und 2 gelten entsprechend, soweit die in § 53a der Strafprozessordnung Genannten das Zeugnis verweigern dürften.
(4) Die Absätze 1 bis 3 gelten nicht, sofern die zeugnisverweigerungsberechtigte Person Verdächtiger im Sinne des § 3 Abs. 2 Satz 2 ist oder tatsächliche Anhaltspunkte den Verdacht begründen, dass sie dessen in § 3 Abs. 1 bezeichnete Bestrebungen durch Entgegennahme oder Weitergabe von Mitteilungen bewusst unterstützt.

§ 4Prüf-, Kennzeichnungs- und Löschungspflichten, Übermittlungen, Zweckbindung

(1) Die erhebende Stelle prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die erhobenen personenbezogenen Daten im Rahmen ihrer Aufgaben allein oder zusammen mit bereits vorliegenden Daten für die in § 1 Abs. 1 Nr. 1 bestimmten Zwecke erforderlich sind. Soweit die Daten für diese Zwecke nicht erforderlich sind und nicht für eine Übermittlung an andere Stellen benötigt werden, sind sie unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu löschen. Die Löschung ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zur Durchführung der Datenschutzkontrolle verwendet werden. Die Protokolldaten sind am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, zu löschen. Die Löschung der Daten unterbleibt, soweit die Daten für eine Mitteilung nach § 12 Abs. 1 oder für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Beschränkungsmaßnahme von Bedeutung sein können. In diesem Fall sind die Daten zu sperren; sie dürfen nur zu diesen Zwecken verwendet werden.

(2) Die verbleibenden Daten sind zu kennzeichnen. Nach einer Übermittlung ist die Kennzeichnung durch den Empfänger aufrechtzuerhalten. Die Daten dürfen nur zu den in § 1 Abs. 1 Nr. 1 und den in Absatz 4 genannten Zwecken verwendet werden.

(3) Der Behördenleiter oder sein Stellvertreter kann anordnen, dass bei der Übermittlung auf die Kennzeichnung verzichtet wird, wenn dies unerlässlich ist, um die Geheimhaltung einer Beschränkungsmaßnahme nicht zu gefährden, und die G 10-Kommission oder, soweit es sich um die Übermittlung durch eine Landesbehörde handelt, die nach Landesrecht zuständige Stelle zugestimmt hat. Bei Gefahr im Verzuge kann die Anordnung bereits vor der Zustimmung getroffen werden. Wird die Zustimmung versagt, ist die Kennzeichnung durch den Übermittlungsempfänger unverzüglich nachzuholen; die übermittelnde Behörde hat ihn hiervon zu unterrichten.

(4) Die Daten dürfen nur übermittelt werden

1.

zur Verhinderung oder Aufklärung von Straftaten, wenn

a)

tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine der in § 3 Abs. 1 und 1a genannten Straftaten plant oder begeht,

b)

bestimmte Tatsachen den Verdacht begründen, dass jemand eine sonstige in § 7 Abs. 4 Satz 1 genannte Straftat plant oder begeht,

2.

zur Verfolgung von Straftaten, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand eine in Nummer 1 bezeichnete Straftat begeht oder begangen hat, oder

3.

zur Vorbereitung und Durchführung eines Verfahrens nach Artikel 21 Abs. 2 Satz 2 des Grundgesetzes oder einer Maßnahme nach § 3 Abs. 1 Satz 1 des Vereinsgesetzes,

soweit sie zur Erfüllung der Aufgaben des Empfängers erforderlich sind.

(5) Sind mit personenbezogenen Daten, die übermittelt werden dürfen, weitere Daten des Betroffenen oder eines Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, ist die Übermittlung auch dieser Daten zulässig; eine Verwendung dieser Daten ist unzulässig. Über die Übermittlung entscheidet ein Bediensteter der übermittelnden Stelle, der die Befähigung zum Richteramt hat. Die Übermittlung ist zu protokollieren.

(6) Der Empfänger darf die übermittelten Daten nur für die Zwecke verwenden, zu deren Erfüllung sie ihm übermittelt worden sind. Er prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die übermittelten Daten für diese Zwecke erforderlich sind. Absatz 1 Satz 2 und 3 gilt entsprechend. Der Empfänger unterrichtet die übermittelnde Stelle unverzüglich über die erfolgte Löschung.

Abschnitt 3

Strategische Beschränkungen

§ 5Voraussetzungen

(1) Auf Antrag des Bundesnachrichtendienstes dürfen Beschränkungen nach § 1 für internationale Telekommunikationsbeziehungen, soweit eine gebündelte Übertragung erfolgt, angeordnet werden. Die jeweiligen Telekommunikationsbeziehungen werden von dem nach § 10 Abs. 1 zuständigen Bundesministerium mit Zustimmung des Parlamentarischen Kontrollgremiums bestimmt. Beschränkungen nach Satz 1 sind nur zulässig zur Sammlung von Informationen über Sachverhalte, deren Kenntnis notwendig ist, um die Gefahr

1.
eines bewaffneten Angriffs auf die Bundesrepublik Deutschland,

2.
der Begehung internationaler terroristischer Anschläge mit unmittelbarem Bezug zur Bundesrepublik Deutschland,

3.
der internationalen Verbreitung von Kriegswaffen im Sinne des Gesetzes über die Kontrolle von Kriegswaffen sowie des unerlaubten Außenwirtschaftsverkehrs mit Waren, Datenverarbeitungsprogrammen und Technologien in Fällen von erheblicher Bedeutung,

4.
der unbefugten gewerbs- oder bandenmäßig organisierten Verbringung von Betäubungsmitteln in das Gebiet der Europäischen Union in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland,

5.
der Beeinträchtigung der Geldwertstabilität im Euro-Währungsraum durch im Ausland begangene Geldfälschungen,

6.
der international organisierten Geldwäsche in Fällen von erheblicher Bedeutung oder

7.
des gewerbs- oder bandenmäßig organisierten Einschleusens von ausländischen Personen in das Gebiet der Europäischen Union in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland

a)
bei unmittelbarem Bezug zu den Gefahrenbereichen nach Nr. 1 bis 3 oder

b)
in Fällen, in denen eine erhebliche Anzahl geschleuster Personen betroffen ist, insbesondere wenn durch die Art der Schleusung von einer Gefahr für ihr Leib oder Leben auszugehen ist, oder

c)

in Fällen von unmittelbarer oder mittelbarer Unterstützung oder Duldung durch ausländische öffentliche Stellen

rechtzeitig zu erkennen und einer solchen Gefahr zu begegnen. In den Fällen von Satz 3 Nr. 1 dürfen Beschränkungen auch für Postverkehrsbeziehungen angeordnet werden; Satz 2 gilt entsprechend.

(2) Bei Beschränkungen von Telekommunikationsbeziehungen darf der Bundesnachrichtendienst nur Suchbegriffe verwenden, die zur Aufklärung von Sachverhalten über den in der Anordnung bezeichneten Gefahrenbereich bestimmt und geeignet sind. Es dürfen keine Suchbegriffe verwendet werden, die

1. Identifizierungsmerkmale enthalten, die zu einer gezielten Erfassung bestimmter Telekommunikationsanschlüsse führen, oder
2. den Kernbereich der privaten Lebensgestaltung betreffen.

Dies gilt nicht für Telekommunikationsanschlüsse im Ausland, sofern ausgeschlossen werden kann, dass Anschlüsse, deren Inhaber oder regelmäßige Nutzer deutsche Staatsangehörige sind, gezielt erfasst werden. Die Durchführung ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zu Zwecken der Datenschutzkontrolle verwendet werden. Sie sind am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, zu löschen.

§ 5aSchutz des Kernbereichs privater Lebensgestaltung

Durch Beschränkungen nach § 1 Abs. 1 Nr. 2 dürfen keine Kommunikationsinhalte aus dem Kernbereich privater Lebensgestaltung erfasst werden. Sind durch eine Beschränkung nach § 1 Abs. 1 Nr. 2 Kommunikationsinhalte aus dem Kernbereich privater Lebensgestaltung erfasst worden, dürfen diese nicht verwertet werden. Sie sind unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu löschen. § 3a Satz 2 bis 7 gilt entsprechend. Die Tatsache der Erfassung der Daten und ihrer Löschung ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zum Zwecke der Durchführung der Datenschutzkontrolle verwendet werden. Sie sind zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich sind, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt.

§ 6Prüf-, Kennzeichnungs- und Löschungspflichten, Zweckbindung

(1) Der Bundesnachrichtendienst prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die erhobenen personenbezogenen Daten im Rahmen seiner Aufgaben allein oder zusammen mit bereits vorliegenden Daten für die in § 5 Abs. 1 Satz 3 bestimmten Zwecke erforderlich sind. Soweit die Daten für diese Zwecke nicht erforderlich sind und nicht für eine Übermittlung an andere Stellen benötigt werden, sind sie unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu löschen. Die

Löschung ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zur Durchführung der Datenschutzkontrolle verwendet werden. Die Protokolldaten sind am Ende des Kalenderjahres zu löschen, das dem Jahr der Protokollierung folgt. Außer in den Fällen der erstmaligen Prüfung nach Satz 1 unterbleibt die Löschung, soweit die Daten für eine Mitteilung nach § 12 Abs. 2 oder für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Beschränkungsmaßnahme von Bedeutung sein können. In diesem Fall sind die Daten zu sperren; sie dürfen nur zu diesen Zwecken verwendet werden.

(2) Die verbleibenden Daten sind zu kennzeichnen. Nach einer Übermittlung ist die Kennzeichnung durch den Empfänger aufrechtzuerhalten. Die Daten dürfen nur zu den in § 5 Abs. 1 Satz 3 genannten Zwecken und für Übermittlungen nach § 7 Abs. 1 bis 4 und § 7a verwendet werden.

(3) Auf Antrag des Bundesnachrichtendienstes dürfen zur Prüfung der Relevanz erfasster Telekommunikationsverkehre auf Anordnung des nach § 10 Abs. 1 zuständigen Bundesministeriums die erhobenen Daten in einem automatisierten Verfahren mit bereits vorliegenden Rufnummern oder anderen Kennungen bestimmter Telekommunikationsanschlüsse abgeglichen werden, bei denen tatsächliche Anhaltspunkte dafür bestehen, dass sie in einem Zusammenhang mit dem Gefahrenbereich stehen, für den die Überwachungsmaßnahme angeordnet wurde. Zu diesem Abgleich darf der Bundesnachrichtendienst auch Rufnummern oder andere Kennungen bestimmter Telekommunikationsanschlüsse im Inland verwenden. Die zu diesem Abgleich genutzten Daten dürfen nicht als Suchbegriffe im Sinne des § 5 Abs. 2 Satz 1 verwendet werden. Der Abgleich und die Gründe für die Verwendung der für den Abgleich genutzten Daten sind zu protokollieren. Die Protokolldaten dürfen ausschließlich zu Zwecken der Datenschutzkontrolle verwendet werden. Sie sind am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, zu vernichten.

