析論我國情報通訊監察法制－以美國法制為比較*

李　榮　耕**

目　次

關鍵字：通訊監察、情報通訊監察、情報監察、國家安全、通訊隱私。
Keywords：communication surveillance, intelligence communication surveillance, national security, communication privacy.

* 在此感謝兩位匿名審稿委員所提供的寶貴意見，使作者有機會補足本文中之闕漏。當然，本文文責仍由作者自負。

** 李榮耕，國立臺北大學法律學院助理教授，美國印地安納大學布魯明頓校區法學院法學博士。

摘 要

為維護國家安全，情報機關常以通訊監察之方式來蒐集資訊，但是，通訊監察的執行，對於監察對象及無辜第三人之通訊隱私常常造成相當大之影響。是故，在執行情報通訊監察時，於程序上應如何衡平國家安全及人民基本權利兩方面之需要，應值深入研究。在此一議題上，美國實務發展已久，也已有極為完整之規定，本文介紹了其中之重要法制，併在討論後指出我國國家情報工作法及通訊保障及監察法中應該修正之處，冀希其得為將來立（修）法及學說研究之參考材料。

A Comparative Study on the Legal Framework of Intelligence Communication Surveillance in the R.O.C. and U.S.

Li , Rong-Geng

Abstract

For the purpose of national security, intelligence agency usually conducts communication surveillance to gather necessary information. However, from time to time, communication surveillance invades the privacy rights of targets and innocent third parties. Thus, it becomes critical to balance national security and the protected fundamental rights while conducting intelligence communication surveillance. This article introduces and analyzes the legal framework of foreign intelligence surveillance of the United States. In addition, we point out the defects of the National Intelligence Services Law and Communication Surveillance and Protection Law.

壹、前　言

通訊監察，除了常用於犯罪偵查外，也是國家進行情報蒐集工作的利器之一[1]。無論是為了何種目的所進行的通訊監察，對於監察對象的通訊隱私來說，都構成了相當程度的侵害。詳言之，不管是偵查通訊監察或是情報通訊監察，於進行通訊監察前，並不會告知相對人，不會取得其同意，也不會給於其表明異議的機會，通訊監察也通常會持續一定的時間，更甚者，其會一併取得與監察目的無關的通訊內容，也會取得無辜第三人的通訊[2]。是故，在通訊監察中，應特別重視到人民隱私權益的保障，以避免國家不當恣意地侵害了監察對象的基本權利。

相較於偵查通訊監察，情報通訊監察所涉及的問題，可能更為錯綜複雜。因為其所監察的對象可能更為廣泛及不特定，監察的案由不一定涉及到特定的犯罪案件，監察的目的也傾向於是作為政策分析或情報預警之用，而非作為刑事審判之證據，所以，偵查通訊監察所適用的各樣要件及程序，似乎不當然能夠適用於情報通訊監察。本論文的目的，便是在探究我國情報通訊監察法制應有之架構及設計。

在我國，關於情報通訊監察的法律規範，主要是「國家情報工作法」（以下簡稱「情工法」）及「通訊保障及監察法」（以下簡稱「通保法」）。本論文將以這兩個法案為主要的討論對象，分析其體系及程序規定。另外，由於美國聯邦於國家安全工作及情報蒐集法制已有完整的規定，且行之有年，所以，本文會一併介紹並討論該國的相關法規，並與我國法律為比較分析，探究其有無值得我國借鏡之處。最後，我們會試著提出我國在情報通訊監察制度上，可以修正之處，併指出修法的方向，以為將來立（修）法及學說發展之參考。

貳、犯罪偵查與國家安全工作之異同

在開始分析我國法規範之前，有一前提問題，值得討論。詳言之，在犯罪偵查及情報工作中，都可能使用到通訊監察，以蒐集所需資訊。既是如此，犯罪偵查及情報工作究竟有何差異或類似之處？

犯罪偵查與國家安全工作或情報蒐集有其不同之處，也其相似的地方。詳言之，一般的犯罪所影響的層面通常較為有限，被害人的人數也通常較少；但是，破壞國家安全或利益的活動影響所及常常極為廣泛，被害的人數也通常遠較一般犯罪為多。就行為人或監察對象來說，兩者也不盡相同。在一般的犯罪裡，前者多半純為本國人，但是，情報蒐集中，監察的對象很可能是以外國人，或是與外國人接觸的本國人為主。另外，一般犯罪裡，固然有較為重大複雜者，不過，整體來說，其還是比情報通訊監察所涉及的情節及活動來得要簡單及輕微。以蒐集所得的資訊來說，犯罪通訊監察所得的資訊，通常是用以作為認定犯罪事實的證據，而在審判期日中提出作為證明被告之犯罪事實之用；情報通訊監察所得的資訊，則多半是作為預警、情報分析、危機因應、政策形成或是國防及外交工作之用。兩者之用途有其區別。

概念上，情報蒐集與一般犯罪偵查工作或許可以如上述般地一分為二，但是，實際運作上，這兩者並不容易區分。舉例來說，兩者的執行單位可能是同一機關。以法務部調查局為例，其便同時負責犯罪偵查及國家安全的情報蒐集。法務部調查局組織法第二條規定，調查局所掌理的事項便同時包含了「外患防制事項」、「洩露國家機密防制事項」、「貪瀆防制及賄選查察事項」、「重大經濟犯罪防制事項」、「毒品防制事項」、「洗錢防制事項」、

1　為了行文方便起見，本文將為犯罪偵查目的所進行的通訊監察簡稱為「偵查通訊監察」，相對地，為維護國家安全或是情報蒐集所進行的，則稱之為「情報通訊監察」。

2　請參照司法院大法官會議第六三一號解釋及其理由書。不過，該號解釋係針對偵查通訊監察所作成，而不涉及情報通訊監察，但其中關於憲法保障人民秘密通訊自由及隱私權益部份之說理，在情報通訊監察法制中仍值注意。

「電腦犯罪防制……事項」、「組織犯罪防制之協同辦理事項」、「兩岸情勢及犯罪活動資料之蒐集、建檔、研析事項」、「國內安全及犯罪調查、防制之諮詢規劃、管理事項」，以及「上級機關特交有關國家安全及國家利益之調查、保防事項」。另外，依照國家情報工作法的規定，海岸巡防署或警政署等傳統上負責犯罪偵查的機關，仍會負責部份國家情報事項，在該職權範圍內，其仍屬於情報機關（情工法第三條）。由此可知，單純就執行機關來看，並不易判斷其所進行的是一般犯罪偵查，或是情報蒐集工作。

再者，就本質來說，情報蒐集工作及一般犯罪活動有很高的重疊性。涉及外國情報之資訊，常常也都與刑法上的犯罪行為有關；相同地，部份刑法上的犯罪行為，也都是外國情報蒐集工作的重點。例如，行為人為外國蒐集我國國防秘密資訊的活動，應當屬於國家安全事項，其行為也可能同時該當了刑法第一一一條第一項的收集國防秘密罪。又例如，將國防秘密交付於外國或其派遣之人的行為，除可能該當刑法第一〇九條第二項外，其行為也會是國家安全工作所防制的對象。從這一方面來看，情報蒐集工作與犯罪偵查在概念上雖然能夠有所區別，不過，在更多的時候，這兩者可能根本沒有本質上的差異，更無法截然二分。

於一般犯罪偵查及情報蒐集中，國家或是行政機關所使用的方式可能相差無幾。其可能都會以通訊監察、跟監，或是向其他機關或團體調取資料等方式蒐集相關的資訊。以通保法為例，為蒐集特定重大犯罪的相關證據，偵查機關可以進行通訊監察（第五條及第六條）。相同地，為避免國家安全遭受危害，綜理國家情報工作機關也可以進行通訊監察，以蒐集外國勢力或境外敵對勢力的情報資訊（第七條）。是故，為進行一般犯罪偵查或情報蒐集，行政機關使用的方式並沒有非常大的差別，其對相對人所可能造成的影響或權利侵害，並無二致。

由上述的說明可以知道，一般犯罪偵查與國家安全工作或情報蒐集間有相當多類似之處。接下來可以追問的是，既然這兩者有許多相似之處，其在程序上是否應遵循相同的規範？例如，國家安全機關為蒐集情報而進行通訊監察時，其所適用的程序要件是否應該與偵查機關為偵查犯罪時所為的通訊監察相同？如果兩者無須遵守同樣的要件，其原因為何？[3] 為要回答這些問題，應先分析討論我國情報通訊監察之相關規定。

參、我國之情報通訊監察法制

關於我國情報蒐集之規範，主要當屬情工法及通保法中情報通訊監察的相關條文。前者的規定屬於我國情報工作的一般性規定，後者則更進一步地規定了進行情報通訊監察時所應遵循的程序。以下分別說明之。

一、國家情報工作法

我國於二〇〇五年公布實施國家情報工作法[4]，用以規範政府所進行的情報蒐集活動。其中較為重要的規定包括了情報工作所得使用的方式、所應蒐集的資訊類型，以及取得資料的處理。

㈠情報工作的進行

情工法第六條第一項規定，執行情報工作必須兼顧國家安全及人民權益的保障，並以適當方式為之。同條第二項列舉了情報機關不得涉入黨政活動的各樣行為規範。情報工作指的是，「情報機關基於職權，對足以影響國家安全或利益之資訊，所進行之蒐集、研析、處理及運用」，也包涵了「應用保防、偵防、安全管制等措施，反制外國或敵對勢力對我國進行情報工作之行為」（同法第三條第一項第二款）。「情報機關」指的則是「國家安全局、國防部軍事情報局、國防部電訊發展室、國防

3 關於國家安全之維護及犯罪偵查間之關係、互動及相關規範之合理設計，國內已有學者曾為文作了極為深入的分析及討論，還請參照，王兆鵬，〈路檢及國境檢查〉，《臺灣本土法學雜誌》，26 期，2001 年 9 月，頁 15 以下。

4 中華民國 94 年 2 月 5 日總統華總一義字第 09400016831 號令。

部軍事安全總隊」等機關（同法第三條第一項第一款」。

同法第七條規定，情報機關應就足以影響國家安全或利益的資訊為蒐集、研析、處理及運用，其中包括了：⑴涉及國家安全或利益之大陸地區或外國資訊、⑵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，以及⑶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（第一項）。同條第二項屬於蒐集資訊方式的重要規定，其授權情報機關可以採取秘密的方式進行運用人員、電子偵測、通（資）訊截收、衛星偵蒐（照）、跟監、錄影（音）及向有關機關（構）調閱資料等方式。使用上述方式蒐集資料時，「並應遵守相關法令之規定」。就解釋上來說，在進行情報通訊監察時所應遵守的「相關法令」，係指現行通保法第七條等規定。

另外，為了執行情報工作，情報工作人員可以採取身分掩護措施（情工法第九條）或是設立掩護機構（同法第十條）。這兩種方式都屬於依法令之行為，而為刑法上的阻卻違法事由（第十一條）。

㈡國家安全資訊的處理

情報機關於獲取足以影響國家安全或利益之資訊時，應即送交國家情報工作主管機關（依情工法第二條，目前為「國家安全局」）處理。如果取得的資訊涉及社會治安之重大事件或重大災難者，除依法處理外，也應該立即送交前述之主管機關（情工法第十八條第一項）。依此規定，情報蒐集所取得的資訊究竟是否可以作為犯罪偵查或刑事審判之用，並不清楚。

二、通訊保障及監察法

情工法屬於情報工作的總則性及一般性規定，進行情報通訊監察時所應遵循的具體程序規範，當屬通保法。單就通保法的體例來觀察，雖然犯罪偵查與情報工作有其本質上之不同，不過，我國立法者仍是選擇在通保法同時規範了這兩種不同通訊監察。關於情報通訊監察，其主要規定在通保法第七到十條，其他的程序規定則是與偵查通訊監察共用相同的條文。也因如此，情報通訊監察在適用通保法時，產生了不少扞格之處。再者，立法者進一步將情報通訊監察區分為一般情報通訊監察，及緊急情報通訊監察，並設計了不同的程序規定。由此可知，立法者並無意以同一套標準規範偵查通訊監察及情報通訊監察。

㈠實質要件（？）

通保法第七條第一項規定，為避免國家安全遭受危害，有進行通訊監察，以蒐集外國勢力或境外勢力情報之必要時，得進行情報通訊監察。不過，條文中的「為避免國家安全遭受危害」應屬進行情報通訊監察之目的，而不是實質要件。嚴格來說，通保法並沒有清楚具體規定情報通訊監察之實質要件為何。

㈡程序

進行情報通訊監察前，情報機關必須要先獲有通訊監察書，方得為之。不過，情報通訊監察書並不是由法院所審核，而是由綜理國家情報工作機關首長（目前為國安局局長[5]）核發。另外，通保法再依受監察對象於我國境內是否設有戶籍，區分核發情報通訊監察書前是否應得到法院同意。

詳言之，依通保法第七條第二項的規定，受監察人在我國境內設有戶籍時，除非有急迫情況，否則綜理國家情報工作機關首長於核發通訊監察書前，必須要先得到管轄高等法院專責法官同意。在有急迫情況時，綜理國家情報工作機關可以逕行核發通訊監察書，但須於事後通知其所在地高等法院專責法院，請求其補行同意。若高院專責法官未於四十八小時內同意，則應立即停止監察（通保法第七條第三項）。由條文反面推知，如果受監察人在我國境內未設有戶籍，無論情況是否急迫，綜理國

5　請參閱通訊保障及監察法施行細則第九條。

家情報工作機關首長都可以逕自核發通訊監察書，進行情報通訊監察，無須法院同意。核發通訊監察書的過程採不公開的形式（通保法第十一條第三項）。解釋上，高等法院審查是否同意核發令狀時，亦係採秘密審理程序。

通保法第七條第一項規定，情報通訊監察所得監察的對象包括了外國勢力、境外敵對勢力或其工作人員在境內、跨境或境外的通訊（通保法第七條第一項）。條文中「外國勢力或境外敵對勢力」指的是「外國政府、外國或境外政治實體或其所屬機關或代表機構」、「由外國政府、外國或境外政治實體指揮或控制之組織」或「以從事國際或跨境恐怖活動為宗旨之組織」（通保法第八條），而「外國勢力或境外敵對勢力工作人員」指的則是「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」、「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」、「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」（通保法第九條）。依照這樣的定義，外國勢力或境外敵對勢力不一定為我國所承認的國家。

㈢通訊監察書的應記載事項

情報通訊監察書之應記載事項，規定於通保法第十一條第一項。依該條項，情報通訊監察書上應記載案由及涉嫌觸犯之法條、監察對象、監察通訊種類及號碼等足資識別之特徵、受監察處所、監察理由、監察期間及方法、聲請機關、執行機關及建置機關等事項。其中執行機關指的是「蒐集通訊內容之機關」，「建置機關」則是「單純提供通訊監察軟硬體設備而未接觸通訊內容之機關」（同條第三項）。不過，情報工作所需資訊不當然與犯罪相關，一律要求必須記載「涉嫌觸犯之法條」，恐不合於情報工作之需求。

㈣監察的期間及延長

情報通訊監察的期間為一年，有必要延長時，應附具體理由，在期間屆滿前二日，提出聲請（通保法第十二條第一項）。在監察期間內，綜理國家情報工作機關首長認為已經沒有監察的必要時，應該立即停止監察（通保法第十二條第三項）。條文中的「提出聲請」應該是立法上的疏誤，因為情報通訊監察中，主要是由綜理情報工作機關核發令狀，或是經法院同意後核發，並沒有向何人「聲請」進行情報通訊監察的規定，也就不會有向何人聲請延長通訊監察的可能。很明顯地，通保法第十二條第一項於這部份的規定係屬立法錯誤，應於日後修正之。

㈤監察的方式

情報通訊監察可以以「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」進行（通保法第十三條第一項本文），其已涵蓋了大多數常用的取得通訊的方式，並有概括規定，應該足以因應實際上的需求。再者，通保法還要求，無論使用何種通訊監察方式，都應維持該通訊的暢通（通保法第十三條第二項）。

值得留心的是，通保法第十三條第一項但書禁止情報機關以於私人住宅裝置竊聽器、錄影設備或其他監察器材等方式進行通訊監察。其中著眼點可能是，在私人住宅內所發生的活動或言行大多較為私密，若是可以加以監察，可能會因而造成對於個人隱私過鉅的侵害或影響，所以，立法者明文禁止之。這樣的條文設計立意固然良好，不過，其可能過於不切實際，並造成情報工作之死角，有害於國家安全。

㈥取得資訊的使用

原則上，依通保法監察所得的資料，不得提供予其他機關（構）、團體或個人。但是，在合於偵查通訊監察或情報通訊監察的目的或其他法律有規定時，則不在此限（通保法第十八條）。此外，通保法進一步規定，經情報通訊監察所取得的資訊僅得供「國家安全預警情報之用」。不過，發現有得進行偵查通訊監察的情形時，綜理國家情報工作機關應將該資料移送司法警察機關、司法機關或軍事審判機

關，由其依法處理（通保法第十條）。

上述條文中的「依法處理」或合於監察目的的意涵為何？從條文本身並無法得知。在適用上可能會因而產生疑義。例如，在取得資訊所涉及的犯罪審判中，該資訊是否具有證據能力？

㈦通訊服務提供業者的協助義務

通保法第十四條為通訊服務提供業者的協助義務規定。其中要求電信事業或郵政事業應協助情報通訊監察的進行。電信業者所使用的通訊系統應該具有配合進行監察的功能，業者本身也負有協助建置並維持通訊監察系統的義務。違反本條規定者，有罰鍰或撤銷特許或許可等相對應的行政處罰，以促使業者能確實遵守其協助義務（通保法第三十一條）。

㈧事後通知

情報通訊監察結束後，執行機關應敘明受監察人的姓名及住居所等資料，報由綜理國家情報工作機關陳報法院通知受監察人。受監察人所指的不只是「監察對象」，還包括了為監察對象發送、傳達、收受通訊或提供通訊器材、處所之人（通保法第四條）。若是其認為通知有害於監察目的之虞或不能通知者，應一併陳報於法院（同法第十五條第一項）。除非有上述妨害監察目的之虞或不能通知的情形，否則，法院接到陳報並審查後，應交由司法事務官，立即通知受監察人（同條第二項及第四項）。不通知的原因消滅後，執行機關應報由綜理國家情報工作機關陳報法院補行通知（第三項）。通知受監察人之事項包括了通訊監察書核發機關及文號、案由、監察對象、監察通訊種類及號碼等足資識別之特徵、受監察處所、監察期間及方法、聲請機關、執行機關，以及有無獲得監察目的之通訊資料等事項（通訊保障及監察法施行細則第二十七條第三項）。

何以必須要通知受監察人情報通訊監察的情事？如果只是要告知其曾受有監察，事後通知的規定顯然沒有太大的意義。另外，依本條規定，現行情報通訊監察的事後通知規定以通知為原則，不通知為例外。這樣的規範模式，是否合於情報工作之實際需求，不無疑義。

㈨執行機關的報告義務

執行機關於開始進行情報通訊監察後，應按月向綜理國家情報工作機關首長報告執行情形，綜理國家情報工作機關首長亦得主動地命執行機關提出報告，說明情報通訊監察進行的情形（通保法第十六條第一項）。由此可知，執行機關僅需要向綜理國家情報工作機關說明情報通訊監察的細節，對於其他機關，如同意核發情報通訊監察書的高等法院專責法官，則沒有此等報告義務。

㈩就建置機關的監督權責

針對通訊監察的建置機關，綜理國家情報工作機關負有監督的權責。監督的方式包括了派員前往，或是使用電子監督設備，監督通訊監察的執行情形（通保法第十六條第二項）。值得注意的是，就通訊監察的執行來說，雖然相當仰賴通訊服務業者（電信業者）的協助，但是，綜理國家情報工作機關對其並無任何監督之權限。

㈪保存及銷燬

通保法第十七條為監察取得資訊的保存及銷燬的規定。其中明文，在有必要時，執行情報通訊監察的機關可以長期保存所取得的資料；無必要者，則可保存五年。逾期後，方予銷燬（第一項）。此外，監察所得資料全部與監察目的無關者，該資料不當然會被銷燬，而是經執行機關報請綜理國家情報工作機關首長，由其許可後，方予以銷燬之（第二項）。

㈫證據排除法則及毒樹果實理論

違反情報通訊監察的程序要求時，有證據排除法則及毒樹果實理論的適用。通保法第七條第四項規定，違反本條第二項及第三項所取得的通訊內容或衍生證據，在其他程序中，不具有證據能力。藉由這樣的規定，可以確保情報工作機關會確實遵守各樣程序規定，以避免濫用情報通訊監察權限，恣意侵害人民通訊隱私。值得注意的是，依照通保法第七條第四項

之規定，情報通訊監察違反該條第二項及第三項以外之程序規定時，似無證據排除之效果。

以上為我國情報通訊監察法制之主要規定及其介紹。他山之石，可以為錯，以下本文接著分析討論美國早期情報通訊監察之運作情形、相關法制發展歷程、規定及實務判決，以為進一步比較研究及提出我國法制修正建議之基礎。

肆、美國情報通訊監察的初期發展及實務立場

早年美國實務便已利用電子通訊監察設備進行情報通訊監察工作，也因而產生各樣法律爭議。美國政府多主張，基於總統的固有職權，為維護國家安全，其得不經司法審查進行情報通訊監察，以蒐集所需的各樣情報資訊。此外，美國聯邦最高法院也傾向於認定，規範偵查通訊監察的各樣要件及程序，並不當然可以直接適用於情報通訊監察。

一、早年的美國實務立場

美國的情報通訊監察，可以追溯到一九四〇年前後的小羅斯福（Franklin D. Roosevelt）總統年代。在當時，美國聯邦政府主張，基於總統的固有權力（inherent authority），不經司法審查授權，行政機關便可為維護國家安全的緣故，進行情報通訊監察。於一九五四年，艾森豪（Eisenhower）總統所任命的檢察總長（Attorney General）柏內爾（Brownell）也力主，在國內及國際安全的相關事務上，可以利用通訊監察，蒐集必要之相關資訊。柏內爾表示，電子通訊已經成為了不法份子彼此聯繫及交換情報的主要工具，通訊監察也因而成為美國政府有效抗制此類活動的利器[6]。在這一個時期，相關法律議題的爭論及案例並不多見。

在一九六七年的*Katz v. United States*案中，美國聯邦最高法院宣示，為犯罪偵查所進行的電話通訊監察必須遵守美國聯邦憲法第四修正案的要求，不過，聯邦最高法院同時指出，為國家安全目的所進行的情報通訊監察是否應事先聲請令狀，並不在本案判決所涵括的範圍之內[7]。亦即，在這一個判決裡，聯邦最高法院僅確認了，為偵查犯罪所進行的通訊監察屬於第四修正案的「搜索」及「扣押」，必須遵守相當理由、特定明確原則及令狀原則等要求。至於為維護國家安全所進行的情報通訊監察應當遵守什麼樣的程序及要件，方符合第四修正案的要求，聯邦最高法院於本案中並未表示任何意見。

在*Katz*案後，為使通訊監察合於該案之判決意旨，聯邦國會制定了「整體犯罪控制及街道安全法案（Title III of Omnibus Crime Control and Safe Streets Act of 1968[8]）」，其中包涵了「美國聯邦通訊監察法（The Wiretap Act）」[9]。法案中詳盡地規範了政府為犯罪偵查而進行通訊監察時所應遵守的程序規範。不過，聯邦國會也明白表示，該法案無意限制總統在為保護國家安全時，所得採取外國情報通訊監察措置[10]。

隨後，於一九七二年，美國聯邦最高法院於*United States v. United States District Court*案（一般慣稱為*Keith*案）[11]中表示，在進行國內

6 Herbert Brownell, *The Public Security and Wire Tapping*, 39 CORNELL L.Q. 195, 202 (1954).

7 Katz v. United States, 389 U.S. 347, 358 n.23 (1967).

8 Pub. L. 90-351, 82 Stat. 197 (1968). *See generally Clifford S. Fishman, Interception of Communication in Exigent Circumstances: The Fourth Amendment, Federal Legislation, and the United States Department of Justice*, 22 GA. L. REV. 1, 5-7 (1987).

9 美國聯邦通訊監察法制的說明，可以參照李榮耕（原名蔡榮耕），〈I am Listening to You －釋字第六三一號解釋、令狀原則及修正後通訊保障及監察法（上）〉，《台灣本土法學雜誌》，104 期，2008 年 3 月，頁 56-60；李榮耕（原名蔡榮耕），〈I am Listening to You －釋字第六三一號解釋、令狀原則及修正後通訊保障及監察法（下）〉，《台灣本土法學雜誌》，105 期，2008 年 4 月，頁 43-56。

10 18 U.S.C. §2511(3). Stephanie Cooper Blum, *What Really is at Stake with the FISA Amendment Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT. L.J. 269, 273-74 (2009).

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

安全情報（domestic security intelligence）的蒐集時，行政機關仍須遵守聯邦憲法第四修正案。不過，法院也說明道，該判決並不適用於涉及外國勢力及其工作人員的案件[12]。*Keith* 案件也促成了之後美國情報通訊監察的法制化。

二、*United States v. United States District Court*（*Keith*）案

Keith 案是美國聯邦最高法院第一次直接審理國家安全、情報工作、通訊監察及聯邦憲法第四修正案間的爭議。在這一個判決中，聯邦最高法院表示，原則上，針對國內勢力或是國內組織進行情報通訊監察時，情報機關仍需遵守憲法第四修正案之規定，但是，因為國家安全事務有其特殊性，其相關要件及程序可以較為彈性。這一個判決也促成了後續情報通訊監察法制的建立。

㈠事實及法院判決理由

在*Keith* 案[13]中，被告因為涉嫌以炸藥破壞公物而被起訴，案件由美國聯邦東密西根地方法院（United States District Court for the Eastern District of Michigan）審理[14]。於審判中，被告要求檢察官開示（disclose）經通訊監察所取得之通訊內容，並進行聽證，以決定其是否具有證據能力。檢察總長出示了一份宣誓書（affidavit），說明其授權進行通訊監察，蒐集情報資訊，以避免國內組織（domestic organization）可能發動的攻擊及推翻現有政府組織。基於這分宣誓書，檢察官主張，雖然該通訊監察未事先經過法院授權，不過其仍為合法，因為總統（行政權）有為維護國家安全（透過檢察總長）進行通訊監察的固有權限[15]。聯邦地方法院未接受檢察官之主張，並認為該通訊監察已違反美國聯邦憲法第四修正案，下命檢察官必須要向被告開示與該通訊監察相關之資訊。檢察官不服此一決定，向美國聯邦第六巡迴法院（the Court of Appeals for the Sixth Circuit）提起上訴（本案之所以慣稱為「*Keith* 案」，因為下令應開示相關證據的聯邦地方法院法官為Damon J. Keith）。第六巡迴法院維持地方法院的看法。美國聯邦政府最後上訴到了美國聯邦最高法院[16]。主筆本案的包威爾（Powell）大法官指出，本案的主要爭議在於，政府是否有權不經司法審查便為維護境內安全（internal security, or domestic security）事務的緣故進行通訊監察？

檢察官主張，從聯邦通訊監察法的規定可以推知，國會有意讓行政機關在有維護國家安全的需要時，可以不經司法審查便直接進行通訊監察。不過，聯邦最高法院並不接受這一個說法，其解釋道，聯邦通訊監察法僅中性地說明，該法不拘束總統依憲法所得行使的權力，並不代表情報通訊監察可以不受到令狀原則或其他必要之限制。

美國聯邦最高法院接著指出，本案的監察對象純粹為國內勢力，而不涉及外國勢力。根據檢察總長的宣誓書，本案監察目的是為了防止或抗制國內團體（domestic organization）所發動的攻擊活動及動亂行為。案件中，並沒有任何的直接或是間接證據可以證明有任何外國勢力牽涉其中。是故，本案的爭議可以進一步限縮為，在進行情報通訊監察時，若監察對象或案由不涉及外國勢力，是否仍需遵守美國聯邦憲法第四修正案的令狀原則？[17]

檢察官進一步主張，因為不法分子大量且頻仍地以電子通訊聯繫彼此及蒐集資訊，所以，只要案件涉及與美國政府敵對的勢力或是團體，美國政府便有權對其境內或跨境之通訊進行監察，以抗制各樣危害國家安全的敵對勢力或組織。如果禁止政府使用情報通訊監察

12 *Id*. at 321-22.
13 United States v. United States District Court, 407 U.S. 297 (1972).
14 *Id*. at 299.
15 *Id*. at 300-01.
16 *Id*. at 300.
17 *Id*. at 309.