§ 7Übermittlungen durch den Bundesnachrichtendienst

(1) Durch Beschränkungen nach § 5 erhobene personenbezogene Daten dürfen nach § 12 des BND-Gesetzes zur Unterrichtung über die in § 5 Abs. 1 Satz 3 genannten Gefahren übermittelt werden.

(2) Durch Beschränkungen nach § 5 erhobene personenbezogene Daten dürfen an die Verfassungsschutzbehörden des Bundes und der Länder sowie an den Militärischen Abschirmdienst übermittelt werden, wenn

1. tatsächliche Anhaltspunkte dafür bestehen, dass die Daten erforderlich sind zur Sammlung und Auswertung von Informationen über Bestrebungen in der Bundesrepublik Deutschland, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 3 Abs. 1 Nr. 1, 3 und 4 des Bundesverfassungsschutzgesetzes genannten Schutzgüter gerichtet sind, oder
2. bestimmte Tatsachen den Verdacht sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten für eine fremde Macht begründen.

(3) Durch Beschränkungen nach § 5 Abs. 1 Satz 1 in Verbindung mit Satz 3 Nr. 3 erhobene personenbezogene Daten dürfen an das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) übermittelt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Kenntnis dieser Daten erforderlich ist

1.

zur Aufklärung von Teilnehmern am Außenwirtschaftsverkehr über Umstände, die für die Einhaltung von Beschränkungen des Außenwirtschaftsverkehrs von Bedeutung sind, oder

2.

im Rahmen eines Verfahrens zur Erteilung einer ausfuhrrechtlichen Genehmigung oder zur Unterrichtung von Teilnehmern am Außenwirtschaftsverkehr, soweit hierdurch eine Genehmigungspflicht für die Ausfuhr von Gütern begründet wird.

(4) Durch Beschränkungen nach § 5 erhobene personenbezogene Daten dürfen zur Verhinderung von Straftaten an die mit polizeilichen Aufgaben betrauten Behörden übermittelt werden, wenn

1.

tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand

a)

Straftaten nach § 89a oder § 129a, auch in Verbindung mit § 129b Abs. 1, sowie den §§ 146, 151 bis 152a oder § 261 des Strafgesetzbuches,

b)

Straftaten nach § 34 Abs. 1 bis 6 und 8, § 35 des Außenwirtschaftsgesetzes, §§ 19 bis 21 oder § 22a Abs. 1 Nr. 4, 5 und 7 des Gesetzes über die Kontrolle von Kriegswaffen oder

c)

Straftaten nach § 29a Abs. 1 Nr. 2, § 30 Abs. 1 Nr. 1, 4 oder § 30a des Betäubungsmittelgesetzes plant oder begeht oder

2.

bestimmte Tatsachen den Verdacht begründen, dass jemand

a)

Straftaten, die in § 3 Abs. 1 Satz 1 Nr. 1 bis 5 und 7, Abs. 1 Satz 2 oder Abs. 1a dieses Gesetzes oder in § 129a Abs. 1 des Strafgesetzbuches bezeichnet sind,

b)

Straftaten nach den §§ 130, 232 Abs. 3, 4 oder Abs. 5 zweiter Halbsatz, §§ 249 bis 251, 255, 305a, 306 bis 306c, 307 Abs. 1 bis 3, § 308 Abs. 1 bis 4, § 309 Abs. 1 bis 5, §§ 313, 314, 315 Abs. 1, 3 oder Abs. 4, § 315b Abs. 3, §§ 316a, 316b Abs. 1 oder Abs. 3 oder § 316c Abs. 1 bis 3 des Strafgesetzbuches oder

c)

Straftaten nach § 96 Abs. 2, auch in Verbindung mit Absatz 4, und § 97 Abs. 1 bis 3 des Aufenthaltsgesetzes

plant oder begeht. Die Daten dürfen zur Verfolgung von Straftaten an die zuständigen Behörden übermittelt werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand eine in Satz 1 bezeichnete Straftat begeht oder begangen hat.

(5) Die Übermittlung ist nur zulässig, soweit sie zur Erfüllung der Aufgaben des Empfängers erforderlich ist. Sind mit personenbezogenen Daten, die übermittelt werden dürfen, weitere Daten des Betroffenen oder eines Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, ist die Übermittlung auch dieser Daten zulässig; eine Verwendung dieser Daten ist unzulässig. Über die Übermittlung entscheidet ein Bediensteter des Bundesnachrichtendienstes, der die Befähigung zum Richteramt hat. Die Übermittlung ist zu protokollieren.

(6) Der Empfänger darf die Daten nur für die Zwecke verwenden, zu deren Erfüllung sie ihm übermittelt worden sind. Er prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die übermittelten Daten für diese Zwecke erforderlich sind. § 4 Abs. 6 Satz 4 und § 6 Abs. 1 Satz 2 und 3 gelten entsprechend.

§ 7aÜbermittlungen durch den Bundesnachrichtendienst an ausländische öffentliche Stellen

(1) Der Bundesnachrichtendienst darf durch Beschränkungen nach § 5 Abs. 1 Satz 3 Nr. 2, 3 und 7 erhobene personenbezogene Daten an die mit nachrichtendienstlichen Aufgaben betrauten ausländischen öffentlichen Stellen übermitteln, soweit

1. die Übermittlung zur Wahrung außen- oder sicherheitspolitischer Belange der Bundesrepublik Deutschland oder erheblicher Sicherheitsinteressen des ausländischen Staates erforderlich ist,
2. überwiegende schutzwürdige Interessen des Betroffenen nicht entgegenstehen, insbesondere in dem ausländischen Staat ein angemessenes Datenschutzniveau gewährleistet ist sowie davon auszugehen ist, dass die Verwendung der Daten durch den Empfänger in Einklang mit grundlegenden rechtsstaatlichen Prinzipien erfolgt, und
3. das Prinzip der Gegenseitigkeit gewahrt ist.

Die Übermittlung bedarf der Zustimmung des Bundeskanzleramtes.

(2) Der Bundesnachrichtendienst darf unter den Voraussetzungen des Absatzes 1 durch Beschränkungen nach § 5 Abs. 1 Satz 3 Nr. 2, 3 und 7 erhobene personenbezogene Daten ferner im Rahmen von Artikel 3 des Zusatzabkommens zu dem Abkommen zwischen den Parteien des Nordatlantikvertrages über die Rechtsstellung ihrer Truppen hinsichtlich der in der Bundesrepublik Deutschland stationierten ausländischen Truppen vom 3. August 1959 (BGBl. 1961 II S. 1183, 1218) an Dienststellen der Stationierungsstreitkräfte übermitteln, soweit dies zur Erfüllung der in deren Zuständigkeit liegenden Aufgaben erforderlich ist.

(3) Über die Übermittlung entscheidet ein Bediensteter des Bundesnachrichtendienstes, der die Befähigung zum Richteramt hat. Die Übermittlung ist zu protokollieren. Der Bundesnachrichtendienst führt einen

Nachweis über den Zweck, die Veranlassung, die Aktenfundstelle und die Empfänger der Übermittlungen nach Absatz 1 und 2. Die Nachweise sind gesondert aufzubewahren, gegen unberechtigten Zugriff zu sichern und am Ende des Kalenderjahres, das dem Jahr ihrer Erstellung folgt, zu vernichten.

(4) Der Empfänger ist zu verpflichten,

1. die übermittelten Daten nur zu dem Zweck zu verwenden, zu dem sie ihm übermittelt wurden,
2. eine angebrachte Kennzeichnung beizubehalten und
3. dem Bundesnachrichtendienst auf Ersuchen Auskunft über die Verwendung zu erteilen.

(5) Das zuständige Bundesministerium unterrichtet monatlich die G10-Kommission über Übermittlungen nach Absatz 1 und 2.

(6) Das Parlamentarische Kontrollgremium ist in Abständen von höchstens sechs Monaten über die vorgenommenen Übermittlungen nach Absatz 1 und 2 zu unterrichten.

§ 8Gefahr für Leib oder Leben einer Person im Ausland

(1) Auf Antrag des Bundesnachrichtendienstes dürfen Beschränkungen nach § 1 für internationale Telekommunikationsbeziehungen im Sinne des § 5 Abs. 1 Satz 1 angeordnet werden, wenn dies erforderlich ist, um eine im Einzelfall bestehende Gefahr für Leib oder Leben einer Person im Ausland rechtzeitig zu erkennen oder ihr zu begegnen und dadurch Belange der Bundesrepublik Deutschland unmittelbar in besonderer Weise berührt sind.

(2) Die jeweiligen Telekommunikationsbeziehungen werden von dem nach § 10 Abs. 1 zuständigen Bundesministerium mit Zustimmung des Parlamentarischen Kontrollgremiums bestimmt. Die Zustimmung bedarf der Mehrheit von zwei Dritteln seiner Mitglieder. Die Bestimmung tritt spätestens nach zwei Monaten außer Kraft. Eine erneute Bestimmung ist zulässig, soweit ihre Voraussetzungen fortbestehen.

(3) Die Anordnung ist nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. Der Bundesnachrichtendienst darf nur Suchbegriffe verwenden, die zur Erlangung von Informationen über die in der Anordnung bezeichnete Gefahr bestimmt und geeignet sind. § 5 Abs. 2 Satz 2 bis 6 gilt entsprechend. Ist die Überwachungsmaßnahme erforderlich, um einer im Einzelfall bestehenden Gefahr für Leib oder Leben einer Person zu begegnen, dürfen die Suchbegriffe auch Identifizierungsmerkmale enthalten, die zu einer gezielten Erfassung der Rufnummer oder einer anderen Kennung des Telekommunikationsanschlusses dieser Person im Ausland führen.