的手段來維護國家安全，顯然與公益需求相違背[18]。

針對上述主張，聯邦最高法院回應道，政府確實有為國家安全而進行情報通訊監察的利益，但是，不可否認地，其本質仍屬於對於人民隱私的嚴重侵害。是故，在為境內安全事務之目的而進行通訊監察時，情報機關仍然必須要遵守美國聯邦憲法第四修正案的誡命。換言之，通訊監察的發動不能僅憑行政機關單方面的決定，必須要有其他機關的制衡，以確保個人的權利自由不會受到不當的侵害[19]。

檢察官又主張，法院並不適合就情報通訊監察或是國家安全事務為事前審查。其舉出來的理由有數端；第一，國家安全涉及大量複雜的因素，遠遠超過法院所能理解。法院並沒有能力審查個案中是否有保護國家安全的相當理由，也無法判斷政府所欲採取的情報蒐集方式是否合於國家安全的需要。第二，法院在審查情報機關的聲請的程序中，會有洩密的危險，進而危及國家安全及情報工作人員的人身安全[20]。

美國聯邦最高法院並不接受上述檢察官的各樣說法。聯邦最高法院解釋道，長久以來，法院都一直在審理社會中各樣難解的案件，認為法院沒有能力審查複雜的國安案件的說法並不合理。再者，並沒有任何的證據顯示司法的事前審查會有洩露機密的疑慮。依照美國聯邦通訊監察法，法院於間諜（espionage）、叛國（treason）或其他陰謀破壞（sabotage）之案件中，便一直都負責著令狀聲請的審查工作，並接觸到機密的資訊。但是，令狀的審查程序並不公開，相對人亦不知悉（*ex parte*），所以不會有洩密的疑慮；再者，也可以經由行政上的管制來避免可能發生的洩密問題[21]。是故，聯邦最高法院判定，在涉及國內勢力或國內團體的國家安全事務上，政府仍必須先經過司法的審查及授權，方得進行情報通訊監察。

不過，聯邦最高法院亦表示，美國聯邦通訊監察法的程序，主要係適用於犯罪偵查，不當然適用於情報通訊監察。其中主要的原因在於，國家安全事務或情報工作與一般犯罪案件有著不同的政策及實務上的考量，所以應適用不同的規定。前者的監察範圍可能更為廣泛，以及涉及更多的消息來源。與一般犯罪監察相比，在涉及國家安全的案件中，其監察對象可能更不容易特定，也可能較偏重於預防不法活動的發生及對於危害的抗制。是故，涉及國家安全的情報通訊監察中只要合於第四修正案中「合理（reasonableness）」的要求，規範情報通訊監察的程序要件未嘗不可有適度的放寬[22]。判決中，聯邦最高法院舉例說明道，與偵查通訊監察相比較，進行情報通訊監察的相當理由、期間及報告義務可以有不同而更有彈性之規定[23]。

美國聯邦最高法院最後表示，本判決僅適用於涉及國內勢力或國內組織（domestic power or domestic organization）之案件；至於針對「外國勢力」所進行的情報通訊監察，則可適用不同的程序及要件[24]。其中，「國內勢力」指的是，由美國人民所組成，且未與外國勢力或其工作人員有顯著關聯性（significant connection）之團體或組織[25]。情報機關就國內勢力所進行之情報通訊監察則須嚴守第四修正案的要求。

18 *Id*. at 310-12.

19 *Id*. at 317-18.

20 *Id*. at, 319.

21 *Id*. at 320-21.

22 *Id*. at 322-23.

23 *Id*. at 323.

24 美國聯邦最高法院於這邊的說理，似乎意味著行政權（總統）可以在不經法院審查的情形下，針對外國勢力及其工作人員進行情報通訊監察。事實上，美國情報監察上訴法院曾於個案中表示，美國總統有其固有的憲法權力，為蒐集外國情報之目的而進行無令狀的情報通訊監察。*In re* Sealed Case, 310 F.3d 717, 742 (For. Intel. Surv. Rev. 2002). 這樣的看法，也是小布希政府於九一一事件後下令國家安全局（National Security Agency）進行無令狀情報通訊監察最重要的理論基礎之一。Blum, *supra* note 10, at 284-86.

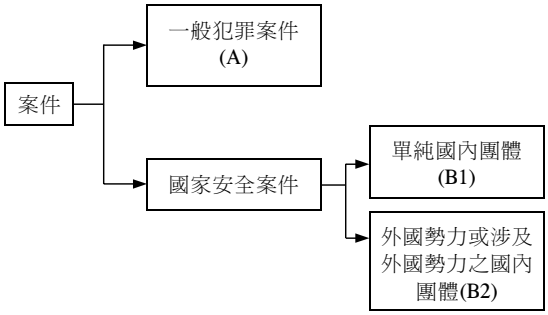
25 *United States District Court*, 407 U.S. at 309 n.8.

但是，聯邦最高法院承認，在部份的案件中，這兩者會有其區分上的困難[26]。

㈡分析

情報工作是否必須要遵守與一般犯罪偵查相同的程序規範？情報通訊監察對象為本國人或外國人，是否應有不同的限制？關於這一些問題，*Keith*案都提供了值得參考的答案及區別標準。

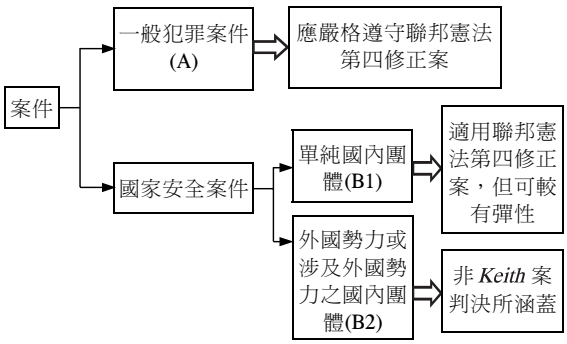
在 *Keith* 案中，聯邦最高法院將案件略分為一般犯罪案件及事涉國家安全的案件。後者再區分為以單純的國內團體或勢力為監察對象，以及與外國勢力有所牽連的國內團體及外國勢力為監察對象。這一個部份，得以下圖說明。



對於一般犯罪案件的通訊監察，偵查機關必須謹守美國聯邦憲法第四修正案的要求，具體的法律規範，當屬美國聯邦通訊監察法等相關規定（上圖中的A）。*Keith*案涉及的是以維護國家安全為目的的情報通訊監察，且監察對象為單純的國內團體（上圖中的B1）。關於這一種類型的情報通訊監察，聯邦最高法院認為，其本質上仍屬對於人民隱私的侵害，為避免情報機關恣意濫用其監察權力，所以其發動及程序仍須受到聯邦憲法第四修正案的規制。不過，聯邦最高法院也承認，情報通訊監察與偵查通訊監察在性質上並不相同，所以，美國聯邦通訊監察法並不適用於情報通訊監察，但是，國會得另以較為彈性的程序來規範之。

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（上圖B2），則不為*Keith*案所涵蓋。該判決並沒有說明行政權（總統）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。再者，*Keith*案也未說明，經情報通訊監察所取得的資訊於刑事審判中是否有證據能力[27]。

*Keith*案在這一個部份的判決說理，可以圖示如下：



針對外國勢力所進行通訊監察是否應遵循令狀原則，*Keith*案並未表示意見，不過，在該案後，多數巡迴法院表示，不經令狀程序，情報機關便可進行情報通訊監察，但是，其無權以因應國內勢力之威脅（domestic threats）為由，逕行為無令狀的情報通訊監察[28]。聯邦巡迴法院的疑慮在於，如果容許國家以維護國家安全為由進行通訊監察，而無須經過司法的事前審查，其可能會假借國家安全之名，恣意侵害人民隱私。尼克森（Richard M. Nixon）總統的水門案，便是最有名的例子之一。

㈢ *Keith* 案的後續影響

在尼克森總統辭職下台後，美國聯邦參議員法蘭克・邱爾吉（Frank Church）組成了調查委員會，針對以維護國家安全為目的所進行的無令狀通訊監察進行研究，最後作成了「邱爾吉委員會報告（Church Committee Reports）」。報告說明道，通訊監察固然能讓行政機關得以

26 *Id*.

27 *See* Beryl A. Howell & Dana J. Lesemann, *FISA's Fruit in Criminal Cases: An Opportunity for Improved Accountability*, 12 UCLA J. INT'L L. & FOREIGN AFF. 145, 149 (2007).

28 *See, e.g.*, Brown v. United States, 484 F.2d 418 (5th Cir. 1973); United States v. Buck, 548 F.2d 871 (9th Cir. 1977).

取得重要資訊及情報，但是，其也同時伴隨著濫用且違憲的疑慮。委員會建議聯邦國會應儘速立法，建立起妥適且完善的機制，以規範外國情報通訊監察。這份報告促成了隨後「美國聯邦外國情報監察法（the Foreign Intelligence Surveillance Act of 1978, FISA）」的制定[29]。在二〇〇一年的九一一事件後，美國聯邦國會通過了「愛國者法案（the USA PATRIOT Act of 2001）」[30]，大幅度地修正了 FISA，尤其是其中關於情報通訊監察的規定。於二〇〇八年，聯邦國會再度針對 FISA 制定「美國聯邦外國情報監察法修正法案（the FISA Amendment Act of 2008, FAA）」[31]。整體來說，FISA主要是規範以美國境內或是跨境通訊所為的情報監察；而FAA所規範的是在美國境外進行的情報通訊監察。以下分別說明其中之重要規定。

伍、美國聯邦外國情報監察法（FISA）及相關法案

美國聯邦國會制定 FISA 的目的在於用以規範美國聯邦政府的情報蒐集活動[32]，而為關於情報通訊監察最主要的法案[33]。因為立法先後的緣故，FISA在很多地方都是以美國聯邦通訊監察法（the Wiretap Act）為立法參考，因而兩者有許多類似之處，但是，美國聯邦國會也認識到情報蒐集工作與犯罪偵查有其本質上之差異，因此，在許多要件上，FISA顯然較為寬鬆有彈性。例如，FISA所規定的監察期間為九十天、一百二十天或一年，而不是美國聯邦通訊監察法所規定的三十天[34]。也因為如此，美國聯邦國會制定了更為嚴謹的程序規定，用以規範經外國情報通訊監察，以適當保護受監察對象的各樣憲法權利，並兼顧國家安全的需要[35]。

一、情報通訊監察之對象及客體

就通訊（電子）監察（electronic surveillance）之對象及客體而言，FISA所規範的態樣有四種，涵蓋了多種取得通訊內容的方式。值得注意的是，法案並沒有規範到所有的通訊類型。

詳言之，當情報通訊監察的進行或是受監察對象與美國有其「土地」上的一定關聯性時，才會有 FISA 的適用。依據法案規定，若已知通訊之一方為美國境內的美國人民，無論監察的是電信通訊（wire communication）或無線通訊（radio communication），且無論執行通訊監察的地點是在美國境內或境外，都有FISA的適用[36]。此一規定的重點在於通訊之一方是境內的美國人民，而不論執行情報通訊監察的地點為何[37]。

若受監察之一方為美國境內之人（無論其是否為美國人民），且是於美國境內執行情報通訊監察，該情報通訊監察亦有FISA的適用[38]。這一個條款所著重的是執行情報通訊監察的地點在美國境內，而不論通訊者為何，是故，其會涵括所有在美國境內及跨境之通訊監察[39]。

由上述的條文可知，FISA並未規範所有的

29 The Foreign Intelligence Surveillance Act of 1978, Pub. L. 95-511, 92 Stat. 1783 (1978).

30 The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56, 115 Stat. 272 (2001).

31 The FISA Amendment Act of 2008, Pub. L. No. 110-261, §403, 122 Stat. 2463 (2008).

32 就整體來說，FISA 包括了情報通訊監察（wire and electronic surveillance）、傳統型態的搜索（physical searches, 50 U.S.C. §§1820-29）、收發話紀錄的監察（pen registers/trap, 50 U.S.C. §§1841-46）及調取商業紀錄（orders for the production of business records and tangible things, 50 U.S.C. §§1861-62）等情報蒐集活動。本文討論的重點是在情報通訊監察的部份，礙於篇幅及集中討論之焦點，其他情報蒐集手段的規範只得暫且不論。

33 50 U.S.C. §1801(f).

34 18 U.S.C. §2518(5).

35 S. Rep. No. 701, at 58-59.

36 50 U.S.C. §1801f(1).

37 *See* S. Rep. No. 604 pt. 1, at 32.

38 50 U.S.C. §1801f(2).

39 *Id*. §1801f(3). *See* S. Rep. No. 604 pt. 1, at 33.

情報通訊監察。舉例來說，於美國境外就針對境外之人所進行的情報通訊監察便不受FISA規範[40]。又例如，當監察的客體是跨境之無線通訊（如無線對講機）時，只要監察對象不是美國境內之人，即便通訊之另一方位於美國境內，也無須遵守FISA之程序[41]。

二、有令狀的情報通訊監察

依據 FISA 的規定，原則上，進行情報通訊監察前，必須要經過司法的事前審查，取得令狀後，方得為之。由於美國聯邦通訊監察法較早制定，且行之有年，所以 FISA 有許多的條文都借鏡於該法案。不過，由於情報通訊監察的性質與偵查通訊監察不同，所以兩者的程序規定及要件仍有其差異。

㈠聲請權人

聯邦官員經檢察總長（Attorney General）、副檢察總長（Deputy Attorney General）及專責國安助理檢察總長（the Assistance Attorney General for National Security）授權批准後，得提出情報通訊監察聲請書[42]。此一規定提高了聲請的門檻。如此一來，等於是限制了情報通訊監察的聲請權人範圍，並提高責任歸屬的層級。

㈡聲請程序

FISA所設計的聲請程序相當嚴謹。首先，聯邦官員提出聲請書時，必須宣誓（oath）或具結（affirmation）其內容屬實。為了確保聲請書的記載合於 FISA 的要求，檢察總長、副檢察總長或專責國安助理檢察總長可以要求其他的官員提出該聲請書相關的文件及資料[43]。條文的目的，是為了確保情報機關所提出的資料的正確性，並確立事後的責任歸屬[44]。

檢察總長、副檢察總長或專責國安助理檢察總長認為聲請書記載有下列各個事項，且合於 FISA 的要求時，得批准授權該聲請：

⑴聲請的聯邦官員人別資料

這裡所記載的，必須是實際提出聲請之人。

⑵監察對象之相關資料或描述，但監察對象不明時，得不予記載這一項屬於監察對象特定明確的要求，目的是為了要降低美國人民受到情報通訊監察的危險[45]。

⑶聲請人所提出相關事實及背景資料，必須足以使檢察總長相信：

(A)監察對象為外國勢力或其工作人員；以及

(B)受監察的處所或設備現為或即將為外國勢力或其工作人員所使用；

FISA 詳細地定義了何謂「外國勢力（foreign power」及「外國勢力之工作人員（agent of foreign power）」[46]。其中「外國勢力」，其除了包括外國政府、機關、組織或國家外，還涵括了不為美國所承認為國家的政治實體，如恐怖組織[47]，或是已經不存在的國家（如東德）[48]。至於外國勢力之工作人員，則可能包括了美國人民或非美國人民。不過，必須是美國人民明知（knowingly）其從事違法或犯罪行為時，方可認定其為外國勢力之工作人員[49]。

⑷最小侵害程序（minimization procedures）的說明

「最小侵害程序」於 FISA 中有非常詳盡的規定及定義[50]。其中包括程序必須要合理、美國人民之資訊的保護、所取得資料的保全、

40 S. Rep. No. 701, 34.

41 現行 FISA 的架構係以通訊者所使用的通訊方式及執行監察的地點為主，並不是著眼於隱私或其他憲法權利的保障。這樣的設計，並不盡妥適，在美國已有文獻提出批評。*See* Blum, *supra* note 10, at 278-80.

42 50 U.S.C. §§1804(a) and 1801(g).

43 *Id*. §1804(b).

44 S. Rep. No. 701, at 49.

45 S. Rep. No. 701, at 49-50.

46 50 U.S.C. §§1801(a) and (b)

47 *Id*. §1801(a)(1).

48 United States v. Squillancote, 221 F.3d 542, 543-44 (4th Cir. 2000).

49 50 U.S.C. §1801(b)(1) and (2).

50 *Id*. §1801(h).

如何避免取得不相關的資訊、時間限制，以及非外國情報資訊的銷毀等規定[51]。FISA 進一步地課與檢察總長制定最小侵害程序準則的義務，供執行機關遵循。雖然情報通訊監察的執行方式有其個案上的不同，但是該準則必須就相類似的監察方式制定一致性的標準[52]。聲請書必須依據檢察總長所制定的準則，具體說明在該個案中執行時應遵守的程序，以避免不必要及不合理的侵害。

⑸所欲取得資訊的性質及受監察之通訊或活動之類型描述；

⑹保證書（certification, certify），用以擔保下列事項：

(A)欲取得的資訊屬於外國情報資訊；

(B)進行監察的重要目的（significant purpose）是為了要取得外國情報資訊；

過去 FISA 規定，情報通訊監察必須是以取得外國情報資訊為目的（the purpose）。於二〇〇一年，美國聯邦國會通過愛國者法案（the USA Patriot Act of 2001[53]），將此一要件修改為現行條文。其中的差別在於，修法前，進行情報監察只能以蒐集外國情報資訊為（唯一）目的；修法後，取得情報可以只是重要目的。換言之，只要蒐集外國情報資訊是重要目的，即便情報通訊監察的主要目的是為了進行外國情報犯罪（foreign intelligence crime）的偵查，亦得進行情報通訊監察[54]。不過，FISA 仍禁止國家以一般犯罪偵查為目的來進行外國情報通訊監察[55]。關於監察目的的修正，目前美國聯邦巡迴法院認為其仍合於美國聯邦憲法的要求[56]。

(C)該資訊無法以一般的偵查方式（normal investigative techniques）取得；

這一個要求與美國聯邦通訊監察法的規定[57]相類似，一般稱之為「最後手段原則」。

(D)所欲取得的資訊合於 FISA 的定義

情報通訊監察所得取得之資訊並非毫無限制。依據 FISA 之規定，情報通訊監察只能用以取得「外國情報資訊（foreign intelligence information）」。外國情報資訊指的是，與美國人民或外國勢力有關，且有必要用以抗制攻擊、破壞行動（sabotage）或秘密（clandestine）情報活動的資訊[58]。

⑺將使用的監察方式，以及為達情報監察目的是否需要進入一定處所；

⑻曾經依 FISA 向法院所提出過的聲請、聲請中所涉及的監察對象、設備、處所以及所使用的監察方式；

⑼情報通訊監察所需的時間，以及取得所需要的資訊後，仍必須繼續監察並取得必要情報資訊的理由。

這一個規定與美國聯邦通訊監察法相類似[59]。主要也是為了避免情報機關進行不必要的情報通訊監察，恣意侵害監察對象的通訊隱私。

㈢外國情報監察法院（Foreign Intelligence Surveillance Court）

FISA 成立了「外國情報監察法院」，專責審查外國情報（電子通訊）監察書（foreign intelligence electronic surveillance order）聲請的准駁。此一特別法院的法官任命權在聯邦最高法院院長，由其自至少十一個以上的聯邦地方法院法選任七名。其中三名法官的住居所與哥倫比亞特區（Columbia District）的距離必須少於

51 S. Rep. No. 701, at 50.

52 *Id*.

53 The USA Patriot Act of 2001, Pub. L. No. 107-56 115 Stat. 272 (2001).

54 外國情報犯罪指的是如破壞行動（sabotage）、國際恐怖主義（international terrorism）、間諜活動（espionage），以及為外國勢力而使用虛偽身份進入美國境內等行為。*See In re* Sealed Case, 310 F.3d at 723.

55 *Id*. at 744.

56 *Id*. at 744-45.

57 18 U.S.C. §2518(1)(c).

58 50 U.S.C. §1801(e).

59 18 U.S.C. §2518(1)(d).

二十英里。本條的目的應係為了確保在必要時，外國情報監察法院法官得以於迅速抵達法院，審理情報機關所提出之各樣聲請。

除了外國情報監察法院，FISA也成立了上訴法院，其由聯邦最高法院院長自聯邦地方法院或巡迴法院中任命三名法官組成。上訴法院的職責在於，當情報機關不服外國情報監察法院的駁回決定時，其可以向上訴法院提起救濟[60]。除此之外，政府若不服核准決定所附加的條件或限制，也可以向上訴法院請求救濟[61]。對於上訴法院的決定，政府可以再上訴於聯邦最高法院[62]。

㈣審查程序

依照FISA規定，令狀的審查程序不公開。合於下列各款要求時，外國情報監察法院得核發情報監察書：

⑴聲請書為聯邦官員所作成，且經檢察總長授權同意而提出[63]。

⑵有相當理由（probable cause）可信：

(A)監察對象為外國勢力或其工作人員，但不得僅因受美國聯邦憲法第一修正案所保護的言論或活動，便認定美國人民為外國勢力或其工作人員；以及

(B)受監察處所或設備現為或即將為外國勢力或其工作人員所使用。

此外，FISA要求法院，於個案中審查是否有相當理由時，應考量監察對象過去的行為以及與現在或未來的行為有關的事實及情狀[64]。具體而言，有無相當理由，還是必須依據個案的情狀來判斷[65]。如線民的信用性、線民取得線報時的整體情狀、線民提供線報後到提出外國情報監察聲請所經過的時間，以及有無其他足以佐證該線報的資訊等，都是在判斷相當理由時，應予考量的因素[66]。不過，從條文的文字可以知道，並不是在有外國情報犯罪的情形下，才能進行外國情報監察[67]。

除了上述的各樣要件外，外國情報監察法院還必須一併審查，聲請人所提出的具體措施，是否合於檢察總長所制定的最小侵害程序準則[68]。如果法院認為聲請人所提出的具體辦法無法最小化情報通訊監察之侵害，可以駁回該聲請，或是附條件地核准聲請。外國情報監察法院有權變更通訊監察書的內容或最小侵害程序的要求[69]。除此之外，其也可以要求聲請人提出更多的相關資訊，以決定是否核發令狀[70]。法院駁回情報機關的聲請時，應以書面說明理由，如果政府要求，則應立即將該理由書送交上級法院。

㈤情報監察書上應記載事項

在授權情報通訊監察的令狀上，法院應詳細記載下列事項：

(A)（如果知悉），受監察對象的人別資料，或是受監察對象的描述；

(B)（如果知悉）受監察處所或是設備；

(C)受監察的通訊或是活動之類型，以及所欲取得資訊之類型；

(D)監察方式，以及是否必須進入到特定處所以進行情報通訊監察；以及

(E)監察期間[71]。

這一個規定與美國聯邦通訊監察法相仿[72]。

60 50 U.S.C. §1803(b).
61 In re Sealed Case, 310 F.3d at 721.
62 50 U.S.C. §1803(b).
63 *Id*. §1805(a)(1).
64 *Id*. §1805(c).
65 *See* United States v. Hammoud, 381 F.3d 316, 322 (4th Cir. 2004).
66 S. Rep. No. 701, at 53.
67 *In re* Sealed Case, 317 F.3d at 738; United States v. Ning Wen, 477 F.3d 896, 898 (7th Cir. 2007).
68 50 U.S.C. §1805(a)(3) and 1804(h).
69 關於最小侵害原則，詳見下伍、四之說明。
70 50 U.S.C. §1804(b) and (c).
71 50 U.S.C. §1805(c)(1).
72 18 U.S.C. §2518(4).

令狀上特定明確的記載，可以確保執行情報通訊監察的機關不會監察無相當理由的通訊，也可以避免其對於通訊隱私造成過度的侵害。

除了上述的應記載事項外，法院於情報監察書上也應一併指示下列事項：

(A)應遵守最小侵害程序；

法院應監督執行機關是否確實遵守最小侵害程序，以避免對監察對象及第三人的隱私造成不必要的侵害。更重要的是，如果監察執行機關違反了法院所要求的程序，將構成藐視法庭罪（contempt of court）[73]。

(B)經聲請人向法院請求，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的資訊、設備或技術協助以進行情報通訊監察。

(C)要求上述的協助義務人以情報機關所核准的程序保管相關紀錄，或是提供保存紀錄所需之協助。

(D)聲請人對協助義務人有補償義務[74]。

FISA要求，如果核發令狀時，法院已經知悉，其就應於監察書中記載監察的處所或設備；但若是不知，則可不予記載。在後者的情形中，法院應具體要求，情報監察機關在針對新的地點或設備進行機動式通訊監察（roving surveillance）後十日內必須通知法院，在有正當理由時，可以延長至六十日[75]。FISA 容許於法院或聲請機關無法確知監察處所或設備時，得不於監察書上記載這一個事項。這樣的彈性規定，是為了因應實際上的需求，因為在許多時候，情報機關都是在進行監察前才能特定監察對象所使用的處所或設備。過於僵硬的規定，恐怕無法因應情報工作的實際需求。不過，不能否認的是，這樣的設計伴隨有情報機關不當侵害人民通訊隱私的疑慮。FISA試圖在這中間取得平衡，一方面容許法院於必要時，在情報通訊監察書上可以不記載監察處所或設備，但是，一旦開始進行監察，情報機關就必須要即時通知法院，使其得以立即審查該情報通訊監察的合法性。

㈥監察期間及延長

於一般情形，情報通訊監察期間為九十日，如果監察對象為非美國人民的外國勢力之工作人員，監察期間可以達一百二十日[76]。但是若監察對象為不涉及美國人民的外國勢力或組織，監察期間可達一年[77]。

具備與聲請令狀相同的要件時，政府得聲請延長情報通訊監察，其程序與聲請令狀之相同[78]。也就是說，聲請延長情報通訊監察之情報機關必須提出與聲請令狀相同之資料及相當理由[79]。審查是否應准予延長時，法院應同時考量原通訊監察是否能達其目的，以及原監察的綜合情狀[80]。

三、無令狀監察

依FISA，情報通訊監察採令狀原則，但在特定情形下，情報機關仍可進行無令狀情報通訊監察，其包括了：㈠經總統同意、㈡緊急情況，及㈢戰爭時期。在這一些情形裡，情報機關必須自行制定行為準則（guideline），並監督其下屬單位之執行[81]。

㈠經總統同意

FISA規定，美國總統經檢察總長（Attorney

---

73 S. Rep. No. 701, at 55.

74 50 U.S.C. §1805(c)(2).