(4) Der Bundesnachrichtendienst prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die erhobenen personenbezogenen Daten im Rahmen seiner Aufgaben allein oder zusammen mit bereits vorliegenden Daten zu dem in Absatz 1 bestimmten Zweck erforderlich sind. Soweit die Daten für diesen Zweck nicht erforderlich sind, sind sie unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu löschen. Die Löschung ist zu protokollieren. § 6 Abs. 1 Satz 4 und 5, Abs. 2 Satz 1

und 2 gilt entsprechend. Die Daten dürfen nur zu den in den Absätzen 1, 5 und 6 genannten Zwecken verwendet werden.

(5) Die erhobenen personenbezogenen Daten dürfen nach § 12 des BND-Gesetzes zur Unterrichtung über die in Absatz 1 genannte Gefahr übermittelt werden.

(6) Die erhobenen personenbezogenen Daten dürfen zur Verhinderung von Straftaten an die zuständigen Behörden übermittelt werden, wenn tatsächliche Anhaltspunkte den Verdacht begründen, dass jemand eine Straftat plant oder begeht, die geeignet ist, zu der Entstehung oder Aufrechterhaltung der in Absatz 1 bezeichneten Gefahr beizutragen. Die Daten dürfen zur Verfolgung von Straftaten an die zuständigen Behörden übermittelt werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand eine in Satz 1 bezeichnete Straftat begeht oder begangen hat. § 7 Abs. 5 und 6 sowie § 7a Abs. 1 und 3 bis 6 gelten entsprechend.

Abschnitt 4
Verfahren

§ 9Antrag

(1) Beschränkungsmaßnahmen nach diesem Gesetz dürfen nur auf Antrag angeordnet werden.

(2) Antragsberechtigt sind im Rahmen ihres Geschäftsbereichs

1. das Bundesamt für Verfassungsschutz,
2. die Verfassungsschutzbehörden der Länder,
3. das Amt für den Militärischen Abschirmdienst und
4. der Bundesnachrichtendienst

durch den Behördenleiter oder seinen Stellvertreter.

(3) Der Antrag ist schriftlich zu stellen und zu begründen. Er muss alle für die Anordnung erforderlichen Angaben enthalten. In den Fällen der §§ 3 und 8 hat der Antragsteller darzulegen, dass die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre.

§ 10Anordnung

(1) Zuständig für die Anordnung von Beschränkungsmaßnahmen ist bei Anträgen der Verfassungsschutzbehörden der Länder die zuständige oberste Landesbehörde, im Übrigen das Bundesministerium des Innern.
(2) Die Anordnung ergeht schriftlich. In ihr sind der Grund der Anordnung und die zur Überwachung berechtigte Stelle anzugeben sowie Art, Umfang und Dauer der Beschränkungsmaßnahme zu bestimmen.
(3) In den Fällen des § 3 muss die Anordnung denjenigen bezeichnen, gegen den sich die Beschränkungsmaßnahme richtet. Bei einer Überwachung der Telekommunikation ist auch die Rufnummer oder eine andere Kennung des Telekommunikationsanschlusses oder die Kennung des Endgerätes, wenn diese allein diesem Endgerät zuzuordnen ist, anzugeben.
(4) In den Fällen der §§ 5 und 8 sind die Suchbegriffe in der Anordnung zu benennen. Ferner sind das Gebiet, über das Informationen gesammelt werden sollen, und die Übertragungswege, die der Beschränkung unterliegen, zu bezeichnen. Weiterhin ist festzulegen, welcher Anteil der auf diesen Übertragungswegen zur Verfügung stehenden Übertragungskapazität überwacht werden darf. In den Fällen des § 5 darf dieser Anteil höchstens 20 vom Hundert betragen.
(5) In den Fällen der §§ 3 und 5 ist die Anordnung auf höchstens drei Monate zu befristen. Verlängerungen um jeweils nicht mehr als drei weitere Monate sind auf Antrag zulässig, soweit die Voraussetzungen der Anordnung fortbestehen.
(6) Die Anordnung ist dem nach § 2 Abs. 1 Satz 1 oder 3 Verpflichteten insoweit mitzuteilen, als dies erforderlich ist, um ihm die Erfüllung seiner Verpflichtungen zu ermöglichen. Die Mitteilung entfällt, wenn die Anordnung ohne seine Mitwirkung ausgeführt werden kann.
(7) Das Bundesamt für Verfassungsschutz unterrichtet die jeweilige Landesbehörde für Verfassungsschutz über die in deren Bereich getroffenen Beschränkungsanordnungen. Die Landesbehörden für Verfassungsschutz teilen dem Bundesamt für Verfassungsschutz die in ihrem Bereich getroffenen Beschränkungsanordnungen mit.

§ 11Durchführung

(1) Die aus der Anordnung sich ergebenden Beschränkungsmaßnahmen sind unter Verantwortung der Behörde, auf deren Antrag die Anordnung ergangen ist, und unter Aufsicht eines Bediensteten vorzunehmen, der die Befähigung zum Richteramt hat.
(2) Die Maßnahmen sind unverzüglich zu beenden, wenn sie nicht mehr erforderlich sind oder die Voraussetzungen der Anordnung nicht mehr vorliegen. Die Beendigung ist der Stelle, die die Anordnung getroffen hat, und dem nach § 2 Abs. 1 Satz 1 oder 3 Verpflichteten, dem die Anordnung mitgeteilt worden ist, anzuzeigen. Die Anzeige an den Verpflichteten entfällt, wenn die Anordnung ohne seine Mitwirkung ausgeführt wurde.
(3) Postsendungen, die zur Öffnung und Einsichtnahme ausgehändigt worden sind, sind dem Postverkehr unverzüglich wieder zuzuführen. Telegramme dürfen dem Postverkehr nicht entzogen werden. Der zur Einsichtnahme berechtigten Stelle ist eine Abschrift des Telegramms zu übergeben.

§ 12Mitteilungen an Betroffene

(1) Beschränkungsmaßnahmen nach § 3 sind dem Betroffenen nach ihrer Einstellung mitzuteilen. Die Mitteilung unterbleibt, solange eine Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden kann oder solange der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist. Erfolgt die nach Satz 2 zurückgestellte Mitteilung nicht binnen zwölf Monaten nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der Zustimmung der G10-Kommission. Die G10-Kommission bestimmt die Dauer der weiteren Zurückstellung. Einer Mitteilung bedarf es nicht, wenn die G10-Kommission einstimmig festgestellt hat, dass

1. eine der Voraussetzungen in Satz 2 auch nach fünf Jahren nach Beendigung der Maßnahme noch vorliegt,
2. sie mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft vorliegt und
3. die Voraussetzungen für eine Löschung sowohl bei der erhebenden Stelle als auch beim Empfänger vorliegen.

(2) Absatz 1 gilt entsprechend für Beschränkungsmaßnahmen nach den §§ 5 und 8, sofern die personenbezogenen Daten nicht unverzüglich gelöscht wurden. Die Frist von fünf Jahren beginnt mit der Erhebung der personenbezogenen Daten.

(3) Die Mitteilung obliegt der Behörde, auf deren Antrag die Anordnung ergangen ist. Wurden personenbezogene Daten übermittelt, erfolgt die Mitteilung im Benehmen mit dem Empfänger.

§ 13Rechtsweg

Gegen die Anordnung von Beschränkungsmaßnahmen nach den §§ 3 und 5 Abs. 1 Satz 3 Nr. 1 und ihren Vollzug ist der Rechtsweg vor der Mitteilung an den Betroffenen nicht zulässig.

Abschnitt 5
Kontrolle

§ 14Parlamentarisches Kontrollgremium

(1) Das nach § 10 Abs. 1 für die Anordnung von Beschränkungsmaßnahmen zuständige Bundesministerium unterrichtet in Abständen von höchstens sechs Monaten das Parlamentarische Kontrollgremium über die Durchführung dieses Gesetzes. Das Gremium erstattet dem Deutschen Bundestag jährlich einen Bericht über Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5, 7a und 8; dabei sind die Grundsätze des § 10 Absatz 1 des Kontrollgremiumgesetzes zu beachten.
(2) Bei Gefahr im Verzuge kann die Zustimmung zu Bestimmungen nach den §§ 5 und 8 durch den Vorsitzenden des Parlamentarischen Kontrollgremiums und seinen Stellvertreter vorläufig erteilt werden. Die Zustimmung des Parlamentarischen Kontrollgremiums ist unverzüglich einzuholen. Die vorläufige Zustimmung tritt spätestens nach zwei Wochen außer Kraft.

§ 15G 10-Kommission

(1) Die G 10-Kommission besteht aus dem Vorsitzenden, der die Befähigung zum Richteramt besitzen muss, und drei Beisitzern sowie vier stellvertretenden Mitgliedern, die an den Sitzungen mit Rede- und Fragerecht teilnehmen können. Bei Stimmengleichheit entscheidet die Stimme des Vorsitzenden. Die Mitglieder der G 10-Kommission sind in ihrer Amtsführung unabhängig und Weisungen nicht unterworfen. Sie nehmen ein öffentliches Ehrenamt wahr und werden von dem Parlamentarischen Kontrollgremium nach Anhörung der Bundesregierung für die Dauer einer Wahlperiode des Deutschen Bundestages mit der Maßgabe bestellt, dass ihre Amtszeit erst mit der Neubestimmung der Mitglieder der Kommission, spätestens jedoch drei Monate nach Ablauf der Wahlperiode endet.
(2) Die Beratungen der G 10-Kommission sind geheim. Die Mitglieder der Kommission sind zur Geheimhaltung der Angelegenheiten verpflichtet, die ihnen bei ihrer Tätigkeit in der Kommission bekannt geworden sind. Dies gilt auch für die Zeit nach ihrem Ausscheiden aus der Kommission.
(3) Der G 10-Kommission ist die für die Erfüllung ihrer Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Deutschen Bundestages gesondert auszuweisen. Der Kommission sind Mitarbeiter mit technischem Sachverstand zur Verfügung zu stellen.
(4) Die G 10-Kommission tritt mindestens einmal im Monat zusammen. Sie gibt sich eine Geschäftsordnung, die der Zustimmung des Parlamentarischen Kontrollgremiums bedarf. Vor der Zustimmung ist die Bundesregierung zu hören.
(5) Die G 10-Kommission entscheidet von Amts wegen oder auf Grund von Beschwerden über die Zulässigkeit und Notwendigkeit von Beschränkungsmaßnahmen. Die Kontrollbefugnis der Kommission erstreckt sich auf die gesamte Erhebung, Verarbeitung und Nutzung der nach diesem Gesetz erlangten personenbezogenen Daten durch Nachrichtendienste des Bundes einschließlich der Entscheidung über die Mitteilung an Betroffene. Der Kommission und ihren Mitarbeitern ist dabei insbesondere

1. Auskunft zu ihren Fragen zu erteilen,
2.

Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Beschränkungsmaßnahme stehen, und

3. jederzeit Zutritt in alle Diensträume zu gewähren.