75 *Id*. §1805(c)(3).

76 *Id.* §1805(d)(1).

77 這裡所指的是 50 U.S.C. §1801(a)(1), (2) and (3)定義的外國勢力團體，其中包括了：(1)外國政府或其組織，無論是否為美國政府所承認；(2)非由美國人民所組成的外國勢力派系；以及(3)為外國政府所承認及控制的政治實體。

78 *See* 50 U.S.C. §1804(a).

79 *Id*. §1805(d)(1).

80 S. Rep. No. 701, at 56.

81 Helene E. Schwartz, *Oversight of Minimization Compliance under the Foreign Intelligence Surveillance Act: How the Watchdogs are Doing Their Jobs*, 12 RUTGERS L. J. 405 (1981).

General），可以授權進行為期一年以內的無令狀情報通訊監察。總統必須以書面的方式授權，不過其得以概括或附條件的方式為授權[82]。為了進行這一種類型的情報通訊監察，檢察總長在經總統授權後，必須要宣誓（oath），並以書面確認下列事項：

(A)該情報通訊監察單純是為了取得外國勢力間的通訊，或僅是為了從外國勢力所支配的處所取得技術情報（technical intelligence），而非為了取得口語通訊（spoken communication）的內容；

(B)沒有因而取得美國人民通訊內容之可能性；以及

(C)檢察總長所制定的最小侵害程序準則合於 FISA 的要求[83]。

除此之外，檢察總長也必須立即將其確認之書面送交外國情報監察法院[84]。

㈡**緊急情狀**

第二種可以進行無令狀監察的類型是在有緊急情狀時。亦即，在合於下列要件時，檢察總長可以於取得令狀前進行情報通訊監察：

(A)檢察總長合理相信有緊急情狀存在，有進行監察之必要，但縱使即時聲請，也無法立即取得令狀；

(B)存在有法院得核發令狀之事實情狀（合於法院得核發令狀的要件）；

(C)檢察總長通知有管轄權的法官，已進行緊急情報通訊監察之情事；以及

(D)檢察總長於七日內必須補聲請令狀[85]。

FISA 進一步規定，在：（1）已經取得所需的情報資料、（2）法院拒絕核發令狀，或是（3）於七日內檢察總長未補聲請令狀等情形時，情報機關必須立即停止該緊急情報通訊監察[86]。於法院拒絕核發令狀的情形，檢察總長得向審查法院提起抗告[87]。

法院未補核發令狀或拒絕核發令狀時，經緊急監察所取得的資訊便不得作為證據之用，也不可於任何聽證、審判、大陪審團、行政部門或立法機關中揭露。另外，除非涉及他人生命或重大的身體危險，且經檢察總長許可，否則在取得受監察的美國人民同意前，不得使用或揭露經緊急情報通訊監察所被取得之資訊[88]。

若法院最終拒絕核發令狀，法院應該通知受監察人情報通訊監察的情事、期間及政府是否因而取得所需的資訊。不過，當政府提出正當理由（good cause）時，法院可以延遲或不予通知[89]。

㈢**戰爭時期**

FISA 規定，在國會通過宣戰案後，總統得經檢察總長，授權進行十五日以內的情報通訊監察[90]。

除了上述三種情形外，前美國總統小布希於九一一事件後，不依 FISA 之規定，逕自下令國家安全局（National Security Agency, NSA）進行無令狀的情報通訊監察，此一措置，多稱之為 NSA 計畫（NSA Program），引起了憲法及法律層面的極大爭議。關於NSA計畫，請見本文肆、八部份之說明及討論。

四、最小侵害程序（minimization procedure）

與美國聯邦通訊監察法相仿，FISA中也有最小侵害程序的規定。所有的情報通訊監察（無論有無令狀）都必須要遵守此一要求。不過，不同的是，FISA更為明確地說明了最小侵

82 S. Rep. No. 701, at 47.
83 50 U.S.C §1802(a)(1).
84 *Id*. §1802(a)(3).
85 *Id*. §1805(e)(1).
86 *Id*. §1805(e)(3).
87 *Id*. §1805(e)(4).
88 *Id*. §1805(e)(5).
89 *Id*. §1806(j).
90 *Id*. §1811.

害程序所涵蓋的面向[91]，並進一步課與了檢察總長依據條文意旨制定最小侵害程序準則之義務。在情報通訊監察聲請書中，聲請人必須記載在該個案中，如何遵守最小侵害程序的具體方式[92]。確認聲請人所提出的具體方式合於準則及 FISA 的要求後，法院才能核發令狀[93]。

最小侵害程序應有其操作上的彈性，因為執行時看似無關緊要的通訊內容，在日後可能會變得非常地重要[94]。是故，目前美國聯邦第四巡迴法院已有判決認為，不能僅因情報機關取得了無辜第三人的通訊，就認為該情報通訊監察違反了最小侵害程序的要求[95]。再者，如果多數的通訊內容都是外國語言時，情報通訊監察的執行機關可以全部予以錄音[96]。當通訊的內容經過加密或加碼時，執行機關得以自動錄音設備來進行情報通訊監察[97]。

五、事後通知及救濟程序

依照 FISA 之規定，當情報通訊監察取得了刑事犯罪的證據時，該證據及其衍生證據在刑事審判程序中仍可有證據能力[98]。目前美國聯邦法院承認，受情報通訊監察的行為同時可能構成了刑事犯罪行為，所以，經情報通訊監察所獲得的資訊，得作為刑事審判之用[99]。不過，FISA 也同時規定，必須遵守一定的程序，方得於刑事審判中使用經情報通訊監察所取得之資訊。首先，必須獲有檢察總長的授權[100]；再者，使用該資料前，必須要通知受通訊監察人[101]。受通訊監察人認為情報通訊監察不合法時，得聲請法院排除該資訊及其衍生證據[102]。這一個條文賦予受通訊監察人聲明不服的機會，並避免情報機關動輒以情報蒐集之名，行犯罪偵查之實。

上述情報通訊監察是否合法的審理程序管轄權限在美國聯邦地方法院。相對於前述的事後通知規定，檢察總長得提出具結書（affidavit），說明相關資訊開示有害於國家安全。此時，法院應以秘密（in camera）及一造（ex parte）的方式審查系爭情報通訊監察的合法性。

目前已有數個美國聯邦巡迴法院表示，上述事後通知規定的設計合於聯邦憲法第四（禁止不合理之搜索扣押）[103]、第五（正當法律程序）[104] 及第六修正案（對質詰問）[105] 的要求。若檢察總長未提出具結書，法院則必須要揭露聲請書及情報通訊監察書，並依職權裁量是否公開其他監察之相關資訊[106]。是故，必要時，法院得在於適當的保全程序及特定的命令下，向被告開示（揭露）部份的聲請書、監察書及

91 FISA 中最小侵害程序的要求，約有四個部份：(1)依監察的目的及監察的技術，情報通訊監察的執行機關所採行的最小侵害程序必須合理，在取得、保存及傳遞情報資訊的同時，必須要最小化對於美國人民的非公開資訊所造成的影響；(2)檢察總長所制定的最小侵害程序準則必須要確保，除非是為分析外國情報資訊，否則，在受監察之美國人民同意前，其非公開及非屬外國情報之資訊不會被散布或利用；(3)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的資訊，以及；(4)除非經法院事後核發令狀，或檢察總長認為其關係他人生命或重大身體的危險，否則依總統下令所進行的無令狀情報通訊監察所取得涉及美國人民的資訊，不得公布、散布、使用或保存逾七十二小時。See id. §1801(h).

92 *Id*. §1804(a)(4)

93 *Id*. §1805(a)(3).

94 *Hammoud*, 381 F.3d at 334.

95 *Id*.

96 United States v. Brown, 908 F.2d 968 (4th Cir. 1990).

97 *In re* Sealed Case, 310 F.3d at 741.

98 United States v. Isa, 923 F.2d 1300, 1304-05 (8th Cir. 1991); United States v. Sarkissian, 841 F.2d 959, 964 (9th Cir. 1988).

99 *Sarkissian*, 841 F.2d at 965.

100 50 U.S.C. §1806(b).

101 *Id*. §1806(c) and (d).

102 *Id*. §1806(e).

103 *Isa*, 923 F.2d at 1306.

104 United States v. Ott, 827 F.2d 473, 476 (9th Cir. 1987).

105 *Isa*, 923 F.2d at 1306.

106 S. Rep. No. 701, at 57.

其他與監察程序相關的資料[107]。

上述的救濟程序涉及到受通訊監察人於訴訟上的防禦權及國家安全間的平衡。當監察合法性的爭議性很高時，法院至少應該要核准揭露部份資訊，使受通訊監察人得以為自己作有利的主張及說明[108]。當法院認為應向受通訊監察人揭露相關資訊，而監察機關認為不應予以揭露時，法院則應該（只能）揭露或是禁止使用該資訊[109]。

六、情報通訊監察所得資料之銷燬

因為通訊監察的特性使然，於執行情報通訊監察時，不免會因而取得與監察目的無關之資料。FISA的要求，一旦確認該通訊內容與情報監察目的無關，且當收發話雙方都位於美國境內時，就應該立即銷毀該資料。唯一的例外情形是，檢察總長認定其涉及他人生命或身體的重大危害時，得下命不予立即銷毀[110]。

七、國會監督

不獨司法監督，FISA也同時有國會監督機制。詳言之，FISA要求，檢察總長應向聯邦眾議院情報委員會（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）提出年度報告，詳實說明（fully inform）情報通訊監察的執行狀況[111]。

此外，FISA還要求，每四年參議院情報委員會應就情報通訊監察的執行情形向參議院及眾議院作成報告。報告的內容應包括 FISA 應否修正、應否廢止或應依原規定授權進行情報通訊監察之分析及建議[112]。

整體來說，FISA 受到美國學界普遍的讚許，認為該法案適當且有效地平衡及滿足了情報工作及人民基本權利的保障兩方面之需求[113]。就實務面來說，不少聯邦法院也都認為，FISA的設計合於聯邦憲法第四修正案保護人民隱私權利的意旨[114]。

八、NSA 計畫的無令狀情報通訊監察

在二〇〇一年九一一事件之後，美國聯邦國會通過了「軍事武力使用授權（the Authorization for Use of Military Force, AUMF）」，其中的§2(a）授權總統得以使用一切必要且適當地武力（all necessary and appropriate force），以對抗所有與九一一事件有關的恐怖份子[115]。AUMF 也因而成為小布希（George W. Bush）總統進行無令狀情報通訊監察的依據之一。

如同先前所述，依據 FISA 的規定，於美國境內進行情報通訊監察前，原則上，應先聲請令狀。然而，在二〇〇一年的九一一事件後，當時的小布希政府便開始進行「恐怖分子監察計畫（the Terrorist Surveillance Program, TSP）」[116]。根據這一個計畫，小布希總統未經 FISA 的法定程序，便直接下令就可疑

---

107 50 U.S.C. §1806(f).

108 S. Rep. No. 701, at 58.

109 *Id*.

110 50 U.S.C. §1806(i).

111 不過，本條的制定目的並不是用以限制國會原本所得行使的權力，國會仍得本於其憲法上之職權，監督情報機關所進行的通訊監察之合法性及是否妥適。*See id*. §1808(a)(1).

112 *Id*. §1808(a)(2).

113 Curtis A. Bradley et al., *February 2, 2006 Letter from Scholars and Former Government Officials to Congressional Leadership in Response to Justice Department Whitepaper of January 19, 2006*, 81 IND. L.J. 1415, 1423 (2006); Juan P. Valdivieso, *Recent Developments: Protect America Act of 2007*, 45 HARV. J. ON LEGIS. 581, 589 (2008).

114 *See e.g.*, United States v. Pelton, 835 F.2d 1067. 1075 (4th Cir. 1987).

115 Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001).

116 *See generally* DAVID COLE, JUSTICE AT WAR 131-45 (2008); Robert Bloom & William J. Dunn, The Constitutional Infirmity of Warrantless NSA Surveillance: *The Abuse of Presidential Power and the Injury of the Fourth Amendment*, 15 WM. & MARY BILL RTS. J. 147 (2006).關於美國聯邦國家安全局所進行的無令狀情報通訊監察，其涉及的問題非常廣泛，涵蓋了憲法、國家安全、權力分立，以及立法權及行政權間的制衡等。礙於篇幅及集中討論重心的需要，本文不擬深入此一議題。中文部份的

與蓋達組織（Qaeda）有關之跨境通訊進行通訊監察，且無論通訊者是否為美國人民[117]。

TSP 在二〇〇五年十二月間為紐約時報（New York Times）所揭露。小布希政府承認了上述的無令狀通訊監察，但是拒絕說明其細節及實施的具體情況[118]。其並進一步主張，基於美國憲法第二條的總統三軍統帥權（Commander in Chief）及國會所通過 AUMF[119]，TSP 的情報通訊監察並不需要經過 FISA 的令狀程序。

許多的學者及非政府組織對於 TSP 提出了極為嚴厲的批評[120]。其抨擊道，FISA 已有情報通訊監察的相關程序，且容許在緊急情形、戰爭時期以及總統下命時等情形下進行無令狀通訊監察，所以，總統不得也無需另闢蹊徑而為情報通訊監察[121]。另外，FISA 也清楚規定，情報通訊監察僅得依 FISA 的程序為之，總統不得違反此一明文[122]。再者，美國聯邦國會也已通過愛國者法案以修正 FISA，顯見立法者已經考慮到國家安全之需要而就情報通訊監察為必要的立（修）法，總統實無理由規避 FISA 的程序而逕自進行情報通訊監察[123]。

面對上述的抨擊，小布希政府反駁道，FISA 並無意禁止總統依其他的法律及程序來進行情報通訊監察，而 AUMF 便是 FISA 以外，總統得以進行通訊監察的規定之一[124]。根據 AUMF，為了抗制恐怖分子，總統可以使用「一切必要且適當地武力」，其當然包括了情報通訊監察等方式的使用[125]。

在二〇〇六年，聯邦法院表示，TSP 已經違反了美國聯邦憲法第四修正案之要求，而屬違憲。於 ACLU v. NSA 案[126] 中，密西根東區聯邦地方法院（the District Court for the Eastern District of Michigan）便表示，TSP 中針對國內人民所進行的情報通訊監察已違反了第四修正案及 FISA 的令狀程序[127]。再者，AUMF 雖授權總統得使用一切必要且適當地武力（all necessary and appropriate force），以對抗恐怖主義，但是，其文字過於概括，不能用以取代 FISA 所規定的程序[128]。最後，法院說明道，根據憲法，總統（行政權）固然有進行情報工作的權限，但是，總統的權限仍是來自憲法，所以，政府在進行情報通訊監察時，還是必須要遵守第四修正案等規定，以維護人民的基本權利[129]。

文獻，可以參考廖元豪，〈多少罪惡假「國家安全」之名而行？一簡介美國反恐措施對人權之侵蝕〉，《月旦法學》，131 期，2006 年 4 月，頁 37 以下。

117 *See* Dan Eggen, *Bush Authorized Domestic Spying*, Wash. Post, Dec. 16, 2005, at A1; James Risen & Eric Lichtblau, B*ush Lets U. S. Spy on Callers Without Courts*, N.Y. Times, Dec. 16, 2005, at A1.

118 Risen & Lichtblau, *id*.; Letter from William E. Moschella, U.S. Assistant Att'y Gen., to Pat Roberts, Chairman, Senate Select Comm. on Intelligence, et. al. 1 (Dec. 22, 2005), available at http://www.usdoj.gov/ag/readingroom/surveillance6.pdf.

119 Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001).

120 *See, e.g.*, Adam Burton, *Fixing FISA for Long War: Regulating Warrantless Surveillance in the Age of Terrorism*, 4 PIERCE L. REV. 381 (2006).

121 *See* Memorandum from Elizabeth B. Bazan & Jennifer K. Elsea, Legislative Attorneys, Cong. Research Serv., Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information 27 (Jan. 5, 2006).

122 William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209, 1232 (2007); 18 U.S.C. §2511(2)(f).

123 COLE, *supra* note 116, at 19.

124 Memorandum from the U.S. Department of Justice, "Legal Authorities Supporting the Activities of the National Security Agency Described by the President," 20-21 (Jan. 19, 2006); Press Briefing, Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, the White House (Dec. 19, 2005) available at http://www.globalsecurity.org/intell/library/news/2005/intell-051219-dni01.htm.

125 Press Briefing, Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, the White House (Dec. 19, 2005) available at http://www.globalsecurity.org/intell/library/news/2005/intell-051219-dni01.htm.

126 ACLU v. NSA, 438 F. Supp. 2d 754 (E.D. Mich. 2006).

127 *Id*. at 733-78.在 2007 年，這一個判決被美國聯邦第六巡迴法院以欠缺當事人適格所推翻。ACLU v. NSA, 493 F.3d 644 (6th Cir. 2007).

128 *NSA*, 438 F. Supp. 2d at 779.

129 *Id*. at 781.

TSP 的所引起的風波持續了一段時間。最終，於二〇〇七年一月間，小布希總統下令終止此一計畫，並依循 FISA 之程序向外國情報監察法院聲請令狀以進行情報通訊監察[130]。但是，相關之訴訟仍繼續進行。在二〇一〇年，加州北區聯邦地方法院（the District Court for the Northern District California）再度宣告 TSP 違憲，並表示，情報機關於進行情報通訊監察時，必須要遵守 FISA 所制定的令狀程序[131]。

九、外國情報通訊監察法修正法案（FAA）

FISA所規範的，主要是於美國境內進行之情報通訊監察。至於在美國境外所進行的情報通訊監察，原則上不為 FISA 所涵蓋。這主要是因為，傳統上認為美國法院就美國境外的事務沒有管轄權限[132]。

㈠美國聯邦憲法第四修正案於美國境外的效力

在美國，原則上，通訊監察應遵守聯邦憲法第四修正案之規定。不過，會有的爭議在於，在美國境外所執行的通訊監察，是否仍應遵循第四修正案的要求？在美國境外之人是否能夠主張其第四修正案的權利？在United States v. Verdugo-Urquidez 案[133] 中，美國聯邦最高法院曾判決，美國聯邦憲法第四修正案不適用於美國執法機關就境外的非美國人民所為的搜索扣押。換言之，在美國境外的外國人並不能依美國聯邦憲法第四修正案主張受有違法搜索，也不能主張排除執法人員因而取得之證據。不過，值得注意的是，Brennan大法官於本案的不同意見書中特別指出，根據多數意見書，美國境外的美國人民仍受有美國聯邦憲法第四修正案的保障[134]。亦即，美國官員針對在美國境外的美國人民為搜索或扣押時，仍應遵守第四修正案的要求。

針對在美國境外的情報通訊監察，於二〇〇七年八月，美國聯邦國會通過了「保護美國法案（the Protect America Act, PAA）」[135]，授權情報機關可以針對：㈠境外但經過美國的通訊，以及㈡合理可信位於境外之人的通訊，進行無令狀的情報通訊監察。㈡之情形引起相當大的爭議，因為，即便通訊之另一方是美國境內的美國人民，情報機關還是可以監察其通訊。也正因為其極富爭議，PAA 訂有落日條款，已於二〇〇八年二月失效[136]。不過，PAA中部份的條文仍為之後的法案所援用。

㈡ FAA 中之重要規定

於二〇〇八年，美國聯邦國會通過了「外國情報監察法修正法案（the FISA Amendment Act of 2008, FAA）」[137]。與PAA相仿，FAA也有落日條款，其將於二〇一二年十二月三十一日失效[138]。FAA 中最重要的規定，當屬其將美國境外之人納入情報監察的規範中。依FAA，美國情報機關就境外之人（美國人民或非美國人民）進行通訊監察時，原則上，亦須經過外國情報監察法院授權後方得為之[139]。

---

130 James Risen, *Bush Signs Law to Widen Reach for Wiretapping*, N.Y. Times, Aug. 6, 2007, at A1, available at http://www.nytimes.com/2007/08/06/washington/06nsa.html? scp=1&sq=Bush%20Signs%20Law%20to%20Widen%20Reach%20for%20Wiretapping&st=cse. *See* Letter from Alberto Gonzales, Attorney General of the United States, to Patrick Leahy, Chairman and Arlen Specter, Ranking Member, Committee on the Judiciary, United States Senate (Jan. 17, 27), available at http://fas.org/irp///agency/doj/fisa/ag011707.pdf.

131 *In re* National Sec. Agency Telecommunications Records Litigation, -- F.Supp.2d --, 2010 WL 1244340 (N.D.Cal., 2010)

132 Fed. R. Crim. P. 41(b); *See also In re* Terrorist Bombing of U.S. Embassies in E. Afr., 552 F3d 157 (2d Cir. 2008).

133 United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

134 *Id*. at 283 n.7 (Brennan, J., dissenting) (1990).

135 Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552.

136 Protect America Act of 2007, Pub. L. No. 110-55, §6(c), 121 Stat. 552, 557.

137 The FISA Amendment Act of 2008, Pub. L. No. 110-261, 122 Stat. 2463 (2008).這一個法案的另一個重點就是溯及地免除了通訊服務業者因協助情報機關而對受監察對象所負的賠償責任。

138 The FISA Amendment Act of 2008, Pub. L. No. 110-261, §403, 122 Stat. 2463 (2008).

139 *See* 50 U.S.C. §§1881a(i), 1881b, and 1881c.

當情報通訊監察對象是「境外的美國人民」時[140]，FAA 規定，只有在合於下列要件時，外國情報監察法院方得核發情報通訊監察書：(A)聲請書是由經檢察總長授權之聯邦官員所作成[141]；(B)有相當理由可信監察對象位於美國境外，且為外國勢力或其工作人員[142]；以及(C)所進行的情報通訊監察合於最小侵害原則[143]。

當監察對象為「境外的非美國人民」時，經過外國情報監察法院核發情報通訊監察書後，檢察總長或是國家情報局局長（Director of National Intelligence）才可以針對美國境外的非美國人民進行情報通訊監察[144]。其實體要件為：(A)合理可信受監察人於受監察時位於美國境外，且不得惡意（intentionally）就位於美國境內之收或發話者之通訊進行監察[145]；(B)所進行的情報通訊監察合於最小侵害原則[146]；以及(C)檢察總長及國家情報局局長必須共同確認情報通訊監察的重要目的（significant purpose）為蒐集外國情報資訊[147]。FAA 也要求，情報通訊監察必須以合於美國聯邦憲法第四修正案的方式為之[148]。

當監察對象為境外之非美國人民時，FAA 並不要求有相當理由可信監察對象為外國勢力或其工作人員，而只需要有相當理由可信監察對象位於美國境外即可。就此來說，美國情報機關因而得以進行情報通訊監察的範圍可以說是極為廣泛[149]。

陸、討論及立（修）法之建議

分析我國及美國關於情報通訊監察之相關法制後可知，我國之規定並不盡完善。一方面，情報機關未有足夠的情通訊監察權限，因而未能有效保護國家安全及利益；另一方面，現行規定有著不當及過度侵害人民基本權利的隱憂。現行法制實有修正的必要。以下本文試著討論及說明通保法中較為重大並應儘速修正之缺失，併提出修（立）法上之具體建議。

一、偵查通訊監察及情報通訊監察應有其區分必要

情報監察的目的，包括了蒐集情報、保護本國不受到外國攻擊或威脅、維護國家安全，以及抗制恐怖主義或其他秘密情報活動（clandestine intelligence activities）等[150]。相對地來說，為犯罪偵查目的所進行的通訊監察，則多是為了蒐集與已經發生的犯罪行為有關的證據。就此而言，兩者常常有其政策上及實際運作上的差異。舉例來說，在進行為維護國家安全的情報蒐集或通訊監察時，往往涉及不同類型的資訊來源，監察的對象也較為廣泛[151]，但是，為偵查犯罪所發動的通訊監察之對象，則多可具體特定。再者，犯罪偵查的對象多境內之人，但情報工作的對象，除了包括我國境內之人外，還會涉及到境外之人士。兩者受到我國法律拘束的程度及強度，並不全然相同。綜上，犯罪偵查與國家安全工作應有不同的規範。

依我國目前現行規定，偵查通訊監察與情報通訊監察都適用「通訊保障及監察法」。這

140 FISA 並未針對這一種類型的情報通訊監察為規範。

141 50 U.S.C. §1881b(c)(1)(A).

142 *Id*. §1881b(c)(1)(B).

143 *Id*. §1881b(c)(1)(C).

144 *Id*. §1881a(a), (i)(3).

145 *Id*. §1881a(i)(2)(B).

146 *Id*. §1881a(i)(2)(C); *see also* §§1801(h), and 1821(4).

147 *Id*. §1881a(g)(2)(A)(v).

148 *Id*. §1881a(b)(5).不過，美國法院一向認為於境外的外國人並不受有第四修正案的保護。*See* United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).是故，如何以「合於美國聯邦憲法第四修正案」的方式，就境外的外國人進行情報通訊監察，並不清楚。

149 也因如此，美國有學者建議，至少應要求，有相當理由可信該境外之外國人為外國勢力或其工作人員，且已與境內之本（美）國人民有所接觸時，才能夠針對其進行情報通訊監察。*E.g.*, Blum, *supra* note 10, at 311.

150 *See* S. Rep. No. 701, at 59.

151 *See United States District Court*, 407 U.S. at 322-23.