Die Kommission kann dem Bundesbeauftragten für den Datenschutz Gelegenheit zur Stellungnahme in Fragen des Datenschutzes geben.

(6) Das zuständige Bundesministerium unterrichtet monatlich die G 10-Kommission über die von ihm angeordneten Beschränkungsmaßnahmen vor deren Vollzug. Bei Gefahr im Verzuge kann es den Vollzug der Beschränkungsmaßnahmen auch bereits vor der Unterrichtung der Kommission anordnen. Anordnungen, die die Kommission für unzulässig oder nicht notwendig erklärt, hat das zuständige Bundesministerium unverzüglich aufzuheben. In den Fällen des § 8 tritt die Anordnung außer Kraft, wenn sie nicht binnen drei Tagen vom Vorsitzenden oder seinem Stellvertreter bestätigt wird. Die Bestätigung der Kommission ist unverzüglich nachzuholen.

(7) Das zuständige Bundesministerium unterrichtet monatlich die G 10-Kommission über Mitteilungen von Bundesbehörden nach § 12 Abs. 1 und 2 oder über die Gründe, die einer Mitteilung entgegenstehen. Hält die Kommission eine Mitteilung für geboten, ist diese unverzüglich vorzunehmen. § 12 Abs. 3 Satz 2 bleibt unberührt, soweit das Benehmen einer Landesbehörde erforderlich ist.

§ 16Parlamentarische Kontrolle in den Ländern

Durch den Landesgesetzgeber wird die parlamentarische Kontrolle der nach § 10 Abs. 1 für die Anordnung von Beschränkungsmaßnahmen zuständigen obersten Landesbehörden und die Überprüfung der von ihnen angeordneten Beschränkungsmaßnahmen geregelt. Personenbezogene Daten dürfen nur dann an Landesbehörden übermittelt werden, wenn die Kontrolle ihrer Verarbeitung und Nutzung durch den Landesgesetzgeber geregelt ist.

Abschnitt 6
Straf- und Bußgeldvorschriften

§ 17Mitteilungsverbote

(1) Wird die Telekommunikation nach diesem Gesetz oder nach den §§ 100a, 100b der Strafprozessordnung überwacht, darf diese Tatsache von Personen, die Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, anderen nicht mitgeteilt werden.

(2) Wird die Aushändigung von Sendungen nach § 2 Abs. 1 Satz 1 oder 3 angeordnet, darf diese Tatsache von Personen, die zur Aushändigung verpflichtet oder mit der Sendungsübermittlung betraut sind oder hieran mitwirken, anderen nicht mitgeteilt werden.
(3) Erfolgt ein Auskunftsersuchen oder eine Auskunftserteilung nach § 2 Abs. 1, darf diese Tatsache oder der Inhalt des Ersuchens oder der erteilten Auskunft von Personen, die zur Beantwortung verpflichtet oder mit der Beantwortung betraut sind oder hieran mitwirken, anderen nicht mitgeteilt werden.

§ 18Straftaten

Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer entgegen § 17 eine Mitteilung macht.

§ 19Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer
1. einer vollziehbaren Anordnung nach § 2 Abs. 1 Satz 1 oder 3 zuwiderhandelt,
2. entgegen § 2 Abs. 2 Satz 2 eine Person betraut oder
3. entgegen § 2 Abs. 2 Satz 3 nicht sicherstellt, dass eine Geheimschutzmaßnahme getroffen wird.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzehntausend Euro geahndet werden.
(3) Bußgeldbehörde im Sinne des § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten ist die nach § 10 Abs. 1 zuständige Stelle.

Abschnitt 7
Schlussvorschriften

§ 20Entschädigung

Die nach § 1 Abs. 1 berechtigten Stellen haben für die Leistungen nach § 2 Abs. 1 eine Entschädigung zu gewähren, deren Umfang sich nach § 23 des Justizvergütungs- und -entschädigungsgesetzes bemisst. In den Fällen der §§ 5 und 8 ist eine Entschädigung zu vereinbaren, deren Höhe sich an den nachgewiesenen tatsächlichen Kosten orientiert.

§ 21Einschränkung von Grundrechten

Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird durch dieses Gesetz eingeschränkt.

附錄五：德國G10法中譯

摘自：周治平，情報機關通訊監察權之研究－德國法之啟示，警大法學論集第１５期，頁２９８，２００８年１０月。

限制書信、郵件及電訊秘密法【Gesetz zur Beschränkung des Brief-,Post-,und Fernmeldegeheimnisses（Gesetz zu Artikel 10 Grundgesetz-G10）】

1968 年制定(聯邦法律公報 BGBl.I 第 949 頁)，2009 年 7 月 31 日最後一次修訂(聯邦法律公報 BGBl.I 2499 頁)

第一節　總則

第一條（法律的對象）

（1） 聯邦及各邦憲法保護局、軍事反情報局及聯邦情報局，基於下述目的，有權在個案中對於電信通訊進行監聽與錄音，也可以開啟及檢視應予秘密之書信及郵件。

1. 為防止危害自由民主基本秩序、聯邦或邦之存續或安全，或駐紮於德國境內之北大西洋公約組織軍隊之安全。
2. 在聯邦情報局法第 1 條第 2 項所規範的職務範圍，聯邦情報局為履行本法第 5 條第 1 項第 3 句第 2 款至第 6 款，以及第 8 條第 1 項第 1 句所規範的目的。

（2） 聯邦機關執行前述第一款之措施，應接受聯邦議會情報監督委員會以及議會一個特設委員會（G10 委員會）之監督。

第二條（郵政電信業者的義務）

（1） 郵政業者或其協助人員，應依權責機關之命令，提供郵件往來的詳細資訊，及交付其受託、轉運或郵遞之傳遞物。依第一句負有義務者，應依權責機關之請求，提供限制命令準備所必要之私人信箱資訊，無須其他命令。而電信業者或其協助人員，應依權責機關之命令，提供命令生效後所發生電信通訊之詳細資訊，及交付電信通訊途徑上的傳遞物，並應促成電信通訊之監聽及記錄。聯邦憲法保護法第 8 條 a 第 2 項第 1 句第 3 款、第 4 款、軍事反情報局法第 4 條 a，以及聯邦情報局法第 2 條 a，不受影響。依第 3 句負有義務者，監聽措施技術上及組織上是否完備，以及應具備之程度等，依電信法第 110 條以及依該法授權訂定之法規命令為之。

（2） 依前項第 1 句或第 3 句負有義務者，在實施限制措施前，應即對受委託執行限制措施者進行

1.挑選。

2.令其接受簡易的安全查核。

3.曉諭第 17 條通知禁止及第 18 條違反之可罰性。

限制措施的實施，只有經過前項審查程序，且曉諭違法之可罰性者，方可委任郵政業者執行。經內政部同意後，第 1 項第 1 句或第 3 句義務機關之首長或代理人，應以書面要求在實施限制措施前必須完成安全查核。第 1 項第 1 句或第 3 句義務人，應依聯邦內政部 1994 年 4 月 29 日頒布之「秘密事項保護之一般行政規定」附件七 1.1 節至 1.4 節、1.6 節、2.1 節、2.3 至 2.5 節之規定，採取保密措施。

（3） 依據第 2 項第 1 句第 2 款所為之安全查核，適用安全查核法之規定。如各邦的法規有相類之規定時，則各邦之限制措施不適用本法。聯邦內政部為聯邦機關各項限制措施的主管機關，其他則依據各邦法所規定之機關管轄。限制措施應委由最近五年內具有相當資格以上之安全查核人員依據聯邦或各邦法實施，而無須重新辦理安全查核。

第二節　個案限制

第三條（前提要件）

（1）有事實足認某人涉嫌計劃、實行或完成下列各款犯罪之嫌疑，而具備第 1 條第 1 項第 1 款之要件者，始得命為限制措施。同樣地，有事實足認某人係以危害自由民主基本秩序，以及聯邦或邦之存續或安全為目的或犯行之組織成員之嫌疑時，亦適用之。

1. 危害和平或內亂罪（刑法第 80 至 83 條）

2. 危害民主法治國家罪（刑法第 84 至 86 條、87 至 89 條 a，以及結社法第 20 條第 1 項第 1 款至第 4 款）
3. 叛國或對外安全的危害行為（刑法第 94 至 96 條、97a 至 100 條 a）
4. 對抗邦之防衛罪
5. 危害駐紮於德國境內之北大西洋公約國軍隊之安全罪（刑法第 87、89、94 至 96 條、98 至 100 條，以及 109 條 e 至 109 條 g）
6. 下列犯罪

（a）刑法第 129 條 a 及第 130 條

（b）犯刑法第 211、212、239a、239b、306 至 306 條 c、308 條第 1 項至第 3 項、315 條第 3 項、第 316 條 b 第 3 項，以及第 316 條 c 第 1 項及第 3 項之罪，而有危害自由民主基本秩序，以及聯邦或邦之存續或安全時。

7. 居留法第 95 條第 1 項第 8 款之罪

（1a）對於停留在德國領海以外之德國船艦，如有事實足認某人涉嫌計劃、實行或完成海關法第 23 條 a 第 1 項及第 3 項之犯罪，得命由聯邦情報局執行第 1 條第 1 項第 1 款之限制措施。

（2）限制命令限於不能或極難以其他方法調查事實，始得為之。此項命令之對象限於犯罪嫌疑人，或依一定事實足認其係收受或傳達對犯罪嫌疑人而發，或犯罪嫌疑人所發送資訊之人，或犯罪嫌疑人利用其聯繫之人。對於郵件的限制措施，限於有事實證明該郵件係限制措施命令對象所發送或收受，始得為之。德國聯邦眾議院以及各邦議會之議員的郵件，不受此措施之限制。

第三條 a（私人生活方式核心領域的保護）

有事實足認藉由第 1 條第 1 項第 1 款所為之各種限制措施，可掌握私人生活方式核心領域的各種認識（Erkenntnisse）時，不得為之。在採取第 1 條第 1 項第 1 款之限制措施時，除自動紀錄方式直接獲悉之資訊外，如有事實足認其監控所得內容包括私人生活方式核心領域時，限制措施應立即中斷。倘若無法確定，僅有自動記錄方式得繼續實施。第 3 句之自動紀錄應立即提交 G10 委員會特定委員或其副委員，據以判斷資料是否可以運用或應銷毀。細節由委員會議事規則定之。委員會特定委員若判定資料可以運用，其決定應立即送交委員會確認。第 2 句中止之限制措施在不違反第 1 句的情形下，得繼續實施。透過第 1 條第 1 項第 1 款規定之限制措施取得私人生活方式核心領域的資訊，不得使用。記錄應立即銷毀。資料登錄與銷毀之事實應做成紀錄。所做成之紀錄僅於資料保護監督目的使用。如對監督目的已無必要，則該紀錄應銷毀之，至遲應於做成紀錄之次年度結束前完成。

第三條 b（合法拒絕證言證人之保護）

（1） 第 1 條第 1 款第 1 項之限制措施係針對刑事訴訟法第 53 條第 1 項第 1 句第 1 款、第 2 款及第 4 款內所明定得拒絕證言之證人，而此等限制措施可預見將獲取可拒絕證言之證人有關資訊時，不得為之。已取得之資訊亦不得使用。相關紀錄應立即銷毀。資訊取得與銷毀之事實應做成記錄。第 2 句及第 3 句之規定，於限制措施非針對刑事訴訟法第 53 條第 1 句第 1 款、第 2 款及第 4 款所明定之證人，且該證人得拒絕證言時，適用之。

（2） 若限制措施可能影響到刑事訴訟法第 53 條第 1 項第 1 句第 3 款至第三 3 款 b 或第 5 款所列之個人，可預期獲得得拒絕證言之人的相關資訊，此時應特別注意比例原則之審查，權衡職務執行之公益和信任或知悉他人事實應保密義務之公益之價值。據此，限制措施或應停止實施，或可能按照採取措施的性質加以設限。

（3） 第 1 項及第 2 項之規定，對刑事訴訟法第 53a 條得拒絕證言之人，適用之。

（4） 有事實足認合法拒絕證言之人係本法第 3 條第 2 項第 2 句之犯罪嫌疑人，或有事實根據足認合法拒絕證言之人以受領或傳遞方式幫助第 3 條第 1 款所列犯罪之企圖時，不適用前 3 項之規定。

第四條（審查、賦予標識及銷燬義務、傳遞、目的拘束）

（1） 情報機關應立即以及其後的六個月內，就所蒐集之個人資料，在自身職務範圍內，對個別或既存已知的資料，隨時審查其是否符合第 1 條第 1 項第 1 款規範目的之必要性。該資料對其目的已無必要，而且也無必要傳遞其他機關時，應立即在具有法官資格之公務員的監督下予以銷燬。銷燬必須作成紀錄。該紀錄僅得在資料保護目的內運用。該紀錄必須於年底銷毀。資料如係為履行第 12 條第 1 項告知義務，或對於限制措施適法性的

司法審查具有重要性時，不得銷燬。於此情形，該資料不得再予運用，僅得在前揭目的範圍內予以利用。

（2） 剩餘之資料必須予以標識。如資料傳遞其他機關，該標識仍應維持。該資料只有符合第1條第1項第1款，以及第4項所規範的目的，方得利用。

（3） 機關首長或其代理人，為了不危害限制措施保密性認有必要，並經G-10委員會同意時；或由各邦機關之傳遞而依各邦法律規定可經權責機關同意時，於傳遞時得命不予標識。如有延遲之虞，命令可在獲得同意前先行下達，但事後未獲同意時，受領機關應立即補行標識，而傳遞機關必須告知受領機關。

（4） 資料僅得因下列要件，且確係受領機關為履行職務確之必要時，方得傳遞。

1. 有下列情形為防止或調查犯罪

(a)有事實根據足認某人涉嫌計劃或實行第3條第1項及第1項a所列舉犯罪之嫌疑。

(b)有特定事實根據足認某人涉嫌計劃或實行第7條第4項第1句所列舉犯罪之嫌疑。

2. 有特定事實根據足認某人涉嫌實行或完成前款犯罪，而為追訴其犯行。

3. 為準備及實施基本法第21條第2項第2句之程序，或社團法第3條第1項第1句的措施。

（5）得傳遞之資料結合了當事人與第三人資料，無法將其分離或分離必須花費鉅額費用時，得一併傳遞，但不得利用。此項傳遞，由傳遞機關內具有法官資格的公務員決定之。傳遞應做成紀錄。

（6）受領機關僅得就該資料傳遞目的係為履行其職務範圍內加以利用。受領機關對該傳遞之資料，應立即以及其後的六個月內，審查其受領必要性。第1項第2句及第3句適用之。受領機關銷燬資料時，應立即通知傳遞機關。

第三節　戰略性限制

第五條（前提要件）

（1）依聯邦情報局之申請，為蒐集通訊資料，得命為第1條國際通訊關係之限制措施。此通訊關係之限制措施，第10條第1項之聯邦部會在下命為限制措施前，要得到議會監督委員會的同意。第一句之限制措施，只有係為及時察覺下列犯罪的危險，而且為防止此類危險而有蒐集相關情報之必要時，方得為之。

1. 對德意志聯邦共和國的武力攻擊。
2. 與德意志聯邦共和國直接有關的國際恐怖攻擊。
3. 軍事武器管制法所指之國際武器擴散，以及重要的商品、資訊處理程式及高科技之非法對外交易。
4. 於歐盟為毒品不法、常業、組合性或組織性的販運，影響德意志聯邦共和國利益重大。
5. 在國外偽造貨幣，而損害歐元流通區的貨幣安定性。
6. 重大國際組織性洗錢活動。
7. 外國人對歐盟地區所為常業、組織性走私，影響德意志聯邦共和國利益重大

（a）與第1款至第3款危害領域具有直接關聯

（b）涉及大量的走私者，尤其走私方式導致生命身體重大危害

（c）外國機關直接或間接支持或容忍

（2）聯邦情報局為確定電信通訊關係之限制措施內所揭示的危險範圍事實之存否，得使用關鍵字詞組（Suchbegriffe）進行搜尋。所使用之關鍵性概念詞組，不得包含

1. 可以導出個人身分特徵之通聯線路。
2. 私人生活核心領域。

如果可以排除國外的通聯線路所有者或經常使用者為德國人時，關鍵字詞組可以包含前述內容。此項實施應做成紀錄。紀錄資料僅得於資料保護監督目的時方得利用。作成之紀錄，應於年度結束時予以銷燬。

第五條a（私人生活方式核心領域之保護）

依第1條第1項第2款限制措施蒐集資訊，不得包含私人生活方式核心領域之通訊內容。若該通

訊內容已包含私人生活方式核心領域，該資訊不得加以運用。該通訊內容應立即在具有法官資格之公務員的監督下銷毀。第 3 條 a 第二句至第七句之規定，適用之。資料登錄與銷毀之事實應做成紀錄。所做成之紀錄僅於資料保護監督目的使用。如對監督目的已無必要，則該紀錄應銷毀之，至遲應於做成紀錄之次年度結束前完成。

第六條（審查、賦予標識及銷燬義務、傳遞、目的拘束）

（1） 聯邦情報局就所蒐集之個人資料，應立即以及其後的六個月內，在自身職務範圍內，對個別或既存已知的資料，隨時審查其是否符合第 5 條第 1 項第 3 款規範目的之必要性。該資料對其目的已無必要，而且也無傳遞其他機關之必要時，應立即在具有法官資格之公務員的監督下予以銷燬。銷燬必須作成紀錄。除了第 1 句的初次審查外，該資料如係為履行第 12 條第 2 項告知義務，或對於限制措施適法性的司法審查具有重要性時，不得銷燬。於此情形，該資料不得再予運用，僅得在前揭目的範圍內予以利用。

（2） 剩餘之資料必須予以標識。如資料傳遞其他機關，該標識仍應維持。該資料只有符合第 5 條第 1 項第 3 句，以及第 7 條第 1 項至第 4 項所規範的目的，方得利用。

（3） 有事實足認與第 10 條第 1 項權責機關所下命之限制措施危害領域有關聯，得依聯邦情報局之申請，將經由自動化程序所獲得之電話號碼或其他特定特徵資料進行比對。比對之電話號碼或其他特定特徵資料，聯邦情報局得於國內運用。此資料不得用於第 5 條第 2 項第 1 句之關鍵字詞組。比對以及運用比對後之資料，應做成紀錄。紀錄資料僅得於資料保護監督目的時方得利用。作成之紀錄，應於年度結束時予以銷燬。

第七條（聯邦情報局的傳遞）

（1） 第 5 條限制措施所蒐集之個人相關資料，僅能依聯邦情報局法第 12 條之規定，就本法第 5 條第 1 項第 3 句所列舉危險事項進行報告時，方得傳遞。

（2） 第 5 條限制措施所蒐集之個人相關資料，有下列情形之一者，得傳遞給聯邦或各邦憲法保護局，或軍事反情報局。

1. 有事實根據足認有於德意志聯邦共和國境內使用暴力或預備使用暴力之行為，而侵害聯邦憲法保護法第 3 條第 1 項第 1、3、4 款保護之法益，而該資料對憲法保護局之情報蒐集或分析確有必要。
2. 有特定事實根據足認有安全危害或為外國勢力從事間諜行為之嫌疑。

（3） 第 5 條第 1 項第 1 句、第 3 句第 3 款之限制措施所蒐集之個人相關資料，於下述情形有事實足認該資料的內容對於事實認知是必要時，得傳遞給聯邦經濟及出口管制局（BAFA）。