樣的立法方式，似值商榷。本文建議，我國可仿照美國聯邦的立法方式，應將情報通訊監察與偵查通訊監察分別規定。其中的理由在於：第一，這兩種通訊監察本質上的並不相同，以同一個法案規範，不免格格不入，甚至是造成矛盾。舉例來說，進行情報通訊監察的案由不當然構成特定犯罪行為，但是，通保法第十一條第一項卻一律要求所有的通訊監察書都必須要記載「涉嫌觸犯之法條」（第一款）[152]。第二，將情報通訊監察規定於通保法中，還可能使得審理法官以審查犯罪通訊監察之標準決定是否同意進行情報通訊監察，而過度限制情報工作機關，使其無法適時進行情蒐活動。是故，情報通訊監察應有單獨立法之必要，以更清楚明確地規範國家的情報蒐集活動，並有效維護國家安全，適當保障人民之通訊隱私[153]。

不過，要注意的是，政府於進行國家安全工作（包括情報通訊監察）時，若涉及本國人民時，仍應遵守各樣保障人民權利的憲法及法律規定。承認此二者應適用不同的程序規範不代表情報機關可以完全不受規制，為所欲為。針對我國人民進行情報通訊監察時，情報機關仍須遵守憲法及正當程序等各樣規定，以避免不當侵害人民之基本權利[154]。

二、情報通訊監察應採行令狀原則

現行通保法中的情報通訊監察規定，綜理國家情報工作機關首長於核發通訊監察書以監察境內設有戶籍人之通訊時，須事先經法院同意。依此，法院有無實質審核權限，並不清楚。本文認為，上述的規定並不盡妥適，有修正之必要。

現行通保法雖然規定，綜理國家情報工作機關首長核發通訊監察書，以監察於我國境內設有戶籍人之通訊時，應事先經過法院同意（通保法第七條第二項），但是，此一規定顯然與令狀程序有別。在一般的令狀程序裡，是由行政機關向法院提出聲請，並說明其必要性，由法院審查該聲請是否合於法定要件，以及是否有進行該強制處分之相當理由。通保法第五條第二項及刑事訴訟法第一二八條及第一二八條之一，皆為適例。不獨我國如此，依FISA規定，亦是由情報機關向法院提出進行情報通訊監察之聲請，法院在審查後，認為合於法定要件時，核發情報通訊監察書，授權情報機關進行監察[155]。然而，現行通保法第七條之規定，在形式上與我國類似的程序不一致，也與外國立法例有別；其在實質上，也有解釋及適用上的疑義。依通保法第七條的文字，實難理解該條中之法院究竟有無實質審查權限。依目前規定，易使得受理法院誤認為，核發通訊監察書者既為綜理國家情報工作機關首長，法院便應「尊重」其對於進行情報通訊監察的判斷，而不得實質審查有無進行監察的必要以及該聲請是否合於法定要件。如此一來，發動情報通訊監察與否幾乎純為情報機關單方面決定，欠缺有效監督制衡機制，殊為不當。

參考我國類似的程序規定及 FISA 的條文後，本文建議，情報通訊監察書之核發程序，應改為由情報機關向法院提出聲請。審查後，若法院認為該聲請合於法定之要件，得核發令狀，授權情報機關進行通訊監察。如此一來，可以明確規範法院就情報通訊監察有其審查權限，決定於具體個案中有無得進行情報通訊監察之必要、相當理由及其他法定要件。

---

152 類似法條的錯誤設計，不在少數，又例如，通訊監察期間屆滿之前二日，得附具體理由，聲請繼續進行通訊監察（通保法第十二條第一項）。此一規定顯然係就偵查通訊監察所為之規定，因為，情報通訊監察是由綜理國家情報工作機關首長核發通訊監察書，並無向何人聲請之程序，也就不會適用到向其聲請繼續監察的規定。

153 本文建議兩者應分別立法，是因為這兩者的規範目的、範圍或對象等，均有不同，以同一部法律規範，極可能因為立法技術或是文字上的限制，使得法官以審查犯罪通訊監察之標準或要件決定是否同意進行情報通訊監察。但這不代表司法機關沒有審查情報通訊監察之能力。情報通訊監察及偵查通訊監察應以各自獨立之法律規範為立法政策的問題；由法官或情報機關決定情報通訊監察之發動乃情報通訊監察應由何權力機關授權之決定。兩者間互有關聯，但分屬不同層次。

154 *See United States District Court*, 407 U.S. at 322-23.

155 50 U.S.C. §§1804, and 1805.

三、程序及實質要件應更為明確具體

進行情報通訊監察之「實質要件」，明文於通保法第七條第一項，其明文：「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。」本文認為，該條文的規定不盡明確，未能提供可供審查的具體標準，不盡妥當，應有修正之必要。

通保法第七條第一項規定，在「為避免國家安全遭受危害」及有「蒐集外國勢力或境外敵對勢力情報之必要」時，可以進行情報通訊監察。不過，「為避免國家安全遭受危害」充其量只屬於情報通訊監察的「目的」，並未能提供可供審查的明確標準或實質要件。至於「蒐集外國勢力或境外敵對勢力情報之必要」，只是標明了在有「必要性」時，方可進行情報通訊監察。不過，必要性有無的判斷，過於模糊，審查時，不免會有過於恣意的危險，使得人民的通訊隱私會有受到情報機關不當侵害之疑慮。

除了有害基本權利外，現行之規定也不利於情報工作。詳言之，即便認為「為避免國家安全遭受危害」屬於發動情報通訊監察的要件，其也可能使得專責法院誤以為必須要是「國家安全受有危害」時，方可同意核發通訊監察書，致使情報機關無法進行必要的情報蒐集工作，預警可能之危險及實害，維護國家利益。這樣的結果，並不妥適。

就理論及實際需求來說，情報通訊監察及偵查通訊監察應可適用不同的要件[156]。情報通訊監察多屬於資訊的蒐集、危害的預警及分析，並不當然是針對具體已產生實際危害之事件，所以，情報通訊監察的範圍勢必會更為廣泛、涉及更多的消息來源、監察的對象也較不特定，是故，實毋須亦不宜以特定犯罪或實際危害作為要件，而應可有較大的彈性。基於上述理由，並參考FISA的規定[157]，本文建議，為維護國家安全及蒐集情報之目的而進行通訊監察時，其要件可以為「為維護國家安全，有相當理由可信監察對象為外國勢力、境外敵對勢力或其工作人員，且可信其參與通訊之進行，並有監察其境內或跨境通訊之必要」。

本文所建議的條文，應較現行規定更為可採。首先，建議條文以「相當理由」為審查標準，具有較高之操作可能性。目前我國許多法規都以「相當理由」作為得否進行強制處分的標準（如刑事訴訟法第一二二條及通訊保障及監察法第五條），且也行之有年，法院在解釋及適用時較為熟悉，情報機關也較得預測聲請之結果。再者，以上述建議之文字為情報通訊監察的要件，較現行規定為清楚及明確，可避免情報機關濫用通訊監察權限，也可以避免法院以發生特定犯罪或是一定危害為要件來審查聲請，過度限制情報通訊監察之進行。

四、監察對象

我國通保法第七條以在我國境內是否設有戶籍，區分在進行監察前是否應經法院的同意。本文認為，這樣的區分標準並不恰當，應予修正。

㈠有無戶籍之區分並不合理

依現行通保法規定，原則上，為國家安全而進行通訊監察前，應由綜理國家情報工作機關首長核發通訊監察書（第七條第一項）。若受監察人在我國境內設有戶籍者，就需經國安局所在地之高等法院專責法官同意，方得核發通訊監察書（第七條第二項本文）。換言之，受監察人在我國境內未設有戶籍時，情報通訊監察的進行，則純由情報機關決定，未有任何

156 *See United States District Court*, 407 U.S. at 323.

157 50 U.S.C §1805.

外部監督。

現行通保法不是以我國人民或外國人民作為是否須經法院同意的區分標準，而是以監察對象是否於我國境內設有戶籍為準。會有這樣的設計，可能是因為我國國籍法以採屬人主義為主，對於「國籍」之認定相當寬鬆，舉凡：1、出生時父或母為中華民國國民；2、出生於父或母死亡後，其父或母死亡時為中華民國國民；3、出生於中華民國領域內，父母均無可考，或均無國籍者；以及 4、歸化者，均具有我國國籍（國籍法第二條第一項）。依據這樣的規定，許多大陸及港澳人民均具有我國國籍，而為我國國民。

雖然我國國籍的認定相當廣泛，然而，依照我國戶籍法規定，有國籍者不當然能夠在我國境內設有戶籍。戶籍法第十五條便規定，在國內未曾設有戶籍，且為我國國民入境後（第一款）、為外國人或無國籍人歸化或回復國籍後（第二款）、或大陸地區人民或港澳居民（第三款）者，經核准定居後，方得於我國境內為初設戶籍登記。而欲在我國「定居」，還必須要符合入出國及移民法第九及十條所規定之程序，方得為之。由此可知，並非所有我國國民均得在境內設有戶籍。目前法制對於戶籍的承認可說相當嚴格。

或許是鑑於我國法制對於國籍的認定相當廣泛，通保法第七條便以是否於我國境內設有戶籍來區分在核發令狀前是否應經法院同意。不過，本文認為，這樣的標準或許為顧及我國特殊之現實情況，不得不的設計，但其規定並不盡合理。首先，無戶籍但有國籍之人仍為我國國民，而享有我國憲法所賦予之各項基本權利，僅因其未取得戶籍，便對其通訊隱私予以較次等的保護，理由似嫌薄弱。畢竟，未具有戶籍的國民，原因多端，不當然就與國家安全有必然的關聯性。如果要區分不同的程序保護，應與國家安全或是情報工作有更實質的關係，方為合理。

再者，在我國境內之無戶籍之人仍可能與我國人民或有戶籍人進行通訊，就該無戶籍之人進行情報通訊監察時，不可避免地，會取得我國人民或設有戶籍之人的通訊內容，因而侵害其通訊隱私，但依現行規定卻無任何外部監督制衡機制，未能顧及我國人民的通訊隱私，不盡妥適。

㈡應以「通訊之一方是否在我國境內」為區分標準

綜上，本文主張，原則上，只要通訊之一方位於我國境內，所進行的情報通訊監察便應有令狀程序之適用，而不應區分監察對象於我國境內是否設有戶籍。如此一來，較能適當保障人民之基本權利，避免情報機關恣意進行監察。

首先，要求法院審查通訊方皆位於國外所進行之情報通訊監察，可能過於不切實際，因為現實上，法院很難確實掌握並瞭解於國外所發生之事實及個案情狀，採行令狀程序的結果，法院極有可能淪於橡皮圖章，無法發揮事實上審查的作用。另一方面，要求我國位於境外之情報機關於進行情報通訊監察前必須要向我國法院聲請令狀，極可能於過程中發生機密外洩等情形，極可能有害於情報工作之順利進行，以及情報工作人員之人身安全。再者，通訊方皆位於外國地區之情形，通常比較不會有不當侵害我國人民基本權利的疑義。此外，於境外的情報工作，往往需要更大的彈性，以為因應。是故，就通訊方皆位於境外所進行之情報通訊監察，無須令狀程序。FISA 也是採取類似之精神及立法方式[158]。本文建議，在我國境內所進行的情報通訊監察，應採令狀原則。至於在我國境外所為之者，則無須採行此一原則。

五、最小侵害原則（the minimization requirement）

158 *See* 50 U.S.C. §1808(f)(1)-(4).依照此規定，FISA 所規定的程序，只是用在與美國之領土有關連的情報蒐集活動，也就是說，必須要是通訊發出者、收受者、雙方或是通訊的取得行為位於美國境內，才有 FISA 的適用。境外的情報通訊監察，目前主要是適用 FAA 的規定。

現行通保法規定，通訊監察（包括為犯罪偵查及情報工作之通訊監察）「應以侵害最少之適當方式為之」（第二條第二項後段）。此為「最小侵害原則（minimization）」之明文。為能使此一原則之內涵更為明確，併使情報機關確實遵守此規定，本文建議，我國將來修（立）法之時，可以仿照FISA之規定[159]，於法條或是施行細則中明定最小侵害原則的意涵，並要求情報機關制定其所屬官員執行情報通訊監察時所應遵守的準則。為確保情報機關謹守上述要求，條文中也可規定，在情報通訊監察的聲請書上，亦應一併載明遵守最小侵害原則的具體方式。法院審查後認為聲請機關所提出的具體方式合於最小侵害原則，才能核發通訊監察書。如此一來，方較能確保情報機關是以「侵害最少之適當方式」進行情報通訊監察。

六、證據排除法則

現行通保法第七條第四項規定，違反同條第二第及第三項之規定所取得的通訊內容，在其他程序中不得作為證據。本條項當屬情報通訊監察的證據排除規定。與通保法第五條或第六條不同的是，本條採的是絕對排除[160]。本文主張，情報通訊監察應繼續採行證據排除法則，以有效嚇阻國家機關假借情報蒐集之名，行犯罪偵查之實，並確保情報機關不致恣意濫用通訊監察的權力[161]。

不過，細究通保法第七條第四項可知，現行條文並不妥適，應與修正。該條項規定：「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，……，均不得採為證據。」但是，監察通訊的方式，並不限於「監聽」，而還包括了「截收、錄音、錄影、攝影、開拆、檢查、影印」[162]等方式，依據該條項規定，證據排除之規定並未涵蓋以違法截收或是錄音等方法所取得的證據。然而，無論是以何種方式得知通訊的內容，都屬於對隱私之侵害，而應亦有證據排除之適用。現行條文文字應純屬立法的漏洞，而非立法者有意排除「監聽」以外之通訊監察方式。在修法之前，監聽以外的違法情報通訊監察行為，應類推通保法第七條第四項之適用，亦有證據排除法則之適用[163]。

另外，通保法第七條第四項規定：「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，……，均不得採為證據。」依法條文字，所適用者，為該條第二項（監察對象為在國內有戶籍之人應先經法院同意）及第三項（緊急情報通訊監察之程序要求）。不過，通保法第七條第一項或是最小侵害原則（同法第二條）等規定皆屬情報通訊監察之要件及程序規定，但依該條第四項，並無證據排除法則之適用。這樣的立法設計，不盡合理。本法認為，通保法中諸多程序規定皆係為保障人民通訊隱私及規範情報通訊監察之重要條文，皆應有證據排除的適用，以確保情報機關遵守各個法定程序。因此，通保法第七條第四項應修正為「違反本法進行通訊監察所取得之內容或所衍生之證據於審判中，均不得採為證據。」，較為合理妥適。

七、經情報通訊監察所取得的資訊是否得作為證據之用？

經情報通訊監察所取得的通訊內容，在刑事審判中是否有證據能力？關此，通保法規

159 50 U.S.C. §1801(h).

160 現行通保法中的證據排除，根據不同的程序及案件類型，有著不同的規定。在偵查通訊監察採的是「相對排除」，但是在情報通訊監察及軍事案件的通訊監察中，卻是採「絕對排除」的設計。相關討論，可以參照李榮耕，〈I am Listening to You－釋字第六三一號解釋、令狀原則及修正後通訊保障及監察法（下）〉，《台灣本土法學雜誌》，105 期，2008 年 4 月，頁 48-50。

161 美國學界不乏有更為激進的看法。其主張，在情報通訊監察所取得的通訊資料中，與恐怖活動或是情報無關者，即便其可以作為犯罪偵查及證據之用，也必須一律排除，以避免情報通訊監察的濫用。再者，即便採取這樣的規定，也不會影響到國家安全的維護。*See* Banks, *supra* note 122, at 1291; Blum, *supra* note 10, at 312-13.