1. 為調查從事國際貿易者是否確實履行國際貿易限制之情況。
2. 依法被賦予許可商品出口的義務，在程序範圍內給予商品出口法律的許可，或報告從事國際貿易之情形。

（4）第 5 條限制措施所蒐集之個人相關資料，有下列情形之一者，為防止犯罪，得傳遞給有警察權之機關。

1. 有事實根據足認某人涉嫌計劃或實行下列犯罪之嫌疑。
   （a）刑法第 89 條 a 或第 129 條 a、第 129 條 b 第 1 項、以及 146 條、151 至 152 條 a，或 261 條之罪。
   （b）外貿法第 34 條第 1 項至第 6 項及第 8 項、第 35 條，以及軍事武器管制法第 19 條至 21 條、或第 22 條 a 第 1 項第 4、5、7 款之武器監督。
   （c）麻醉藥品法第 29 條 a 第 1 項第 2 款、第 30 條第 1 項第 1 款及第 4 款，或第 30 條 a 之罪。
2. 有特定事實根據足認某人涉嫌計劃或實行下列犯罪之嫌疑。
   （a）第 3 條第 1 項第 1 句第 1 款至第 5 款、第 7 款、第 1 項第 2 句或 1a，以及第 2 句，或刑法第 129 條 a 第 1 項所列之罪。
   （b）刑法第 130 條、第 232 條第 3 項、4 項或第 5 項前半、第 249 條至 251 條、第 255 條、第 305 條 a、第 306 至 306c、第 307 第 1 項至第 3 項、第 308 第 1 項至第 4 項、第 309 第 1 項至第 5 項、第 313 條、第 314 條、第 315 條第 1、3、4 項、第 315 條 b 第 3 項，或第 316 條 a、第 316 條 b 第 1、3 項、第 316 條 c 第 1 至 3 項之罪。
   （c）居留法第 96 條第 2 項、第 4 項以及第 97 條第 1 項至第 3 項。

有特定事實根據足認某人實行或完成第一句所列犯罪之嫌疑，為追訴其犯罪，可以將資料傳遞給管轄機關。

（5）傳遞只有在受領機關為履行其職務所必須者，方得為之。得傳遞之資料結合了當事人與第三人資料，無法將其分離或分離必須花費鉅額費用時，得一併傳遞，但不得利用。此項傳遞，由聯邦情報局內具有法官資格的公務員決定之。傳遞應做成紀錄。

（6）受領機關僅得就該資料傳遞目的係為履行其職務範圍內加以利用。受領機關對該傳遞之資料，應立即以及其後的六個月內，審查其受領必要性。第 4 條第 6 項第 4 句，及第 6 條第 1 項第 2 句及第 3 句之規定，適用之。

第七條 a（聯邦情報局對外國政府機關之傳遞）

（1）有下列情形之一者，聯邦情報局得將依第五條第一項第三句第二款、第三款及第七款限制措施所蒐集之個人資料傳遞給負責情報業務之外國政府機關：

1. 對維護德意志聯邦共和國外交或安全政策利益，或對外國政府之安全有顯著影響所必須

2. 不損及當事人值得保護之利益，特別是外國政府資料保護水準之完善能獲得保證，並據以推斷接受該個人資料者在運用此資料時能符合法治國家原則。

3. 維持平等互惠原則

此項傳遞行為需聯邦總理府之同意。

（2）如果根據德意志聯邦共和國與北大西洋公約組織與各會員國於 1959 年 8 月 3 日(聯邦法律公報，1961 Ⅱ 頁 1183、1218)針對外國軍隊駐紮在德意志聯邦共和國軍隊所簽訂的協定之附加條款第三款的範圍，聯邦情報局在符合第一項的前提條件下，且該個人資料對外國駐軍完成其任務有必要性時，得將依第五條第一項第三句第二款、第三款及第七款將限制措施所蒐集之個人資料傳遞與外國駐軍。

（3）資料傳遞需由聯邦情報局內具有法官資格之公務員決定。資料傳遞需做成紀錄。聯邦情報局應針對資料傳遞之目的、原因、來源及第一項、第二項明定之受領機關提供證明。所提供之各項證明應另外儲存，並防止未經授權之查閱；證明至遲應在提出的次年度結束前銷毀。

（4）資料受領機關負有下列義務：

1. 傳遞之資料僅能於傳遞目的範圍內使用，

2. 需保持適當標識，

3. 回覆聯邦情報局對資料運用之查詢。

（5）主管之聯邦部會每月需將第一項及第二項所列之資料傳遞情形告知 G10 委員會。

（6）第一項及第二項之傳遞，最遲應於傳遞後六個月內告知國會監督委員會。

第八條（在外國之人的生命身體之危險）

（1） 於個案情形，為適時察知或防止在國外之個人身體或生命危險之必要，而且此項危險會以特別方式直接涉及德意志聯邦共和國利益時，得依聯邦情報局之申請，命為第 5 條第 1 項第 1 句所謂的第 1 條國際通訊關係之限制措施。第 5 條第 1 項第 2 句之規定，準用之。

（2） 國會監督委員會之決議，必須經全體委員三分之二之多數同意。決議至遲於兩個月後失效。如決議的前提仍持續存在，得再為決議。

（3） 限制命令限於不能或極難以其他方法調查事實，始得為之。聯邦情報局為蒐集命令內所列舉之危險情報，得運用關鍵性概念詞組進行特定及適當之搜尋。第 5 條第 2 項第 2 句至第 6 句之規定，準用之。

（4） 聯邦情報局就所蒐集之個人資料，應立即以及其後的六個月內，在自身職務範圍內，對個別或既存已知的資料，隨時審查其是否符合第 1 項規範目的之必要性。該資料對其目的已無必要，而且也無傳遞其他機關之必要時，應立即在具有法官資格之公務員的監督下予以銷燬。銷燬必須作成紀錄。第 6 條第 1 項第 4 句及第 5 句，以及第 2 項第 1 句第 2 句之規定，準用之。該資料只有符合第 1 項、第 5 項及第 6 項所規範的目的，方得利用。

（5） 蒐集之個人相關資料，僅能依聯邦情報局法第 12 條之規定，就本條第 1 項所列舉危險事項進行報告時，方得傳遞。

（6） 蒐集之個人相關資料，如有事實根據足認某人涉嫌計劃或實行第 1 項危險之發生或維持之罪的嫌移，為防止犯罪，得傳遞給管轄機關。有特定事實根據足認某人實行或完成第一句所列犯罪之嫌疑，為追訴其犯罪，可以將資料傳遞給管轄機關。第 7 條第 5 項及第

6 項及第 7 條 a 第 1 項、第 3 項至第 6 項之規定，適用之。

第四節　程序

第九條（申請）

（1）本法的限制措施命令僅得透過申請下命。

（2）下列機關在自身業務範圍內，其機關首長或其代理人有申請限制措施之權限。

1. 聯邦憲法保護局。
2. 各邦憲法保護局。
3. 軍事反情報局。
4. 聯邦情報局。

（3）申請應以書面為之，而且必須附記理由。申請必須包含命令內所必要的事項。第 3 條及第 8 條之情形，申請者必須說明不能或極難以其他方法調查事實之理由。

第十條（命令）

（1）　有權下達限制措施命令者，如係各邦憲法保護局申請者，由各邦最高行政機關管轄；其他情形，由聯邦總理委任之機關管轄。

（2）　命令之下達應以書面為之。命令內必須明示命令的根據及有權執行通訊監察機關，以及明定限制措施的類別、範圍其期間。

（3）　第 3 條之情形，命令必須明示限制的對象。如係對電信之通訊監察，應明示電話號碼或通訊聯繫的標識。

（4）　第 5 條及第 8 條之情形，應將關鍵性概念詞組明定於命令內。此外必須載明情報蒐集範圍及傳送路徑。另外應予明定依此傳送路徑可運用的傳送容量得受到多少程度的監察。第 5 條之情形，最高可達百分之二十。

（5）　第 3 條及第 5 條之情形，命令之期限最長不得超過三個月。如命令之前提要件仍持續存在，得申請延長，每次延長期限亦不得超過三個月。

（6）　如為履行其義務而有必要時，命令必須通知第 2 條第 1 項第 1 句或第 3 句之義務人。如無須其協助亦可達成任務時，毋庸通知。

（7）　聯邦憲法保護局如在各邦管轄範圍內進行限制措施時，應將限制措施命令通知各邦憲法保護局。各邦憲法保護局在各邦管轄範圍內進行限制措施時，應將限制措施命令通知聯邦憲法保護局。

第十一條（實施）

（1）　因命令所產生之限制措施，由申請機關負責，並在具法官資格之公務員的監督下執行。

（2）　措施已無執行必要，或命令之前提要件已不存在時，應立即停止執行。停止執行時，應通知下達命令機關，以及第 2 條第 1 項第 1 句及第 3 句之義務人。如限制措施命令不用義務人之協助時，則停止執行時毋庸通知。

（3）開啟或閱覽傳遞中的郵件後，應立即將該郵件重新傳遞。電報不得擷取。有權閱覽之機關應交付電報影本。

第十二條（對當事人的通知）

（1）　依第 3 條所為之限制措施，在限制措施終止後，應通知當事人。如限制措施目的之危害尚未結束，或是通知將可預期對聯邦或各邦福祉造成不利益時，得不予通知。若在通訊監察結束後的 12 個月內仍不通知受監察人，得在 G-10 委員會的同意下延長不通知的期限，期限長短應由 G-10 委員會一併審查。有下列情形之一，經 G10 委員會一致同意者，得不通知當事人。

1. 第 2 句之要件在停止執行後五年內仍存在。
2. 限制措施要件在未來仍很有可能存在。
3. 執行機關或受領機關依法有銷燬的義務。

（2）　個人相關資料如未立即銷燬，第 1 項之規定於第 5 條及第 8 條限制措施，適用之。五年期限，從個人相關資料的蒐集時起算。

（3）　通知義務人，為限制措施命令之申請機關。個人相關資料被傳遞時，其通知應經受領機關同意。

第十三條（救濟途徑）

第 3 條及第 5 條第 1 項第 3 句第 1 款的限制措施命令，以及對於該當命令之執行，在通知當事人之前，不提供其救濟途徑。

第五節　監督

第十四條（聯邦議會監督委員會）

（1）　第 10 條第 1 項下達限制措施命令之權責機關，應每隔最長六個月期限內，向聯邦議會監督委員會報告本法的執行情形。該委員會每年應就本法第 3 條、第 5 條及第 8 條之限制措施種類、範圍及執行情形，向聯邦議會進行報告，此時必須兼顧國會對聯邦情報工作監督法（Kontrollgremiumgesetz）第 10 條第 1 項之原則。

（2）　議會監督委員會對第 5 條及第 8 條之限制措施之同意決議如有延遲之虞，主席或其代理人得暫時同意，並應立即尋求委員會同意。暫時同意至遲應於兩週後失效。

第十五條（G10 委員會）

（1）　G10 委員會由四名正委員以及四名具有發言權與質詢權，得參會議的副委員所組成，主席須具有法官資格。表決可否同票數時，由主席決定之。G10 委員會的委員獨立行使職務，不服從任何指示。委員是榮譽職，經聯邦政府實施聽證後，由聯邦議會監督委員會任命之。其任期從監督委員會決議新任成員起算，至遲應於聯邦議會任期結束後三個月內終止。

（2）　G10 委員會採秘密方式進行審議。委員會成員因工作所獲悉的各項事件負有保密義務。退離職後，亦同。

（3）　G10 委員會為履行其職務，得自由使用必要的人力及設備，而此類設備必須明定於聯邦議會的個別計劃內。委員會亦得自由運用具有專業技術知識的輔助人員。

（4）　G10 委員會至少每個月開會一次。委員會得制定議事規則，但必須經聯邦議會監督委員會同意。在同意前，應聽取聯邦政府的意見。

（5）　G10 委員會依職權或申請，決定限制措施的容許性及必要性。委員會的監督權限，包含決定是否告知限制措施的當事人，以及聯邦情報機關所蒐集個人相關資料之處理與運用的全般程序。委員會及輔助人員特別享有以下的權利

1. 要求相關機關對委員會之質詢給予答覆。
2. 得閱覽全般資料，特別是與限制措施有關的資料及資料處理程式。
3. 得隨時進入執行處所。

有關資料保護的問題，委員會得給予聯邦資料保護監察人陳述意見的機會。

（6）　聯邦權責機關每個月應就自己所下命之限制措施，在執行前向 G10 委員會報告。有延遲之虞時，聯邦權責機關在向委員會報告前，亦得先命執行限制措施。如委員會不同意或認無必要時，聯邦權責機關應立即停止執行。第 8 條之情形，命令未於三日內獲委員會同意時，該命令自動失效。委員會無法於期限內做出決定時，主席或其代理人得暫時同意，並應立即尋求委員會追認同意。

（7）　聯邦權責機關每個月應就第 12 條第 1 項及第 2 項聯邦機關的通知情形，或是不予通知的理由向 G10 委員會報告。G10 委員會認有告知必要時，權責機關應立即報告。邦機關同意是必要時，第 12 條第 3 項第 2 句不受影響。

第十六條（邦議會的監督）

各邦議會對第 10 條第 1 項有權命為限制措施之各邦最高行政機關的監督，以及對最高行政機關限制措施的審查，由各邦立法機關定之。只有經各邦立法機關就個人相關資料之處理及利用訂定監督機制者，方得將資料傳遞給各邦的其他行政機關。

第六節　罰責及罰鍰規定

第十七條（通知的禁止）

（1）　依本法或刑事訴訟法第 100 條 a 或第 100 條 b，對電信通訊實施通訊監察時，電信業者或其協助人員不得將此情形通知他人。

（2）　第 2 條第 1 項第 1 句或第 3 句命交付郵遞物之情形，郵政業者或其協助人員不得將此情形通知他人。

（3）　依第 2 條第 1 項所為之資訊請求或資訊提供，負有答覆義務或受委任而有答覆義務者，不得將此情形、請求內容或提供資訊通知他人。

第十八條（違法行為）
違反第 17 條之規定而為通知者，處二年以下有期徒刑併科罰金。

第十九條（行政罰法）
（1）下列行為為違反行政法上義務
1. 違反第 2 條第 1 項第 1 句或第 3 句之執行命令。
2. 違反第 2 條第 2 項第 2 句之程序而予以委任。
3. 未依第 2 條第 2 項第 3 句之規定採取保密措施。
（2）違反行政法上義務，得處以一萬五千歐元以下之罰鍰。
（3）本法第 10 條第 1 項之權責機關，為行政罰法第 36 條第 1 項第 1 款之裁罰機關。

第七節　最後規定
第二十條（補償）
第 1 條第 1 項權責機關，對第 2 條第 1 項義務機關之履行，在證人及鑑定人補償法第 23 條範圍內，應予補償。第 5 條及第 8 條之補償額度，以義務機關所證明之事實上支出為準。

第二十一條（基本權的限制）
書信、郵件及電訊秘密的基本權（基本法第 10 條法），將因本法受到限制。

附錄六：我國通訊保障及監察法

通訊保障及監察法

【制定修正】民國 96 年 6 月 15 日

【公布日期】民國 96 年 7 月 11 日

【法規沿革】

1.中華民國八十八年七月十四日總統（88）華總一義字第 8800159870 號令制訂全文 34 條；並自公布日起施行

2.中華民國九十五年五月三十日總統華總一義字第 09500075751 號令修正公布第5、34條條文；並自九十五年七月一日施行

3.中華民國九十六年七月十一日總統華總一義字第 09600088081 號令修正公布第5～7、11、12、14～17、32、34條條文；並自公布後五個月施行

【法規內容】

第一條（立法目的）

為保障人民秘密通訊自由不受非法侵害，並確保國家安全，維持社會秩序，特制定本法。

第二條（通訊監察之限度）

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。

第三條（通訊之定義）

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。

第四條（受監察人之定義）

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。

第五條（發通訊監察書之情形）

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之指示。

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。

第六條（口頭執行通訊監察）

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

第七條（收集情報通訊監察之目的及對象）

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户籍者，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。

第八條（外國勢力及境外敵對勢力之定義）

前條第一項所稱外國勢力或境外敵對勢力如下：

一、外國政府、外國或境外政治實體或其所屬機關或代表機構。

二、由外國政府、外國或境外政治實體指揮或控制之組織。

三、以從事國際或跨境恐怖活動為宗旨之組織。

第九條（外國勢力或境外敵對勢力工作人員之定義）

第七條第一項所稱外國勢力或境外敵對勢力工作人員如下：

一、為外國勢力或境外敵對勢力從事秘密情報蒐集活動或其他秘密情報活動，而有危害國家安全之虞，或教唆或幫助他人為之者。

二、為外國勢力或境外敵對勢力從事破壞行為或國際或跨境恐怖活動，或教唆或幫助他人為之者。

三、擔任外國勢力或境外敵對勢力之官員或受僱人或國際恐怖組織之成員者。

第十條（所得資料之運用及處置）

依第七條規定執行通訊監察所得資料，僅作為國家安全預警情報之用。但發現有第五條所定情事者，應將所得資料移送司法警察機關、司法機關或軍事審判機關依法處理。

第十一條（通訊監察書應載事項）

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。

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。

第十二條（監察通訊之期間及延長）

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。

第十三條（監察通訊之方法）

監察通訊以截收、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。

第十四條（執行機關及電信郵政機關之協助義務）【相關罰則】第二項~§31

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。

第十五條（結束時之通知義務）

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

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

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

關於執行機關陳報事項經法院審查後，交由司法事務官通知受監察人。

第十六條（執行機關之報告義務）

執行機關於監察通訊後，應按月向檢察官、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報告執行情形。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並得隨時命執行機關提出報告。

第五條、第六條通訊監察之監督，偵查中由檢察機關、審判中由法院，第七條通訊監察之監督，由綜理國家情報工作機關，派員至建置機關，或使用電子監督設備，監督通訊監察執行情形。偵查中案件，法院得隨時派員監督執行機關執行情形。

第十七條（監察所得資料之留存及銷燬）

監察通訊所得資料，應加封緘或其他標識，由執行機關蓋印，保存完整眞實，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，執行機關應記錄該通訊監察事實，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。

第十八條（監察所得資料之保守秘密）

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

第十九條（洩漏監察所得資料之賠償）

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

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

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

第二十條（賠償金額之計算）

前條之損害賠償總額，按其監察通訊日數，以每一受監察人每日新臺幣一千元以上五千元以下計算。但能證明其所受之損害額高於該金額者，不在此限。

前項監察通訊日數不明者，以三十日計算。

第二十一條（損害賠償請求權之消滅時效）

損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者亦同。

第二十二條（執行職務洩漏資料之賠償）

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

依前項規定請求國家賠償者，適用第十九條第二項、第三項及第二十條之規定。

第二十三條（補充法）

損害賠償除依本法規定外，適用民法及國家賠償法規定。

第二十四條（罰則 1）【相關規定】第一項須告訴乃論~§30

違法監察他人通訊者，處五年以下有期徒刑。

執行或協助執行通訊監察之公務員或從業人員，假借職務或業務上之權力、機會或方法，犯前項之罪者，處六月以上五年以下有期徒刑。

意圖營利而犯前二項之罪者，處一年以上七年以下有期徒刑。

第二十五條（罰則 2）【相關規定】第一項須告訴乃論~§30

明知為違法監察通訊所得之資料，而無故洩漏或交付之者，處三年以下有期徒刑。

意圖營利而犯前項之罪者，處六月以上五年以下有期徒刑。

第二十六條（沒收）

前二條違法監察通訊所得之資料，不問屬於犯人與否，均沒收之。

犯人不明時，得單獨宣告沒收。

第二十七條（公務員洩漏資料之刑罰）

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

第二十八條（非公務員洩漏資料之處罰）【相關規定】須告訴乃論~§30

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

第二十九條（不罰之情形）

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。

【參考裁判】89,簡上,284

第三十條（告訴乃論）

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。

第三十一條（罰則）

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，由交通部處以新臺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。

第三十二條（軍事審判之準用）

軍事審判機關於偵查、審判現役軍人犯罪時，其通訊監察準用本法之規定。

前項通訊監察書於偵查現役軍人犯罪時，由軍事檢察官向該管軍事審判官聲請核發。軍事審判官並得於通訊監察書上，對執行人員為適當之指示。

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，以及有無繼續監聽之需要。軍事審判官依經驗法則、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，應撤銷原通訊監察書。

違反前三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。

第三十三條（施行細則）

本法施行細則，由行政院會同司法院定之。

第三十四條（施行日）

本法自公布日施行。

本法修正條文自公布後五個月施行。

附錄七：我國通訊保障及監察法施行細則

通訊保障及監察法施行細則
【公布日期】96.12.11 【公布機關】行政院&司法院

【法規沿革】
1.中華民國八十九年三月十五日行政院令、司法院(89)院台廳刑一字第 04471 號令會同訂定發布全文 30 條；並自發布日起施行
2.中華民國九十一年六月二十七日行政院院臺法字第 0910033057 號令、司法院(九一)院台廳刑一字第 14149 號令修正發布第 25 條條文>>原條文
3.中華民國九十六年十二月十一日行政院院臺法字第 0960056006 號令、司法院院台廳刑一字第 0960025721 號令會銜修正發布全文 36 條；並自九十六年十二月十一日施行

【法規內容】

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 4 條
檢察官依本法第五條或第六條規定聲請核發通訊監察書者，應備聲請書，載明本法第十一條第一項所列事項，並敘明理由、檢附相關文件及有關釋明資料，向該管法院為之。