162 請參閱通保法第十三條第一項。

163 相類似的立場，可以參照台灣高等法院暨所屬法院 96 年法律座談會刑事類提案第 42 號。

定，經情報通訊監察所取得的資料，「僅作為國家安全預警情報之用」。但是，如果因而發現了通保法第五條所定之情事時，情報機關「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」（第十條），其並未明定，該資料於刑事審判中是否有證據能力。就此問題，本文傾向採取肯定之立場，其中理由如下。

首先，從通保法第七條可以推論得知，經情報通訊監察所得的資訊可以在刑事審判中作為證據之用。詳言之，該條第四項規定，違反該條第二或三項所取得的通訊內容或衍生證據，於刑事審判或其他程序中，均不得採為證據[164]。反面推論可知，只要情報通訊監察合於通保法第七條第二項或第三項之規定，所取得的資訊於刑事審判程序中便應有證據能力，可作為認定被告犯罪之用。

第二，就比較立法例上來看，上述的結論亦應為可採。依 FISA 的規定，負責情報通訊監察的聯邦官員得諮詢負責犯罪偵查的官員，以整合必要資源，防制恐怖份子所可能造成的危害[165]。此一規定等於是容許情報機關向偵查機關揭露其於進行情報通訊監察時所取得的資訊。再者，美國實務上並不認為外國情報監察及刑事偵查可以或應該一分為二，涇渭分明[166]。近來美國聯邦巡迴法院判決多承認，經情報通訊監察所合法取得的證據及其衍生證據，在刑事程序中仍有其證據能力[167]。

最後，採取上述立場，也較符合實務運作上的需要。詳言之，透過情報通訊監察，情報機關除了能取得與國家安全相關的通訊內容外，也可能會因而知悉與犯罪有關的資訊。尤其是許多的外國勢力或敵對勢力或其工作人員於我國境內的行為多半都已經構成犯罪[168]。如果這一些犯罪資訊不得作為證據之用，那便無異於是要求情報機關必須要對這些通訊內容「聽若不聞」。這樣的結果，著實過於不切實際，也有害於國家訴追犯罪的重要利益。綜合上述理由，本文認為，法制上應准許情報機關得將經情報通訊監察所取得的犯罪資訊移送與犯罪偵查機關，而該資訊亦應可以在刑事審判中作為證據之用。但是，若情報通訊監察違反法定程序，所取得之證據及衍生證據便應予排除，自不待言。

八、事後通知（Post Notice）及救濟

關於情報通訊監察的事後通知（post notice）機制，在制度上有兩種規範方式，第一，是要求情報機關必須要通知受監察人，僅在例外時，方得豁免此一義務。另一種方式為，欲使用經情報通訊監察所取得之資料作為證據時，方須通知受監察人。前者如我國現行通保法第十五條之規定，後者則是如 FISA 之立法方式[169]。本文認為，因情報工作的特性，要求一律通知受監察人，極可能引起國際糾紛或外交事件，或危害我國情報工作人員安全，並不妥適。是故，制度上可以參考 FISA 之設計，改為原則上無須通知受監察人，但是在刑事審判中欲以經情報通訊監察取得之資料作為認定受監察人犯罪之證據時，則應告知其情報通訊監察之相關事項。

詳言之，若提出經情報通訊監察所得之資

164 通保法第七條第三項規定，違反同條第一或二項進行「監聽」所取的證據及衍生證據不具有證據能力。這樣的規定會造成一個問題，使用監聽以外的監察方式所取得的證據及衍生證據，是否便無通保法第七條第三項的適用，從而一律有證據能力？實務上似認為，類似條文中的「監聽」的真意是「監察」。請參照台灣高等法院暨所屬法院 96 年法律座談會刑事類提案第 42 號。另外，也已有文獻針對這裡的立法疏失提出討論。請參照李榮耕，同註 160，頁 48-49。

165 50 U.S.C. §1806(k).

166 *Sarkissian*, 841 F.2d at 965.

167 *Isa*, 923 F.2d at 1304-05; *Sarkissian*, 841 F.2d at 964.

168 其通常都已經構成「外國情報犯罪（foreign intelligence crime）」，其包括了諸如破壞行動（sabotage）、國際恐怖主義（international terrorism）、間諜活動（espionage），以及為外國勢力而使用虛偽身份進入境內等行為。這一類的行為，在我國刑法中，皆為可罰之行為。*See In re* Sealed Case, 310 F.3d at 723.

169 50 U.S.C. §1806(c), and (d).

訊作為對被告（受監察人）不利之證據，應告知其情報通訊監察及相關事項，使其有機會於其刑事審判程序中提起救濟，主張原情報通訊監察違法，進而請求法院審查該情報通訊監察之合法性。再者，此一事後通知規定亦可避免行政機關濫用情報蒐集的權力，恣意侵害人民的通訊隱私。不過，參考 FISA 之規定後，本文也建議，為維護國家安全及利益，應容許於通知將有害國家安全或危害他人生命身體安全時，由綜理情報工作機關首長陳報法院後，不予通知。

九、保存及銷燬

關於情報通訊監察所得的資料之保存及銷燬，主要的規定在通保法第十七條。該條將監察所得的資料區分為與監察目的有關及與監察目的無關兩類。前者「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」，於作為案件證據之用而留存於案卷中或為監察目的而有必要時，可以「長期留存」，無此必要者，只得於通訊監察結束後，「保存五年，逾期予以銷燬」（第一項）。監察所得資料與監察目的無關時，則由執行機關報請綜理國家情報工作機關首長許可後，予以銷燬（第二項）。本文認為，現行保存及銷燬的規定使得情報機關得以單方面決定是否銷燬及保存監察所得資料的期間，並不合理，應有修正之必要。

詳言之，進行情報通訊監察時，情報機關所取得的資料勢必會包含與監察目的有關及與監察目的無關的通訊內容，此乃通訊監察之本質使然，無可厚非。與監察目的相關的資料，自是應予保存，供情報機關作後續之分析使用。所得資料與監察目的無關時，可以再區分為有正當理由繼續保存者，以及無正當理由保存者兩類。有正當理由繼續保存者，如該資料可能仍可以作為犯罪偵查之用，此時，該資料應依通保法第十條的規定，移送相關偵查或審判機關，通保法第十七條第一項也容許行政機關繼續保存（「供案件證據之用留存於該案卷」）。較有疑義者為後者的情形，也就是所得到之資料與監察目的無關，亦與犯罪情事無關時，政府並無繼續保有該資訊的正當性，是故，其應立即銷毀所取得之通訊內容。但是，通保法卻規定，需經「綜理國家情報工作機關首長許可」後，方可銷燬。這樣的規定，並不合理。參考 FISA 之規定[170]後，本文認為，情報通訊監察所得資料與監察目的無關，且未供刑事案件證據之用者，應立即銷燬之。

十、應建立客觀中立之外部監督機制

依 FISA 之規定，聯邦參眾議院的情報或司法委員會皆可就情報通訊監察之執行情況及法制設計為通盤整體之瞭解及監督，以確認 FISA 應否修正或廢止，確保情報機關擁有足夠的情報蒐集能力及人民之隱私權益獲有充分之保障。此項規定實值參考。本文建議，今後修（立）法時，應於立法院或其他適當機關設置客觀中立之委員會，以於外部監督情報通訊監察之執行及定期檢討相關法制，俾同時滿足維護國家安全及保障人民基本權利之需要。

柒、結　論

無論是就犯罪偵查或是情報蒐集，通訊監察都是極為有力的工具，不過，其應該因為不同的目的及對象而有不同之要件及程序規定。在我國，關於情報通訊監察，其主要規範當屬通保法。

在美國，在一九七二年便於 *Keith* 案中處理了關於情報通訊監察的爭議。這一個判決也促成了 FISA 的制定。FISA 及相關的法案詳盡地規範了美國情報機關於執行情報通訊監察時所應遵循的程序，其包括了令狀程序、外國情報監察法院的設置、審查程序、監察期間及延

170 50 U.S.C. §1806(i). 本條規定：「除非經檢察總長認定，該通訊內容涉及他人生命或身體重大危害，否則，在情報通訊監察中所取得與監察目的無關之通訊內容，且收發話雙方都為於美國境內者，皆應立即銷燬」。

長、無令狀情報通訊監察之情形、最小侵害程序、事後通知、所得資訊之使用及銷燬，以及國會監督等。相關的條文，均值我國參考。

在比較我國及美國之相關規範後可以發現，我國通保法的規定有許多不足之處，無法因應國家安全工作的實際需求，也有過度侵害人民基本權利的疑慮，實有修正之必要。首先，因為性質上的根本差異，情報通訊監察與偵查通訊監察應分別單獨立法，不宜以同一部法律規範。情報通訊監察，應明確地改採令狀原則，由情報機關提出聲請，法院審查核發情報通訊監察書後，方得為之。進行情報通訊監察的要件及程序應更為具體明確，現行條文中的「避免國家安全遭受危害」實是過於空泛。情報通訊監察的對象不應再區分於我國境內有無戶籍，而應以通訊之一方是否位於我國境內決定。

在執行情報通訊監察時，情報機關應遵守最小侵害原則，以避免過度侵害人民之通訊隱私，相關條文中，應明確定義最小侵害原則之意涵，以供情報機關遵循。違法的情報通訊監察應皆有證據排除法則的適用，以達到嚇阻情報機關的效果。本文認為，經合法情報通訊監察所取得的資訊，在刑事審判程序中應可採為證據，較為合理。情報通訊結束後，因為情報工作的特性使然，應以不通知為原則，但是在刑事審判程序中使用經情報通訊所獲得之資訊時，則應告知監察對象相關情事，使其得於審判程序中為有效之訴訟上防禦。另外，經情報通訊監察所取得的資料，若與監察目的無關，也沒有繼續保存的正當理由（如供刑事偵查或審判之用）時，應立即銷燬，以確實保障人民之通訊隱私。最後，制度上應有客觀獨立之監督機制，以通盤監督情報通訊監察之執行情形及檢討相關法制之設計，以確保情報機關擁有足夠之情報蒐集能力及妥適保障人民權益。

參考文獻

一、中文：

- 王兆鵬，〈路檢及國境檢查〉，《臺灣本土法學雜誌》，26 期，2001 年 9 月，頁 15 以下。
- 李榮耕（原名蔡榮耕），〈I am Listening to You －釋字第六三一號解釋、令狀原則及修正後通訊保障及監察法（上）〉，《台灣本土法學雜誌》，104 期，2008 年 3 月。
- 李榮耕（原名蔡榮耕），〈I am Listening to You －釋字第六三一號解釋、令狀原則及修正後通訊保障及監察法（下）〉，《台灣本土法學雜誌》，105 期，2008 年 4 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》，131 期，2006 年 4 月。

二、英文期刊書籍

- Adam Burton, *Fixing FISA for Long War: Regulating Warrantless Surveillance in the Age of Terrorism*, 4 PIERCE L. REV. 381 (2006).
- Beryl A. Howell & Dana J. Lesemann, *FISA's Fruit in Criminal Cases: An Opportunity for Improved Accountability*, 12 UCLA J. INT'L L. & FOREIGN AFF. 145 (2007).
- Clifford S. Fishman, *Interception of Communication in Exigent Circumstances: The Fourth Amendment, Federal Legislation, and the United States Department of Justice*, 22 GA. L. REV. 1 (1987).
- Curtis A. Bradley et al., *February 2, 2006 Letter from Scholars and Former Government Officials to Congressional Leadership in Response to Justice Department Whitepaper of January 19, 2006*, 81 IND. L.J. 1415 (2006)
- DAVID COLE, JUSTICE AT WAR (2008)
- Helene E. Schwartz, *Oversight of Minimization Compliance under the Foreign Intelligence Surveillance Act: How the Watchdogs* are

Doing Their Jobs, 12 RUTGERS L. J. 405 (1981).
- Herbert Brownell, *The Public Security and Wire Tapping*, 39 CORNELL L.Q. 195 (1954).
- Juan P. Valdivieso, *Recent Developments: Protect America Act of 2007*, 45 HARV. J. ON LEGIS. 581 (2008).
- Robert Bloom & William J. Dunn, *The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury of the Fourth Amendment*, 15 WM. & MARY BILL RTS. J. 147 (2006).
- Stephanie Cooper Blum, *What Really is at Stake with the FISA Amendment Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT. L.J. 269 (2009).
- William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209 (2007).

三、英文報章

- Dan Eggen, *Bush Authorized Domestic Spying*, Wash. Post, Dec. 16, 2005, at A1
- James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, Dec. 16, 2005, at A1.

四、美國聯邦法院判決

- ACLU v. NSA, 438 F. Supp. 2d 754 (E.D. Mich. 2006).
- ACLU v. NSA, 493 F.3d 644 (6th Cir. 2007).
- Brown v. United States, 484 F.2d 418 (5th Cir. 1973)
- In re Sealed Case, 310 F.3d 717 (For. Intel. Surv. Rev. 2002).
- Katz v. United States, 389 U.S. 347, 358 n.23 (1967).
- United States v. Brown, 908 F.2d 968 (4th Cir. 1990).
- United States v. Buck, 548 F.2d 871 (9th Cir. 1977).
- United States v. Hammoud, 381 F.3d 316, 322 (4th Cir. 2004).
- United States v. Isa, 923 F.2d 1300 (8th Cir. 1991)
- United States v. Ning Wen, 477 F.3d 896 (7th Cir. 2007).
- United States v. Ott, 827 F.2d 473 (9th Cir. 1987).
- United States v. Pelton, 835 F.2d 1067 (4th Cir. 1987).
- United States v. Sarkissian, 841 F.2d 959 (9th Cir. 1988).
- United States v. Squillancote, 221 F.3d 542 (4th Cir. 2000).
- United States v. United States District Court, 407 U.S. 297 (1972).
- United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).