司法警察機關依本法第五條規定向檢察官提出聲請者，應備文載明本法第十一條第一項所列事項，並敘明理由、檢附相關文件及有關釋明資料，向有管轄權之檢察機關為之。

司法警察機關依本法第六條規定報請檢察官以口頭通知先予執行通訊監察者，應於十六小時內備妥前項文件陳報該管檢察官。

第 5 條
法院就核發通訊監察書之聲請，其准予核發者，應即製作通訊監察書交付聲請人；不予核發者，應以書面復知聲請人。

第 6 條
執行機關執行通訊監察時，如發現有危害國家安全情事者，應將相關資料移送綜理國家情報工作機關。

第 7 條
法官依本法第五條第四項規定撤銷原核發之通訊監察書者，應以書面通知檢察官。

前項情形，檢察官應立即通知執行機關，執行機關應立即停止監聽，填寫停止執行通知單送建置機關或協助執行之電信事業及其他協助執行機關，並陳報檢察官及法院。

第 8 條

檢察官依本法第六條第一項規定以口頭通知執行機關先予執行通訊監察者，執行機關應製作紀錄，載明通知之時間、方式、內容及檢察官之姓名，留存以備查考。

前項情形，檢察官應於通知執行機關之時起二十四小時內，以書面記載本法第十一條第一項之事項，敘明具體理由、檢附相關文件，並載明通知先予執行之時間，聲請該管法院補發通訊監察書，並副知執行機關。

執行機關依第一項規定先予執行通訊監察者，如經法院核復不予補發，或自檢察官向法院聲請之時起四十八小時未獲法院補發通訊監察書者，執行機關應立即停止監察，並陳報檢察官及法院。

前項情形，執行機關應即通知建置機關或協助執行之電信事業或郵政事業及其他協助執行機關停止監察。

第 9 條

本法第七條所稱綜理國家情報工作機關，指國家安全局。

第 10 條

依本法第十條但書規定將通訊監察所得資料移送司法警察機關、司法機關或軍事審判機關者，應移送有管轄權之機關，管轄權不明者，移送其直接上級機關依法處理。

第 11 條

依本法第五條或第六條規定聲請通訊監察者，其聲請書所載明本法第十一條第一項第五款之監察理由，應包括下列事項：

一、受監察人涉嫌本法第五條第一項或第六條第一項犯罪之具體事實。

二、受監察之通訊與上述犯罪具有關連性之具體事證。

三、就上述犯罪曾經嘗試其他蒐證方法而無效果之具體事實，或不能或難以其他方法蒐集或調查證據之具體理由。

第 12 條

綜理國家情報工作機關依本法第七條第二項及第三項規定，通知高等法院專責法官同意通訊監察者，應備聲請書並記載下列事項：

一、案由。

二、監察對象及其境內戶籍資料。

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、監察理由及其必要性。

六、監察期間。

七、監察方法。

八、執行機關。

九、建置機關。

第 13 條

本法第七條第三項之停止監察，執行機關應立即填寫停止執行通知單送建置機關或協助執行之電信事業或郵政事業及其他協助執行機關，並陳報綜理國家情報工作機關首長及高等法院專責法官。

第 14 條

本法第十二條第一項通訊監察期間之起算，依通訊監察書之記載；未記載者，自通訊監察書核發日起算。但依本法第六條第一項先予執行通訊監察者，自通知先予執

行之日起算；依本法第七條第二項但書先予核發通訊監察書者，自核發之日起算。

第 15 條

本法第十二條第二項、第三項之停止監察，執行機關應立即填寫停止執行通知單送建置機關或協助執行之電信事業或郵政事業及其他協助執行機關，並陳報檢察官、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。

第 16 條

建置機關所屬人員不得接觸通訊內容，亦不得在現譯區域直接截收、聽取或以其他方法蒐集通訊內容。

第 17 條

執行電信監察之執行處所，應置監察機房工作日誌，由工作人員按日登載，並陳報機房所屬單位主管核閱。

前項執行處所，應訂定有關監察機房進出人員之資格限制、進出之理由及時間等規定，送上級機關備查。

第 18 條

執行機關於執行通訊監察時，發現有應予扣押之物，或有迅速處理之必要者，應即報告檢察官、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。

第 19 條

執行機關執行通訊監察，應依通訊監察書所載內容，以通訊監察書及協助執行通知單通知建置機關或協助執行之電信事業或郵政事業及其他協助執行機關協助執行。但依本法第六條第一項規定先予執行通訊監察者，得僅以協助執行通知單通知之。

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 22 條

為監督執行機關執行情形，司法院於必要時，得提出需求，由電信事業設置能立即自動傳輸行動電信通訊監察上線及下線資訊之設備，即時將有關第二十條第二項前段全部行動通訊監察上線及下線資訊，以專線或其他保密方式，傳輸至台灣高等法院通訊監察管理系統。

行動以外電信有關前項通訊監察上線及下線資訊，電信事業應即時以專線或其他保密方式，傳輸至台灣高等法院通訊監察管理系統。

第 23 條

執行機關依第二十一條第一項但書規定派員至電信機房附設之監錄場所執行通訊監察時，應備函將該執行人員之姓名及職級通知該電信事業。

前項執行人員應遵守電信事業之門禁管制及機房管理相關規定；如有違反，電信事業得拒絕其進入機房附設之監錄場所，並得通知其所屬機關。

因可歸責於第一項執行人員之事由致電信事業之機房設備損壞者，執行機關應負賠償責任。

第 24 條

電信事業及郵政事業依本法第十四條第二項規定協助執行通訊監察時，以不影響其正常運作及通訊暢通為原則，且不得直接參與執行本法第十三條第一項所定之監察方法。

執行機關因特殊案件需要，得請求建置機關要求電信事業指派技術人員協助執行，並提供通訊系統及通訊網路等相關資料。電信事業如有正當理由無法提供協助，應以書面告知執行機關。

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。

第 25 條

執行機關透過郵政事業之協助執行通訊監察時，執行人員應持通訊監察書及協助執行通知單，會同該郵政事業指定之工作人員，檢出受監察人之郵件，並由郵政人員將該郵件之種類、號碼、寄件人及收件人之姓名、地址、原寄局名及交寄日期等資料，登入一式三份之清單，一份交執行人員簽收，二份由郵政事業留存。

受監察人之郵件應依通訊監察書所記載內容處理，其時間以當班或二小時內放行為原則。放行之郵件應恢復原狀並保持完整，由郵政人員在留存之二份清單上簽名，並註明回收字樣，其中一份清單交執行人員收執，一份併協助執行通知單及通訊監察書由郵政事業存檔。

第 26 條

本法第十四條第二項所稱協助執行通訊監察之義務，指電信事業及郵政事業應使其通訊系統之軟硬體設備具有配合執行通訊監察時所需之功能，並於執行機關執行通訊監察時予以協助，必要時並應提供場地、電力及相關介接設備及本施行細則所定之其他配合事項。

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。

第 27 條

執行機關應於通訊監察結束後，依本法第十五條第一項規定，於七日內以書面載明下列事項，報由檢察官、綜理國家情報工作機關於收文後五日內陳報法院審查：

一、通訊監察書核發機關及文號。

二、案由。

三、監察對象。

四、監察通訊種類及號碼等足資識別之特徵。

五、受監察處所。

六、監察期間及方法。

七、聲請機關。

八、執行機關。

九、建置機關。

十、監察通訊所得內容及有無獲得監察目的之相關資料。

十一、其他相關事項及附件。

前項所稱通訊監察結束，包括本法第五條第四項之撤銷原核發之通訊監察書、本法第十二條第一項通訊監察期間屆滿、本法第六條第二項、第七條第三項、第十二條第二項及第十二條第三項其受監察人在境內設有戶籍之停止監察之情形。

法院審查後通知受監察人時，應以書面載明下列事項：

一、通訊監察書核發機關及文號。

二、案由。

三、監察對象。

四、監察通訊種類及號碼等足資識別之特徵。

五、受監察處所。

六、監察期間及方法。

七、聲請機關。

八、執行機關。

九、有無獲得監察目的之通訊資料。

執行機關認通知有妨害監察目的之虞或不能通知之情形，依本法第十五條第一項陳報之案件，經法院據以不通知受監察人者，執行機關應每二月檢討通知有妨害監察目的之虞或不能通知之情形是否消滅，報由檢察官、綜理國家情報工作機關陳報法院審查。但本法第七條第二項及第三項之通訊監察，受監察人實際上無從通知或其不通知原因短期內無法消滅者，得經法院同意，不為定期檢討或延長其檢討期限。

第 28 條

法院審查執行機關依本法第十五條第一項之陳報，如認通知無妨害監察目的之虞或無不能通知之情形，得逕通知受監察人，並副知執行機關、檢察官或綜理國家情報工作機關首長。

第 29 條

執行機關依本法第十六條第一項規定按月向檢察官、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報告通訊監察執行情形，應於次月七日前以書面載明第二十七條第一項各款事項報告之。

第 30 條

執行機關依本法第七條之通訊監察書為通訊監察者，應於通訊監察結束或停止後七日內，以書面向綜理國家情報工作機關首長提出報告。綜理國家情報工作機關首長命執行機關報告者，執行機關應即報告。

前項書面，應載明第二十七條第一項各款事項。

第 31 條

法院、檢察機關為使用電子監督設備執行監督，得建置相應之通訊監察線上查核系統。

依本法第七條所為之通訊監察，其監督除由綜理國家情報工作機關首長派員為之外，亦得由高等法院專責法官會同監督。

第 32 條

電信事業或郵政事業與其他協助執行機關保管之通訊監察書及執行通知單等與通訊監察有關之文件，應妥善保管，並於通訊監察結束二年後依該事業或協助執行機關之規定辦理銷燬。

第 33 條

本法第二十條第二項所稱監察通訊日數不明，包括下列情形：

一、違反本法或其他法律規定監察他人通訊，而其監察通訊日數不明或無從計算者。

二、違反本法或其他法律規定洩漏、提供或使用通訊監察所得之資料，而無從計算其監察日數者。

第 34 條

本法第三十二條所稱現役軍人，依軍事審判法之規定。

本細則關於司法警察機關之規定，於軍法警察機關準用之。

第 35 條

檢察官、法官、綜理國家情報工作機關首長於本法中華民國九十六年七月十一日修正之條文施行前依法核發通訊監察書，仍應依修正條文施行前之法定程序執行通訊監察、報告執行情形及通知受監察人。

第 36 條

本細則自中華民國九十六年十二月十一日施行。